# COMPENDIUM PUTNAM

*The William Lowell Putnam Mathematical Competition*

1985 - 2022

**Gerard Romo Garrido**

Toomates Coolección vol. 66

# Toomates Coolección

Los libros de **Toomates** son materiales digitales y gratuitos. Son digitales porque están pensados para ser consultados mediante un ordenador, tablet o móvil. Son gratuitos porque se ofrecen a la comunidad educativa sin coste alguno. Los libros de texto pueden ser digitales o en papel, gratuitos o en venta, y ninguna de estas opciones es necesariamente mejor o peor que las otras. Es más: Suele suceder que los mejores docentes son los que piden a sus alumnos la compra de un libro de texto en papel, esto es un hecho. Lo que no es aceptable, por inmoral y mezquino, es el modelo de las llamadas "**licencias digitales**" con las que las editoriales pretenden cobrar a los estudiantes, una y otra vez, por acceder a los mismos contenidos (unos contenidos que, además, son de una bajísima calidad). Este modelo de negocio es miserable, pues impide el compartir un mismo libro, incluso entre dos hermanos, pretende convertir a los estudiantes en un mercado cautivo, exige a los estudiantes y a las escuelas costosísimas líneas de Internet, pretende pervertir el conocimiento, que es algo social, público, convirtiéndolo en un producto de propiedad privada, accesible solo a aquellos que se lo puedan permitir, y solo de una manera encapsulada, fragmentada, impidiendo el derecho del alumno de poseer todo el libro, de acceder a todo el libro, de moverse libremente por todo el libro.
Nadie puede pretender ser neutral ante esto: Mirar para otro lado y aceptar el modelo de licencias digitales es admitir un mundo más injusto, es participar en la denegación del acceso al conocimiento a aquellos que no disponen de medios económicos, y esto en un mundo en el que las modernas tecnologías actuales permiten, por primera vez en la historia de la Humanidad, poder compartir el conocimiento sin coste alguno, con algo tan simple como es un archivo "pdf". **El conocimiento no es una mercancía**.
El proyecto Toomates tiene como objetivo la promoción y difusión entre el profesorado y el colectivo de estudiantes de unos materiales didácticos libres, gratuitos y de calidad, que fuerce a las editoriales a competir ofreciendo alternativas de pago atractivas aumentando la calidad de unos libros de texto que actualmente son muy mediocres, y no mediante retorcidas técnicas comerciales.
 Todos los libros se ofrecen en dos versiones: En formato "**pdf**" para una cómoda lectura y en el formato "**doc**" de MSWord para permitir y facilitar su edición y generar versiones parcial o totalmente modificadas.

**¡Libérate de la tiranía y mediocridad de las editoriales! Crea, utiliza y comparte tus propios materiales didácticos**

Toomates Coolección **Problem Solving** (en español):
Geometría Axiomática , Problemas de Geometría 1 , Problemas de Geometría 2
Introducción a la Geometría , Álgebra , Teoría de números , Combinatoria , Probabilidad
Trigonometría , Desigualdades , Números complejos , Funciones

Toomates Coolección **Llibres de Text** (en catalán):
Nombres (Preàlgebra) , Àlgebra , Proporcionalitat , Mesures geomètriques , Geometria analítica
Combinatòria i Probabilitat , Estadística , Trigonometria , Funcions , Nombres Complexos ,
Àlgebra Lineal , Geometria Lineal , Càlcul Infinitesimal , Programació Lineal , Mates amb Excel

Toomates Coolección **Compendiums**:
Ámbito PAU: Catalunya TEC Catalunya CCSS Galicia País Vasco Portugal A Portugal B Italia
Ámbito Canguro: ESP , CAT , FR , USA , UK , AUS
Ámbito USA: Mathcounts AMC 8 AMC 10 AMC 12 AIME USAJMO USAMO Putnam
Ámbito español: OME , OMEFL , OMEC , OMEA , OMEM , CDP
Ámbito internacional: IMO OMI IGO SMT INMO CMO REOIM Arquimede HMMT
Ámbito Pruebas acceso: ACM4 , CFGS , PAP
Recopilatorios Pizzazz!: Book A Book B Book C Book D Book E Pre-Algebra Algebra
Recopilatorios AHSME: Book 1 Book 2 Book 3 Book 4 Book 5 Book 6 Book 7 Book 8 Book 9

¡Genera tus propias versiones de estos libros! Siempre que es posible se ofrecen las versiones editables "MS Word" de todos los materiales, para facilitar su edición.

**¡Ayuda a mejorar!** Envía cualquier duda, observación, comentario o sugerencia a **toomates@gmail.com**

**¡No utilices una versión anticuada!** Todos estos libros se revisan y amplían constantemente. Descarga totalmente gratis la última versión de estos documentos en los correspondientes enlaces superiores, en los que siempre encontrarás la versión más actualizada.

Consulta el **Catálogo de libros** de la biblioteca Toomates Coolección en http://www.toomates.net/biblioteca.htm

Encontrarás muchos más materiales para el aprendizaje de las matemáticas en **www.toomates.net**

Visita mi **Canal de Youtube**: **https://www.youtube.com/c/GerardRomo**

Versión de este documento: **18/08/2023**

# Índice.



* The "2020" competition was postponed to February 20, 2021 due to the COVID-19 pandemic, then held in an unofficial mode with no prizes or official results.

# Fuentes.

https://kskedlaya.org/putnam-archive/

# The Forty-Sixth Annual William Lowell Putnam Competition
## Saturday, December 7, 1985

A–1 Determine, with proof, the number of ordered triples $(A_1, A_2, A_3)$ of sets which have the property that

(i) $A_1 \cup A_2 \cup A_3 = \{1,2,3,4,5,6,7,8,9,10\}$, and

(ii) $A_1 \cap A_2 \cap A_3 = \emptyset$.

Express your answer in the form $2^a 3^b 5^c 7^d$, where $a,b,c,d$ are nonnegative integers.

A–2 Let $T$ be an acute triangle. Inscribe a rectangle $R$ in $T$ with one side along a side of $T$. Then inscribe a rectangle $S$ in the triangle formed by the side of $R$ opposite the side on the boundary of $T$, and the other two sides of $T$, with one side along the side of $R$. For any polygon $X$, let $A(X)$ denote the area of $X$. Find the maximum value, or show that no maximum exists, of $\frac{A(R)+A(S)}{A(T)}$, where $T$ ranges over all triangles and $R,S$ over all rectangles as above.

A–3 Let $d$ be a real number. For each integer $m \geq 0$, define a sequence $\{a_m(j)\}$, $j = 0,1,2,\dots$ by the condition

$$\begin{aligned} a_m(0) &= d/2^m, \\ a_m(j+1) &= (a_m(j))^2 + 2a_m(j), \qquad j \geq 0. \end{aligned}$$

Evaluate $\lim_{n\to\infty} a_n(n)$.

A–4 Define a sequence $\{a_i\}$ by $a_1 = 3$ and $a_{i+1} = 3^{a_i}$ for $i \geq 1$. Which integers between 00 and 99 inclusive occur as the last two digits in the decimal expansion of infinitely many $a_i$?

A–5 Let $I_m = \int_0^{2\pi} \cos(x)\cos(2x)\cdots\cos(mx)\,dx$. For which integers $m$, $1 \leq m \leq 10$ is $I_m \neq 0$?

A–6 If $p(x) = a_0 + a_1 x + \cdots + a_m x^m$ is a polynomial with real coefficients $a_i$, then set

$$\Gamma(p(x)) = a_0^2 + a_1^2 + \cdots + a_m^2.$$

Let $F(x) = 3x^2 + 7x + 2$. Find, with proof, a polynomial $g(x)$ with real coefficients such that

(i) $g(0) = 1$, and

(ii) $\Gamma(f(x)^n) = \Gamma(g(x)^n)$

for every integer $n \geq 1$.

B–1 Let $k$ be the smallest positive integer for which there exist distinct integers $m_1, m_2, m_3, m_4, m_5$ such that the polynomial

$$p(x) = (x-m_1)(x-m_2)(x-m_3)(x-m_4)(x-m_5)$$

has exactly $k$ nonzero coefficients. Find, with proof, a set of integers $m_1, m_2, m_3, m_4, m_5$ for which this minimum $k$ is achieved.

B–2 Define polynomials $f_n(x)$ for $n \geq 0$ by $f_0(x) = 1$, $f_n(0) = 0$ for $n \geq 1$, and

$$\frac{d}{dx} f_{n+1}(x) = (n+1) f_n(x+1)$$

for $n \geq 0$. Find, with proof, the explicit factorization of $f_{100}(1)$ into powers of distinct primes.

B–3 Let

$$\begin{array}{cccc} a_{1,1} & a_{1,2} & a_{1,3} & \dots \\ a_{2,1} & a_{2,2} & a_{2,3} & \dots \\ a_{3,1} & a_{3,2} & a_{3,3} & \dots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

be a doubly infinite array of positive integers, and suppose each positive integer appears exactly eight times in the array. Prove that $a_{m,n} > mn$ for some pair of positive integers $(m,n)$.

B–4 Let $C$ be the unit circle $x^2 + y^2 = 1$. A point $p$ is chosen randomly on the circumference $C$ and another point $q$ is chosen randomly from the interior of $C$ (these points are chosen independently and uniformly over their domains). Let $R$ be the rectangle with sides parallel to the $x$ and $y$-axes with diagonal $pq$. What is the probability that no point of $R$ lies outside of $C$?

B–5 Evaluate $\int_0^\infty t^{-1/2} e^{-1985(t+t^{-1})}\,dt$. You may assume that $\int_{-\infty}^\infty e^{-x^2}\,dx = \sqrt{\pi}$.

B–6 Let $G$ be a finite set of real $n \times n$ matrices $\{M_i\}$, $1 \leq i \leq r$, which form a group under matrix multiplication. Suppose that $\sum_{i=1}^r \operatorname{tr}(M_i) = 0$, where $\operatorname{tr}(A)$ denotes the trace of the matrix $A$. Prove that $\sum_{i=1}^r M_i$ is the $n \times n$ zero matrix.

# The Forty-Seventh Annual William Lowell Putnam Competition
## Saturday, December 6, 1986

A–1 Find, with explanation, the maximum value of $f(x) = x^3 - 3x$ on the set of all real numbers $x$ satisfying $x^4 + 36 \leq 13x^2$.

A–2 What is the units (i.e., rightmost) digit of

$$\left\lfloor \frac{10^{20000}}{10^{100}+3} \right\rfloor ?$$

A–3 Evaluate $\sum_{n=0}^{\infty} \operatorname{Arccot}(n^2+n+1)$, where $\operatorname{Arccot} t$ for $t \geq 0$ denotes the number $\theta$ in the interval $0 < \theta \leq \pi/2$ with $\cot\theta = t$.

A–4 A *transversal* of an $n \times n$ matrix $A$ consists of $n$ entries of $A$, no two in the same row or column. Let $f(n)$ be the number of $n \times n$ matrices $A$ satisfying the following two conditions:

(a) Each entry $\alpha_{i,j}$ of $A$ is in the set $\{-1, 0, 1\}$.

(b) The sum of the $n$ entries of a transversal is the same for all transversals of $A$.

An example of such a matrix $A$ is

$$A = \begin{pmatrix} -1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Determine with proof a formula for $f(n)$ of the form

$$f(n) = a_1 b_1^n + a_2 b_2^n + a_3 b_3^n + a_4,$$

where the $a_i$'s and $b_i$'s are rational numbers.

A–5 Suppose $f_1(x), f_2(x), \dots, f_n(x)$ are functions of $n$ real variables $x = (x_1, \dots, x_n)$ with continuous second-order partial derivatives everywhere on $\mathbb{R}^n$. Suppose further that there are constants $c_{ij}$ such that

$$\frac{\partial f_i}{\partial x_j} - \frac{\partial f_j}{\partial x_i} = c_{ij}$$

for all $i$ and $j$, $1 \leq i \leq n$, $1 \leq j \leq n$. Prove that there is a function $g(x)$ on $\mathbb{R}^n$ such that $f_i + \partial g/\partial x_i$ is linear for all $i$, $1 \leq i \leq n$. (A linear function is one of the form

$$a_0 + a_1 x_1 + a_2 x_2 + \cdots + a_n x_n.)$$

A–6 Let $a_1, a_2, \dots, a_n$ be real numbers, and let $b_1, b_2, \dots, b_n$ be distinct positive integers. Suppose that there is a polynomial $f(x)$ satisfying the identity

$$(1-x)^n f(x) = 1 + \sum_{i=1}^{n} a_i x^{b_i}.$$

Find a simple expression (not involving any sums) for $f(1)$ in terms of $b_1, b_2, \dots, b_n$ and $n$ (but independent of $a_1, a_2, \dots, a_n$).

B–1 Inscribe a rectangle of base $b$ and height $h$ in a circle of radius one, and inscribe an isosceles triangle in the region of the circle cut off by one base of the rectangle (with that side as the base of the triangle). For what value of $h$ do the rectangle and triangle have the same area?

B–2 Prove that there are only a finite number of possibilities for the ordered triple $T = (x-y, y-z, z-x)$, where $x, y, z$ are complex numbers satisfying the simultaneous equations

$$x(x-1) + 2yz = y(y-1) + 2zx = z(z-1) + 2xy,$$

and list all such triples $T$.

B–3 Let $\Gamma$ consist of all polynomials in $x$ with integer coefficients. For $f$ and $g$ in $\Gamma$ and $m$ a positive integer, let $f \equiv g \pmod{m}$ mean that every coefficient of $f - g$ is an integral multiple of $m$. Let $n$ and $p$ be positive integers with $p$ prime. Given that $f, g, h, r$ and $s$ are in $\Gamma$ with $rf + sg \equiv 1 \pmod{p}$ and $fg \equiv h \pmod{p}$, prove that there exist $F$ and $G$ in $\Gamma$ with $F \equiv f \pmod{p}$, $G \equiv g \pmod{p}$, and $FG \equiv h \pmod{p^n}$.

B–4 For a positive real number $r$, let $G(r)$ be the minimum value of $|r - \sqrt{m^2 + 2n^2}|$ for all integers $m$ and $n$. Prove or disprove the assertion that $\lim_{r\to\infty} G(r)$ exists and equals 0.

B–5 Let $f(x,y,z) = x^2 + y^2 + z^2 + xyz$. Let $p(x,y,z), q(x,y,z), r(x,y,z)$ be polynomials with real coefficients satisfying

$$f(p(x,y,z), q(x,y,z), r(x,y,z)) = f(x,y,z).$$

Prove or disprove the assertion that the sequence $p, q, r$ consists of some permutation of $\pm x, \pm y, \pm z$, where the number of minus signs is 0 or 2.

B–6 Suppose $A, B, C, D$ are $n \times n$ matrices with entries in a field $F$, satisfying the conditions that $AB^T$ and $CD^T$ are symmetric and $AD^T - BC^T = I$. Here $I$ is the $n \times n$ identity matrix, and if $M$ is an $n \times n$ matrix, $M^T$ is its transpose. Prove that $A^T D - C^T B = I$.

# The Forty-Eighth Annual William Lowell Putnam Competition
## Saturday, December 5, 1987

A–1 Curves $A, B, C$ and $D$ are defined in the plane as follows:

$$\begin{aligned} A &= \left\{ (x,y) : x^2 - y^2 = \frac{x}{x^2+y^2} \right\}, \\ B &= \left\{ (x,y) : 2xy + \frac{y}{x^2+y^2} = 3 \right\}, \\ C &= \left\{ (x,y) : x^3 - 3xy^2 + 3y = 1 \right\}, \\ D &= \left\{ (x,y) : 3x^2y - 3x - y^3 = 0 \right\}. \end{aligned}$$

Prove that $A \cap B = C \cap D$.

A–2 The sequence of digits

$$123456789101112131415161718192021\dots$$

is obtained by writing the positive integers in order. If the $10^n$-th digit in this sequence occurs in the part of the sequence in which the $m$-digit numbers are placed, define $f(n)$ to be $m$. For example, $f(2) = 2$ because the 100th digit enters the sequence in the placement of the two-digit integer 55. Find, with proof, $f(1987)$.

A–3 For all real $x$, the real-valued function $y = f(x)$ satisfies

$$y'' - 2y' + y = 2e^x.$$

(a) If $f(x) > 0$ for all real $x$, must $f'(x) > 0$ for all real $x$? Explain.

(b) If $f'(x) > 0$ for all real $x$, must $f(x) > 0$ for all real $x$? Explain.

A–4 Let $P$ be a polynomial, with real coefficients, in three variables and $F$ be a function of two variables such that

$$P(ux, uy, uz) = u^2 F(y - x, z - x) \quad \text{for all real } x, y, z, u,$$

and such that $P(1,0,0) = 4$, $P(0,1,0) = 5$, and $P(0,0,1) = 6$. Also let $A, B, C$ be complex numbers with $P(A,B,C) = 0$ and $|B - A| = 10$. Find $|C - A|$.

A–5 Let

$$\vec{G}(x,y) = \left( \frac{-y}{x^2+4y^2}, \frac{x}{x^2+4y^2}, 0 \right).$$

Prove or disprove that there is a vector-valued function

$$\vec{F}(x,y,z) = (M(x,y,z), N(x,y,z), P(x,y,z))$$

with the following properties:

(i) $M, N, P$ have continuous partial derivatives for all $(x,y,z) \neq (0,0,0)$;

(ii) $\mathrm{Curl}\,\vec{F} = \vec{0}$ for all $(x,y,z) \neq (0,0,0)$;

(iii) $\vec{F}(x,y,0) = \vec{G}(x,y)$.

A–6 For each positive integer $n$, let $a(n)$ be the number of zeroes in the base 3 representation of $n$. For which positive real numbers $x$ does the series

$$\sum_{n=1}^{\infty} \frac{x^{a(n)}}{n^3}$$

converge?

B–1 Evaluate

$$\int_2^4 \frac{\sqrt{\ln(9-x)}\,dx}{\sqrt{\ln(9-x)} + \sqrt{\ln(x+3)}}.$$

B–2 Let $r, s$ and $t$ be integers with $0 \leq r$, $0 \leq s$ and $r + s \leq t$. Prove that

$$\frac{\binom{s}{0}}{\binom{t}{r}} + \frac{\binom{s}{1}}{\binom{t}{r+1}} + \cdots + \frac{\binom{s}{s}}{\binom{t}{r+s}} = \frac{t+1}{(t+1-s)\binom{t-s}{r}}.$$

B–3 Let $F$ be a field in which $1 + 1 \neq 0$. Show that the set of solutions to the equation $x^2 + y^2 = 1$ with $x$ and $y$ in $F$ is given by $(x,y) = (1,0)$ and

$$(x,y) = \left( \frac{r^2-1}{r^2+1}, \frac{2r}{r^2+1} \right)$$

where $r$ runs through the elements of $F$ such that $r^2 \neq -1$.

B–4 Let $(x_1, y_1) = (0.8, 0.6)$ and let $x_{n+1} = x_n \cos y_n - y_n \sin y_n$ and $y_{n+1} = x_n \sin y_n + y_n \cos y_n$ for $n = 1, 2, 3, \dots$. For each of $\lim_{n\to\infty} x_n$ and $\lim_{n\to\infty} y_n$, prove that the limit exists and find it or prove that the limit does not exist.

B–5 Let $O_n$ be the $n$-dimensional vector $(0, 0, \cdots, 0)$. Let $M$ be a $2n \times n$ matrix of complex numbers such that whenever $(z_1, z_2, \dots, z_{2n})M = O_n$, with complex $z_i$, not all zero, then at least one of the $z_i$ is not real. Prove that for arbitrary real numbers $r_1, r_2, \dots, r_{2n}$, there are complex numbers $w_1, w_2, \dots, w_n$ such that

$$\mathrm{re}\left[ M \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \right] = \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}.$$

(Note: if $C$ is a matrix of complex numbers, $\mathrm{re}(C)$ is the matrix whose entries are the real parts of the entries of $C$.)

B–6 Let $F$ be the field of $p^2$ elements, where $p$ is an odd prime. Suppose $S$ is a set of $(p^2-1)/2$ distinct nonzero elements of $F$ with the property that for each $a \neq 0$ in $F$, exactly one of $a$ and $-a$ is in $S$. Let $N$ be the number of elements in the intersection $S \cap \{2a : a \in S\}$. Prove that $N$ is even.

# The Forty-Ninth Annual William Lowell Putnam Competition
## Saturday, December 3, 1988

A–1 Let $R$ be the region consisting of the points $(x,y)$ of the cartesian plane satisfying both $|x|-|y| \leq 1$ and $|y| \leq 1$. Sketch the region $R$ and find its area.

A–2 A not uncommon calculus mistake is to believe that the product rule for derivatives says that $(fg)' = f'g'$. If $f(x) = e^{x^2}$, determine, with proof, whether there exists an open interval $(a,b)$ and a nonzero function $g$ defined on $(a,b)$ such that this wrong product rule is true for $x$ in $(a,b)$.

A–3 Determine, with proof, the set of real numbers $x$ for which

$$\sum_{n=1}^{\infty} \left( \frac{1}{n} \csc \frac{1}{n} - 1 \right)^x$$

converges.

A–4 (a) If every point of the plane is painted one of three colors, do there necessarily exist two points of the same color exactly one inch apart?

(b) What if "three" is replaced by "nine"?

A–5 Prove that there exists a *unique* function $f$ from the set $\mathrm{R}^+$ of positive real numbers to $\mathrm{R}^+$ such that

$$f(f(x)) = 6x - f(x)$$

and

$$f(x) > 0$$

for all $x > 0$.

A–6 If a linear transformation $A$ on an $n$-dimensional vector space has $n+1$ eigenvectors such that any $n$ of them are linearly independent, does it follow that $A$ is a scalar multiple of the identity? Prove your answer.

B–1 A *composite* (positive integer) is a product $ab$ with $a$ and $b$ not necessarily distinct integers in $\{2,3,4,\dots\}$. Show that every composite is expressible as $xy+xz+yz+1$, with $x,y,z$ positive integers.

B–2 Prove or disprove: If $x$ and $y$ are real numbers with $y \geq 0$ and $y(y+1) \leq (x+1)^2$, then $y(y-1) \leq x^2$.

B–3 For every $n$ in the set $\mathrm{N} = \{1,2,\dots\}$ of positive integers, let $r_n$ be the minimum value of $|c - d\sqrt{3}|$ for all nonnegative integers $c$ and $d$ with $c+d = n$. Find, with proof, the smallest positive real number $g$ with $r_n \leq g$ for all $n \in \mathrm{N}$.

B–4 Prove that if $\sum_{n=1}^{\infty} a_n$ is a convergent series of positive real numbers, then so is $\sum_{n=1}^{\infty} (a_n)^{n/(n+1)}$.

B–5 For positive integers $n$, let $M_n$ be the $2n+1$ by $2n+1$ skew-symmetric matrix for which each entry in the first $n$ subdiagonals below the main diagonal is 1 and each of the remaining entries below the main diagonal is -1. Find, with proof, the rank of $M_n$. (According to one definition, the rank of a matrix is the largest $k$ such that there is a $k \times k$ submatrix with nonzero determinant.)

One may note that

$$M_1 = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix}$$

$$M_2 = \begin{pmatrix} 0 & -1 & -1 & 1 & 1 \\ 1 & 0 & -1 & -1 & 1 \\ 1 & 1 & 0 & -1 & -1 \\ -1 & 1 & 1 & 0 & -1 \\ -1 & -1 & 1 & 1 & 0 \end{pmatrix}.$$

B–6 Prove that there exist an infinite number of ordered pairs $(a,b)$ of integers such that for every positive integer $t$, the number $at+b$ is a triangular number if and only if $t$ is a triangular number. (The triangular numbers are the $t_n = n(n+1)/2$ with $n$ in $\{0,1,2,\dots\}$.)

# The Fiftieth Annual William Lowell Putnam Competition
# Saturday, December 2, 1989

A–1 How many primes among the positive integers, written as usual in base 10, are alternating 1's and 0's, beginning and ending with 1?

A–2 Evaluate $\int_0^a \int_0^b e^{\max\{b^2x^2, a^2y^2\}}\,dy\,dx$ where $a$ and $b$ are positive.

A–3 Prove that if

$$11z^{10} + 10iz^9 + 10iz - 11 = 0,$$

then $|z| = 1$. (Here $z$ is a complex number and $i^2 = -1$.)

A–4 If $\alpha$ is an irrational number, $0 < \alpha < 1$, is there a finite game with an honest coin such that the probability of one player winning the game is $\alpha$? (An honest coin is one for which the probability of heads and the probability of tails are both $\frac{1}{2}$. A game is finite if with probability 1 it must end in a finite number of moves.)

A–5 Let $m$ be a positive integer and let $\mathcal{G}$ be a regular $(2m+1)$-gon inscribed in the unit circle. Show that there is a positive constant $A$, independent of $m$, with the following property. For any points $p$ inside $\mathcal{G}$ there are two distinct vertices $v_1$ and $v_2$ of $\mathcal{G}$ such that

$$|\,|p - v_1| - |p - v_2|\,| < \frac{1}{m} - \frac{A}{m^3}.$$

Here $|s - t|$ denotes the distance between the points $s$ and $t$.

A–6 Let $\alpha = 1 + a_1x + a_2x^2 + \cdots$ be a formal power series with coefficients in the field of two elements. Let

$$a_n = \begin{cases} 1 & \text{if every block of zeros in the binary expansion of } n \text{ has an even number of zeros in the block} \\ 0 & \text{otherwise.} \end{cases}$$

(For example, $a_{36} = 1$ because $36 = 100100_2$ and $a_{20} = 0$ because $20 = 10100_2$.) Prove that $\alpha^3 + x\alpha + 1 = 0$.

B–1 A dart, thrown at random, hits a square target. Assuming that any two parts of the target of equal area are equally likely to be hit, find the probability that the point hit is nearer to the center than to any edge. Express your answer in the form $\frac{a\sqrt{b}+c}{d}$, where $a, b, c, d$ are integers.

B–2 Let $S$ be a non-empty set with an associative operation that is left and right cancellative ($xy = xz$ implies $y = z$, and $yx = zx$ implies $y = z$). Assume that for every $a$ in $S$ the set $\{a^n : n = 1, 2, 3, \ldots\}$ is finite. Must $S$ be a group?

B–3 Let $f$ be a function on $[0, \infty)$, differentiable and satisfying

$$f'(x) = -3f(x) + 6f(2x)$$

for $x > 0$. Assume that $|f(x)| \le e^{-\sqrt{x}}$ for $x \ge 0$ (so that $f(x)$ tends rapidly to 0 as $x$ increases). For $n$ a non-negative integer, define

$$\mu_n = \int_0^\infty x^n f(x)\,dx$$

(sometimes called the $n$th moment of $f$).

a) Express $\mu_n$ in terms of $\mu_0$.

b) Prove that the sequence $\{\mu_n \frac{3^n}{n!}\}$ always converges, and that the limit is 0 only if $\mu_0 = 0$.

B–4 Can a countably infinite set have an uncountable collection of non-empty subsets such that the intersection of any two of them is finite?

B–5 Label the vertices of a trapezoid $T$ (quadrilateral with two parallel sides) inscribed in the unit circle as $A, B, C, D$ so that $AB$ is parallel to $CD$ and $A, B, C, D$ are in counterclockwise order. Let $s_1$, $s_2$, and $d$ denote the lengths of the line segments $AB$, $CD$, and $OE$, where E is the point of intersection of the diagonals of $T$, and $O$ is the center of the circle. Determine the least upper bound of $\frac{s_1 - s_2}{d}$ over all such $T$ for which $d \neq 0$, and describe all cases, if any, in which it is attained.

B–6 Let $(x_1, x_2, \ldots x_n)$ be a point chosen at random from the $n$-dimensional region defined by $0 < x_1 < x_2 < \cdots < x_n < 1$. Let $f$ be a continuous function on $[0, 1]$ with $f(1) = 0$. Set $x_0 = 0$ and $x_{n+1} = 1$. Show that the expected value of the Riemann sum

$$\sum_{i=0}^{n} (x_{i+1} - x_i) f(x_{i+1})$$

is $\int_0^1 f(t)P(t)\,dt$, where $P$ is a polynomial of degree $n$, independent of $f$, with $0 \le P(t) \le 1$ for $0 \le t \le 1$.

# The 51st William Lowell Putnam Mathematical Competition
# Saturday, December 8, 1990

A–1 Let

$$T_0 = 2, T_1 = 3, T_2 = 6,$$

and for $n \geq 3$,

$$T_n = (n+4)T_{n-1} - 4nT_{n-2} + (4n-8)T_{n-3}.$$

The first few terms are

$$2, 3, 6, 14, 40, 152, 784, 5168, 40576.$$

Find, with proof, a formula for $T_n$ of the form $T_n = A_n + B_n$, where $\{A_n\}$ and $\{B_n\}$ are well-known sequences.

A–2 Is $\sqrt{2}$ the limit of a sequence of numbers of the form $\sqrt[3]{n} - \sqrt[3]{m}$ $(n, m = 0, 1, 2, \dots)$?

A–3 Prove that any convex pentagon whose vertices (no three of which are collinear) have integer coordinates must have area greater than or equal to 5/2.

A–4 Consider a paper punch that can be centered at any point of the plane and that, when operated, removes from the plane precisely those points whose distance from the center is irrational. How many punches are needed to remove every point?

A–5 If $\mathbf{A}$ and $\mathbf{B}$ are square matrices of the same size such that $\mathbf{ABAB} = \mathbf{0}$, does it follow that $\mathbf{BABA} = \mathbf{0}$?

A–6 If $X$ is a finite set, let $X$ denote the number of elements in $X$. Call an ordered pair $(S, T)$ of subsets of $\{1, 2, \dots, n\}$ *admissible* if $s > |T|$ for each $s \in S$, and $t > |S|$ for each $t \in T$. How many admissible ordered pairs of subsets of $\{1, 2, \dots, 10\}$ are there? Prove your answer.

B–1 Find all real-valued continuously differentiable functions $f$ on the real line such that for all $x$,

$$(f(x))^2 = \int_0^x [(f(t))^2 + (f'(t))^2]\,dt + 1990.$$

B–2 Prove that for $|x| < 1$, $|z| > 1$,

$$1 + \sum_{j=1}^{\infty} (1 + x^j) P_j = 0,$$

where $P_j$ is

$$\frac{(1-z)(1-zx)(1-zx^2)\cdots(1-zx^{j-1})}{(z-x)(z-x^2)(z-x^3)\cdots(z-x^j)}.$$

B–3 Let $S$ be a set of $2 \times 2$ integer matrices whose entries $a_{ij}$ (1) are all squares of integers and, (2) satisfy $a_{ij} \leq 200$. Show that if $S$ has more than 50387 $(= 15^4 - 15^2 - 15 + 2)$ elements, then it has two elements that commute.

B–4 Let $G$ be a finite group of order $n$ generated by $a$ and $b$. Prove or disprove: there is a sequence

$$g_1, g_2, g_3, \dots, g_{2n}$$

such that

(1) every element of $G$ occurs exactly twice, and

(2) $g_{i+1}$ equals $g_i a$ or $g_i b$ for $i = 1, 2, \dots, 2n$. (Interpret $g_{2n+1}$ as $g_1$.)

B–5 Is there an infinite sequence $a_0, a_1, a_2, \dots$ of nonzero real numbers such that for $n = 1, 2, 3, \dots$ the polynomial

$$p_n(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

has exactly $n$ distinct real roots?

B–6 Let $S$ be a nonempty closed bounded convex set in the plane. Let $K$ be a line and $t$ a positive number. Let $L_1$ and $L_2$ be support lines for $S$ parallel to $K_1$, and let $\overline{L}$ be the line parallel to $K$ and midway between $L_1$ and $L_2$. Let $B_S(K, t)$ be the band of points whose distance from $\overline{L}$ is at most $(t/2)w$, where $w$ is the distance between $L_1$ and $L_2$. What is the smallest $t$ such that

$$S \cap \bigcap_K B_S(K, t) \neq \emptyset$$

for all $S$? ($K$ runs over all lines in the plane.)

# The 52nd William Lowell Putnam Mathematical Competition
## Saturday, December 7, 1991

A–1 A $2\times 3$ rectangle has vertices as $(0,0),(2,0),(0,3)$, and $(2,3)$. It rotates $90^\circ$ clockwise about the point $(2,0)$. It then rotates $90^\circ$ clockwise about the point $(5,0)$, then $90^\circ$ clockwise about the point $(7,0)$, and finally, $90^\circ$ clockwise about the point $(10,0)$. (The side originally on the $x$-axis is now back on the $x$-axis.) Find the area of the region above the $x$-axis and below the curve traced out by the point whose initial position is (1,1).

A–2 Let $\mathbf{A}$ and $\mathbf{B}$ be different $n\times n$ matrices with real entries. If $\mathbf{A}^3=\mathbf{B}^3$ and $\mathbf{A}^2\mathbf{B}=\mathbf{B}^2\mathbf{A}$, can $\mathbf{A}^2+\mathbf{B}^2$ be invertible?

A–3 Find all real polynomials $p(x)$ of degree $n\geq 2$ for which there exist real numbers $r_1<r_2<\cdots<r_n$ such that

1. $p(r_i)=0, \qquad i=1,2,\dots,n$, and
2. $p'\left(\frac{r_i+r_{i+1}}{2}\right)=0 \qquad i=1,2,\dots,n-1$,

where $p'(x)$ denotes the derivative of $p(x)$.

A–4 Does there exist an infinite sequence of closed discs $D_1,D_2,D_3,\dots$ in the plane, with centers $c_1,c_2,c_3,\dots$, respectively, such that

1. the $c_i$ have no limit point in the finite plane,
2. the sum of the areas of the $D_i$ is finite, and
3. every line in the plane intersects at least one of the $D_i$?

A–5 Find the maximum value of

$$\int_0^y \sqrt{x^4+(y-y^2)^2}\,dx$$

for $0\leq y\leq 1$.

A–6 Let $A(n)$ denote the number of sums of positive integers

$$a_1+a_2+\cdots+a_r$$

which add up to $n$ with

$$a_1>a_2+a_3, a_2>a_3+a_4,\dots,$$
$$a_{r-2}>a_{r-1}+a_r, a_{r-1}>a_r.$$

Let $B(n)$ denote the number of $b_1+b_2+\cdots+b_s$ which add up to $n$, with

1. $b_1\geq b_2\geq\cdots\geq b_s$,
2. each $b_i$ is in the sequence $1,2,4,\dots,g_j,\dots$ defined by $g_1=1$, $g_2=2$, and $g_j=g_{j-1}+g_{j-2}+1$, and
3. if $b_1=g_k$ then every element in $\{1,2,4,\dots,g_k\}$ appears at least once as a $b_i$.

Prove that $A(n)=B(n)$ for each $n\geq 1$.

(For example, $A(7)=5$ because the relevant sums are $7, 6+1, 5+2, 4+3, 4+2+1$, and $B(7)=5$ because the relevant sums are $4+2+1, 2+2+2+1, 2+2+1+1+1, 2+1+1+1+1+1, 1+1+1+1+1+1+1$.)

B–1 For each integer $n\geq 0$, let $S(n)=n-m^2$, where $m$ is the greatest integer with $m^2\leq n$. Define a sequence $(a_k)_{k=0}^\infty$ by $a_0=A$ and $a_{k+1}=a_k+S(a_k)$ for $k\geq 0$. For what positive integers $A$ is this sequence eventually constant?

B–2 Suppose $f$ and $g$ are non-constant, differentiable, real-valued functions defined on $(-\infty,\infty)$. Furthermore, suppose that for each pair of real numbers $x$ and $y$,

$$f(x+y)=f(x)f(y)-g(x)g(y),$$
$$g(x+y)=f(x)g(y)+g(x)f(y).$$

If $f'(0)=0$, prove that $(f(x))^2+(g(x))^2=1$ for all $x$.

B–3 Does there exist a real number $L$ such that, if $m$ and $n$ are integers greater than $L$, then an $m\times n$ rectangle may be expressed as a union of $4\times 6$ and $5\times 7$ rectangles, any two of which intersect at most along their boundaries?

B–4 Suppose $p$ is an odd prime. Prove that

$$\sum_{j=0}^{p}\binom{p}{j}\binom{p+j}{j}\equiv 2^p+1 \pmod{p^2}.$$

B–5 Let $p$ be an odd prime and let $\mathbb{Z}_p$ denote (the field of) integers modulo $p$. How many elements are in the set

$$\{x^2 : x\in\mathbb{Z}_p\}\cap\{y^2+1 : y\in\mathbb{Z}_p\}?$$

B–6 Let $a$ and $b$ be positive numbers. Find the largest number $c$, in terms of $a$ and $b$, such that

$$a^x b^{1-x}\leq a\frac{\sinh ux}{\sinh u}+b\frac{\sinh u(1-x)}{\sinh u}$$

for all $u$ with $0<|u|\leq c$ and for all $x$, $0<x<1$. (Note: $\sinh u=(e^u-e^{-u})/2$.)

# The 53rd William Lowell Putnam Mathematical Competition
## Saturday, December 5, 1992

A–1 Prove that $f(n) = 1 - n$ is the only integer-valued function defined on the integers that satisfies the following conditions.

(i) $f(f(n)) = n$, for all integers $n$;

(ii) $f(f(n+2)+2) = n$ for all integers $n$;

(iii) $f(0) = 1$.

A–2 Define $C(\alpha)$ to be the coefficient of $x^{1992}$ in the power series about $x = 0$ of $(1+x)^\alpha$. Evaluate

$$\int_0^1 \left( C(-y-1) \sum_{k=1}^{1992} \frac{1}{y+k} \right) dy.$$

A–3 For a given positive integer $m$, find all triples $(n,x,y)$ of positive integers, with $n$ relatively prime to $m$, which satisfy

$$(x^2+y^2)^m = (xy)^n.$$

A–4 Let $f$ be an infinitely differentiable real-valued function defined on the real numbers. If

$$f\left(\frac{1}{n}\right) = \frac{n^2}{n^2+1}, \qquad n = 1,2,3,\ldots,$$

compute the values of the derivatives $f^{(k)}(0), k = 1,2,3,\ldots$.

A–5 For each positive integer $n$, let $a_n = 0$ (or 1) if the number of 1's in the binary representation of $n$ is even (or odd), respectively. Show that there do not exist positive integers $k$ and $m$ such that

$$a_{k+j} = a_{k+m+j} = a_{k+2m+j},$$

for $0 \leq j \leq m-1$.

A–6 Four points are chosen at random on the surface of a sphere. What is the probability that the center of the sphere lies inside the tetrahedron whose vertices are at the four points? (It is understood that each point is independently chosen relative to a uniform distribution on the sphere.)

B–1 Let $S$ be a set of $n$ distinct real numbers. Let $A_S$ be the set of numbers that occur as averages of two distinct elements of $S$. For a given $n \geq 2$, what is the smallest possible number of elements in $A_S$?

B–2 For nonnegative integers $n$ and $k$, define $Q(n,k)$ to be the coefficient of $x^k$ in the expansion of $(1+x+x^2+x^3)^n$. Prove that

$$Q(n,k) = \sum_{j=0}^{k} \binom{n}{j} \binom{n}{k-2j},$$

where $\binom{a}{b}$ is the standard binomial coefficient. (Reminder: For integers $a$ and $b$ with $a \geq 0$, $\binom{a}{b} = \frac{a!}{b!(a-b)!}$ for $0 \leq b \leq a$, with $\binom{a}{b} = 0$ otherwise.)

B–3 For any pair $(x,y)$ of real numbers, a sequence $(a_n(x,y))_{n\geq 0}$ is defined as follows:

$$a_0(x,y) = x,$$
$$a_{n+1}(x,y) = \frac{(a_n(x,y))^2 + y^2}{2}, \qquad \text{for } n \geq 0.$$

Find the area of the region

$$\{(x,y) | (a_n(x,y))_{n\geq 0} \text{ converges}\}.$$

B–4 Let $p(x)$ be a nonzero polynomial of degree less than 1992 having no nonconstant factor in common with $x^3 - x$. Let

$$\frac{d^{1992}}{dx^{1992}} \left( \frac{p(x)}{x^3 - x} \right) = \frac{f(x)}{g(x)}$$

for polynomials $f(x)$ and $g(x)$. Find the smallest possible degree of $f(x)$.

B–5 Let $D_n$ denote the value of the $(n-1)\times(n-1)$ determinant

$$\begin{bmatrix} 3 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 4 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 5 & 1 & \cdots & 1 \\ 1 & 1 & 1 & 6 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \cdots & n+1 \end{bmatrix}.$$

Is the set $\left\{\frac{D_n}{n!}\right\}_{n\geq 2}$ bounded?

B–6 Let $\mathscr{M}$ be a set of real $n \times n$ matrices such that

(i) $I \in \mathscr{M}$, where $I$ is the $n \times n$ identity matrix;

(ii) if $A \in \mathscr{M}$ and $B \in \mathscr{M}$, then either $AB \in \mathscr{M}$ or $-AB \in \mathscr{M}$, but not both;

(iii) if $A \in \mathscr{M}$ and $B \in \mathscr{M}$, then either $AB = BA$ or $AB = -BA$;

(iv) if $A \in \mathscr{M}$ and $A \neq I$, there is at least one $B \in \mathscr{M}$ such that $AB = -BA$.

Prove that $\mathscr{M}$ contains at most $n^2$ matrices.

# The 54th William Lowell Putnam Mathematical Competition
# Saturday, December 4, 1993

A–1 The horizontal line $y = c$ intersects the curve $y = 2x - 3x^3$ in the first quadrant as in the figure. Find $c$ so that the areas of the two shaded regions are equal. [Figure not included. The first region is bounded by the $y$-axis, the line $y = c$ and the curve; the other lies under the curve and above the line $y = c$ between their two points of intersection.]

A–2 Let $(x_n)_{n\geq 0}$ be a sequence of nonzero real numbers such that $x_n^2 - x_{n-1}x_{n+1} = 1$ for $n = 1,2,3,\dots$. Prove there exists a real number $a$ such that $x_{n+1} = ax_n - x_{n-1}$ for all $n \geq 1$.

A–3 Let $\mathscr{P}_n$ be the set of subsets of $\{1,2,\dots,n\}$. Let $c(n,m)$ be the number of functions $f : \mathscr{P}_n \to \{1,2,\dots,m\}$ such that $f(A \cap B) = \min\{f(A), f(B)\}$. Prove that

$$c(n,m) = \sum_{j=1}^{m} j^n.$$

A–4 Let $x_1, x_2, \dots, x_{19}$ be positive integers each of which is less than or equal to 93. Let $y_1, y_2, \dots, y_{93}$ be positive integers each of which is less than or equal to 19. Prove that there exists a (nonempty) sum of some $x_i$'s equal to a sum of some $y_j$'s.

A–5 Show that

$$\int_{-100}^{-10} \left( \frac{x^2 - x}{x^3 - 3x + 1} \right)^2 dx +$$
$$\int_{\frac{1}{101}}^{\frac{1}{11}} \left( \frac{x^2 - x}{x^3 - 3x + 1} \right)^2 dx +$$
$$\int_{\frac{101}{100}}^{\frac{11}{10}} \left( \frac{x^2 - x}{x^3 - 3x + 1} \right)^2 dx$$

is a rational number.

A–6 The infinite sequence of 2's and 3's

$$2,3,3,2,3,3,3,2,3,3,3,2,3,3,2,3,3,$$
$$3,2,3,3,3,2,3,3,3,2,3,3,2,3,3,3,2,\dots$$

has the property that, if one forms a second sequence that records the number of 3's between successive 2's, the result is identical to the given sequence. Show that there exists a real number $r$ such that, for any $n$, the $n$th term of the sequence is 2 if and only if $n = 1 + \lfloor rm \rfloor$ for some nonnegative integer $m$. (Note: $\lfloor x \rfloor$ denotes the largest integer less than or equal to $x$.)

B–1 Find the smallest positive integer $n$ such that for every integer $m$ with $0 < m < 1993$, there exists an integer $k$ for which

$$\frac{m}{1993} < \frac{k}{n} < \frac{m+1}{1994}.$$

B–2 Consider the following game played with a deck of $2n$ cards numbered from 1 to $2n$. The deck is randomly shuffled and $n$ cards are dealt to each of two players. Beginning with $A$, the players take turns discarding one of their remaining cards and announcing its number. The game ends as soon as the sum of the numbers on the discarded cards is divisible by $2n+1$. The last person to discard wins the game. Assuming optimal strategy by both $A$ and $B$, what is the probability that $A$ wins?

B–3 Two real numbers $x$ and $y$ are chosen at random in the interval (0,1) with respect to the uniform distribution. What is the probability that the closest integer to $x/y$ is even? Express the answer in the form $r + s\pi$, where $r$ and $s$ are rational numbers.

B–4 The function $K(x,y)$ is positive and continuous for $0 \leq x \leq 1, 0 \leq y \leq 1$, and the functions $f(x)$ and $g(x)$ are positive and continuous for $0 \leq x \leq 1$. Suppose that for all $x$, $0 \leq x \leq 1$,

$$\int_0^1 f(y)K(x,y)\,dy = g(x)$$

and

$$\int_0^1 g(y)K(x,y)\,dy = f(x).$$

Show that $f(x) = g(x)$ for $0 \leq x \leq 1$.

B–5 Show there do not exist four points in the Euclidean plane such that the pairwise distances between the points are all odd integers.

B–6 Let $S$ be a set of three, not necessarily distinct, positive integers. Show that one can transform $S$ into a set containing 0 by a finite number of applications of the following rule: Select two of the three integers, say $x$ and $y$, where $x \leq y$ and replace them with $2x$ and $y - x$.

# The 55th William Lowell Putnam Mathematical Competition
## Saturday, December 3, 1994

A–1 Suppose that a sequence $a_1, a_2, a_3, \dots$ satisfies $0 < a_n \leq a_{2n} + a_{2n+1}$ for all $n \geq 1$. Prove that the series $\sum_{n=1}^\infty a_n$ diverges.

A–2 Let $A$ be the area of the region in the first quadrant bounded by the line $y = \frac{1}{2}x$, the $x$-axis, and the ellipse $\frac{1}{9}x^2 + y^2 = 1$. Find the positive number $m$ such that $A$ is equal to the area of the region in the first quadrant bounded by the line $y = mx$, the $y$-axis, and the ellipse $\frac{1}{9}x^2 + y^2 = 1$.

A–3 Show that if the points of an isosceles right triangle of side length 1 are each colored with one of four colors, then there must be two points of the same color whch are at least a distance $2 - \sqrt{2}$ apart.

A–4 Let $A$ and $B$ be $2 \times 2$ matrices with integer entries such that $A, A+B, A+2B, A+3B$, and $A+4B$ are all invertible matrices whose inverses have integer entries. Show that $A+5B$ is invertible and that its inverse has integer entries.

A–5 Let $(r_n)_{n \geq 0}$ be a sequence of positive real numbers such that $\lim_{n \to \infty} r_n = 0$. Let $S$ be the set of numbers representable as a sum

$$r_{i_1} + r_{i_2} + \cdots + r_{i_{1994}},$$

with $i_1 < i_2 < \cdots < i_{1994}$. Show that every nonempty interval $(a,b)$ contains a nonempty subinterval $(c,d)$ that does not intersect $S$.

A–6 Let $f_1, \dots, f_{10}$ be bijections of the set of integers such that for each integer $n$, there is some composition $f_{i_1} \circ f_{i_2} \circ \cdots \circ f_{i_m}$ of these functions (allowing repetitions) which maps 0 to $n$. Consider the set of 1024 functions

$$\mathscr{F} = \{f_1^{e_1} \circ f_2^{e_2} \circ \cdots \circ f_{10}^{e_{10}}\},$$

$e_i = 0$ or 1 for $1 \leq i \leq 10$. ($f_i^0$ is the identity function and $f_i^1 = f_i$.) Show that if $A$ is any nonempty finite set of integers, then at most 512 of the functions in $\mathscr{F}$ map $A$ to itself.

B–1 Find all positive integers $n$ that are within 250 of exactly 15 perfect squares.

B–2 For which real numbers $c$ is there a straight line that intersects the curve

$$x^4 + 9x^3 + cx^2 + 9x + 4$$

in four distinct points?

B–3 Find the set of all real numbers $k$ with the following property: For any positive, differentiable function $f$ that satisfies $f'(x) > f(x)$ for all $x$, there is some number $N$ such that $f(x) > e^{kx}$ for all $x > N$.

B–4 For $n \geq 1$, let $d_n$ be the greatest common divisor of the entries of $A^n - I$, where

$$A = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \quad \text{and} \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Show that $\lim_{n \to \infty} d_n = \infty$.

B–5 For any real number $\alpha$, define the function $f_\alpha(x) = \lfloor \alpha x \rfloor$. Let $n$ be a positive integer. Show that there exists an $\alpha$ such that for $1 \leq k \leq n$,

$$f_\alpha^k(n^2) = n^2 - k = f_{\alpha^k}(n^2).$$

B–6 For any integer $n$, set

$$n_a = 101a - 100 \cdot 2^a.$$

Show that for $0 \leq a, b, c, d \leq 99$, $n_a + n_b \equiv n_c + n_d \pmod{10100}$ implies $\{a, b\} = \{c, d\}$.

# The 56th William Lowell Putnam Mathematical Competition
## Saturday, December 2, 1995

A–1 Let $S$ be a set of real numbers which is closed under multiplication (that is, if $a$ and $b$ are in $S$, then so is $ab$). Let $T$ and $U$ be disjoint subsets of $S$ whose union is $S$. Given that the product of any *three* (not necessarily distinct) elements of $T$ is in $T$ and that the product of any three elements of $U$ is in $U$, show that at least one of the two subsets $T,U$ is closed under multiplication.

A–2 For what pairs $(a,b)$ of positive real numbers does the improper integral

$$\int_b^\infty \left(\sqrt{\sqrt{x+a}-\sqrt{x}}-\sqrt{\sqrt{x}-\sqrt{x-b}}\right)dx$$

converge?

A–3 The number $d_1d_2\dots d_9$ has nine (not necessarily distinct) decimal digits. The number $e_1e_2\dots e_9$ is such that each of the nine 9-digit numbers formed by replacing just one of the digits $d_i$ is $d_1d_2\dots d_9$ by the corresponding digit $e_i$ ($1 \leq i \leq 9$) is divisible by 7. The number $f_1f_2\dots f_9$ is related to $e_1e_2\dots e_9$ is the same way: that is, each of the nine numbers formed by replacing one of the $e_i$ by the corresponding $f_i$ is divisible by 7. Show that, for each $i$, $d_i - f_i$ is divisible by 7. [For example, if $d_1d_2\dots d_9 = 199501996$, then $e_6$ may be 2 or 9, since 199502996 and 199509996 are multiples of 7.]

A–4 Suppose we have a necklace of $n$ beads. Each bead is labeled with an integer and the sum of all these labels is $n-1$. Prove that we can cut the necklace to form a string whose consecutive labels $x_1,x_2,\dots,x_n$ satisfy

$$\sum_{i=1}^k x_i \leq k-1 \qquad \text{for} \quad k=1,2,\dots,n.$$

A–5 Let $x_1,x_2,\dots,x_n$ be differentiable (real-valued) functions of a single variable $f$ which satisfy

$$\begin{aligned}
\frac{dx_1}{dt} &= a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\
\frac{dx_2}{dt} &= a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\
\vdots & \qquad\qquad\qquad \vdots \\
\frac{dx_n}{dt} &= a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n
\end{aligned}$$

for some constants $a_{ij} > 0$. Suppose that for all $i$, $x_i(t) \to 0$ as $t \to \infty$. Are the functions $x_1,x_2,\dots,x_n$ necessarily linearly dependent?

A–6 Suppose that each of $n$ people writes down the numbers 1,2,3 in random order in one column of a $3 \times n$ matrix, with all orders equally likely and with the orders for different columns independent of each other. Let the row sums $a,b,c$ of the resulting matrix be rearranged (if necessary) so that $a \leq b \leq c$. Show that for some $n \geq 1995$, it is at least four times as likely that both $b = a+1$ and $c = a+2$ as that $a = b = c$.

B–1 For a partition $\pi$ of $\{1,2,3,4,5,6,7,8,9\}$, let $\pi(x)$ be the number of elements in the part containing $x$. Prove that for any two partitions $\pi$ and $\pi'$, there are two distinct numbers $x$ and $y$ in $\{1,2,3,4,5,6,7,8,9\}$ such that $\pi(x) = \pi(y)$ and $\pi'(x) = \pi'(y)$. [A *partition* of a set $S$ is a collection of disjoint subsets (parts) whose union is $S$.]

B–2 An ellipse, whose semi-axes have lengths $a$ and $b$, rolls without slipping on the curve $y = c\sin\left(\frac{x}{a}\right)$. How are $a,b,c$ related, given that the ellipse completes one revolution when it traverses one period of the curve?

B–3 To each positive integer with $n^2$ decimal digits, we associate the determinant of the matrix obtained by writing the digits in order across the rows. For example, for $n = 2$, to the integer 8617 we associate $\det\begin{pmatrix} 8 & 6 \\ 1 & 7 \end{pmatrix} = 50$. Find, as a function of $n$, the sum of all the determinants associated with $n^2$-digit integers. (Leading digits are assumed to be nonzero; for example, for $n = 2$, there are 9000 determinants.)

B–4 Evaluate

$$\sqrt[8]{2207 - \frac{1}{2207 - \frac{1}{2207-\dots}}}.$$

Express your answer in the form $\frac{a+b\sqrt{c}}{d}$, where $a,b,c,d$ are integers.

B–5 A game starts with four heaps of beans, containing 3,4,5 and 6 beans. The two players move alternately. A move consists of taking **either**

a) one bean from a heap, provided at least two beans are left behind in that heap, **or**

b) a complete heap of two or three beans.

The player who takes the last heap wins. To win the game, do you want to move first or second? Give a winning strategy.

B–6 For a positive real number $\alpha$, define

$$S(\alpha) = \{\lfloor n\alpha \rfloor : n = 1,2,3,\dots\}.$$

Prove that $\{1,2,3,\dots\}$ cannot be expressed as the disjoint union of three sets $S(\alpha), S(\beta)$ and $S(\gamma)$. [As usual, $\lfloor x \rfloor$ is the greatest integer $\leq x$.]

# Solutions to the 56th William Lowell Putnam Mathematical Competition
# Saturday, December 2, 1995

Kiran Kedlaya

A–1 Suppose on the contrary that there exist $t_1, t_2 \in T$ with $t_1t_2 \in U$ and $u_1, u_2 \in U$ with $u_1u_2 \in T$. Then $(t_1t_2)u_1u_2 \in U$ while $t_1t_2(u_1u_2) \in T$, contradiction.

A–2 The integral converges iff $a = b$. The easiest proof uses "big-O" notation and the fact that $(1+x)^{1/2} = 1 + x/2 + O(x^2)$ for $|x| < 1$. (Here $O(x^2)$ means bounded by a constant times $x^2$.)

So

$$\begin{aligned}\sqrt{x+a}-\sqrt{x} &= x^{1/2}(\sqrt{1+a/x}-1)\\ &= x^{1/2}(1+a/2x+O(x^{-2})),\end{aligned}$$

hence

$$\sqrt{\sqrt{x+a}-\sqrt{x}} = x^{1/4}(a/4x+O(x^{-2}))$$

and similarly

$$\sqrt{\sqrt{x}-\sqrt{x-b}} = x^{1/4}(b/4x+O(x^{-2})).$$

Hence the integral we're looking at is

$$\int_b^\infty x^{1/4}((a-b)/4x+O(x^{-2}))\,dx.$$

The term $x^{1/4}O(x^{-2})$ is bounded by a constant times $x^{-7/4}$, whose integral converges. Thus we only have to decide whether $x^{-3/4}(a-b)/4$ converges. But $x^{-3/4}$ has divergent integral, so we get convergence if and only if $a = b$ (in which case the integral telescopes anyway).

A–3 Let $D$ and $E$ be the numbers $d_1 \dots d_9$ and $e_1 \dots e_9$, respectively. We are given that $(e_i - d_i)10^{9-i} + D \equiv 0 \pmod 7$ and $(f_i - e_i)10^{9-i} + E \equiv 0 \pmod 7$ for $i = 1, \dots, 9$. Sum the first relation over $i = 1, \dots, 9$ and we get $E - D + 9D \equiv 0 \pmod 7$, or $E + D \equiv 0 \pmod 7$. Now add the first and second relations for any particular value of $i$ and we get $(f_i - d_i)10^{9-i} + E + D \equiv 0 \pmod 7$. But we know $E + D$ is divisible by 7, and 10 is coprime to 7, so $d_i - f_i \equiv 0 \pmod 7$.

A–4 Let $s_k = x_1 + \cdots + x_k - k(n-1)/n$, so that $s_n = s_0 = 0$. These form a cyclic sequence that doesn't change when you rotate the necklace, except that the entire sequence gets translated by a constant. In particular, it makes sense to choose $x_i$ for which $s_i$ is maximum and make that one $x_n$; this way $s_i \leq 0$ for all $i$, which gives $x_1 + \cdots + x_i \leq i(n-1)/n$, but the right side may be replaced by $i - 1$ since the left side is an integer.

A–5 Everyone (presumably) knows that the set of solutions of a system of linear first-order differential equations with constant coefficients is $n$-dimensional, with basis vectors of the form $f_i(t)\vec{v}_i$ (i.e. a function times a constant vector), where the $\vec{v}_i$ are linearly independent. In particular, our solution $\vec{x}(t)$ can be written as $\sum_{i=1}^n c_i f_i(t)\vec{v}_1$.

Choose a vector $\vec{w}$ orthogonal to $\vec{v}_2, \dots, \vec{v}_n$ but not to $\vec{v}_1$. Since $\vec{x}(t) \to 0$ as $t \to \infty$, the same is true of $\vec{w} \cdot \vec{x}$; but that is simply $(\vec{w} \cdot \vec{v}_1)c_1 f_1(t)$. In other words, if $c_i \neq 0$, then $f_i(t)$ must also go to 0.

However, it is easy to exhibit a solution which does not go to 0. The sum of the eigenvalues of the matrix $A = (a_{ij})$, also known as the trace of $A$, being the sum of the diagonal entries of $A$, is nonnegative, so $A$ has an eigenvalue $\lambda$ with nonnegative real part, and a corresponding eigenvector $\vec{v}$. Then $e^{\lambda t}\vec{v}$ is a solution that does not go to 0. (If $\lambda$ is not real, add this solution to its complex conjugate to get a real solution, which still doesn't go to 0.)

Hence one of the $c_i$, say $c_1$, is zero, in which case $\vec{x}(t) \cdot \vec{w} = 0$ for all $t$.

A–6 View this as a random walk/Markov process with states $(i, j, k)$ the triples of integers with sum 0, corresponding to the difference between the first, second and third rows with their average (twice the number of columns). Adding a new column adds on a random permutation of the vector $(1, 0, -1)$. I prefer to identify the triple $(i, j, k)$ with the point $(i-j) + (j-k)\omega + (k-i)\omega^2$ in the plane, where $\omega$ is a cube root of unity. Then adding a new column corresponds to moving to one of the six neighbors of the current position in a triangular lattice.

What we'd like to argue is that for large enough $n$, the ratio of the probabilities of being in any two particular states goes to 1. Then in fact, we'll see that eventually, about six times as many matrices have $a = b - 1, b = c - 1$ than $a = b = c$. This is a pain to prove, though, and in fact is way more than we actually need.

Let $C_n$ and $A_n$ be the probability that we are at the origin, or at a particular point adjacent to the origin, respectively. Then $C_{n+1} = A_n$. (In fact, $C_{n+1}$ is $1/6$ times the sum of the probabilities of being at each neighbor of the origin at time $n$, but these are all $A_n$.) So the desired result, which is that $C_n/A_n \geq 2/3$ for some large $n$, is equivalent to $A_{n+1}/A_n \geq 2/3$.

Suppose on the contrary that this is not the case; then $A_n < c(2/3)^n$ for some constant $n$. However, if $n = 6m$, the probability that we chose each of the six types of moves $m$ times is already $(6m)!/[m!^6 6^{6m}]$, which by Stirling's approximation is asymptotic to a constant times $m^{-5/2}$. This term alone is bigger than $c(2/3)^n$, so we must have $A_{n+1}/A_n \geq 2/3$ for some $n$. (In fact, we must have $A_{n+1}/A_n \geq 1-\varepsilon$ for any $\varepsilon > 0$.)

B–1 For a given $\pi$, no more than three different values of $\pi(x)$ are possible (four would require one part each of size at least 1,2,3,4, and that's already more than 9 elements). If no such $x,y$ exist, each pair $(\pi(x),\pi'(x))$ occurs for at most 1 element of $x$, and since there are only $3\times 3$ possible pairs, each must occur exactly once. In particular, each value of $\pi(x)$ must occur 3 times. However, clearly any given value of $\pi(x)$ occurs $k\pi(x)$ times, where $k$ is the number of distinct partitions of that size. Thus $\pi(x)$ can occur 3 times only if it equals 1 or 3, but we have three distinct values for which it occurs, contradiction.

B–2 For those who haven't taken enough physics, "rolling without slipping" means that the perimeter of the ellipse and the curve pass at the same rate, so all we're saying is that the perimeter of the ellipse equals the length of one period of the sine curve. So set up the integrals:

$$\int_0^{2\pi} \sqrt{(-a\sin\theta)^2+(b\cos\theta)^2}\,d\theta = \int_0^{2\pi a} \sqrt{1+(c/a\cos x/a)^2}\,dx.$$

Let $\theta = x/a$ in the second integral and write 1 as $\sin^2\theta+\cos^2\theta$ and you get

$$\int_0^{2\pi} \sqrt{a^2\sin^2\theta+b^2\cos^2\theta}\,d\theta = \int_0^{2\pi} \sqrt{a^2\sin^2\theta+(a^2+c^2)\cos^2\theta}\,d\theta.$$

Since the left side is increasing as a function of $b$, we have equality if and only if $b^2=a^2+c^2$.

B–3 For $n=1$ we obviously get 45, while for $n=3$ the answer is 0 because it both changes sign (because determinants are alternating) and remains unchanged (by symmetry) when you switch any two rows other than the first one. So only $n=2$ is left. By the multilinearity of the determinant, the answer is the determinant of the matrix whose first (resp. second) row is the sum of all possible first (resp. second) rows. There are 90 first rows whose sum is the vector $(450,405)$, and 100 second rows whose sum is $(450,450)$. Thus the answer is $450\times 450 - 450\times 405 = 45\times 450 = 20250$.

B–4 The infinite continued fraction is defined as the limit of the sequence $L_0 = 2207, L_{n+1} = 2207-1/L_n$. Notice that the sequence is strictly decreasing (by induction) and thus indeed has a limit $L$, which satisfies $L = 2207-1/L$, or rewriting, $L^2-2207L+1=0$. Moreover, we want the greater of the two roots.

Now how to compute the eighth root of $L$? Notice that if $x$ satisfies the quadratic $x^2-ax+1=0$, then we have

$$\begin{aligned} 0 &= (x^2-ax+1)(x^2+ax+1) \\ &= x^4-(a^2-2)x^2+1. \end{aligned}$$

Clearly, then, the positive square roots of the quadratic $x^2-bx+1$ satisfy the quadratic $x^2-(b^2+2)^{1/2}x+1=0$. Thus we compute that $L^{1/2}$ is the greater root of $x^2-47x+1=0$, $L^{1/4}$ is the greater root of $x^2-7x+1=0$, and $L^{1/8}$ is the greater root of $x^2-3x+1=0$, otherwise known as $(3+\sqrt{5})/2$.

B–5 This problem is dumb if you know the Sprague-Grundy theory of normal impartial games (see Conway, Berlekamp and Guy, *Winning Ways*, for details). I'll describe how it applies here. To each position you assign a *nim-value* as follows. A position with no moves (in which case the person to move has just lost) takes value 0. Any other position is assigned the smallest number not assigned to a valid move from that position.

For a single pile, one sees that an empty pile has value 0, a pile of 2 has value 1, a pile of 3 has value 2, a pile of 4 has value 0, a pile of 5 has value 1, and a pile of 6 has value 0.

You add piles just like in standard Nim: the nim-value of the composite of two games (where at every turn you pick a game and make a move there) is the "base 2 addition without carries" (i.e. exclusive OR) of the nim-values of the constituents. So our starting position, with piles of 3, 4, 5, 6, has nim-value $2\oplus 0\oplus 1\oplus 0 = 3$.

A position is a win for the player to move if and only if it has a nonzero value, in which case the winning strategy is to always move to a 0 position. (This is always possible from a nonzero position and never from a zero position, which is precisely the condition that defines the set of winning positions.) In this case, the winning move is to reduce the pile of 3 down to 2, and you can easily describe the entire strategy if you so desire.

B–6 Obviously $\alpha,\beta,\gamma$ have to be greater than 1, and no two can both be rational, so without loss of generality assume that $\alpha$ and $\beta$ are irrational. Let $\{x\} = x-\lfloor x\rfloor$ denote the fractional part of $x$. Then $m\in S(\alpha)$ if and only if $f(m/\alpha)\in(1-1/\alpha,1)\cup\{0\}$. In particular, this means that $S(\alpha)\cap\{1,\dots,n\}$ contains $\lceil (n+1)/\alpha\rceil - 1$ elements, and similarly. Hence for every integer $n$,

$$n = \left\lceil \frac{n+1}{\alpha}\right\rceil + \left\lceil \frac{n+1}{\beta}\right\rceil + \left\lceil \frac{n+1}{\gamma}\right\rceil - 3.$$

Dividing through by $n$ and taking the limit as $n\to\infty$ shows that $1/\alpha+1/\beta+1/\gamma = 1$. That in turn implies that for all $n$,

$$\left\{-\frac{n+1}{\alpha}\right\} + \left\{-\frac{n+1}{\beta}\right\} + \left\{-\frac{n+1}{\gamma}\right\} = 2.$$

Our desired contradiction is equivalent to showing that the left side actually takes the value 1 for some $n$. Since the left side is an integer, it suffices to show that $\{-(n+1)/\alpha\} + \{-(n+1)/\beta\} < 1$ for some $n$.

A result in ergodic theory (the two-dimensional version of the Weil equidistribution theorem) states that if $1, r, s$ are linearly independent over the rationals, then the set of points $(\{nr\}, \{ns\}$ is dense (and in fact equidistributed) in the unit square. In particular, our claim definitely holds unless $a/\alpha + b/\beta = c$ for some integers $a, b, c$.

On the other hand, suppose that such a relation does hold. Since $\alpha$ and $\beta$ are irrational, by the one-dimensional Weil theorem, the set of points $(\{-n/\alpha\}, \{-n/\beta\}$ is dense in the set of $(x, y)$ in the unit square such that $ax + by$ is an integer. It is simple enough to show that this set meets the region $\{(x, y) \in [0,1]^2 : x + y < 1\}$ unless $a + b$ is an integer, and that would imply that $1/\alpha + 1/\beta$, a quantity between 0 and 1, is an integer. We have our desired contradiction.

# The 57th William Lowell Putnam Mathematical Competition
## Saturday, December 7, 1996

A–1 Find the least number $A$ such that for any two squares of combined area 1, a rectangle of area $A$ exists such that the two squares can be packed in the rectangle (without interior overlap). You may assume that the sides of the squares are parallel to the sides of the rectangle.

A–2 Let $C_1$ and $C_2$ be circles whose centers are 10 units apart, and whose radii are 1 and 3. Find, with proof, the locus of all points $M$ for which there exists points $X$ on $C_1$ and $Y$ on $C_2$ such that $M$ is the midpoint of the line segment $XY$.

A–3 Suppose that each of 20 students has made a choice of anywhere from 0 to 6 courses from a total of 6 courses offered. Prove or disprove: there are 5 students and 2 courses such that all 5 have chosen both courses or all 5 have chosen neither course.

A–4 Let $S$ be the set of ordered triples $(a,b,c)$ of distinct elements of a finite set $A$. Suppose that

1. $(a,b,c) \in S$ if and only if $(b,c,a) \in S$;
2. $(a,b,c) \in S$ if and only if $(c,b,a) \notin S$;
3. $(a,b,c)$ and $(c,d,a)$ are both in $S$ if and only if $(b,c,d)$ and $(d,a,b)$ are both in $S$.

Prove that there exists a one-to-one function $g$ from $A$ to $R$ such that $g(a) < g(b) < g(c)$ implies $(a,b,c) \in S$. Note: $R$ is the set of real numbers.

A–5 If $p$ is a prime number greater than 3 and $k = \lfloor 2p/3 \rfloor$, prove that the sum

$$\binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{k}$$

of binomial coefficients is divisible by $p^2$.

A–6 Let $c > 0$ be a constant. Give a complete description, with proof, of the set of all continuous functions $f : R \to R$ such that $f(x) = f(x^2 + c)$ for all $x \in R$. Note that $R$ denotes the set of real numbers.

B–1 Define a **selfish** set to be a set which has its own cardinality (number of elements) as an element. Find, with proof, the number of subsets of $\{1, 2, \ldots, n\}$ which are *minimal* selfish sets, that is, selfish sets none of whose proper subsets is selfish.

B–2 Show that for every positive integer $n$,

$$\left(\frac{2n-1}{e}\right)^{\frac{2n-1}{2}} < 1 \cdot 3 \cdot 5 \cdots (2n-1) < \left(\frac{2n+1}{e}\right)^{\frac{2n+1}{2}}.$$

B–3 Given that $\{x_1, x_2, \ldots, x_n\} = \{1, 2, \ldots, n\}$, find, with proof, the largest possible value, as a function of $n$ (with $n \geq 2$), of

$$x_1x_2 + x_2x_3 + \cdots + x_{n-1}x_n + x_nx_1.$$

B–4 For any square matrix $A$, we can define $\sin A$ by the usual power series:

$$\sin A = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} A^{2n+1}.$$

Prove or disprove: there exists a $2 \times 2$ matrix $A$ with real entries such that

$$\sin A = \begin{pmatrix} 1 & 1996 \\ 0 & 1 \end{pmatrix}.$$

B–5 Given a finite string $S$ of symbols $X$ and $O$, we write $\Delta(S)$ for the number of $X$'s in $S$ minus the number of $O$'s. For example, $\Delta(XOOXOOX) = -1$. We call a string $S$ **balanced** if every substring $T$ of (consecutive symbols of) $S$ has $-2 \leq \Delta(T) \leq 2$. Thus, $XOOXOOX$ is not balanced, since it contains the substring $OOXOO$. Find, with proof, the number of balanced strings of length $n$.

B–6 Let $(a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)$ be the vertices of a convex polygon which contains the origin in its interior. Prove that there exist positive real numbers $x$ and $y$ such that

$$(a_1, b_1)x^{a_1}y^{b_1} + (a_2, b_2)x^{a_2}y^{b_2} + \cdots + (a_n, b_n)x^{a_n}y^{b_n} = (0,0).$$

# Solutions to the 57th William Lowell Putnam Mathematical Competition
# Saturday, December 7, 1996

Manjul Bhargava and Kiran Kedlaya

A–1 If $x$ and $y$ are the sides of two squares with combined area 1, then $x^2+y^2=1$. Suppose without loss of generality that $x \geq y$. Then the shorter side of a rectangle containing both squares without overlap must be at least $x$, and the longer side must be at least $x+y$. Hence the desired value of $A$ is the maximum of $x(x+y)$.

To find this maximum, we let $x = \cos\theta, y = \sin\theta$ with $\theta \in [0, \pi/4]$. Then we are to maximize

$$\begin{aligned}\cos^2\theta + \sin\theta\cos\theta &= \frac{1}{2}(1+\cos 2\theta + \sin 2\theta) \\ &= \frac{1}{2} + \frac{\sqrt{2}}{2}\cos(2\theta - \pi/4) \\ &\leq \frac{1+\sqrt{2}}{2},\end{aligned}$$

with equality for $\theta = \pi/8$. Hence this value is the desired value of $A$.

A–2 Let $O_1$ and $O_2$ be the centers of $C_1$ and $C_2$, respectively. (We are assuming $C_1$ has radius 1 and $C_2$ has radius 3.) Then the desired locus is an annulus centered at the midpoint of $O_1O_2$, with inner radius 1 and outer radius 2.

For a fixed point $Q$ on $C_2$, the locus of the midpoints of the segments $PQ$ for $P$ lying on $C_1$ is the image of $C_1$ under a homothety centered at $Q$ of radius $1/2$, which is a circle of radius $1/2$. As $Q$ varies, the center of this smaller circle traces out a circle $C_3$ of radius $3/2$ (again by homothety). By considering the two positions of $Q$ on the line of centers of the circles, one sees that $C_3$ is centered at the midpoint of $O_1O_2$, and the locus is now clearly the specified annulus.

A–3 The claim is false. There are $\binom{6}{3} = 20$ ways to choose 3 of the 6 courses; have each student choose a different set of 3 courses. Then each pair of courses is chosen by 4 students (corresponding to the four ways to complete this pair to a set of 3 courses) and is not chosen by 4 students (corresponding to the 3-element subsets of the remaining 4 courses).

Note: Assuming that no two students choose the same courses, the above counterexample is unique (up to permuting students). This may be seen as follows: Given a group of students, suppose that for any pair of courses (among the six) there are at most 4 students taking both, and at most 4 taking neither. Then there are at most $120 = (4+4)\binom{6}{2}$ pairs $(s,p)$, where $s$ is a student, and $p$ is a set of two courses of which $s$ is taking either both or none. On the other hand, if a student $s$ is taking $k$ courses, then he/she occurs in $f(k) = \binom{k}{2} + \binom{6-k}{2}$ such pairs $(s,p)$. As $f(k)$ is minimized for $k=3$, it follows that every student occurs in at least $6 = \binom{3}{2} + \binom{3}{2}$ such pairs $(s,p)$. Hence there can be at most $120/6 = 20$ students, with equality only if each student takes 3 courses, and for each set of two courses, there are exactly 4 students who take both and exactly 4 who take neither. Since there are only 4 ways to complete a given pair of courses to a set of 3, and only 4 ways to choose 3 courses not containing the given pair, the only way for there to be 20 students (under our hypotheses) is if all sets of 3 courses are in fact taken. This is the desired conclusion.

However, Robin Chapman has pointed out that the solution is not unique in the problem as stated, because a given selection of courses may be made by more than one student. One alternate solution is to identify the 6 courses with pairs of antipodal vertices of an icosahedron, and have each student pick a different face and choose the three vertices touching that face. In this example, each of 10 selections is made by a pair of students.

A–4 In fact, we will show that such a function $g$ exists with the property that $(a,b,c) \in S$ if and only if $g(d) < g(e) < g(f)$ for some cyclic permutation $(d,e,f)$ of $(a,b,c)$. We proceed by induction on the number of elements in $A$. If $A = \{a,b,c\}$ and $(a,b,c) \in S$, then choose $g$ with $g(a) < g(b) < g(c)$, otherwise choose $g$ with $g(a) > g(b) > g(c)$.

Now let $z$ be an element of $A$ and $B = A - \{z\}$. Let $a_1, \dots, a_n$ be the elements of $B$ labeled such that $g(a_1) < g(a_2) < \cdots < g(a_n)$. We claim that there exists a unique $i \in \{1, \dots, n\}$ such that $(a_i, z, a_{i+1}) \in S$, where hereafter $a_{n+k} = a_k$.

We show existence first. Suppose no such $i$ exists; then for all $i, k \in \{1, \dots, n\}$, we have $(a_{i+k}, z, a_i) \notin S$. This holds by property 1 for $k=1$ and by induction on $k$ in general, noting that

$$\begin{aligned}(a_{i+k+1}, z, a_{i+k}), &(a_{i+k}, z, a_i) \in S \\ &\Rightarrow (a_{i+k}, a_{i+k+1}, z), (z, a_i, a_{i+k}) \in S \\ &\Rightarrow (a_{i+k+1}, z, a_i) \in S.\end{aligned}$$

Applying this when $k=n$, we get $(a_{i-1}, z, a_i) \in S$, contradicting the fact that $(a_i, z, a_{i-1}) \in S$. Hence existence follows.

Now we show uniqueness. Suppose $(a_i, z, a_{i+1}) \in S$; then for any $j \neq i-1, i, i+1$, we have $(a_i, a_{i+1}, a_j), (a_j, a_{j+1}, a_i) \in S$ by the assumption on $G$.

Therefore

$$\begin{aligned}(a_i,z,a_{i+1}),(a_{i+1},a_j,a_i)\in S &\Rightarrow (a_j,a_i,z)\in S\\ (a_i,z,a_j),(a_j,a_{j+1},a_i)\in S &\Rightarrow (z,a_j,a_{j+1}),\end{aligned}$$

so $(a_j,z,a_{j+1})\notin S$. The case $j=i+1$ is ruled out by

$$(a_i,z,a_{i+1}),(a_{i+1},a_{i+2},a_i)\in S\Rightarrow (z,a_{i+1},a_{i+2})\in S$$

and the case $j=i-1$ is similar.

Finally, we put $g(z)$ in $(g(a_n),+\infty)$ if $i=n$, and $(g(a_i),g(a_{i+1}))$ otherwise; an analysis similar to that above shows that $g$ has the desired property.

A–5 (due to Lenny Ng) For $1\le n\le p-1$, $p$ divides $\binom{p}{n}$ and

$$\begin{aligned}\frac{1}{p}\binom{p}{n} &= \frac{1}{n}\frac{p-1}{1}\frac{p-2}{2}\cdots\frac{p-n+1}{n-1}\\ &\equiv \frac{(-1)^{n-1}}{n}\pmod p,\end{aligned}$$

where the congruence $x\equiv y\pmod p$ means that $x-y$ is a rational number whose numerator, in reduced form, is divisible by $p$. Hence it suffices to show that

$$\sum_{n=1}^{k}\frac{(-1)^{n-1}}{n}\equiv 0\pmod p.$$

We distinguish two cases based on $p\pmod 6$. First suppose $p=6r+1$, so that $k=4r$. Then

$$\begin{aligned}\sum_{n=1}^{4r}\frac{(-1)^{n-1}}{n} &= \sum_{n=1}^{4r}\frac{1}{n}-2\sum_{n=1}^{2r}\frac{1}{2n}\\ &= \sum_{n=1}^{2r}\left(\frac{1}{n}-\frac{1}{n}\right)+\sum_{n=2r+1}^{3r}\left(\frac{1}{n}+\frac{1}{6r+1-n}\right)\\ &= \sum_{n=2r+1}^{3r}\frac{p}{n(p-n)}\equiv 0\pmod p,\end{aligned}$$

since $p=6r+1$.

Now suppose $p=6r+5$, so that $k=4r+3$. A similar argument gives

$$\begin{aligned}\sum_{n=1}^{4r+3}\frac{(-1)^{n-1}}{n} &= \sum_{n=1}^{4r+3}\frac{1}{n}+2\sum_{n=1}^{2r+1}\frac{1}{2n}\\ &= \sum_{n=1}^{2r+1}\left(\frac{1}{n}-\frac{1}{n}\right)+\sum_{n=2r+2}^{3r+2}\left(\frac{1}{n}+\frac{1}{6r+5-n}\right)\\ &= \sum_{n=2r+2}^{3r+2}\frac{p}{n(p-n)}\equiv 0\pmod p.\end{aligned}$$

A–6 We first consider the case $c\le 1/4$; we shall show in this case $f$ must be constant. The relation

$$f(x)=f(x^2+c)=f((-x)^2+c)=f(-x)$$

proves that $f$ is an even function. Let $r_1\le r_2$ be the roots of $x^2+c-x$, both of which are real. If $x>r_2$, define $x_0=x$ and $x_{n+1}=\sqrt{x_n-c}$ for each positive integer $x$. By induction on $n$, $r_2<x_{n+1}<x_n$ for all $n$, so the sequence $\{x_n\}$ tends to a limit $L$ which is a root of $x^2+c=x$ not less than $r_2$. Of course this means $L=r_2$. Since $f(x)=f(x_n)$ for all $n$ and $x_n\to r_2$, we conclude $f(x)=f(r_2)$, so $f$ is constant on $x\ge r_2$.

If $r_1<x<r_2$ and $x_n$ is defined as before, then by induction, $x_n<x_{n+1}<r_2$. Note that the sequence can be defined because $r_1>c$; the latter follows by noting that the polynomial $x^2-x+c$ is positive at $x=c$ and has its minimum at $1/2>c$, so both roots are greater than $c$. In any case, we deduce that $f(x)$ is also constant on $r_1\le x\le r_2$.

Finally, suppose $x<r_1$. Now define $x_0=x, x_{n+1}=x_n^2+c$. Given that $x_n<r_1$, we have $x_{n+1}>x_n$. Thus if we had $x_n<r_1$ for all $n$, by the same argument as in the first case we deduce $x_n\to r_1$ and so $f(x)=f(r_1)$. Actually, this doesn't happen; eventually we have $x_n>r_1$, in which case $f(x)=f(x_n)=f(r_1)$ by what we have already shown. We conclude that $f$ is a constant function. (Thanks to Marshall Buck for catching an inaccuracy in a previous version of this solution.)

Now suppose $c>1/4$. Then the sequence $x_n$ defined by $x_0=0$ and $x_{n+1}=x_n^2+c$ is strictly increasing and has no limit point. Thus if we define $f$ on $[x_0,x_1]$ as any continuous function with equal values on the endpoints, and extend the definition from $[x_n,x_{n+1}]$ to $[x_{n+1},x_{n+2}]$ by the relation $f(x)=f(x^2+c)$, and extend the definition further to $x<0$ by the relation $f(x)=f(-x)$, the resulting function has the desired property. Moreover, any function with that property clearly has this form.

B–1 Let $[n]$ denote the set $\{1,2,\dots,n\}$, and let $f_n$ denote the number of minimal selfish subsets of $[n]$. Then the number of minimal selfish subsets of $[n]$ not containing $n$ is equal to $f_{n-1}$. On the other hand, for any minimal selfish subset of $[n]$ containing $n$, by subtracting 1 from each element, and then taking away the element $n-1$ from the set, we obtain a minimal selfish subset of $[n-2]$ (since 1 and $n$ cannot both occur in a selfish set). Conversely, any minimal selfish subset of $[n-2]$ gives rise to a minimal selfish subset of $[n]$ containing $n$ by the inverse procedure. Hence the number of minimal selfish subsets of $[n]$ containing $n$ is $f_{n-2}$. Thus we obtain $f_n=f_{n-1}+f_{n-2}$. Since $f_1=f_2=1$, we have $f_n=F_n$, where $F_n$ denotes the $n$th term of the Fibonacci sequence.

B–2 By estimating the area under the graph of $\ln x$ using upper and lower rectangles of width 2, we get

$$\begin{aligned}\int_1^{2n-1}\ln x\,dx &\le 2(\ln(3)+\cdots+\ln(2n-1))\\ &\le \int_3^{2n+1}\ln x\,dx.\end{aligned}$$

Since $\int\ln x\,dx=x\ln x-x+C$, we have, upon exponentiating and taking square roots,

$$\begin{aligned}\left(\frac{2n-1}{e}\right)^{\frac{2n-1}{2}} &< (2n-1)^{\frac{2n-1}{2}} e^{-n+1} \\ &\leq 1\cdot 3\cdots(2n-1) \\ &\leq (2n+1)^{\frac{2n+1}{2}} \frac{e^{-n+1}}{3^{3/2}} \\ &< \left(\frac{2n+1}{e}\right)^{\frac{2n+1}{2}},\end{aligned}$$

using the fact that $1 < e < 3$.

B–3 View $x_1, \dots, x_n$ as an arrangement of the numbers $1, 2, \dots, n$ on a circle. We prove that the optimal arrangement is

$$\dots, n-4, n-2, n, n-1, n-3, \dots$$

To show this, note that if $a, b$ is a pair of adjacent numbers and $c, d$ is another pair (read in the same order around the circle) with $a < d$ and $b > c$, then the segment from $b$ to $c$ can be reversed, increasing the sum by

$$ac + bd - ab - cd = (d-a)(b-c) > 0.$$

Now relabel the numbers so they appear in order as follows:

$$\dots, a_{n-4}, a_{n-2}, a_n = n, a_{n-1}, a_{n-3}, \dots$$

where without loss of generality we assume $a_{n-1} > a_{n-2}$. By considering the pairs $a_{n-2}, a_n$ and $a_{n-1}, a_{n-3}$ and using the trivial fact $a_n > a_{n-1}$, we deduce $a_{n-2} > a_{n-3}$. We then compare the pairs $a_{n-4}, a_{n-2}$ and $a_{n-1}, a_{n-3}$, and using that $a_{n-1} > a_{n-2}$, we deduce $a_{n-3} > a_{n-4}$. Continuing in this fashion, we prove that $a_n > a_{n-1} > \cdots > a_1$ and so $a_k = k$ for $k = 1, 2, \dots, n$, i.e. that the optimal arrangement is as claimed. In particular, the maximum value of the sum is

$$\begin{aligned}1\cdot 2 + (n-1)\cdot n + 1\cdot 3 + 2\cdot 4 + \cdots + (n-2)\cdot n \\ &= 2 + n^2 - n + (1^2-1) + \cdots + [(n-1)^2 - 1] \\ &= n^2 - n + 2 - (n-1) + \frac{(n-1)n(2n-1)}{6} \\ &= \frac{2n^3 + 3n^2 - 11n + 18}{6}.\end{aligned}$$

Alternate solution: We prove by induction that the value given above is an upper bound; it is clearly a lower bound because of the arrangement given above. Assume this is the case for $n-1$. The optimal arrangement for $n$ is obtained from some arrangement for $n-1$ by inserting $n$ between some pair $x, y$ of adjacent terms. This operation increases the sum by $nx + ny - xy = n^2 - (n-x)(n-y)$, which is an increasing function of both $x$ and $y$. In particular, this difference is maximal when $x$ and $y$ equal $n-1$ and $n-2$. Fortunately, this yields precisely the difference between the claimed upper bound for $n$ and the assumed upper bound for $n-1$, completing the induction.

B–4 Suppose such a matrix $A$ exists. If the eigenvalues of $A$ (over the complex numbers) are distinct, then there exists a complex matrix $C$ such that $B = CAC^{-1}$ is diagonal. Consequently, $\sin B$ is diagonal. But then $\sin A = C^{-1}(\sin B)C$ must be diagonalizable, a contradiction. Hence the eigenvalues of $A$ are the same, and $A$ has a conjugate $B = CAC^{-1}$ over the complex numbers of the form

$$\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}.$$

A direct computation shows that

$$\sin B = \begin{pmatrix} \sin x & y\cdot\cos x \\ 0 & \sin x \end{pmatrix}.$$

Since $\sin A$ and $\sin B$ are conjugate, their eigenvalues must be the same, and so we must have $\sin x = 1$. This implies $\cos x = 0$, so that $\sin B$ is the identity matrix, as must be $\sin A$, a contradiction. Thus $A$ cannot exist.

Alternate solution (due to Craig Helfgott and Alex Popa): Define both $\sin A$ and $\cos A$ by the usual power series. Since $A$ commutes with itself, the power series identity

$$\sin^2 A + \cos^2 A = I$$

holds. But if $\sin A$ is the given matrix, then by the above identity, $\cos^2 A$ must equal $\begin{pmatrix} 0 & -2\cdot 1996 \\ 0 & 0 \end{pmatrix}$ which is a nilpotent matrix. Thus $\cos A$ is also nilpotent. However, the square of any $2\times 2$ nilpotent matrix must be zero (e.g., by the Cayley-Hamilton theorem). This is a contradiction.

B–5 Consider a $1\times n$ checkerboard, in which we write an $n$-letter string, one letter per square. If the string is balanced, we can cover each pair of adjacent squares containing the same letter with a $1\times 2$ domino, and these will not overlap (because no three in a row can be the same). Moreover, any domino is separated from the next by an even number of squares, since they must cover opposite letters, and the sequence must alternate in between.

Conversely, any arrangement of dominoes where adjacent dominoes are separated by an even number of squares corresponds to a unique balanced string, once we choose whether the string starts with $X$ or $O$. In other words, the number of balanced strings is twice the number of acceptable domino arrangements.

We count these arrangements by numbering the squares $0, 1, \dots, n-1$ and distinguishing whether the dominoes start on even or odd numbers. Once this is decided, one simply chooses whether or not to put a domino in each eligible position. Thus we have $2^{\lfloor n/2 \rfloor}$ arrangements in the first case and $2^{\lfloor (n-1)/2 \rfloor}$ in the second, but note that the case of no dominoes has been counted twice. Hence the number of balanced strings is

$$2^{\lfloor (n+2)/2 \rfloor} + 2^{\lfloor (n+1)/2 \rfloor} - 2.$$

B–6 We will prove the claim assuming only that the convex hull of the points $(a_i, b_i)$ contains the origin in its interior. (Thanks to Marshall Buck for pointing out that the last three words are necessary in the previous sentence!) Let $u = \log x, v = \log y$ so that the left-hand side of the given equation is

$$(a_1, b_1) \exp(a_1 u + b_1 v) + (a_2, b_2) \exp(a_2 u + b_2 v) + \cdots + (a_n, b_n) \exp(a_n u + b_n v). \quad (1)$$

Now note that (1) is the gradient of the function

$$f(u, v) = exp(a_1 u + b_1 v) + exp(a_2 u + b_2 v) + \cdots + exp(a_n u + b_n v),$$

and so it suffices to show $f$ has a critical point. We will in fact show $f$ has a global minimum.

Clearly we have

$$f(u, v) \geq \exp\left(\max_i (a_i u + b_i v)\right).$$

Note that this maximum is positive for $(u, v) \neq (0, 0)$: if we had $a_i u + b_i v < 0$ for all $i$, then the subset $ur + vs < 0$ of the $rs$-plane would be a half-plane containing all of the points $(a_i, b_i)$, whose convex hull would then not contain the origin, a contradiction.

The function $\max_i (a_i u + b_i v)$ is clearly continuous on the unit circle $u^2 + v^2 = 1$, which is compact. Hence it has a global minimum $M > 0$, and so for all $u, v$,

$$\max_i (a_i u + b_i v) \geq M \sqrt{u^2 + v^2}.$$

In particular, $f \geq n + 1$ on the disk of radius $\sqrt{(n+1)/M}$. Since $f(0, 0) = n$, the infimum of $f$ is the same over the entire $uv$-plane as over this disk, which again is compact. Hence $f$ attains its infimal value at some point in the disk, which is the desired global minimum.

Noam Elkies has suggested an alternate solution as follows: for $r > 0$, draw the loop traced by (1) as $(u, v)$ travels counterclockwise around the circle $u^2 + v^2 = r^2$. For $r = 0$, this of course has winding number 0 about any point, but for $r$ large, one can show this loop has winding number 1 about the origin, so somewhere in between the loop must pass through the origin. (Proving this latter fact is a little tricky.)

# The 58th William Lowell Putnam Mathematical Competition
# Saturday, December 6, 1997

A–1 A rectangle, $HOMF$, has sides $HO = 11$ and $OM = 5$. A triangle $ABC$ has $H$ as the intersection of the altitudes, $O$ the center of the circumscribed circle, $M$ the midpoint of $BC$, and $F$ the foot of the altitude from $A$. What is the length of $BC$?

A–2 Players $1, 2, 3, \dots, n$ are seated around a table, and each has a single penny. Player 1 passes a penny to player 2, who then passes two pennies to player 3. Player 3 then passes one penny to Player 4, who passes two pennies to Player 5, and so on, players alternately passing one penny or two to the next player who still has some pennies. A player who runs out of pennies drops out of the game and leaves the table. Find an infinite set of numbers $n$ for which some player ends up with all $n$ pennies.

A–3 Evaluate

$$\int_0^\infty \left( x - \frac{x^3}{2} + \frac{x^5}{2\cdot 4} - \frac{x^7}{2\cdot 4\cdot 6} + \cdots \right) \left( 1 + \frac{x^2}{2^2} + \frac{x^4}{2^2\cdot 4^2} + \frac{x^6}{2^2\cdot 4^2\cdot 6^2} + \cdots \right) dx.$$

A–4 Let $G$ be a group with identity $e$ and $\phi : G \to G$ a function such that

$$\phi(g_1)\phi(g_2)\phi(g_3) = \phi(h_1)\phi(h_2)\phi(h_3)$$

whenever $g_1 g_2 g_3 = e = h_1 h_2 h_3$. Prove that there exists an element $a \in G$ such that $\psi(x) = a\phi(x)$ is a homomorphism (i.e. $\psi(xy) = \psi(x)\psi(y)$ for all $x, y \in G$).

A–5 Let $N_n$ denote the number of ordered $n$-tuples of positive integers $(a_1, a_2, \dots, a_n)$ such that $1/a_1 + 1/a_2 + \dots + 1/a_n = 1$. Determine whether $N_{10}$ is even or odd.

A–6 For a positive integer $n$ and any real number $c$, define $x_k$ recursively by $x_0 = 0$, $x_1 = 1$, and for $k \geq 0$,

$$x_{k+2} = \frac{c x_{k+1} - (n-k) x_k}{k+1}.$$

Fix $n$ and then take $c$ to be the largest value for which $x_{n+1} = 0$. Find $x_k$ in terms of $n$ and $k$, $1 \leq k \leq n$.

B–1 Let $\{x\}$ denote the distance between the real number $x$ and the nearest integer. For each positive integer $n$, evaluate

$$F_n = \sum_{m=1}^{6n-1} \min\left(\left\{\frac{m}{6n}\right\}, \left\{\frac{m}{3n}\right\}\right).$$

(Here $\min(a,b)$ denotes the minimum of $a$ and $b$.)

B–2 Let $f$ be a twice-differentiable real-valued function satisfying

$$f(x) + f''(x) = -x g(x) f'(x),$$

where $g(x) \geq 0$ for all real $x$. Prove that $|f(x)|$ is bounded.

B–3 For each positive integer $n$, write the sum $\sum_{m=1}^{n} 1/m$ in the form $p_n/q_n$, where $p_n$ and $q_n$ are relatively prime positive integers. Determine all $n$ such that 5 does not divide $q_n$.

B–4 Let $a_{m,n}$ denote the coefficient of $x^n$ in the expansion of $(1 + x + x^2)^m$. Prove that for all [integers] $k \geq 0$,

$$0 \leq \sum_{i=0}^{\lfloor \frac{2k}{3} \rfloor} (-1)^i a_{k-i,i} \leq 1.$$

B–5 Prove that for $n \geq 2$,

$$\overbrace{2^{2^{\cdots^{2}}}}^{n \text{ terms}} \equiv \overbrace{2^{2^{\cdots^{2}}}}^{n-1 \text{ terms}} \pmod{n}.$$

B–6 The dissection of the 3–4–5 triangle shown below (into four congruent right triangles similar to the original) has diameter $5/2$. Find the least diameter of a dissection of this triangle into four parts. (The diameter of a dissection is the least upper bound of the distances between pairs of points belonging to the same part.)

# Solutions to the 58th William Lowell Putnam Mathematical Competition
# Saturday, December 6, 1997

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A–1 The centroid $G$ of the triangle is collinear with $H$ and $O$ (Euler line), and the centroid lies two-thirds of the way from $A$ to $M$. Therefore $H$ is also two-thirds of the way from $A$ to $F$, so $AF = 15$. Since the triangles $BFH$ and $AFC$ are similar (they're right triangles and

$$\angle HBC = \pi/2 - \angle C = \angle CAF),$$

we have

$$BF/FH = AF/FC$$

or

$$BF \cdot FC = FH \cdot AF = 75.$$

Now

$$BC^2 = (BF+FC)^2 = (BF-FC)^2 + 4BF \cdot FC,$$

but

$$BF - FC = BM + MF - (MC - MF) = 2MF = 22,$$

so

$$BC = \sqrt{22^2 + 4 \cdot 75} = \sqrt{784} = 28.$$

A–2 We show more precisely that the game terminates with one player holding all of the pennies if and only if $n = 2^m + 1$ or $n = 2^m + 2$ for some $m$. First suppose we are in the following situation for some $k \geq 2$. (Note: for us, a "move" consists of two turns, starting with a one-penny pass.)

- Except for the player to move, each player has $k$ pennies;
- The player to move has at least $k$ pennies.

We claim then that the game terminates if and only if the number of players is a power of 2. First suppose the number of players is even; then after $m$ complete rounds, every other player, starting with the player who moved first, will have $m$ more pennies than initially, and the others will all have 0. Thus we are reduced to the situation with half as many players; by this process, we eventually reduce to the case where the number of players is odd. However, if there is more than one player, after two complete rounds everyone has as many pennies as they did before (here we need $m \geq 2$), so the game fails to terminate. This verifies the claim.

Returning to the original game, note that after one complete round, $\lfloor \frac{n-1}{2} \rfloor$ players remain, each with 2 pennies except for the player to move, who has either 3 or 4 pennies. Thus by the above argument, the game terminates if and only if $\lfloor \frac{n-1}{2} \rfloor$ is a power of 2, that is, if and only if $n = 2^m + 1$ or $n = 2^m + 2$ for some $m$.

A–3 Note that the series on the left is simply $x \exp(-x^2/2)$. By integration by parts,

$$\int_0^\infty x^{2n+1} e^{-x^2/2} dx = 2n \int_0^\infty x^{2n-1} e^{-x^2/2} dx$$

and so by induction,

$$\int_0^\infty x^{2n+1} e^{-x^2/2} dx = 2 \times 4 \times \cdots \times 2n.$$

Thus the desired integral is simply

$$\sum_{n=0}^\infty \frac{1}{2^n n!} = \sqrt{e}.$$

A–4 In order to have $\psi(x) = a\phi(x)$ for all $x$, we must in particular have this for $x = e$, and so we take $a = \phi(e)^{-1}$. We first note that

$$\phi(g)\phi(e)\phi(g^{-1}) = \phi(e)\phi(g)\phi(g^{-1})$$

and so $\phi(g)$ commutes with $\phi(e)$ for all $g$. Next, we note that

$$\phi(x)\phi(y)\phi(y^{-1}x^{-1}) = \phi(e)\phi(xy)\phi(y^{-1}x^{-1})$$

and using the commutativity of $\phi(e)$, we deduce

$$\phi(e)^{-1}\phi(x)\phi(e)^{-1}\phi(y) = \phi(e)^{-1}\phi(xy)$$

or $\psi(xy) = \psi(x)\psi(y)$, as desired.

A–5 We may discard any solutions for which $a_1 \neq a_2$, since those come in pairs; so assume $a_1 = a_2$. Similarly, we may assume that $a_3 = a_4$, $a_5 = a_6$, $a_7 = a_8$, $a_9 = a_{10}$. Thus we get the equation

$$2/a_1 + 2/a_3 + 2/a_5 + 2/a_7 + 2/a_9 = 1.$$

Again, we may assume $a_1 = a_3$ and $a_5 = a_7$, so we get $4/a_1 + 4/a_5 + 2/a_9 = 1$; and $a_1 = a_5$, so $8/a_1 + 2/a_9 = 1$. This implies that $(a_1 - 8)(a_9 - 2) = 16$, which by counting has 5 solutions. Thus $N_{10}$ is odd.

A–6 Clearly $x_{n+1}$ is a polynomial in $c$ of degree $n$, so it suffices to identify $n$ values of $c$ for which $x_{n+1} = 0$. We claim these are $c = n-1-2r$ for $r = 0, 1, \ldots, n-1$; in this case, $x_k$ is the coefficient of $t^{k-1}$ in the polynomial $f(t) = (1-t)^r(1+t)^{n-1-r}$. This can be verified by noticing that $f$ satisfies the differential equation

$$\frac{f'(t)}{f(t)} = \frac{n-1-r}{1+t} - \frac{r}{1-t}$$

(by logarithmic differentiation) or equivalently,

$$\begin{aligned}(1-t^2)f'(t) &= f(t)[(n-1-r)(1-t)-r(1+t)] \\ &= f(t)[(n-1-2r)-(n-1)t]\end{aligned}$$

and then taking the coefficient of $t^k$ on both sides:

$$\begin{gathered}(k+1)x_{k+2}-(k-1)x_k = \\ (n-1-2r)x_{k+1}-(n-1)x_k.\end{gathered}$$

In particular, the largest such $c$ is $n-1$, and $x_k = \binom{n-1}{k-1}$ for $k=1,2,\dots,n$.

Greg Kuperberg has suggested an alternate approach to show directly that $c=n-1$ is the largest root, without computing the others. Note that the condition $x_{n+1}=0$ states that $(x_1,\dots,x_n)$ is an eigenvector of the matrix

$$A_{ij} = \begin{cases} i & j=i+1 \\ n-j & j=i-1 \\ 0 & \text{otherwise} \end{cases}$$

with eigenvalue $c$. By the Perron-Frobenius theorem, $A$ has a unique eigenvector with positive entries, whose eigenvalue has modulus greater than or equal to that of any other eigenvalue, which proves the claim.

B–1 It is trivial to check that $\frac{m}{6n} = \{\frac{m}{6n}\} \leq \{\frac{m}{3n}\}$ for $1 \leq m \leq 2n$, that $1-\frac{m}{3n} = \{\frac{m}{3n}\} \leq \{\frac{m}{6n}\}$ for $2n \leq m \leq 3n$, that $\frac{m}{3n}-1 = \{\frac{m}{3n}\} \leq \{\frac{m}{6n}\}$ for $3n \leq m \leq 4n$, and that $1-\frac{m}{6n} = \{\frac{m}{6n}\} \leq \{\frac{m}{3n}\}$ for $4n \leq m \leq 6n$. Therefore the desired sum is

$$\begin{aligned}&\sum_{m=1}^{2n-1}\frac{m}{6n} + \sum_{m=2n}^{3n-1}\left(1-\frac{m}{3n}\right) \\ &+ \sum_{m=3n}^{4n-1}\left(\frac{m}{3n}-1\right) + \sum_{m=4n}^{6n-1}\left(1-\frac{m}{6n}\right) = n.\end{aligned}$$

B–2 It suffices to show that $|f(x)|$ is bounded for $x \geq 0$, since $f(-x)$ satisfies the same equation as $f(x)$. But then

$$\begin{aligned}\frac{d}{dx}\left((f(x))^2+(f'(x))^2\right) &= 2f'(x)(f(x)+f''(x)) \\ &= -2xg(x)(f'(x))^2 \leq 0,\end{aligned}$$

so that $(f(x))^2 \leq (f(0))^2+(f'(0))^2$ for $x \geq 0$.

B–3 The only such $n$ are the numbers 1–4, 20–24, 100–104, and 120–124. For the proof let

$$H_n = \sum_{m=1}^{n}\frac{1}{m}$$

and introduce the auxiliary function

$$I_n = \sum_{1\leq m\leq n, (m,5)=1}\frac{1}{m}.$$

It is immediate (e.g., by induction) that $I_n \equiv 1,-1,1,0,0 \pmod 5$ for $n \equiv 1,2,3,4,5 \pmod 5$ respectively, and moreover, we have the equality

$$H_n = \sum_{m=0}^{k}\frac{1}{5^m}I_{\lfloor n/5^m\rfloor},$$

where $k=k(n)$ denotes the largest integer such that $5^k \leq n$. We wish to determine those $n$ such that the above sum has nonnegative 5–valuation. (By the 5–valuation of a number $a$ we mean the largest integer $v$ such that $a/5^v$ is an integer.)

If $\lfloor n/5^k\rfloor \leq 3$, then the last term in the above sum has 5–valuation $-k$, since $I_1$, $I_2$, $I_3$ each have valuation 0; on the other hand, all other terms must have 5–valuation strictly larger than $-k$. It follows that $H_n$ has 5–valuation exactly $-k$; in particular, $H_n$ has nonnegative 5–valuation in this case if and only if $k=0$, i.e., $n=1$, 2, or 3.

Suppose now that $\lfloor n/5^k\rfloor = 4$. Then we must also have $20 \leq \lfloor n/5^{k-1}\rfloor \leq 24$. The former condition implies that the last term of the above sum is $I_4/5^k = 1/(12\cdot 5^{k-2})$, which has 5–valuation $-(k-2)$.

It is clear that $I_{20} \equiv I_{24} \equiv 0 \pmod{25}$; hence if $\lfloor n/5^{k-1}\rfloor$ equals 20 or 24, then the second–to–last term of the above sum (if it exists) has valuation at least $-(k-3)$. The third–to–last term (if it exists) is of the form $I_r/5^{k-2}$, so that the sum of the last term and the third to last term takes the form $(I_r+1/12)/5^{k-2}$. Since $I_r$ can be congruent only to 0,1, or -1 (mod 5), and $1/12 \equiv 3 \pmod 5$, we conclude that the sum of the last term and third–to–last term has valuation $-(k-2)$, while all other terms have valuation strictly higher. Hence $H_n$ has nonnegative 5–valuation in this case only when $k \leq 2$, leading to the values $n=4$ (arising from $k=0$), 20,24 (arising from $k=1$ and $\lfloor n/5^{k-1}\rfloor = 20$ and 24 resp.), 101, 102, 103, and 104 (arising from $k=2$, $\lfloor n/5^{k-1}\rfloor = 20$) and 120, 121, 122, 123, and 124 (arising from $k=2$, $\lfloor n/5^{k-1}\rfloor = 24$).

Finally, suppose $\lfloor n/5^k\rfloor = 4$ and $\lfloor n/5^{k-1}\rfloor = 21$, 22, or 23. Then as before, the first condition implies that the last term of the sum in (*) has valuation $-(k-2)$, while the second condition implies that the second–to–last term in the same sum has valuation $-(k-1)$. Hence all terms in the sum (*) have 5–valuation strictly higher than $-(k-1)$, except for the second–to–last term, and therefore $H_n$ has 5–valuation $-(k-1)$ in this case. In particular, $H_n$ is integral (mod 5) in this case if and only if $k \leq 1$, which gives the additional values $n=21$, 22, and 23.

B–4 Let $s_k = \sum_i (-1)^i a_{k-1,i}$ be the given sum (note that $a_{k-1,i}$ is nonzero precisely for $i=0,\dots,\lfloor\frac{2k}{3}\rfloor$). Since

$$a_{m+1,n} = a_{m,n}+a_{m,n-1}+a_{m,n-2},$$

we have

$$\begin{aligned} s_k - s_{k-1} + s_{k+2} &= \sum_i (-1)^i (a_{n-i,i} + a_{n-i,i+1} + a_{n-i,i+2}) \\ &= \sum_i (-1)^i a_{n-i+1,i+2} = s_{k+3}. \end{aligned}$$

By computing $s_0 = 1, s_1 = 1, s_2 = 0$, we may easily verify by induction that $s_{4j} = s_{4j+1} = 1$ and $s_{4j+2} = s_{4j+3} = 0$ for all $j \geq 0$. (Alternate solution suggested by John Rickert: write $S(x,y) = \sum_{i=0}^{\infty}(y + xy^2 + x^2y^3)^i$, and note note that $s_k$ is the coefficient of $y^k$ in $S(-1,y) = (1+y)/(1-y^4)$.)

B–5 Define the sequence $x_1 = 2$, $x_n = 2^{x_{n-1}}$ for $n > 1$. It suffices to show that for every $n$, $x_m \equiv x_{m+1} \equiv \cdots \pmod n$ for some $m < n$. We do this by induction on $n$, with $n = 2$ being obvious.

Write $n = 2^a b$, where $b$ is odd. It suffices to show that $x_m \equiv \cdots$ modulo $2^a$ and modulo $b$, for some $m < n$. For the former, we only need $x_{n-1} \geq a$, but clearly $x_{n-1} \geq n$ by induction on $n$. For the latter, note that $x_m \equiv x_{m+1} \equiv \cdots \pmod b$ as long as $x_{m-1} \equiv x_m \equiv \cdots \pmod{\phi(b)}$, where $\phi(n)$ is the Euler totient function. By hypothesis, this occurs for some $m < \phi(b) + 1 \leq n$. (Thanks to Anoop Kulkarni for catching a lethal typo in an earlier version.)

B–6 The answer is $25/13$. Place the triangle on the cartesian plane so that its vertices are at $C = (0,0), A = (0,3), B = (4,0)$. Define also the points $D = (20/13, 24/13)$, and $E = (27/13, 0)$. We then compute that

$$\begin{aligned} \frac{25}{13} &= AD = BE = DE \\ \frac{27}{13} &= BC - CE = BE < BC \\ \frac{39}{13} &= AC < \sqrt{AC^2 + CE^2} = AE \\ \frac{40}{13} &= AB - AD = BD < AB \end{aligned}$$

and that $AD < CD$. In any dissection of the triangle into four parts, some two of $A,B,C,D,E$ must belong to the same part, forcing the least diameter to be at least $25/13$.

We now exhibit a dissection with least diameter $25/13$. (Some variations of this dissection are possible.) Put $F = (15/13, 19/13)$, $G = (15/13, 0)$, $H = (0, 19/13)$, $J = (32/15, 15/13)$, and divide $ABC$ into the convex polygonal regions $ADFH$, $BEJ$, $CGFH$, $DFGEJ$. To check that this dissection has least diameter $25/13$, it suffices (by the following remark) to check that the distances

$$\begin{gathered} AD, AF, AH, BE, BJ, DE, CF, CG, CH, \\ DF, DG, DH, DJ, EF, EG, EJ, FG, FH, FJ, GJ \end{gathered}$$

are all at most $25/13$. This can be checked by a long numerical calculation, which we omit in favor of some shortcuts: note that $ADFH$ and $BEJ$ are contained in circular sectors centered at $A$ and $B$, respectively, of radius $25/13$ and angle less than $\pi/3$, while $CGFH$ is a rectangle with diameter $CF < 25/13$.

**Remark.** The preceding argument uses implicitly the fact that for $P$ a simple closed polygon in the plane, if we let $S$ denote the set of points on or within $P$, then the maximum distance between two points of $S$ occurs between some pair of vertices of $P$. This is an immediate consequence of the compactness of $S$ (which guarantees the existence of a maximum) and the convexity of the function taking $(x,y) \in S \times S$ to the squared distance between $x$ and $y$ (which is obvious in terms of Cartesian coordinates).

# The 59th William Lowell Putnam Mathematical Competition
## Saturday, December 5, 1998

A–1 A right circular cone has base of radius 1 and height 3. A cube is inscribed in the cone so that one face of the cube is contained in the base of the cone. What is the side-length of the cube?

A–2 Let $s$ be any arc of the unit circle lying entirely in the first quadrant. Let $A$ be the area of the region lying below $s$ and above the $x$-axis and let $B$ be the area of the region lying to the right of the $y$-axis and to the left of $s$. Prove that $A+B$ depends only on the arc length, and not on the position, of $s$.

A–3 Let $f$ be a real function on the real line with continuous third derivative. Prove that there exists a point $a$ such that

$$f(a)\cdot f'(a)\cdot f''(a)\cdot f'''(a)\geq 0.$$

A–4 Let $A_1=0$ and $A_2=1$. For $n>2$, the number $A_n$ is defined by concatenating the decimal expansions of $A_{n-1}$ and $A_{n-2}$ from left to right. For example $A_3=A_2A_1=10, A_4=A_3A_2=101, A_5=A_4A_3=10110$, and so forth. Determine all $n$ such that 11 divides $A_n$.

A–5 Let $\mathscr{F}$ be a finite collection of open discs in $\mathbb{R}^2$ whose union contains a set $E\subseteq\mathbb{R}^2$. Show that there is a pairwise disjoint subcollection $D_1,\ldots,D_n$ in $\mathscr{F}$ such that

$$E\subseteq\cup_{j=1}^n 3D_j.$$

Here, if $D$ is the disc of radius $r$ and center $P$, then $3D$ is the disc of radius $3r$ and center $P$.

A–6 Let $A,B,C$ denote distinct points with integer coordinates in $\mathbb{R}^2$. Prove that if

$$(|AB|+|BC|)^2<8\cdot[ABC]+1$$

then $A,B,C$ are three vertices of a square. Here $|XY|$ is the length of segment $XY$ and $[ABC]$ is the area of triangle $ABC$.

B–1 Find the minimum value of

$$\frac{(x+1/x)^6-(x^6+1/x^6)-2}{(x+1/x)^3+(x^3+1/x^3)}$$

for $x>0$.

B–2 Given a point $(a,b)$ with $0<b<a$, determine the minimum perimeter of a triangle with one vertex at $(a,b)$, one on the $x$-axis, and one on the line $y=x$. You may assume that a triangle of minimum perimeter exists.

B–3 let $H$ be the unit hemisphere $\{(x,y,z):x^2+y^2+z^2=1,z\geq 0\}$, $C$ the unit circle $\{(x,y,0):x^2+y^2=1\}$, and $P$ the regular pentagon inscribed in $C$. Determine the surface area of that portion of $H$ lying over the planar region inside $P$, and write your answer in the form $A\sin\alpha+B\cos\beta$, where $A,B,\alpha,\beta$ are real numbers.

B–4 Find necessary and sufficient conditions on positive integers $m$ and $n$ so that

$$\sum_{i=0}^{mn-1}(-1)^{\lfloor i/m\rfloor+\lfloor i/n\rfloor}=0.$$

B–5 Let $N$ be the positive integer with 1998 decimal digits, all of them 1; that is,

$$N=1111\cdots 11.$$

Find the thousandth digit after the decimal point of $\sqrt{N}$.

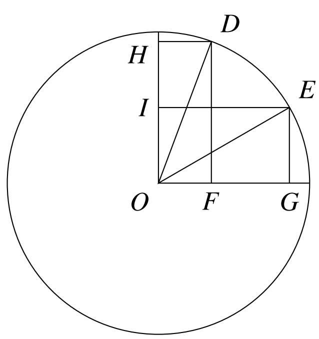
B–6 Prove that, for any integers $a,b,c$, there exists a positive integer $n$ such that $\sqrt{n^3+an^2+bn+c}$ is not an integer.

# Solutions to the 59th William Lowell Putnam Mathematical Competition
# Saturday, December 5, 1998

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A–1 Consider the plane containing both the axis of the cone and two opposite vertices of the cube's bottom face. The cross section of the cone and the cube in this plane consists of a rectangle of sides $s$ and $s\sqrt{2}$ inscribed in an isosceles triangle of base 2 and height 3, where $s$ is the side-length of the cube. (The $s\sqrt{2}$ side of the rectangle lies on the base of the triangle.) Similar triangles yield $s/3 = (1 - s\sqrt{2}/2)/1$, or $s = (9\sqrt{2} - 6)/7$.

A–2 First solution: to fix notation, let $A$ be the area of region $DEFG$, and $B$ be the area of $DEIH$; further let $C$ denote the area of sector $ODE$, which only depends on the arc length of $s$. If $[XYZ]$ denotes the area of triangle $[XYZ]$, then we have $A = C + [OEG] - [ODF]$ and $B = C + [ODH] - [OEI]$. But clearly $[OEG] = [OEI]$ and $[ODF] = [ODH]$, and so $A + B = 2C$.




Second solution: We may parametrize a point in $s$ by any of $x$, $y$, or $\theta = \tan^{-1}(y/x)$. Then $A$ and $B$ are just the integrals of $y\,dx$ and $x\,dy$ over the appropriate intervals; thus $A + B$ is the integral of $x\,dy - y\,dx$ (minus because the limits of integration are reversed). But $d\theta = x\,dy - y\,dx$, and so $A + B = \Delta\theta$ is precisely the radian measure of $s$. (Of course, one can perfectly well do this problem by computing the two integrals separately. But what's the fun in that?)

A–3 If at least one of $f(a)$, $f'(a)$, $f''(a)$, or $f'''(a)$ vanishes at some point $a$, then we are done. Hence we may assume each of $f(x)$, $f'(x)$, $f''(x)$, and $f'''(x)$ is either strictly positive or strictly negative on the real line. By replacing $f(x)$ by $-f(x)$ if necessary, we may assume $f''(x) > 0$; by replacing $f(x)$ by $f(-x)$ if necessary, we may assume $f'''(x) > 0$. (Notice that these substitutions do not change the sign of $f(x)f'(x)f''(x)f'''(x)$.) Now $f''(x) > 0$ implies that $f'(x)$ is increasing, and $f'''(x) > 0$ implies that $f'(x)$ is convex, so that $f'(x + a) > f'(x) + af''(x)$ for all $x$ and $a$. By letting $a$ increase in the latter inequality, we see that $f'(x + a)$ must be positive for sufficiently large $a$; it follows that $f'(x) > 0$ for all $x$. Similarly, $f'(x) > 0$ and $f''(x) > 0$ imply that $f(x) > 0$ for all $x$. Therefore $f(x)f'(x)f''(x)f'''(x) > 0$ for all $x$, and we are done.

A–4 The number of digits in the decimal expansion of $A_n$ is the Fibonacci number $F_n$, where $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n > 2$. It follows that the sequence $\{A_n\}$, modulo 11, satisfies the recursion $A_n = (-1)^{F_{n-2}} A_{n-1} + A_{n-2}$. (Notice that the recursion for $A_n$ depends only on the value of $F_{n-2}$ modulo 2.) Using these recursions, we find that $A_7 \equiv 0$ and $A_8 \equiv 1$ modulo 11, and that $F_7 \equiv 1$ and $F_8 \equiv 1$ modulo 2. It follows that $A_n \equiv A_{n+6} \pmod{11}$ for all $n \geq 1$. We find that among $A_1, A_2, A_3, A_4, A_5$, and $A_6$, only $A_1$ vanishes modulo 11. Thus 11 divides $A_n$ if and only if $n = 6k + 1$ for some nonnegative integer $k$.

A–5 Define the sequence $D_i$ by the following greedy algorithm: let $D_1$ be the disc of largest radius (breaking ties arbitrarily), let $D_2$ be the disc of largest radius not meeting $D_1$, let $D_3$ be the disc of largest radius not meeting $D_1$ or $D_2$, and so on, up to some final disc $D_n$. To see that $E \subseteq \cup_{j=1}^{n} 3D_j$, consider a point in $E$; if it lies in one of the $D_i$, we are done. Otherwise, it lies in a disc $D$ of radius $r$, which meets one of the $D_i$ having radius $s \geq r$ (this is the only reason a disc can be skipped in our algorithm). Thus the centers lie at a distance $t < s + r$, and so every point at distance less than $r$ from the center of $D$ lies at distance at most $r + t < 3s$ from the center of the corresponding $D_i$.

A–6 Recall the inequalities $|AB|^2 + |BC|^2 \geq 2|AB||BC|$ (AM-GM) and $|AB||BC| \geq 2[ABC]$ (Law of Sines). Also recall that the area of a triangle with integer coordinates is half an integer (if its vertices lie at $(0,0), (p,q), (r,s)$, the area is $|ps - qr|/2$), and that if $A$ and $B$ have integer coordinates, then $|AB|^2$ is an integer (Pythagoras). Now observe that

$$\begin{aligned} 8[ABC] &\leq |AB|^2 + |BC|^2 + 4[ABC] \\ &\leq |AB|^2 + |BC|^2 + 2|AB||BC| \\ &< 8[ABC] + 1, \end{aligned}$$

and that the first and second expressions are both integers. We conclude that $8[ABC] = |AB|^2 + |BC|^2 + 4[ABC]$, and so $|AB|^2 + |BC|^2 = 2|AB||BC| = 4[ABC]$; that is, $B$ is a right angle and $AB = BC$, as desired.

B–1 Notice that

$$\frac{(x + 1/x)^6 - (x^6 + 1/x^6) - 2}{(x + 1/x)^3 + (x^3 + 1/x^3)} =$$
$$(x + 1/x)^3 - (x^3 + 1/x^3) = 3(x + 1/x)$$

(difference of squares). The latter is easily seen (e.g., by AM-GM) to have minimum value 6 (achieved at $x=1$).

B–2 Consider a triangle as described by the problem; label its vertices $A,B,C$ so that $A=(a,b)$, $B$ lies on the $x$-axis, and $C$ lies on the line $y=x$. Further let $D=(a,-b)$ be the reflection of $A$ in the $x$-axis, and let $E=(b,a)$ be the reflection of $A$ in the line $y=x$. Then $AB=DB$ and $AC=CE$, and so the perimeter of $ABC$ is $DB+BC+CE\geq DE=\sqrt{(a-b)^2+(a+b)^2}=\sqrt{2a^2+2b^2}$. It is clear that this lower bound can be achieved; just set $B$ (resp. $C$) to be the intersection between the segment $DE$ and the $x$-axis (resp. line $x=y$); thus the minimum perimeter is in fact $\sqrt{2a^2+2b^2}$.

B–3 We use the well-known result that the surface area of the "sphere cap" $\{(x,y,z)\,|\,x^2+y^2+z^2=1, z\geq z_0\}$ is simply $2\pi(1-z_0)$. (This result is easily verified using calculus; we omit the derivation here.) Now the desired surface area is just $2\pi$ minus the surface areas of five identical halves of sphere caps; these caps, up to isometry, correspond to $z_0$ being the distance from the center of the pentagon to any of its sides, i.e., $z_0=\cos\frac{\pi}{5}$. Thus the desired area is $2\pi-\frac{5}{2}\left(2\pi(1-\cos\frac{\pi}{5})\right)=5\pi\cos\frac{\pi}{5}-3\pi$ (i.e., $B=\pi/2$).

B–4 For convenience, define $f_{m,n}(i)=\lfloor\frac{i}{m}\rfloor+\lfloor\frac{i}{n}\rfloor$, so that the given sum is $S(m,n)=\sum_{i=0}^{mn-1}(-1)^{f_{m,n}(i)}$. If $m$ and $n$ are both odd, then $S(m,n)$ is the sum of an odd number of $\pm1$'s, and thus cannot be zero. Now consider the case where $m$ and $n$ have opposite parity. Note that $\lfloor\frac{i}{m}\rfloor+\lfloor k-\frac{i+1}{m}\rfloor=k-1$ for all integers $i,k,m$. Thus $\lfloor\frac{i}{m}\rfloor+\lfloor\frac{mn-i-1}{m}\rfloor=n-1$ and $\lfloor\frac{i}{n}\rfloor+\lfloor\frac{mn-i-1}{n}\rfloor=m-1$; this implies that $f_{m,n}(i)+f_{m,n}(mn-i-1)=m+n-2$ is odd, and so $(-1)^{f_{m,n}(i)}=-(-1)^{f_{m,n}(mn-i-1)}$ for all $i$. It follows that $S(m,n)=0$ if $m$ and $n$ have opposite parity.

Now suppose that $m=2k$ and $n=2l$ are both even. Then $\lfloor\frac{2j}{2m}\rfloor=\lfloor\frac{2j+1}{2m}\rfloor$ for all $j$, so $S$ can be computed as twice the sum over only even indices:

$$S(2k,2l)=2\sum_{i=0}^{2kl-1}(-1)^{f_{k,l}(i)}=S(k,l)(1+(-1)^{k+l}).$$

Thus $S(2k,2l)$ vanishes if and only if $S(k,l)$ vanishes (if $1+(-1)^{k+l}=0$, then $k$ and $l$ have opposite parity and so $S(k,l)$ also vanishes).

Piecing our various cases together, we easily deduce that $S(m,n)=0$ if and only if the highest powers of 2 dividing $m$ and $n$ are different.

B–5 Write $N=(10^{1998}-1)/9$. Then

$$\begin{aligned}\sqrt{N}&=\frac{10^{999}}{3}\sqrt{1-10^{-1998}}\\&=\frac{10^{999}}{3}(1-\frac{1}{2}10^{-1998}+r),\end{aligned}$$

where $r<10^{-2000}$. Now the digits after the decimal point of $10^{999}/3$ are given by $.3333\ldots$, while the digits after the decimal point of $\frac{1}{6}10^{-999}$ are given by $.00000\ldots1666666\ldots$. It follows that the first 1000 digits of $\sqrt{N}$ are given by $.33333\ldots3331$; in particular, the thousandth digit is 1.

B–6 First solution: Write $p(n)=n^3+an^2+bn+c$. Note that $p(n)$ and $p(n+2)$ have the same parity, and recall that any perfect square is congruent to 0 or 1 (mod 4). Thus if $p(n)$ and $p(n+2)$ are perfect squares, they are congruent mod 4. But $p(n+2)-p(n)\equiv 2n^2+2b$ (mod 4), which is not divisible by 4 if $n$ and $b$ have opposite parity.

Second solution: We prove more generally that for any polynomial $P(z)$ with integer coefficients which is not a perfect square, there exists a positive integer $n$ such that $P(n)$ is not a perfect square. Of course it suffices to assume $P(z)$ has no repeated factors, which is to say $P(z)$ and its derivative $P'(z)$ are relatively prime.

In particular, if we carry out the Euclidean algorithm on $P(z)$ and $P'(z)$ without dividing, we get an integer $D$ (the discriminant of $P$) such that the greatest common divisor of $P(n)$ and $P'(n)$ divides $D$ for any $n$. Now there exist infinitely many primes $p$ such that $p$ divides $P(n)$ for some $n$: if there were only finitely many, say, $p_1,\ldots,p_k$, then for any $n$ divisible by $m=P(0)p_1p_2\cdots p_k$, we have $P(n)\equiv P(0) \pmod{m}$, that is, $P(n)/P(0)$ is not divisible by $p_1,\ldots,p_k$, so must be $\pm1$, but then $P$ takes some value infinitely many times, contradiction. In particular, we can choose some such $p$ not dividing $D$, and choose $n$ such that $p$ divides $P(n)$. Then $P(n+kp)\equiv P(n)+kpP'(n)(\bmod\, p)$ (write out the Taylor series of the left side); in particular, since $p$ does not divide $P'(n)$, we can find some $k$ such that $P(n+kp)$ is divisible by $p$ but not by $p^2$, and so is not a perfect square.

Third solution: (from David Rusin, David Savitt, and Richard Stanley independently) Assume that $n^3+an^2+bn+c$ is a square for all $n>0$. For sufficiently large $n$,

$$\begin{aligned}(n^{3/2}+\frac{1}{2}an^{1/2}-1)^2&<n^3+an^2+bn+c\\&<(n^{3/2}+\frac{1}{2}an^{1/2}+1)^2;\end{aligned}$$

thus if $n$ is a large even perfect square, we have $n^3+an^2+bn+c=(n^{3/2}+\frac{1}{2}an^{1/2})^2$. We conclude this is an equality of polynomials, but the right-hand side is not a perfect square for $n$ an even non-square, contradiction. (The reader might try generalizing this approach to arbitrary polynomials. A related argument, due to Greg Kuperberg: write $\sqrt{n^3+an^2+bn+c}$ as $n^{3/2}$ times a power series in $1/n$ and take two finite differences to get an expression which tends to 0 as $n\to\infty$, contradiction.)

Note: in case $n^3+an^2+bn+c$ has no repeated factors, it is a square for only finitely many $n$, by a theorem of Siegel; work of Baker gives an explicit (but large) bound on such $n$. (I don't know whether the graders will accept this as a solution, though.)

# The 60th William Lowell Putnam Mathematical Competition
## Saturday, December 4, 1999

A–1 Find polynomials $f(x)$,$g(x)$, and $h(x)$, if they exist, such that for all $x$,

$$|f(x)|-|g(x)|+h(x) = \begin{cases} -1 & \text{if } x<-1 \\ 3x+2 & \text{if } -1 \leq x \leq 0 \\ -2x+2 & \text{if } x>0. \end{cases}$$

A–2 Let $p(x)$ be a polynomial that is nonnegative for all real $x$. Prove that for some $k$, there are polynomials $f_1(x),\dots,f_k(x)$ such that

$$p(x) = \sum_{j=1}^{k} (f_j(x))^2.$$

A–3 Consider the power series expansion

$$\frac{1}{1-2x-x^2} = \sum_{n=0}^{\infty} a_n x^n.$$

Prove that, for each integer $n \geq 0$, there is an integer $m$ such that

$$a_n^2 + a_{n+1}^2 = a_m.$$

A–4 Sum the series

$$\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} \frac{m^2 n}{3^m(n3^m+m3^n)}.$$

A–5 Prove that there is a constant $C$ such that, if $p(x)$ is a polynomial of degree 1999, then

$$|p(0)| \leq C\int_{-1}^{1} |p(x)|\,dx.$$

A–6 The sequence $(a_n)_{n\geq 1}$ is defined by $a_1=1, a_2=2, a_3=24$, and, for $n \geq 4$,

$$a_n = \frac{6a_{n-1}^2 a_{n-3} - 8a_{n-1}a_{n-2}^2}{a_{n-2}a_{n-3}}.$$

Show that, for all n, $a_n$ is an integer multiple of $n$.

B–1 Right triangle $ABC$ has right angle at $C$ and $\angle BAC = \theta$; the point $D$ is chosen on $AB$ so that $|AC| = |AD| = 1$; the point $E$ is chosen on $BC$ so that $\angle CDE = \theta$. The perpendicular to $BC$ at $E$ meets $AB$ at $F$. Evaluate $\lim_{\theta\to 0} |EF|$.

B–2 Let $P(x)$ be a polynomial of degree $n$ such that $P(x) = Q(x)P''(x)$, where $Q(x)$ is a quadratic polynomial and $P''(x)$ is the second derivative of $P(x)$. Show that if $P(x)$ has at least two distinct roots then it must have $n$ distinct roots.

B–3 Let $A = \{(x,y) : 0 \leq x,y < 1\}$. For $(x,y) \in A$, let

$$S(x,y) = \sum_{\frac{1}{2}\leq\frac{m}{n}\leq 2} x^m y^n,$$

where the sum ranges over all pairs $(m,n)$ of positive integers satisfying the indicated inequalities. Evaluate

$$\lim_{(x,y)\to(1,1),(x,y)\in A} (1-xy^2)(1-x^2y)S(x,y).$$

B–4 Let $f$ be a real function with a continuous third derivative such that $f(x), f'(x), f''(x), f'''(x)$ are positive for all $x$. Suppose that $f'''(x) \leq f(x)$ for all $x$. Show that $f'(x) < 2f(x)$ for all $x$.

B–5 For an integer $n \geq 3$, let $\theta = 2\pi/n$. Evaluate the determinant of the $n\times n$ matrix $I+A$, where $I$ is the $n\times n$ identity matrix and $A = (a_{jk})$ has entries $a_{jk} = \cos(j\theta + k\theta)$ for all $j,k$.

B–6 Let $S$ be a finite set of integers, each greater than 1. Suppose that for each integer $n$ there is some $s \in S$ such that $\gcd(s,n) = 1$ or $\gcd(s,n) = s$. Show that there exist $s,t \in S$ such that $\gcd(s,t)$ is prime.

# Solutions to the 60th William Lowell Putnam Mathematical Competition
# Saturday, December 4, 1999

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A–1 Note that if $r(x)$ and $s(x)$ are any two functions, then

$$\max(r,s) = (r+s+|r-s|)/2.$$

Therefore, if $F(x)$ is the given function, we have

$$\begin{aligned} F(x) &= \max\{-3x-3,0\} - \max\{5x,0\} + 3x + 2 \\ &= (-3x-3+|3x+3|)/2 \\ &\quad - (5x+|5x|)/2 + 3x + 2 \\ &= |(3x+3)/2| - |5x/2| - x + \frac{1}{2}, \end{aligned}$$

so we may set $f(x) = (3x+3)/2$, $g(x) = 5x/2$, and $h(x) = -x + \frac{1}{2}$.

A–2 First solution: First factor $p(x) = q(x)r(x)$, where $q$ has all real roots and $r$ has all complex roots. Notice that each root of $q$ has even multiplicity, otherwise $p$ would have a sign change at that root. Thus $q(x)$ has a square root $s(x)$.

Now write $r(x) = \prod_{j=1}^{k}(x-a_j)(x-\overline{a_j})$ (possible because $r$ has roots in complex conjugate pairs). Write $\prod_{j=1}^{k}(x-a_j) = t(x) + iu(x)$ with $t,x$ having real coefficients. Then for $x$ real,

$$\begin{aligned} p(x) &= q(x)r(x) \\ &= s(x)^2(t(x)+iu(x))(\overline{t(x)+iu(x)}) \\ &= (s(x)t(x))^2 + (s(x)u(x))^2. \end{aligned}$$

(Alternatively, one can factor $r(x)$ as a product of quadratic polynomials with real coefficients, write each as a sum of squares, then multiply together to get a sum of many squares.)

Second solution: We proceed by induction on the degree of $p$, with base case where $p$ has degree 0. As in the first solution, we may reduce to a smaller degree in case $p$ has any real roots, so assume it has none. Then $p(x) > 0$ for all real $x$, and since $p(x) \to \infty$ for $x \to \pm\infty$, $p$ has a minimum value $c$. Now $p(x) - c$ has real roots, so as above, we deduce that $p(x) - c$ is a sum of squares. Now add one more square, namely $(\sqrt{c})^2$, to get $p(x)$ as a sum of squares.

A–3 First solution: Computing the coefficient of $x^{n+1}$ in the identity $(1-2x-x^2)\sum_{m=0}^{\infty} a_m x^m = 1$ yields the recurrence $a_{n+1} = 2a_n + a_{n-1}$; the sequence $\{a_n\}$ is then characterized by this recurrence and the initial conditions $a_0 = 1, a_1 = 2$.

Define the sequence $\{b_n\}$ by $b_{2n} = a_{n-1}^2 + a_n^2$, $b_{2n+1} = a_n(a_{n-1} + a_{n+1})$. Then

$$\begin{aligned} 2b_{2n+1} + b_{2n} &= 2a_n a_{n+1} + 2a_{n-1}a_n + a_{n-1}^2 + a_n^2 \\ &= 2a_n a_{n+1} + a_{n-1}a_{n+1} + a_n^2 \\ &= a_{n+1}^2 + a_n^2 = b_{2n+2}, \end{aligned}$$

and similarly $2b_{2n} + b_{2n-1} = b_{2n+1}$, so that $\{b_n\}$ satisfies the same recurrence as $\{a_n\}$. Since further $b_0 = 1, b_1 = 2$ (where we use the recurrence for $\{a_n\}$ to calculate $a_{-1} = 0$), we deduce that $b_n = a_n$ for all $n$. In particular, $a_n^2 + a_{n+1}^2 = b_{2n+2} = a_{2n+2}$.

Second solution: Note that

$$\begin{aligned} &\frac{1}{1-2x-x^2} \\ &\qquad = \frac{1}{2\sqrt{2}}\left(\frac{\sqrt{2}+1}{1-(1+\sqrt{2})x} + \frac{\sqrt{2}-1}{1-(1-\sqrt{2})x}\right) \end{aligned}$$

and that

$$\frac{1}{1+(1\pm\sqrt{2})x} = \sum_{n=0}^{\infty}(1\pm\sqrt{2})^n x^n,$$

so that

$$a_n = \frac{1}{2\sqrt{2}}\left((\sqrt{2}+1)^{n+1} - (1-\sqrt{2})^{n+1}\right).$$

A simple computation (omitted here) now shows that $a_n^2 + a_{n+1}^2 = a_{2n+2}$.

Third solution (by Richard Stanley): Let $A$ be the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$. A simple induction argument shows that

$$A^{n+2} = \begin{pmatrix} a_n & a_{n+1} \\ a_{n+1} & a_{n+2} \end{pmatrix}.$$

The desired result now follows from comparing the top left corner entries of the equality $A^{n+2}A^{n+2} = A^{2n+4}$.

A–4 Denote the series by $S$, and let $a_n = 3^n/n$. Note that

$$\begin{aligned} S &= \sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\frac{1}{a_m(a_m+a_n)} \\ &= \sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\frac{1}{a_n(a_m+a_n)}, \end{aligned}$$

where the second equality follows by interchanging $m$

and $n$. Thus

$$\begin{aligned} 2S &= \sum_m \sum_n \left( \frac{1}{a_m(a_m+a_n)} + \frac{1}{a_n(a_m+a_n)} \right) \\ &= \sum_m \sum_n \frac{1}{a_m a_n} \\ &= \left( \sum_{n=1}^\infty \frac{n}{3^n} \right)^2. \end{aligned}$$

But

$$\sum_{n=1}^\infty \frac{n}{3^n} = \frac{3}{4}$$

since, e.g., it's $f'(1)$, where

$$f(x) = \sum_{n=0}^\infty \frac{x^n}{3^n} = \frac{3}{3-x},$$

and we conclude that $S = 9/32$.

A–5 First solution: (by Reid Barton) Let $r_1, \dots, r_{1999}$ be the roots of $P$. Draw a disc of radius $\varepsilon$ around each $r_i$, where $\varepsilon < 1/3998$; this disc covers a subinterval of $[-1/2, 1/2]$ of length at most $2\varepsilon$, and so of the 2000 (or fewer) uncovered intervals in $[-1/2, 1/2]$, one, which we call $I$, has length at least $\delta = (1-3998\varepsilon)/2000 > 0$. We will exhibit an explicit lower bound for the integral of $|P(x)|/P(0)$ over this interval, which will yield such a bound for the entire integral.

Note that

$$\frac{|P(x)|}{|P(0)|} = \prod_{i=1}^{1999} \frac{|x-r_i|}{|r_i|}.$$

Also note that by construction, $|x - r_i| \geq \varepsilon$ for each $x \in I$. If $|r_i| \leq 1$, then we have $\frac{|x-r_i|}{|r_i|} \geq \varepsilon$. If $|r_i| > 1$, then

$$\frac{|x-r_i|}{|r_i|} = |1 - x/r_i| \geq 1 - |x/r_i| \geq= 1/2 > \varepsilon.$$

We conclude that $\int_I |P(x)/P(0)|\,dx \geq \delta\varepsilon$, independent of $P$.

Second solution: It will be a bit more convenient to assume $P(0) = 1$ (which we may achieve by rescaling unless $P(0) = 0$, in which case there is nothing to prove) and to prove that there exists $D > 0$ such that $\int_{-1}^1 |P(x)|\,dx \geq D$, or even such that $\int_0^1 |P(x)|\,dx \geq D$.

We first reduce to the case where $P$ has all of its roots in $[0,1]$. If this is not the case, we can factor $P(x)$ as $Q(x)R(x)$, where $Q$ has all roots in the interval and $R$ has none. Then $R$ is either always positive or always negative on $[0,1]$; assume the former. Let $k$ be the largest positive real number such that $R(x) - kx \geq 0$ on $[0,1]$; then

$$\begin{aligned} \int_{-1}^1 |P(x)|\,dx &= \int_{-1}^1 |Q(x)R(x)|\,dx \\ &> \int_{-1}^1 |Q(x)(R(x)-kx)|\,dx, \end{aligned}$$

and $Q(x)(R(x)-kx)$ has more roots in $[0,1]$ than does $P$ (and has the same value at 0). Repeating this argument shows that $\int_0^1 |P(x)|\,dx$ is greater than the corresponding integral for some polynomial with all of its roots in $[0,1]$.

Under this assumption, we have

$$P(x) = c \prod_{i=1}^{1999} (x - r_i)$$

for some $r_i \in (0,1]$. Since

$$P(0) = -c \prod r_i = 1,$$

we have

$$|c| \geq \prod |r_i^{-1}| \geq 1.$$

Thus it suffices to prove that if $Q(x)$ is a *monic* polynomial of degree 1999 with all of its roots in $[0,1]$, then $\int_0^1 |Q(x)|\,dx \geq D$ for some constant $D > 0$. But the integral of $\int_0^1 \prod_{i=1}^{1999} |x - r_i|\,dx$ is a continuous function for $r_i \in [0,1]$. The product of all of these intervals is compact, so the integral achieves a minimum value for some $r_i$. This minimum is the desired $D$.

Third solution (by Abe Kunin): It suffices to prove the stronger inequality

$$\sup_{x \in [-1,1]} |P(x)| \leq C \int_{-1}^1 |P(x)|\,dx$$

holds for some $C$. But this follows immediately from the following standard fact: any two norms on a finite-dimensional vector space (here the polynomials of degree at most 1999) are equivalent. (The proof of this statement is also a compactness argument: $C$ can be taken to be the maximum of the L1-norm divided by the sup norm over the set of polynomials with L1-norm 1.)

Note: combining the first two approaches gives a constructive solution with a constant that is better than that given by the first solution, but is still far from optimal. I don't know offhand whether it is even known what the optimal constant and/or the polynomials achieving that constant are.

A–6 Rearranging the given equation yields the much more tractable equation

$$\frac{a_n}{a_{n-1}} = 6\frac{a_{n-1}}{a_{n-2}} - 8\frac{a_{n-2}}{a_{n-3}}.$$

Let $b_n = a_n/a_{n-1}$; with the initial conditions $b_2 = 2, b_3 = 12$, one easily obtains $b_n = 2^{n-1}(2^{n-2}-1)$, and so

$$a_n = 2^{n(n-1)/2} \prod_{i=1}^{n-1} (2^i - 1).$$

To see that $n$ divides $a_n$, factor $n$ as $2^k m$, with $m$ odd. Then note that $k \leq n \leq n(n-1)/2$, and that there exists $i \leq m-1$ such that $m$ divides $2^i - 1$, namely $i = \phi(m)$ (Euler's totient function: the number of integers in $\{1, \dots, m\}$ relatively prime to $m$).

B–1 The answer is 1/3. Let $G$ be the point obtained by reflecting $C$ about the line $AB$. Since $\angle ADC = \frac{\pi-\theta}{2}$, we find that $\angle BDE = \pi - \theta - \angle ADC = \frac{\pi-\theta}{2} = \angle ADC = \pi - \angle BDC = \pi - \angle BDG$, so that $E, D, G$ are collinear. Hence

$$|EF| = \frac{|BE|}{|BC|} = \frac{|BE|}{|BG|} = \frac{\sin(\theta/2)}{\sin(3\theta/2)},$$

where we have used the law of sines in $\triangle BDG$. But by l'Hôpital's Rule,

$$\lim_{\theta \to 0} \frac{\sin(\theta/2)}{\sin(3\theta/2)} = \lim_{\theta \to 0} \frac{\cos(\theta/2)}{3\cos(3\theta/2)} = 1/3.$$

B–2 First solution: Suppose that $P$ does not have $n$ distinct roots; then it has a root of multiplicity at least 2, which we may assume is $x = 0$ without loss of generality. Let $x^k$ be the greatest power of $x$ dividing $P(x)$, so that $P(x) = x^k R(x)$ with $R(0) \neq 0$; a simple computation yields

$$P''(x) = (k^2 - k)x^{k-2}R(x) + 2kx^{k-1}R'(x) + x^k R''(x).$$

Since $R(0) \neq 0$ and $k \geq 2$, we conclude that the greatest power of $x$ dividing $P''(x)$ is $x^{k-2}$. But $P(x) = Q(x)P''(x)$, and so $x^2$ divides $Q(x)$. We deduce (since $Q$ is quadratic) that $Q(x)$ is a constant $C$ times $x^2$; in fact, $C = 1/(n(n-1))$ by inspection of the leading-degree terms of $P(x)$ and $P''(x)$.

Now if $P(x) = \sum_{j=0}^n a_j x^j$, then the relation $P(x) = Cx^2 P''(x)$ implies that $a_j = Cj(j-1)a_j$ for all $j$; hence $a_j = 0$ for $j \leq n-1$, and we conclude that $P(x) = a_n x^n$, which has all identical roots.

Second solution (by Greg Kuperberg): Let $f(x) = P''(x)/P(x) = 1/Q(x)$. By hypothesis, $f$ has at most two poles (counting multiplicity).

Recall that for any complex polynomial $P$, the roots of $P'$ lie within the convex hull of $P$. To show this, it suffices to show that if the roots of $P$ lie on one side of a line, say on the positive side of the imaginary axis, then $P'$ has no roots on the other side. That follows because if $r_1, \dots, r_n$ are the roots of $P$,

$$\frac{P'(z)}{P(z)} = \sum_{i=1}^n \frac{1}{z - r_i}$$

and if $z$ has negative real part, so does $1/(z - r_i)$ for $i = 1, \dots, n$, so the sum is nonzero.

The above argument also carries through if $z$ lies on the imaginary axis, provided that $z$ is not equal to a root of $P$. Thus we also have that no roots of $P'$ lie on the sides of the convex hull of $P$, unless they are also roots of $P$.

From this we conclude that if $r$ is a root of $P$ which is a vertex of the convex hull of the roots, and which is not also a root of $P'$, then $f$ has a single pole at $r$ (as $r$ cannot be a root of $P''$). On the other hand, if $r$ is a root of $P$ which is also a root of $P'$, it is a multiple root, and then $f$ has a double pole at $r$.

If $P$ has roots not all equal, the convex hull of its roots has at least two vertices.

B–3 We first note that

$$\sum_{m,n>0} x^m y^n = \frac{xy}{(1-x)(1-y)}.$$

Subtracting $S$ from this gives two sums, one of which is

$$\sum_{m \geq 2n+1} x^m y^n = \sum_n y^n \frac{x^{2n+1}}{1-x} = \frac{x^3 y}{(1-x)(1-x^2 y)}$$

and the other of which sums to $xy^3/[(1-y)(1-xy^2)]$. Therefore

$$\begin{aligned} S(x,y) &= \frac{xy}{(1-x)(1-y)} - \frac{x^3 y}{(1-x)(1-x^2 y)} \\ &\quad - \frac{xy^3}{(1-y)(1-xy^2)} \\ &= \frac{xy(1+x+y+xy-x^2y^2)}{(1-x^2y)(1-xy^2)} \end{aligned}$$

and the desired limit is

$$\lim_{(x,y)\to(1,1)} xy(1+x+y+xy-x^2y^2) = 3.$$

B–4 (based on work by Daniel Stronger) We make repeated use of the following fact: if $f$ is a differentiable function on all of $\mathbb{R}$, $\lim_{x\to-\infty} f(x) \geq 0$, and $f'(x) > 0$ for all $x \in \mathbb{R}$, then $f(x) > 0$ for all $x \in \mathbb{R}$. (Proof: if $f(y) < 0$ for some $x$, then $f(x) < f(y)$ for all $x < y$ since $f' > 0$, but then $\lim_{x\to-\infty} f(x) \leq f(y) < 0$.)

From the inequality $f'''(x) \leq f(x)$ we obtain

$$f'' f'''(x) \leq f''(x)f(x) < f''(x)f(x) + f'(x)^2$$

since $f'(x)$ is positive. Applying the fact to the difference between the right and left sides, we get

$$\frac{1}{2}(f''(x))^2 < f(x)f'(x). \tag{1}$$

On the other hand, since $f(x)$ and $f'''(x)$ are both positive for all $x$, we have

$$2f'(x)f''(x) < 2f'(x)f''(x) + 2f(x)f'''(x).$$

Applying the fact to the difference between the sides yields

$$f'(x)^2 \leq 2f(x)f''(x). \tag{2}$$

Combining (1) and (2), we obtain

$$\begin{aligned}\frac{1}{2}\left(\frac{f'(x)^2}{2f(x)}\right)^2 &< \frac{1}{2}(f''(x))^2\\ &< f(x)f'(x),\end{aligned}$$

or $(f'(x))^3 < 8f(x)^3$. We conclude $f'(x) < 2f(x)$, as desired.

Note: one can actually prove the result with a smaller constant in place of 2, as follows. Adding $\frac{1}{2}f'(x)f'''(x)$ to both sides of (1) and again invoking the original bound $f'''(x) \leq f(x)$, we get

$$\begin{aligned}\frac{1}{2}[f'(x)f'''(x)+(f''(x))^2] &< f(x)f'(x)+\frac{1}{2}f'(x)f'''(x)\\ &\leq \frac{3}{2}f(x)f'(x).\end{aligned}$$

Applying the fact again, we get

$$\frac{1}{2}f'(x)f''(x) < \frac{3}{4}f(x)^2.$$

Multiplying both sides by $f'(x)$ and applying the fact once more, we get

$$\frac{1}{6}(f'(x))^3 < \frac{1}{4}f(x)^3.$$

From this we deduce $f'(x) < (3/2)^{1/3}f(x) < 2f(x)$, as desired.

I don't know what the best constant is, except that it is not less than 1 (because $f(x) = e^x$ satisfies the given conditions).

B–5 First solution: We claim that the eigenvalues of $A$ are 0 with multiplicity $n-2$, and $n/2$ and $-n/2$, each with multiplicity 1. To prove this claim, define vectors $v^{(m)}$, $0 \leq m \leq n-1$, componentwise by $(v^{(m)})_k = e^{ikm\theta}$, and note that the $v^{(m)}$ form a basis for $\mathbb{C}^n$. (If we arrange the $v^{(m)}$ into an $n\times n$ matrix, then the determinant of this matrix is a Vandermonde product which is nonzero.) Now note that

$$\begin{aligned}(Av^{(m)})_j &= \sum_{k=1}^n \cos(j\theta+k\theta)e^{ikm\theta}\\ &= \frac{e^{ij\theta}}{2}\sum_{k=1}^n e^{ik(m+1)\theta}+\frac{e^{-ij\theta}}{2}\sum_{k=1}^n e^{ik(m-1)\theta}.\end{aligned}$$

Since $\sum_{k=1}^n e^{ik\ell\theta} = 0$ for integer $\ell$ unless $n\,|\,\ell$, we conclude that $Av^{(m)} = 0$ for $m = 0$ or for $2 \leq m \leq n-1$. In addition, we find that $(Av^{(1)})_j = \frac{n}{2}e^{-ij\theta} = \frac{n}{2}(v^{(n-1)})_j$ and $(Av^{(n-1)})_j = \frac{n}{2}e^{ij\theta} = \frac{n}{2}(v^{(1)})_j$, so that $A(v^{(1)} \pm v^{(n-1)}) = \pm\frac{n}{2}(v^{(1)} \pm v^{(n-1)})$. Thus $\{v^{(0)}, v^{(2)}, v^{(3)}, \dots, v^{(n-2)}, v^{(1)}+v^{(n-1)}, v^{(1)}-v^{(n-1)}\}$ is a basis for $\mathbb{C}^n$ of eigenvectors of $A$ with the claimed eigenvalues.

Finally, the determinant of $I+A$ is the product of $(1+\lambda)$ over all eigenvalues $\lambda$ of $A$; in this case, $\det(I+A) = (1+n/2)(1-n/2) = 1-n^2/4$.

Second solution (by Mohamed Omar): Set $x = e^{i\theta}$ and write

$$A = \frac{1}{2}u^Tu + \frac{1}{2}v^Tv = \frac{1}{2}\begin{pmatrix}u^T & v^T\end{pmatrix}\begin{pmatrix}u\\ v\end{pmatrix}$$

for

$$u = \begin{pmatrix}x & x^2 & \cdots & x^n\end{pmatrix}, v = \begin{pmatrix}x^{-1} & x^{-2} & \cdots & x^n\end{pmatrix}.$$

We now use the fact that for $R$ an $n\times m$ matrix and $S$ an $m\times n$ matrix,

$$\det(I_n+RS) = \det(I_m+SR).$$

This yields

$$\begin{aligned}&\det(I_N+A)\\ &= \det\left(I_n + \frac{1}{2}\begin{pmatrix}u^T & v^T\end{pmatrix}\begin{pmatrix}u\\ v\end{pmatrix}\right)\\ &= \det\left(I_2 + \frac{1}{2}\begin{pmatrix}u\\ v\end{pmatrix}\begin{pmatrix}u^T & v^T\end{pmatrix}\right)\\ &= \frac{1}{4}\det\begin{pmatrix}2+uu^T & uv^T\\ vu^T & 2+vv^T\end{pmatrix}\\ &= \frac{1}{4}\det\begin{pmatrix}2+(x^2+\cdots+x^{2n}) & n\\ n & 2+(x^{-2}+\cdots+x^{-2n})\end{pmatrix}\\ &= \frac{1}{4}\det\begin{pmatrix}2 & n\\ n & 2\end{pmatrix} = 1-\frac{n^2}{4}.\end{aligned}$$

B–6 First solution: Choose a sequence $p_1, p_2, \dots$ of primes as follows. Let $p_1$ be any prime dividing an element of $S$. To define $p_{j+1}$ given $p_1, \dots, p_j$, choose an integer $N_j \in S$ relatively prime to $p_1\cdots p_j$ and let $p_{j+1}$ be a prime divisor of $N_j$, or stop if no such $N_j$ exists.

Since $S$ is finite, the above algorithm eventually terminates in a finite sequence $p_1, \dots, p_k$. Let $m$ be the smallest integer such that $p_1\cdots p_m$ has a divisor in $S$. (By the assumption on $S$ with $n = p_1\cdots p_k$, $m = k$ has this property, so $m$ is well-defined.) If $m = 1$, then $p_1 \in S$, and we are done, so assume $m \geq 2$. Any divisor $d$ of $p_1\cdots p_m$ in $S$ must be a multiple of $p_m$, or else it would also be a divisor of $p_1\cdots p_{m-1}$, contradicting the choice of $m$. But now $\gcd(d, N_{m-1}) = p_m$, as desired.

Second solution (from `sci.math`): Let $n$ be the smallest integer such that $\gcd(s,n) > 1$ for all $s$ in $n$; note that $n$ obviously has no repeated prime factors. By the condition on $S$, there exists $s \in S$ which divides $n$.

On the other hand, if $p$ is a prime divisor of $s$, then by the choice of $n$, $n/p$ is relatively prime to some element $t$ of $S$. Since $n$ cannot be relatively prime to $t$, $t$ is divisible by $p$, but not by any other prime divisor of $n$ (as those primes divide $n/p$). Thus $\gcd(s,t) = p$, as desired.

# The 61st William Lowell Putnam Mathematical Competition
## Saturday, December 2, 2000

A–1 Let $A$ be a positive real number. What are the possible values of $\sum_{j=0}^{\infty} x_j^2$, given that $x_0, x_1, \ldots$ are positive numbers for which $\sum_{j=0}^{\infty} x_j = A$?

A–2 Prove that there exist infinitely many integers $n$ such that $n, n+1, n+2$ are each the sum of the squares of two integers. [Example: $0 = 0^2 + 0^2$, $1 = 0^2 + 1^2$, $2 = 1^2 + 1^2$.]

A–3 The octagon $P_1P_2P_3P_4P_5P_6P_7P_8$ is inscribed in a circle, with the vertices around the circumference in the given order. Given that the polygon $P_1P_3P_5P_7$ is a square of area 5, and the polygon $P_2P_4P_6P_8$ is a rectangle of area 4, find the maximum possible area of the octagon.

A–4 Show that the improper integral

$$\lim_{B\to\infty} \int_0^B \sin(x)\sin(x^2)\,dx$$

converges.

A–5 Three distinct points with integer coordinates lie in the plane on a circle of radius $r > 0$. Show that two of these points are separated by a distance of at least $r^{1/3}$.

A–6 Let $f(x)$ be a polynomial with integer coefficients. Define a sequence $a_0, a_1, \ldots$ of integers such that $a_0 = 0$ and $a_{n+1} = f(a_n)$ for all $n \geq 0$. Prove that if there exists a positive integer $m$ for which $a_m = 0$ then either $a_1 = 0$ or $a_2 = 0$.

B–1 Let $a_j, b_j, c_j$ be integers for $1 \leq j \leq N$. Assume for each $j$, at least one of $a_j, b_j, c_j$ is odd. Show that there exist integers $r$, $s$, $t$ such that $ra_j + sb_j + tc_j$ is odd for at least $4N/7$ values of $j$, $1 \leq j \leq N$.

B–2 Prove that the expression

$$\frac{gcd(m,n)}{n}\binom{n}{m}$$

is an integer for all pairs of integers $n \geq m \geq 1$.

B–3 Let $f(t) = \sum_{j=1}^{N} a_j \sin(2\pi jt)$, where each $a_j$ is real and $a_N$ is not equal to 0. Let $N_k$ denote the number of zeroes (including multiplicities) of $\frac{d^k f}{dt^k}$. Prove that

$$N_0 \leq N_1 \leq N_2 \leq \cdots \text{ and } \lim_{k\to\infty} N_k = 2N.$$

[Editorial clarification: only zeroes in $[0,1)$ should be counted.]

B–4 Let $f(x)$ be a continuous function such that $f(2x^2-1) = 2xf(x)$ for all $x$. Show that $f(x) = 0$ for $-1 \leq x \leq 1$.

B–5 Let $S_0$ be a finite set of positive integers. We define finite sets $S_1, S_2, \ldots$ of positive integers as follows: the integer $a$ is in $S_{n+1}$ if and only if exactly one of $a-1$ or $a$ is in $S_n$. Show that there exist infinitely many integers $N$ for which $S_N = S_0 \cup \{N + a : a \in S_0\}$.

B–6 Let $B$ be a set of more than $2^{n+1}/n$ distinct points with coordinates of the form $(\pm 1, \pm 1, \ldots, \pm 1)$ in $n$-dimensional space with $n \geq 3$. Show that there are three distinct points in $B$ which are the vertices of an equilateral triangle.

# Solutions to the 61st William Lowell Putnam Mathematical Competition
# Saturday, December 2, 2000

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A–1 The possible values comprise the interval $(0, A^2)$.

To see that the values must lie in this interval, note that

$$\left(\sum_{j=0}^m x_j\right)^2 = \sum_{j=0}^m x_j^2 + \sum_{0 \leq j < k \leq m} 2x_j x_k,$$

so $\sum_{j=0}^m x_j^2 \leq A^2 - 2x_0 x_1$. Letting $m \to \infty$, we have $\sum_{j=0}^\infty x_j^2 \leq A^2 - 2x_0x_1 < A^2$.

To show that all values in $(0, A^2)$ can be obtained, we use geometric progressions with $x_1/x_0 = x_2/x_1 = \cdots = d$ for variable $d$. Then $\sum_{j=0}^\infty x_j = x_0/(1-d)$ and

$$\sum_{j=0}^\infty x_j^2 = \frac{x_0^2}{1-d^2} = \frac{1-d}{1+d}\left(\sum_{j=0}^\infty x_j\right)^2.$$

As $d$ increases from 0 to 1, $(1-d)/(1+d)$ decreases from 1 to 0. Thus if we take geometric progressions with $\sum_{j=0}^\infty x_j = A$, $\sum_{j=0}^\infty x_j^2$ ranges from 0 to $A^2$. Thus the possible values are indeed those in the interval $(0, A^2)$, as claimed.

A–2 First solution: Let $a$ be an even integer such that $a^2+1$ is not prime. (For example, choose $a \equiv 2 \pmod 5$, so that $a^2+1$ is divisible by 5.) Then we can write $a^2+1$ as a difference of squares $x^2-b^2$, by factoring $a^2+1$ as $rs$ with $r \geq s > 1$, and setting $x = (r+s)/2$, $b = (r-s)/2$. Finally, put $n = x^2-1$, so that $n = a^2+b^2$, $n+1 = x^2$, $n+2 = x^2+1$.

Second solution: It is well-known that the equation $x^2 - 2y^2 = 1$ has infinitely many solutions (the so-called "Pell" equation). Thus setting $n = 2y^2$ (so that $n = y^2+y^2$, $n+1 = x^2+0^2$, $n+2 = x^2+1^2$) yields infinitely many $n$ with the desired property.

Third solution: As in the first solution, it suffices to exhibit $x$ such that $x^2-1$ is the sum of two squares. We will take $x = 3^{2^n}$, and show that $x^2-1$ is the sum of two squares by induction on $n$: if $3^{2^n}-1 = a^2+b^2$, then

$$\begin{aligned}(3^{2^{n+1}}-1) &= (3^{2^n}-1)(3^{2^n}+1) \\ &= (3^{2^{n-1}}a+b)^2 + (a - 3^{2^{n-1}}b)^2.\end{aligned}$$

Fourth solution (by Jonathan Weinstein): Let $n = 4k^4 + 4k^2 = (2k^2)^2 + (2k)^2$ for any integer $k$. Then $n+1 = (2k^2+1)^2 + 0^2$ and $n+2 = (2k^2+1)^2 + 1^2$.

A–3 The maximum area is $3\sqrt{5}$.

We deduce from the area of $P_1P_3P_5P_7$ that the radius of the circle is $\sqrt{5/2}$. An easy calculation using the Pythagorean Theorem then shows that the rectangle $P_2P_4P_6P_8$ has sides $\sqrt{2}$ and $2\sqrt{2}$. For notational ease, denote the area of a polygon by putting brackets around the name of the polygon.

By symmetry, the area of the octagon can be expressed as

$$[P_2P_4P_6P_8] + 2[P_2P_3P_4] + 2[P_4P_5P_6].$$

Note that $[P_2P_3P_4]$ is $\sqrt{2}$ times the distance from $P_3$ to $P_2P_4$, which is maximized when $P_3$ lies on the midpoint of arc $P_2P_4$; similarly, $[P_4P_5P_6]$ is $\sqrt{2}/2$ times the distance from $P_5$ to $P_4P_6$, which is maximized when $P_5$ lies on the midpoint of arc $P_4P_6$. Thus the area of the octagon is maximized when $P_3$ is the midpoint of arc $P_2P_4$ and $P_5$ is the midpoint of arc $P_4P_6$. In this case, it is easy to calculate that $[P_2P_3P_4] = \sqrt{5}-1$ and $[P_4P_5P_6] = \sqrt{5}/2 - 1$, and so the area of the octagon is $3\sqrt{5}$.

A–4 To avoid some improper integrals at 0, we may as well replace the left endpoint of integration by some $\varepsilon > 0$. We now use integration by parts:

$$\begin{aligned}\int_\varepsilon^B \sin x \sin x^2\,dx &= \int_\varepsilon^B \frac{\sin x}{2x} \sin x^2 (2x\,dx) \\ &= -\frac{\sin x}{2x}\cos x^2\Big|_\varepsilon^B \\ &\quad + \int_\varepsilon^B \left(\frac{\cos x}{2x} - \frac{\sin x}{2x^2}\right)\cos x^2\,dx.\end{aligned}$$

Now $\frac{\sin x}{2x}\cos x^2$ tends to 0 as $B \to \infty$, and the integral of $\frac{\sin x}{2x^2}\cos x^2$ converges absolutely by comparison with $1/x^2$. Thus it suffices to note that

$$\begin{aligned}\int_\varepsilon^B \frac{\cos x}{2x}\cos x^2\,dx &= \int_\varepsilon^B \frac{\cos x}{4x^2}\cos x^2 (2x\,dx) \\ &= \frac{\cos x}{4x^2}\sin x^2\Big|_\varepsilon^B \\ &\quad - \int_\varepsilon^B \frac{2x\cos x - \sin x}{4x^3}\sin x^2\,dx,\end{aligned}$$

and that the final integral converges absolutely by comparison to $1/x^3$.

An alternate approach is to first rewrite $\sin x \sin x^2$ as $\frac{1}{2}(\cos(x^2-x) - \cos(x^2+x))$. Then

$$\begin{aligned}\int_\varepsilon^B \cos(x^2+x)\,dx &= -\frac{\sin(x^2+x)}{2x+1}\Big|_\varepsilon^B \\ &\quad - \int_\varepsilon^B \frac{2\sin(x^2+x)}{(2x+1)^2}\,dx\end{aligned}$$

converges absolutely, and $\int_0^B \cos(x^2 - x)$ can be treated similarly.

A–5 Let $a,b,c$ be the distances between the points. Then the area of the triangle with the three points as vertices is $abc/4r$. On the other hand, the area of a triangle whose vertices have integer coordinates is at least 1/2 (for example, by Pick's Theorem). Thus $abc/4r \geq 1/2$, and so

$$\max\{a,b,c\} \geq (abc)^{1/3} \geq (2r)^{1/3} > r^{1/3}.$$

A–6 Recall that if $f(x)$ is a polynomial with integer coefficients, then $m-n$ divides $f(m)-f(n)$ for any integers $m$ and $n$. In particular, if we put $b_n = a_{n+1} - a_n$, then $b_n$ divides $b_{n+1}$ for all $n$. On the other hand, we are given that $a_0 = a_m = 0$, which implies that $a_1 = a_{m+1}$ and so $b_0 = b_m$. If $b_0 = 0$, then $a_0 = a_1 = \cdots = a_m$ and we are done. Otherwise, $|b_0| = |b_1| = |b_2| = \cdots$, so $b_n = \pm b_0$ for all $n$.

Now $b_0 + \cdots + b_{m-1} = a_m - a_0 = 0$, so half of the integers $b_0, \dots, b_{m-1}$ are positive and half are negative. In particular, there exists an integer $0 < k < m$ such that $b_{k-1} = -b_k$, which is to say, $a_{k-1} = a_{k+1}$. From this it follows that $a_n = a_{n+2}$ for all $n \geq k-1$; in particular, for $m = n$, we have

$$a_0 = a_m = a_{m+2} = f(f(a_0)) = a_2.$$

B–1 Consider the seven triples $(a,b,c)$ with $a,b,c \in \{0,1\}$ not all zero. Notice that if $r_j, s_j, t_j$ are not all even, then four of the sums $ar_j + bs_j + ct_j$ with $a,b,c \in \{0,1\}$ are even and four are odd. Of course the sum with $a = b = c = 0$ is even, so at least four of the seven triples with $a,b,c$ not all zero yield an odd sum. In other words, at least $4N$ of the tuples $(a,b,c,j)$ yield odd sums. By the pigeonhole principle, there is a triple $(a,b,c)$ for which at least $4N/7$ of the sums are odd.

B–2 Since $\gcd(m,n)$ is an integer linear combination of $m$ and $n$, it follows that

$$\frac{gcd(m,n)}{n}\binom{n}{m}$$

is an integer linear combination of the integers

$$\frac{m}{n}\binom{n}{m} = \binom{n-1}{m-1} \text{ and } \frac{n}{n}\binom{n}{m} = \binom{n}{m}$$

and hence is itself an integer.

B–3 Put $f_k(t) = \frac{df^k}{dt^k}$. Recall Rolle's theorem: if $f(t)$ is differentiable, then between any two zeroes of $f(t)$ there exists a zero of $f'(t)$. This also applies when the zeroes are not all distinct: if $f$ has a zero of multiplicity $m$ at $t = x$, then $f'$ has a zero of multiplicity at least $m-1$ there.

Therefore, if $0 \leq a_0 \leq a_1 \leq \cdots \leq a_r < 1$ are the roots of $f_k$ in $[0,1)$, then $f_{k+1}$ has a root in each of the intervals $(a_0,a_1),(a_1,a_2),\dots,(a_{r-1},a_r)$, so long as we adopt the convention that the empty interval $(t,t)$ actually contains the point $t$ itself. There is also a root in the "wraparound" interval $(a_r,a_0)$. Thus $N_{k+1} \geq N_k$.

Next, note that if we set $z = e^{2\pi it}$; then

$$f_{4k}(t) = \frac{1}{2i}\sum_{j=1}^{N} j^{4k} a_j (z^j - z^{-j})$$

is equal to $z^{-N}$ times a polynomial of degree $2N$. Hence as a function of $z$, it has at most $2N$ roots; therefore $f_k(t)$ has at most $2N$ roots in $[0,1]$. That is, $N_k \leq 2N$ for all $N$.

To establish that $N_k \to 2N$, we make precise the observation that

$$f_k(t) = \sum_{j=1}^{N} j^{4k} a_j \sin(2\pi jt)$$

is dominated by the term with $j = N$. At the points $t = (2i+1)/(2N)$ for $i = 0,1,\dots,N-1$, we have $N^{4k} a_N \sin(2\pi Nt) = \pm N^{4k} a_N$. If $k$ is chosen large enough so that

$$|a_N| N^{4k} > |a_1| 1^{4k} + \cdots + |a_{N-1}|(N-1)^{4k},$$

then $f_k((2i+1)/2N)$ has the same sign as $a_N \sin(2\pi Nat)$, which is to say, the sequence $f_k(1/2N), f_k(3/2N), \dots$ alternates in sign. Thus between these points (again including the "wraparound" interval) we find $2N$ sign changes of $f_k$. Therefore $\lim_{k\to\infty} N_k = 2N$.

B–4 For $t$ real and not a multiple of $\pi$, write $g(t) = \frac{f(\cos t)}{\sin t}$. Then $g(t+\pi) = g(t)$; furthermore, the given equation implies that

$$g(2t) = \frac{f(2\cos^2 t - 1)}{\sin(2t)} = \frac{2(\cos t) f(\cos t)}{\sin(2t)} = g(t).$$

In particular, for any integer $n$ and $k$, we have

$$g(1 + n\pi/2^k) = g(2^k + n\pi) = g(2^k) = g(1).$$

Since $f$ is continuous, $g$ is continuous where it is defined; but the set $\{1 + n\pi/2^k | n,k \in \mathbb{Z}\}$ is dense in the reals, and so $g$ must be constant on its domain. Since $g(-t) = -g(t)$ for all $t$, we must have $g(t) = 0$ when $t$ is not a multiple of $\pi$. Hence $f(x) = 0$ for $x \in (-1,1)$. Finally, setting $x = 0$ and $x = 1$ in the given equation yields $f(-1) = f(1) = 0$.

B–5 We claim that all integers $N$ of the form $2^k$, with $k$ a positive integer and $N > \max\{S_0\}$, satisfy the desired conditions.

It follows from the definition of $S_n$, and induction on $n$, that

$$\begin{aligned}\sum_{j \in S_n} x^j &\equiv (1+x) \sum_{j \in S_{n-1}} x^j \\ &\equiv (1+x)^n \sum_{j \in S_0} x^j \pmod 2.\end{aligned}$$

From the identity $(x+y)^2 \equiv x^2 + y^2 \pmod 2$ and induction on $n$, we have $(x+y)^{2^n} \equiv x^{2^n} + y^{2^n} \pmod 2$. Hence if we choose $N$ to be a power of 2 greater than $\max\{S_0\}$, then

$$\sum_{j \in S_n} \equiv (1+x^N) \sum_{j \in S_0} x^j$$

and $S_N = S_0 \cup \{N + a : a \in S_0\}$, as desired.

B–6 For each point $P$ in $B$, let $S_P$ be the set of points with all coordinates equal to $\pm 1$ which differ from $P$ in exactly one coordinate. Since there are more than $2^{n+1}/n$ points in $B$, and each $S_P$ has $n$ elements, the cardinalities of the sets $S_P$ add up to more than $2^{n+1}$, which is to say, more than twice the total number of points. By the pigeonhole principle, there must be a point in three of the sets, say $S_P, S_Q, S_R$. But then any two of $P, Q, R$ differ in exactly two coordinates, so $PQR$ is an equilateral triangle, as desired.

# The 62nd William Lowell Putnam Mathematical Competition
# Saturday, December 1, 2001

A1 Consider a set $S$ and a binary operation $*$, i.e., for each $a,b \in S$, $a*b \in S$. Assume $(a*b)*a = b$ for all $a,b \in S$. Prove that $a*(b*a) = b$ for all $a,b \in S$.

A2 You have coins $C_1, C_2, \ldots, C_n$. For each $k$, $C_k$ is biased so that, when tossed, it has probability $1/(2k+1)$ of falling heads. If the $n$ coins are tossed, what is the probability that the number of heads is odd? Express the answer as a rational function of $n$.

A3 For each integer $m$, consider the polynomial

$$P_m(x) = x^4 - (2m+4)x^2 + (m-2)^2.$$

For what values of $m$ is $P_m(x)$ the product of two non-constant polynomials with integer coefficients?

A4 Triangle $ABC$ has an area 1. Points $E, F, G$ lie, respectively, on sides $BC$, $CA$, $AB$ such that $AE$ bisects $BF$ at point $R$, $BF$ bisects $CG$ at point $S$, and $CG$ bisects $AE$ at point $T$. Find the area of the triangle $RST$.

A5 Prove that there are unique positive integers $a$, $n$ such that $a^{n+1} - (a+1)^n = 2001$.

A6 Can an arc of a parabola inside a circle of radius 1 have a length greater than 4?

B1 Let $n$ be an even positive integer. Write the numbers $1, 2, \ldots, n^2$ in the squares of an $n \times n$ grid so that the $k$-th row, from left to right, is

$$(k-1)n+1, (k-1)n+2, \ldots, (k-1)n+n.$$

Color the squares of the grid so that half of the squares in each row and in each column are red and the other half are black (a checkerboard coloring is one possibility). Prove that for each coloring, the sum of the numbers on the red squares is equal to the sum of the numbers on the black squares.

B2 Find all pairs of real numbers $(x,y)$ satisfying the system of equations

$$\frac{1}{x} + \frac{1}{2y} = (x^2+3y^2)(3x^2+y^2)$$
$$\frac{1}{x} - \frac{1}{2y} = 2(y^4 - x^4).$$

B3 For any positive integer $n$, let $\langle n \rangle$ denote the closest integer to $\sqrt{n}$. Evaluate

$$\sum_{n=1}^{\infty} \frac{2^{\langle n \rangle} + 2^{-\langle n \rangle}}{2^n}.$$

B4 Let $S$ denote the set of rational numbers different from $\{-1, 0, 1\}$. Define $f : S \to S$ by $f(x) = x - 1/x$. Prove or disprove that

$$\bigcap_{n=1}^{\infty} f^{(n)}(S) = \emptyset,$$

where $f^{(n)}$ denotes $f$ composed with itself $n$ times.

B5 Let $a$ and $b$ be real numbers in the interval $(0, 1/2)$, and let $g$ be a continuous real-valued function such that $g(g(x)) = ag(x) + bx$ for all real $x$. Prove that $g(x) = cx$ for some constant $c$.

B6 Assume that $(a_n)_{n \geq 1}$ is an increasing sequence of positive real numbers such that $\lim a_n/n = 0$. Must there exist infinitely many positive integers $n$ such that $a_{n-i} + a_{n+i} < 2a_n$ for $i = 1, 2, \ldots, n-1$?

# Solutions to the 62nd William Lowell Putnam Mathematical Competition
# Saturday, December 1, 2001

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A–1 The hypothesis implies $((b*a)*b)*(b*a)=b$ for all $a,b\in S$ (by replacing $a$ by $b*a$), and hence $a*(b*a)=b$ for all $a,b\in S$ (using $(b*a)*b=a$).

A–2 Let $P_n$ denote the desired probability. Then $P_1=1/3$, and, for $n>1$,

$$\begin{aligned} P_n &= \left(\frac{2n}{2n+1}\right)P_{n-1}+\left(\frac{1}{2n+1}\right)(1-P_{n-1}) \\ &= \left(\frac{2n-1}{2n+1}\right)P_{n-1}+\frac{1}{2n+1}. \end{aligned}$$

The recurrence yields $P_2=2/5$, $P_3=3/7$, and by a simple induction, one then checks that for general $n$ one has $P_n=n/(2n+1)$.

Note: Richard Stanley points out the following noninductive argument. Put $f(x)=\prod_{k=1}^n(x+2k)/(2k+1)$; then the coefficient of $x^i$ in $f(x)$ is the probability of getting exactly $i$ heads. Thus the desired number is $(f(1)-f(-1))/2$, and both values of $f$ can be computed directly: $f(1)=1$, and

$$f(-1)=\frac{1}{3}\times\frac{3}{5}\times\cdots\times\frac{2n-1}{2n+1}=\frac{1}{2n+1}.$$

A–3 By the quadratic formula, if $P_m(x)=0$, then $x^2=m\pm 2\sqrt{2m}+2$, and hence the four roots of $P_m$ are given by $S=\{\pm\sqrt{m}\pm\sqrt{2}\}$. If $P_m$ factors into two nonconstant polynomials over the integers, then some subset of $S$ consisting of one or two elements form the roots of a polynomial with integer coefficients.

First suppose this subset has a single element, say $\sqrt{m}\pm\sqrt{2}$; this element must be a rational number. Then $(\sqrt{m}\pm\sqrt{2})^2=2+m\pm 2\sqrt{2m}$ is an integer, so $m$ is twice a perfect square, say $m=2n^2$. But then $\sqrt{m}\pm\sqrt{2}=(n\pm 1)\sqrt{2}$ is only rational if $n=\pm 1$, i.e., if $m=2$.

Next, suppose that the subset contains two elements; then we can take it to be one of $\{\sqrt{m}\pm\sqrt{2}\}$, $\{\sqrt{2}\pm\sqrt{m}\}$ or $\{\pm(\sqrt{m}+\sqrt{2})\}$. In all cases, the sum and the product of the elements of the subset must be a rational number. In the first case, this means $2\sqrt{m}\in\mathbb{Q}$, so $m$ is a perfect square. In the second case, we have $2\sqrt{2}\in\mathbb{Q}$, contradiction. In the third case, we have $(\sqrt{m}+\sqrt{2})^2\in\mathbb{Q}$, or $m+2+2\sqrt{2m}\in\mathbb{Q}$, which means that $m$ is twice a perfect square.

We conclude that $P_m(x)$ factors into two nonconstant polynomials over the integers if and only if $m$ is either a square or twice a square.

Note: a more sophisticated interpretation of this argument can be given using Galois theory. Namely, if $m$ is neither a square nor twice a square, then the number fields $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{2})$ are distinct quadratic fields, so their compositum is a number field of degree 4, whose Galois group acts transitively on $\{\pm\sqrt{m}\pm\sqrt{2}\}$. Thus $P_m$ is irreducible.

A–4 Choose $r,s,t$ so that $EC=rBC, FA=sCA, GB=tCB$, and let $[XYZ]$ denote the area of triangle $XYZ$. Then $[ABE]=[AFE]$ since the triangles have the same altitude and base. Also $[ABE]=(BE/BC)[ABC]=1-r$, and $[ECF]=(EC/BC)(CF/CA)[ABC]=r(1-s)$ (e.g., by the law of sines). Adding this all up yields

$$\begin{aligned} 1 &= [ABE]+[ABF]+[ECF] \\ &= 2(1-r)+r(1-s)=2-r-rs \end{aligned}$$

or $r(1+s)=1$. Similarly $s(1+t)=t(1+r)=1$.

Let $f:[0,\infty)\to[0,\infty)$ be the function given by $f(x)=1/(1+x)$; then $f(f(f(r)))=r$. However, $f(x)$ is strictly decreasing in $x$, so $f(f(x))$ is increasing and $f(f(f(x)))$ is decreasing. Thus there is at most one $x$ such that $f(f(f(x)))=x$; in fact, since the equation $f(z)=z$ has a positive root $z=(-1+\sqrt{5})/2$, we must have $r=s=t=z$.

We now compute $[ABF]=(AF/AC)[ABC]=z$, $[ABR]=(BR/BF)[ABF]=z/2$, analogously $[BCS]=[CAT]=z/2$, and $[RST]=|[ABC]-[ABR]-[BCS]-[CAT]|=|1-3z/2|=\frac{7-3\sqrt{5}}{4}$.

Note: the key relation $r(1+s)=1$ can also be derived by computing using homogeneous coordinates or vectors.

A–5 Suppose $a^{n+1}-(a+1)^n=2001$. Notice that $a^{n+1}+[(a+1)^n-1]$ is a multiple of $a$; thus $a$ divides $2002=2\times 7\times 11\times 13$.

Since 2001 is divisible by 3, we must have $a\equiv 1 \pmod 3$, otherwise one of $a^{n+1}$ and $(a+1)^n$ is a multiple of 3 and the other is not, so their difference cannot be divisible by 3. Now $a^{n+1}\equiv 1 \pmod 3$, so we must have $(a+1)^n\equiv 1 \pmod 3$, which forces $n$ to be even, and in particular at least 2.

If $a$ is even, then $a^{n+1}-(a+1)^n\equiv-(a+1)^n \pmod 4$. Since $n$ is even, $-(a+1)^n\equiv -1 \pmod 4$. Since $2001\equiv 1 \pmod 4$, this is impossible. Thus $a$ is odd, and so must divide $1001=7\times 11\times 13$. Moreover, $a^{n+1}-(a+1)^n\equiv a \pmod 4$, so $a\equiv 1 \pmod 4$.

Of the divisors of $7\times 11\times 13$, those congruent to 1 mod 3 are precisely those not divisible by 11 (since 7 and 13 are both congruent to 1 mod 3). Thus $a$ divides $7\times 13$. Now $a\equiv 1 \pmod 4$ is only possible if $a$ divides 13.

We cannot have $a = 1$, since $1 - 2^n \neq 2001$ for any $n$. Thus the only possibility is $a = 13$. One easily checks that $a = 13, n = 2$ is a solution; all that remains is to check that no other $n$ works. In fact, if $n > 2$, then $13^{n+1} \equiv 2001 \equiv 1 \pmod 8$. But $13^{n+1} \equiv 13 \pmod 8$ since $n$ is even, contradiction. Thus $a = 13, n = 2$ is the unique solution.

Note: once one has that $n$ is even, one can use that $2002 = a^{n+1} + 1 - (a+1)^n$ is divisible by $a+1$ to rule out cases.

A–6 The answer is yes. Consider the arc of the parabola $y = Ax^2$ inside the circle $x^2 + (y-1)^2 = 1$, where we initially assume that $A > 1/2$. This intersects the circle in three points, $(0,0)$ and $(\pm\sqrt{2A-1}/A, (2A-1)/A)$. We claim that for $A$ sufficiently large, the length $L$ of the parabolic arc between $(0,0)$ and $(\sqrt{2A-1}/A, (2A-1)/A)$ is greater than 2, which implies the desired result by symmetry. We express $L$ using the usual formula for arclength:

$$\begin{aligned} L &= \int_0^{\sqrt{2A-1}/A} \sqrt{1+(2Ax)^2}\,dx \\ &= \frac{1}{2A}\int_0^{2\sqrt{2A-1}} \sqrt{1+x^2}\,dx \\ &= 2 + \frac{1}{2A}\left(\int_0^{2\sqrt{2A-1}} (\sqrt{1+x^2}-x)\,dx - 2\right), \end{aligned}$$

where we have artificially introduced $-x$ into the integrand in the last step. Now, for $x \geq 0$,

$$\sqrt{1+x^2} - x = \frac{1}{\sqrt{1+x^2}+x} > \frac{1}{2\sqrt{1+x^2}} \geq \frac{1}{2(x+1)};$$

since $\int_0^\infty dx/(2(x+1))$ diverges, so does $\int_0^\infty (\sqrt{1+x^2} - x)\,dx$. Hence, for sufficiently large $A$, we have $\int_0^{2\sqrt{2A-1}} (\sqrt{1+x^2}-x)\,dx > 2$, and hence $L > 2$.

Note: a numerical computation shows that one must take $A > 34.7$ to obtain $L > 2$, and that the maximum value of $L$ is about 4.0027, achieved for $A \approx 94.1$.

B–1 Let $R$ (resp. $B$) denote the set of red (resp. black) squares in such a coloring, and for $s \in R \cup B$, let $f(s)n + g(s) + 1$ denote the number written in square $s$, where $0 \leq f(s), g(s) \leq n-1$. Then it is clear that the value of $f(s)$ depends only on the row of $s$, while the value of $g(s)$ depends only on the column of $s$. Since every row contains exactly $n/2$ elements of $R$ and $n/2$ elements of $B$,

$$\sum_{s\in R} f(s) = \sum_{s\in B} f(s).$$

Similarly, because every column contains exactly $n/2$ elements of $R$ and $n/2$ elements of $B$,

$$\sum_{s\in R} g(s) = \sum_{s\in B} g(s).$$

It follows that

$$\sum_{s\in R} f(s)n + g(s) + 1 = \sum_{s\in B} f(s)n + g(s) + 1,$$

as desired.

Note: Richard Stanley points out a theorem of Ryser (see Ryser, *Combinatorial Mathematics*, Theorem 3.1) that can also be applied. Namely, if $A$ and $B$ are $0-1$ matrices with the same row and column sums, then there is a sequence of operations on $2\times 2$ matrices of the form

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

or vice versa, which transforms $A$ into $B$. If we identify 0 and 1 with red and black, then the given coloring and the checkerboard coloring both satisfy the sum condition. Since the desired result is clearly true for the checkerboard coloring, and performing the matrix operations does not affect this, the desired result follows in general.

B–2 By adding and subtracting the two given equations, we obtain the equivalent pair of equations

$$\begin{aligned} 2/x &= x^4 + 10x^2y^2 + 5y^4 \\ 1/y &= 5x^4 + 10x^2y^2 + y^4. \end{aligned}$$

Multiplying the former by $x$ and the latter by $y$, then adding and subtracting the two resulting equations, we obtain another pair of equations equivalent to the given ones,

$$3 = (x+y)^5, \qquad 1 = (x-y)^5.$$

It follows that $x = (3^{1/5}+1)/2$ and $y = (3^{1/5}-1)/2$ is the unique solution satisfying the given equations.

B–3 Since $(k-1/2)^2 = k^2 - k + 1/4$ and $(k+1/2)^2 = k^2 + k + 1/4$, we have that $\langle n\rangle = k$ if and only if $k^2 - k + 1 \leq n \leq k^2 + k$. Hence

$$\begin{aligned} \sum_{n=1}^\infty \frac{2^{\langle n\rangle} + 2^{-\langle n\rangle}}{2^n} &= \sum_{k=1}^\infty \sum_{n, \langle n\rangle = k} \frac{2^{\langle n\rangle} + 2^{-\langle n\rangle}}{2^n} \\ &= \sum_{k=1}^\infty \sum_{n=k^2-k+1}^{k^2+k} \frac{2^k + 2^{-k}}{2^n} \\ &= \sum_{k=1}^\infty (2^k + 2^{-k})(2^{-k^2+k} - 2^{-k^2-k}) \\ &= \sum_{k=1}^\infty (2^{-k(k-2)} - 2^{-k(k+2)}) \\ &= \sum_{k=1}^\infty 2^{-k(k-2)} - \sum_{k=3}^\infty 2^{-k(k-2)} \\ &= 3. \end{aligned}$$

Alternate solution: rewrite the sum as $\sum_{n=1}^{\infty} 2^{-(n+\langle n\rangle)} + \sum_{n=1}^{\infty} 2^{-(n-\langle n\rangle)}$. Note that $\langle n\rangle \neq \langle n+1\rangle$ if and only if $n = m^2+m$ for some $m$. Thus $n+\langle n\rangle$ and $n-\langle n\rangle$ each increase by 1 except at $n = m^2+m$, where the former skips from $m^2+2m$ to $m^2+2m+2$ and the latter repeats the value $m^2$. Thus the sums are

$$\sum_{n=1}^{\infty} 2^{-n} - \sum_{m=1}^{\infty} 2^{-m^2} + \sum_{n=0}^{\infty} 2^{-n} + \sum_{m=1}^{\infty} 2^{-m^2} = 2+1 = 3.$$

B–4 For a rational number $p/q$ expressed in lowest terms, define its *height* $H(p/q)$ to be $|p|+|q|$. Then for any $p/q \in S$ expressed in lowest terms, we have $H(f(p/q)) = |q^2-p^2|+|pq|$; since by assumption $p$ and $q$ are nonzero integers with $|p| \neq |q|$, we have

$$\begin{aligned} H(f(p/q)) - H(p/q) &= |q^2-p^2| + |pq| - |p| - |q| \\ &\geq 3 + |pq| - |p| - |q| \\ &= (|p|-1)(|q|-1) + 2 \geq 2. \end{aligned}$$

It follows that $f^{(n)}(S)$ consists solely of numbers of height strictly larger than $2n+2$, and hence

$$\cap_{n=1}^{\infty} f^{(n)}(S) = \emptyset.$$

Note: many choices for the height function are possible: one can take $H(p/q) = \max|p|,|q|$, or $H(p/q)$ equal to the total number of prime factors of $p$ and $q$, and so on. The key properties of the height function are that on one hand, there are only finitely many rationals with height below any finite bound, and on the other hand, the height function is a sufficiently "algebraic" function of its argument that one can relate the heights of $p/q$ and $f(p/q)$.

B–5 Note that $g(x) = g(y)$ implies that $g(g(x)) = g(g(y))$ and hence $x = y$ from the given equation. That is, $g$ is injective. Since $g$ is also continuous, $g$ is either strictly increasing or strictly decreasing. Moreover, $g$ cannot tend to a finite limit $L$ as $x \to +\infty$, or else we'd have $g(g(x)) - ag(x) = bx$, with the left side bounded and the right side unbounded. Similarly, $g$ cannot tend to a finite limit as $x \to -\infty$. Together with monotonicity, this yields that $g$ is also surjective.

Pick $x_0$ arbitrary, and define $x_n$ for all $n \in \mathbb{Z}$ recursively by $x_{n+1} = g(x_n)$ for $n > 0$, and $x_{n-1} = g^{-1}(x_n)$ for $n < 0$. Let $r_1 = (a+\sqrt{a^2+4b})/2$ and $r_2 = (a-\sqrt{a^2+4b})/2$ and $r_2$ be the roots of $x^2-ax-b = 0$, so that $r_1 > 0 > r_2$ and $1 > |r_1| > |r_2|$. Then there exist $c_1, c_2 \in \mathbb{R}$ such that $x_n = c_1 r_1^n + c_2 r_2^n$ for all $n \in \mathbb{Z}$.

Suppose $g$ is strictly increasing. If $c_2 \neq 0$ for some choice of $x_0$, then $x_n$ is dominated by $r_2^n$ for $n$ sufficiently negative. But taking $x_n$ and $x_{n+2}$ for $n$ sufficiently negative of the right parity, we get $0 < x_n < x_{n+2}$ but $g(x_n) > g(x_{n+2})$, contradiction. Thus $c_2 = 0$; since $x_0 = c_1$ and $x_1 = c_1 r_1$, we have $g(x) = r_1 x$ for all $x$. Analogously, if $g$ is strictly decreasing, then $c_2 = 0$ or else $x_n$ is dominated by $r_1^n$ for $n$ sufficiently positive. But taking $x_n$ and $x_{n+2}$ for $n$ sufficiently positive of the right parity, we get $0 < x_{n+2} < x_n$ but $g(x_{n+2}) < g(x_n)$, contradiction. Thus in that case, $g(x) = r_2 x$ for all $x$.

B–6 Yes, there must exist infinitely many such $n$. Let $S$ be the convex hull of the set of points $(n, a_n)$ for $n \geq 0$. Geometrically, $S$ is the intersection of all convex sets (or even all halfplanes) containing the points $(n, a_n)$; algebraically, $S$ is the set of points $(x, y)$ which can be written as $c_1(n_1, a_{n_1}) + \cdots + c_k(n_k, a_{n_k})$ for some $c_1, \ldots, c_k$ which are nonnegative of sum 1.

We prove that for infinitely many $n$, $(n, a_n)$ is a vertex on the upper boundary of $S$, and that these $n$ satisfy the given condition. The condition that $(n, a_n)$ is a vertex on the upper boundary of $S$ is equivalent to the existence of a line passing through $(n, a_n)$ with all other points of $S$ below it. That is, there should exist $m > 0$ such that

$$a_k < a_n + m(k-n) \qquad \forall k \geq 1. \tag{1}$$

We first show that $n = 1$ satisfies (1). The condition $a_k/k \to 0$ as $k \to \infty$ implies that $(a_k - a_1)/(k-1) \to 0$ as well. Thus the set $\{(a_k - a_1)/(k-1)\}$ has an upper bound $m$, and now $a_k \leq a_1 + m(k-1)$, as desired.

Next, we show that given one $n$ satisfying (1), there exists a larger one also satisfying (1). Again, the condition $a_k/k \to 0$ as $k \to \infty$ implies that $(a_k - a_n)/(k-n) \to 0$ as $k \to \infty$. Thus the sequence $\{(a_k - a_n)/(k-n)\}_{k>n}$ has a maximum element; suppose $k = r$ is the largest value that achieves this maximum, and put $m = (a_r - a_n)/(r-n)$. Then the line through $(r, a_r)$ of slope $m$ lies strictly above $(k, a_k)$ for $k > r$ and passes through or lies above $(k, a_k)$ for $k < r$. Thus (1) holds for $n = r$ with $m$ replaced by $m - \varepsilon$ for suitably small $\varepsilon > 0$.

By induction, we have that (1) holds for infinitely many $n$. For any such $n$ there exists $m > 0$ such that for $i = 1, \ldots, n-1$, the points $(n-i, a_{n-i})$ and $(n+i, a_{n+i})$ lie below the line through $(n, a_n)$ of slope $m$. That means $a_{n+i} < a_n + mi$ and $a_{n-i} < a_n - mi$; adding these together gives $a_{n-i} + a_{n+i} < 2a_n$, as desired.

# The 63rd William Lowell Putnam Mathematical Competition
## Saturday, December 7, 2002

A1 Let $k$ be a fixed positive integer. The $n$-th derivative of $\frac{1}{x^k-1}$ has the form $\frac{P_n(x)}{(x^k-1)^{n+1}}$ where $P_n(x)$ is a polynomial. Find $P_n(1)$.

A2 Given any five points on a sphere, show that some four of them must lie on a closed hemisphere.

A3 Let $n \geq 2$ be an integer and $T_n$ be the number of non-empty subsets $S$ of $\{1,2,3,\ldots,n\}$ with the property that the average of the elements of $S$ is an integer. Prove that $T_n - n$ is always even.

A4 In Determinant Tic-Tac-Toe, Player 1 enters a 1 in an empty $3 \times 3$ matrix. Player 0 counters with a 0 in a vacant position, and play continues in turn until the $3 \times 3$ matrix is completed with five 1's and four 0's. Player 0 wins if the determinant is 0 and player 1 wins otherwise. Assuming both players pursue optimal strategies, who will win and how?

A5 Define a sequence by $a_0 = 1$, together with the rules $a_{2n+1} = a_n$ and $a_{2n+2} = a_n + a_{n+1}$ for each integer $n \geq 0$. Prove that every positive rational number appears in the set

$$\left\{ \frac{a_{n-1}}{a_n} : n \geq 1 \right\} = \left\{ \frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{2}, \ldots \right\}.$$

A6 Fix an integer $b \geq 2$. Let $f(1) = 1$, $f(2) = 2$, and for each $n \geq 3$, define $f(n) = nf(d)$, where $d$ is the number of base-$b$ digits of $n$. For which values of $b$ does

$$\sum_{n=1}^{\infty} \frac{1}{f(n)}$$

converge?

B1 Shanille O'Keal shoots free throws on a basketball court. She hits the first and misses the second, and thereafter the probability that she hits the next shot is equal to the proportion of shots she has hit so far. What is the probability she hits exactly 50 of her first 100 shots?

B2 Consider a polyhedron with at least five faces such that exactly three edges emerge from each of its vertices. Two players play the following game:

> Each player, in turn, signs his or her name on a previously unsigned face. The winner is the player who first succeeds in signing three faces that share a common vertex.

Show that the player who signs first will always win by playing as well as possible.

B3 Show that, for all integers $n > 1$,

$$\frac{1}{2ne} < \frac{1}{e} - \left(1 - \frac{1}{n}\right)^n < \frac{1}{ne}.$$

B4 An integer $n$, unknown to you, has been randomly chosen in the interval $[1, 2002]$ with uniform probability. Your objective is to select $n$ in an **odd** number of guesses. After each incorrect guess, you are informed whether $n$ is higher or lower, and you **must** guess an integer on your next turn among the numbers that are still feasibly correct. Show that you have a strategy so that the chance of winning is greater than $2/3$.

B5 A palindrome in base $b$ is a positive integer whose base-$b$ digits read the same backwards and forwards; for example, 2002 is a 4-digit palindrome in base 10. Note that 200 is not a palindrome in base 10, but it is the 3-digit palindrome 242 in base 9, and 404 in base 7. Prove that there is an integer which is a 3-digit palindrome in base $b$ for at least 2002 different values of $b$.

B6 Let $p$ be a prime number. Prove that the determinant of the matrix

$$\begin{pmatrix} x & y & z \\ x^p & y^p & z^p \\ x^{p^2} & y^{p^2} & z^{p^2} \end{pmatrix}$$

is congruent modulo $p$ to a product of polynomials of the form $ax + by + cz$, where $a, b, c$ are integers. (We say two integer polynomials are congruent modulo $p$ if corresponding coefficients are congruent modulo $p$.)

# Solutions to the 63rd William Lowell Putnam Mathematical Competition
# Saturday, December 7, 2002

Kiran Kedlaya and Lenny Ng

A–1 By differentiating $P_n(x)/(x^k-1)^{n+1}$, we find that $P_{n+1}(x) = (x^k-1)P_n'(x) - (n+1)kx^{k-1}P_n(x)$; substituting $x=1$ yields $P_{n+1}(1) = -(n+1)kP_n(1)$. Since $P_0(1)=1$, an easy induction gives $P_n(1) = (-k)^n n!$ for all $n \geq 0$.

Note: one can also argue by expanding in Taylor series around 1. Namely, we have

$$\frac{1}{x^k-1} = \frac{1}{k(x-1)+\cdots} = \frac{1}{k}(x-1)^{-1} + \cdots,$$

so

$$\frac{d^n}{dx^n}\frac{1}{x^k-1} = \frac{(-1)^n n!}{k(x-1)^{-n-1}}$$

and

$$\begin{aligned} P_n(x) &= (x^k-1)^{n+1}\frac{d^n}{dx^n}\frac{1}{x^k-1} \\ &= (k(x-1)+\cdots)^{n+1}\left(\frac{(-1)^n n!}{k}(x-1)^{-n-1}+\cdots\right) \\ &= (-k)^n n! + \cdots. \end{aligned}$$

A–2 Draw a great circle through two of the points. There are two closed hemispheres with this great circle as boundary, and each of the other three points lies in one of them. By the pigeonhole principle, two of those three points lie in the same hemisphere, and that hemisphere thus contains four of the five given points.

Note: by a similar argument, one can prove that among any $n+3$ points on an $n$-dimensional sphere, some $n+2$ of them lie on a closed hemisphere. (One cannot get by with only $n+2$ points: put them at the vertices of a regular simplex.) Namely, any $n$ of the points lie on a great sphere, which forms the boundary of two hemispheres; of the remaining three points, some two lie in the same hemisphere.

A–3 Note that each of the sets $\{1\},\{2\},\dots,\{n\}$ has the desired property. Moreover, for each set $S$ with integer average $m$ that does not contain $m$, $S \cup \{m\}$ also has average $m$, while for each set $T$ of more than one element with integer average $m$ that contains $m$, $T \setminus \{m\}$ also has average $m$. Thus the subsets other than $\{1\},\{2\},\dots,\{n\}$ can be grouped in pairs, so $T_n - n$ is even.

A–4 (partly due to David Savitt) Player 0 wins with optimal play. In fact, we prove that Player 1 cannot prevent Player 0 from creating a row of all zeroes, a column of all zeroes, or a $2 \times 2$ submatrix of all zeroes. Each of these forces the determinant of the matrix to be zero.

For $i,j = 1,2,3$, let $A_{ij}$ denote the position in row $i$ and column $j$. Without loss of generality, we may assume that Player 1's first move is at $A_{11}$. Player 0 then plays at $A_{22}$:

$$\begin{pmatrix} 1 & * & * \\ * & 0 & * \\ * & * & * \end{pmatrix}$$

After Player 1's second move, at least one of $A_{23}$ and $A_{32}$ remains vacant. Without loss of generality, assume $A_{23}$ remains vacant; Player 0 then plays there.

After Player 1's third move, Player 0 wins by playing at $A_{21}$ if that position is unoccupied. So assume instead that Player 1 has played there. Thus of Player 1's three moves so far, two are at $A_{11}$ and $A_{21}$. Hence for $i$ equal to one of 1 or 3, and for $j$ equal to one of 2 or 3, the following are both true:

(a) The $2 \times 2$ submatrix formed by rows 2 and $i$ and by columns 2 and 3 contains two zeroes and two empty positions.

(b) Column $j$ contains one zero and two empty positions.

Player 0 next plays at $A_{ij}$. To prevent a zero column, Player 1 must play in column $j$, upon which Player 0 completes the $2 \times 2$ submatrix in (a) for the win.

Note: one can also solve this problem directly by making a tree of possible play sequences. This tree can be considerably collapsed using symmetries: the symmetry between rows and columns, the invariance of the outcome under reordering of rows or columns, and the fact that the scenario after a sequence of moves does not depend on the order of the moves (sometimes called "transposition invariance").

Note (due to Paul Cheng): one can reduce Determinant Tic-Tac-Toe to a variant of ordinary tic-tac-toe. Namely, consider a tic-tac-toe grid labeled as follows:

| | | |
|---|---|---|
| $A_{11}$ | $A_{22}$ | $A_{33}$ |
| $A_{23}$ | $A_{31}$ | $A_{12}$ |
| $A_{32}$ | $A_{13}$ | $A_{21}$ |

Then each term in the expansion of the determinant occurs in a row or column of the grid. Suppose Player 1 first plays in the top left. Player 0 wins by playing first in the top row, and second in the left column. Then there are only one row and column left for Player 1 to threaten, and Player 1 cannot already threaten both on the third move, so Player 0 has time to block both.

A–5 It suffices to prove that for any relatively prime positive integers $r,s$, there exists an integer $n$ with $a_n = r$ and $a_{n+1} = s$. We prove this by induction on $r+s$, the case $r+s = 2$ following from the fact that $a_0 = a_1 = 1$. Given $r$ and $s$ not both 1 with $\gcd(r,s) = 1$, we must have $r \neq s$. If $r > s$, then by the induction hypothesis we have $a_n = r-s$ and $a_{n+1} = s$ for some $n$; then $a_{2n+2} = r$ and $a_{2n+3} = s$. If $r < s$, then we have $a_n = r$ and $a_{n+1} = s-r$ for some $n$; then $a_{2n+1} = r$ and $a_{2n+2} = s$.

Note: a related problem is as follows. Starting with the sequence

$$\frac{0}{1}, \frac{1}{0},$$

repeat the following operation: insert between each pair $\frac{a}{b}$ and $\frac{c}{d}$ the pair $\frac{a+c}{b+d}$. Prove that each positive rational number eventually appears.

Observe that by induction, if $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive terms in the sequence, then $bc - ad = 1$. The same holds for consecutive terms of the $n$-th *Farey sequence*, the sequence of rational numbers in $[0,1]$ with denominator (in lowest terms) at most $n$.

A–6 The sum converges for $b = 2$ and diverges for $b \geq 3$. We first consider $b \geq 3$. Suppose the sum converges; then the fact that $f(n) = nf(d)$ whenever $b^{d-1} \leq n \leq b^d - 1$ yields

$$\sum_{n=1}^{\infty} \frac{1}{f(n)} = \sum_{d=1}^{\infty} \frac{1}{f(d)} \sum_{n=b^{d-1}}^{b^d-1} \frac{1}{n}. \qquad (1)$$

However, by comparing the integral of $1/x$ with a Riemann sum, we see that

$$\begin{aligned}\sum_{n=b^{d-1}}^{b^d-1} \frac{1}{n} &> \int_{b^{d-1}}^{b^d} \frac{dx}{x} \\ &= \log(b^d) - \log(b^{d-1}) = \log b,\end{aligned}$$

where log denotes the natural logarithm. Thus (1) yields

$$\sum_{n=1}^{\infty} \frac{1}{f(n)} > (\log b) \sum_{n=1}^{\infty} \frac{1}{f(n)},$$

a contradiction since $\log b > 1$ for $b \geq 3$. Therefore the sum diverges.

For $b = 2$, we have a slightly different identity because $f(2) \neq 2f(2)$. Instead, for any positive integer $i$, we have

$$\sum_{n=1}^{2^i-1} \frac{1}{f(n)} = 1 + \frac{1}{2} + \frac{1}{6} + \sum_{d=3}^{i} \frac{1}{f(d)} \sum_{n=2^{d-1}}^{2^d-1} \frac{1}{n}. \qquad (2)$$

Again comparing an integral to a Riemann sum, we see that for $d \geq 3$,

$$\begin{aligned}\sum_{n=2^{d-1}}^{2^d-1} \frac{1}{n} &< \frac{1}{2^{d-1}} - \frac{1}{2^d} + \int_{2^{d-1}}^{2^d} \frac{dx}{x} \\ &= \frac{1}{2^d} + \log 2 \\ &\leq \frac{1}{8} + \log 2 < 0.125 + 0.7 < 1.\end{aligned}$$

Put $c = \frac{1}{8} + \log 2$ and $L = 1 + \frac{1}{2} + \frac{1}{6(1-c)}$. Then we can prove that $\sum_{n=1}^{2^i-1} \frac{1}{f(n)} < L$ for all $i \geq 2$ by induction on $i$. The case $i = 2$ is clear. For the induction, note that by (2),

$$\begin{aligned}\sum_{n=1}^{2^i-1} \frac{1}{f(n)} &< 1 + \frac{1}{2} + \frac{1}{6} + c \sum_{d=3}^{i} \frac{1}{f(d)} \\ &< 1 + \frac{1}{2} + \frac{1}{6} + c\frac{1}{6(1-c)} \\ &= 1 + \frac{1}{2} + \frac{1}{6(1-c)} = L,\end{aligned}$$

as desired. We conclude that $\sum_{n=1}^{\infty} \frac{1}{f(n)}$ converges to a limit less than or equal to $L$.

Note: the above argument proves that the sum for $b = 2$ is at most $L < 2.417$. One can also obtain a lower bound by the same technique, namely $1 + \frac{1}{2} + \frac{1}{6(1-c')}$ with $c' = \log 2$. This bound exceeds 2.043. (By contrast, summing the first 100000 terms of the series only yields a lower bound of 1.906.) Repeating the same arguments with $d \geq 4$ as the cutoff yields the upper bound 2.185 and the lower bound 2.079.

B–1 The probability is $1/99$. In fact, we show by induction on $n$ that after $n$ shots, the probability of having made any number of shots from 1 to $n-1$ is equal to $1/(n-1)$. This is evident for $n = 2$. Given the result for $n$, we see that the probability of making $i$ shots after $n+1$ attempts is

$$\begin{aligned}\frac{i-1}{n}\frac{1}{n-1} + \left(1 - \frac{i}{n}\right)\frac{1}{n-1} &= \frac{(i-1)+(n-i)}{n(n-1)} \\ &= \frac{1}{n},\end{aligned}$$

as claimed.

B–2 (Note: the problem statement assumes that all polyhedra are connected and that no two edges share more than one face, so we will do likewise. In particular, these are true for all convex polyhedra.) We show that in fact the first player can win on the third move. Suppose the polyhedron has a face $A$ with at least four edges. If the first player plays there first, after the second player's first move there will be three consecutive faces $B,C,D$ adjacent to $A$ which are all unoccupied. The first player wins by playing in $C$; after the second player's second move, at least one of $B$ and $D$ remains unoccupied, and either is a winning move for the first player.

It remains to show that the polyhedron has a face with at least four edges. (Thanks to Russ Mann for suggesting the following argument.) Suppose on the contrary that each face has only three edges. Starting with any face $F_1$ with vertices $v_1, v_2, v_3$, let $v_4$ be the other endpoint of the third edge out of $v_1$. Then the faces adjacent to $F_1$ must have vertices $v_1, v_2, v_4$; $v_1, v_3, v_4$; and $v_2, v_3, v_4$. Thus $v_1, v_2, v_3, v_4$ form a polyhedron by themselves, contradicting the fact that the given polyhedron is connected and has at least five vertices. (One can also deduce this using Euler's formula $V - E + F = 2 - 2g$, where $V, E, F$ are the numbers of vertices, edges and faces, respectively, and $g$ is the genus of the polyhedron. For a convex polyhedron, $g = 0$ and you get the "usual" Euler's formula.)

Note: Walter Stromquist points out the following counterexample if one relaxes the assumption that a pair of faces may not share multiple edges. Take a tetrahedron and remove a smaller tetrahedron from the center of an edge; this creates two small triangular faces and turns two of the original faces into hexagons. Then the second player can draw by signing one of the hexagons, one of the large triangles, and one of the small triangles. (He does this by "mirroring": wherever the first player signs, the second player signs the other face of the same type.)

B–3 The desired inequalities can be rewritten as

$$1 - \frac{1}{n} < \exp\left(1 + n \log\left(1 - \frac{1}{n}\right)\right) < 1 - \frac{1}{2n}.$$

By taking logarithms, we can rewrite the desired inequalities as

$$\begin{aligned} -\log\left(1 - \frac{1}{2n}\right) &< -1 - n\log\left(1 - \frac{1}{n}\right) \\ &< -\log\left(1 - \frac{1}{n}\right). \end{aligned}$$

Rewriting these in terms of the Taylor expansion of $-\log(1-x)$, we see that the desired result is also equivalent to

$$\sum_{i=1}^{\infty} \frac{1}{i 2^i n^i} < \sum_{i=1}^{\infty} \frac{1}{(i+1)n^i} < \sum_{i=1}^{\infty} \frac{1}{i n^i},$$

which is evident because the inequalities hold term by term.

Note: David Savitt points out that the upper bound can be improved from $1/(ne)$ to $2/(3ne)$ with a slightly more complicated argument. (In fact, for any $c > 1/2$, one has an upper bound of $c/(ne)$, but only for $n$ above a certain bound depending on $c$.)

B–4 Use the following strategy: guess $1, 3, 4, 6, 7, 9, \dots$ until the target number $n$ is revealed to be equal to or lower than one of these guesses. If $n \equiv 1 \pmod 3$, it will be guessed on an odd turn. If $n \equiv 0 \pmod 3$, it will be guessed on an even turn. If $n \equiv 2 \pmod 3$, then $n+1$ will be guessed on an even turn, forcing a guess of $n$ on the next turn. Thus the probability of success with this strategy is $1335/2002 > 2/3$.

Note: for any positive integer $m$, this strategy wins when the number is being guessed from $[1, m]$ with probability $\frac{1}{m}\lfloor\frac{2m+1}{3}\rfloor$. We can prove that this is best possible as follows. Let $a_m$ denote $m$ times the probability of winning when playing optimally. Also, let $b_m$ denote $m$ times the corresponding probability of winning if the objective is to select the number in an even number of guesses instead. (For definiteness, extend the definitions to incorporate $a_0 = 0$ and $b_0 = 0$.)

We first claim that $a_m = 1 + \max_{1 \le k \le m}\{b_{k-1} + b_{m-k}\}$ and $b_m = \max_{1 \le k \le m}\{a_{k-1} + a_{m-k}\}$ for $m \ge 1$. To establish the first recursive identity, suppose that our first guess is some integer $k$. We automatically win if $n = k$, with probability $1/m$. If $n < k$, with probability $(k-1)/m$, then we wish to guess an integer in $[1, k-1]$ in an even number of guesses; the probability of success when playing optimally is $b_{k-1}/(k-1)$, by assumption. Similarly, if $n < k$, with probability $(m-k)/m$, then the subsequent probability of winning is $b_{m-k}/(m-k)$. In sum, the overall probability of winning if $k$ is our first guess is $(1 + b_{k-1} + b_{m-k})/m$. For optimal strategy, we choose $k$ such that this quantity is maximized. (Note that this argument still holds if $k = 1$ or $k = m$, by our definitions of $a_0$ and $b_0$.) The first recursion follows, and the second recursion is established similarly.

We now prove by induction that $a_m = \lfloor (2m+1)/3 \rfloor$ and $b_m = \lfloor 2m/3 \rfloor$ for $m \ge 0$. The inductive step relies on the inequality $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x + y \rfloor$, with equality when one of $x, y$ is an integer. Now suppose that $a_i = \lfloor (2i+1)/3 \rfloor$ and $b_i = \lfloor 2i/3 \rfloor$ for $i < m$. Then

$$\begin{aligned} 1 + b_{k-1} + b_{m-k} &= 1 + \left\lfloor \frac{2(k-1)}{3} \right\rfloor + \left\lfloor \frac{2(m-k)}{3} \right\rfloor \\ &\le \left\lfloor \frac{2m}{3} \right\rfloor \end{aligned}$$

and similarly $a_{k-1} + a_{m-k} \le \lfloor (2m+1)/3 \rfloor$, with equality in both cases attained, e.g., when $k = 1$. The inductive formula for $a_m$ and $b_m$ follows.

B–5 (due to Dan Bernstein) Put $N = 2002!$. Then for $d = 1, \dots, 2002$, the number $N^2$ written in base $b = N/d - 1$ has digits $d^2, 2d^2, d^2$. (Note that these really are digits because $2(2002)^2 < (2002!)^2/2002 - 1$.)

Note: one can also produce an integer $N$ which has base $b$ digits $1, *, 1$ for $n$ different values of $b$, as follows. Choose $c$ with $0 < c < 2^{1/n}$. For $m$ a large positive integer, put $N = 1 + (m+1)\cdots(m+n)\lfloor cm \rfloor^{n-2}$. For $m$ sufficiently large, the bases

$$b = \frac{N-1}{(m+i)m^{n-2}} = \prod_{j \ne i}(m+j)$$

for $i = 1, \ldots, n$ will have the properties that $N \equiv 1 \pmod{b}$ and $b^2 < N < 2b^2$ for $m$ sufficiently large.

Note (due to Russ Mann): one can also give a "nonconstructive" argument. Let $N$ be a large positive integer. For $b \in (N^2, N^3)$, the number of 3-digit base-$b$ palindromes in the range $[b^2, N^6 - 1]$ is at least

$$\left\lfloor \frac{N^6 - b^2}{b} \right\rfloor - 1 \geq \frac{N^6}{b^2} - b - 2,$$

since there is a palindrome in each interval $[kb, (k+1)b - 1]$ for $k = b, \ldots, b^2 - 1$. Thus the average number of bases for which a number in $[1, N^6 - 1]$ is at least

$$\frac{1}{N^6} \sum_{b=N^2+1}^{N^3-1} \left( \frac{N^6}{b} - b - 2 \right) \geq \log(N) - c$$

for some constant $c > 0$. Take $N$ so that the right side exceeds 2002; then at least one number in $[1, N^6 - 1]$ is a base-$b$ palindrome for at least 2002 values of $b$.

B–6 We prove that the determinant is congruent modulo $p$ to

$$x \prod_{i=0}^{p-1} (y + ix) \prod_{i,j=0}^{p-1} (z + ix + jy). \tag{3}$$

We first check that

$$\prod_{i=0}^{p-1} (y + ix) \equiv y^p - x^{p-1} y \pmod{p}. \tag{4}$$

Since both sides are homogeneous as polynomials in $x$ and $y$, it suffices to check (4) for $x = 1$, as a congruence between polynomials. Now note that the right side has $0, 1, \ldots, p-1$ as roots modulo $p$, as does the left side. Moreover, both sides have the same leading coefficient. Since they both have degree only $p$, they must then coincide.

We thus have

$$\begin{aligned}
&x \prod_{i=0}^{p-1} (y + ix) \prod_{i,j=0}^{p-1} (z + ix + jy) \\
&\quad \equiv x(y^p - x^{p-1} y) \prod_{j=0}^{p-1} ((z + jy)^p - x^{p-1}(z + jy)) \\
&\quad \equiv (xy^p - x^p y) \prod_{j=0}^{p-1} (z^p - x^{p-1} z + jy^p - jx^{p-1} y) \\
&\quad \equiv (xy^p - x^p y)((z^p - x^{p-1} z)^p \\
&\qquad - (y^p - x^{p-1} y)^{p-1} (z^p - x^{p-1} z)) \\
&\quad \equiv (xy^p - x^p y)(z^{p^2} - x^{p^2 - p} z^p) \\
&\qquad - x(y^p - x^{p-1} y)^p (z^p - x^{p-1} z) \\
&\quad \equiv xy^p z^{p^2} - x^p y z^{p^2} - x^{p^2 - p + 1} y^p z^p + x^{p^2} y z^p \\
&\qquad - xy^{p^2} z^p + x^{p^2 - p + 1} y^p z^p + x^p y^{p^2} z - x^{p^2} y^p z \\
&\quad \equiv xy^p z^{p^2} + yz^p x^{p^2} + zx^p y^{p^2} \\
&\qquad - xz^p y^{p^2} - yx^p z^{p^2} - zy^p x^{p^2},
\end{aligned}$$

which is precisely the desired determinant.

Note: a simpler conceptual proof is as follows. (Everything in this paragraph will be modulo $p$.) Note that for any integers $a, b, c$, the column vector $[ax + by + cz, (ax + by + cz)^p, (ax + by + cz)^{p^2}]$ is a linear combination of the columns of the given matrix. Thus $ax + by + cz$ divides the determinant. In particular, all of the factors of (3) divide the determinant; since both (3) and the determinant have degree $p^2 + p + 1$, they agree up to a scalar multiple. Moreover, they have the same coefficient of $z^{p^2} y^p x$ (since this term only appears in the expansion of (3) when you choose the first term in each factor). Thus the determinant is congruent to (3), as desired.

Either argument can be used to generalize to a corresponding $n \times n$ determinant, called a Moore determinant; we leave the precise formulation to the reader. Note the similarity with the classical Vandermonde determinant: if $A$ is the $n \times n$ matrix with $A_{ij} = x_i^j$ for $i, j = 0, \ldots, n-1$, then

$$\det(A) = \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

# The 64th William Lowell Putnam Mathematical Competition
# Saturday, December 6, 2003

A1 Let $n$ be a fixed positive integer. How many ways are there to write $n$ as a sum of positive integers,

$$n = a_1 + a_2 + \cdots + a_k,$$

with $k$ an arbitrary positive integer and $a_1 \leq a_2 \leq \cdots \leq a_k \leq a_1 + 1$? For example, with $n = 4$ there are four ways: 4, 2+2, 1+1+2, 1+1+1+1.

A2 Let $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ be nonnegative real numbers. Show that

$$\begin{aligned} &(a_1 a_2 \cdots a_n)^{1/n} + (b_1 b_2 \cdots b_n)^{1/n} \\ &\leq [(a_1+b_1)(a_2+b_2)\cdots(a_n+b_n)]^{1/n}. \end{aligned}$$

A3 Find the minimum value of

$$|\sin x + \cos x + \tan x + \cot x + \sec x + \csc x|$$

for real numbers $x$.

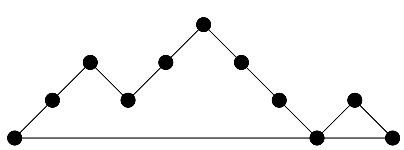
A4 Suppose that $a, b, c, A, B, C$ are real numbers, $a \neq 0$ and $A \neq 0$, such that

$$|ax^2 + bx + c| \leq |Ax^2 + Bx + C|$$

for all real numbers $x$. Show that

$$|b^2 - 4ac| \leq |B^2 - 4AC|.$$

A5 A Dyck $n$-path is a lattice path of $n$ upsteps $(1,1)$ and $n$ downsteps $(1,-1)$ that starts at the origin $O$ and never dips below the $x$-axis. A return is a maximal sequence of contiguous downsteps that terminates on the $x$-axis. For example, the Dyck 5-path illustrated has two returns, of length 3 and 1 respectively.




Show that there is a one-to-one correspondence between the Dyck $n$-paths with no return of even length and the Dyck $(n-1)$-paths.

A6 For a set $S$ of nonnegative integers, let $r_S(n)$ denote the number of ordered pairs $(s_1, s_2)$ such that $s_1 \in S$, $s_2 \in S$, $s_1 \neq s_2$, and $s_1 + s_2 = n$. Is it possible to partition the nonnegative integers into two sets $A$ and $B$ in such a way that $r_A(n) = r_B(n)$ for all $n$ ?

B1 Do there exist polynomials $a(x), b(x), c(y), d(y)$ such that

$$1 + xy + x^2y^2 = a(x)c(y) + b(x)d(y)$$

holds identically?

B2 Let $n$ be a positive integer. Starting with the sequence $1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}$, form a new sequence of $n-1$ entries $\frac{3}{4}, \frac{5}{12}, \ldots, \frac{2n-1}{2n(n-1)}$ by taking the averages of two consecutive entries in the first sequence. Repeat the averaging of neighbors on the second sequence to obtain a third sequence of $n-2$ entries, and continue until the final sequence produced consists of a single number $x_n$. Show that $x_n < 2/n$.

B3 Show that for each positive integer n,

$$n! = \prod_{i=1}^{n} \operatorname{lcm}\{1, 2, \ldots, \lfloor n/i \rfloor\}.$$

(Here lcm denotes the least common multiple, and $\lfloor x \rfloor$ denotes the greatest integer $\leq x$.)

B4 Let $f(z) = az^4 + bz^3 + cz^2 + dz + e = a(z-r_1)(z-r_2)(z-r_3)(z-r_4)$ where $a, b, c, d, e$ are integers, $a \neq 0$. Show that if $r_1 + r_2$ is a rational number and $r_1 + r_2 \neq r_3 + r_4$, then $r_1 r_2$ is a rational number.

B5 Let $A, B$, and $C$ be equidistant points on the circumference of a circle of unit radius centered at $O$, and let $P$ be any point in the circle's interior. Let $a, b, c$ be the distance from $P$ to $A, B, C$, respectively. Show that there is a triangle with side lengths $a, b, c$, and that the area of this triangle depends only on the distance from $P$ to $O$.

B6 Let $f(x)$ be a continuous real-valued function defined on the interval $[0,1]$. Show that

$$\int_0^1 \int_0^1 |f(x) + f(y)| \, dx \, dy \geq \int_0^1 |f(x)| \, dx.$$

# Solutions to the 64th William Lowell Putnam Mathematical Competition
## Saturday, December 6, 2003

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A1 There are $n$ such sums. More precisely, there is exactly one such sum with $k$ terms for each of $k = 1, \dots, n$ (and clearly no others). To see this, note that if $n = a_1 + a_2 + \cdots + a_k$ with $a_1 \leq a_2 \leq \cdots \leq a_k \leq a_1 + 1$, then

$$\begin{aligned} ka_1 &= a_1 + a_1 + \cdots + a_1 \\ &\leq n \leq a_1 + (a_1+1) + \cdots + (a_1+1) \\ &= ka_1 + k - 1. \end{aligned}$$

However, there is a unique integer $a_1$ satisfying these inequalities, namely $a_1 = \lfloor n/k \rfloor$. Moreover, once $a_1$ is fixed, there are $k$ different possibilities for the sum $a_1 + a_2 + \cdots + a_k$: if $i$ is the last integer such that $a_i = a_1$, then the sum equals $ka_1 + (i-1)$. The possible values of $i$ are $1, \dots, k$, and exactly one of these sums comes out equal to $n$, proving our claim.

**Note:** In summary, there is a unique partition of $n$ with $k$ terms that is "as equally spaced as possible". One can also obtain essentially the same construction inductively: except for the all-ones sum, each partition of $n$ is obtained by "augmenting" a unique partition of $n-1$.

A2 **First solution:** Assume without loss of generality that $a_i + b_i > 0$ for each $i$ (otherwise both sides of the desired inequality are zero). Then the AM-GM inequality gives

$$\left( \frac{a_1 \cdots a_n}{(a_1+b_1)\cdots(a_n+b_n)} \right)^{1/n} \leq \frac{1}{n} \left( \frac{a_1}{a_1+b_1} + \cdots + \frac{a_n}{a_n+b_n} \right),$$

and likewise with the roles of $a$ and $b$ reversed. Adding these two inequalities and clearing denominators yields the desired result.

**Second solution:** Write the desired inequality in the form

$$(a_1+b_1)\cdots(a_n+b_n) \geq [(a_1\cdots a_n)^{1/n} + (b_1 \cdots b_n)^{1/n}]^n,$$

expand both sides, and compare the terms on both sides in which $k$ of the terms are among the $a_i$. On the left, one has the product of each $k$-element subset of $\{1, \dots, n\}$; on the right, one has

$$\binom{n}{k} (a_1 \cdots a_n)^{k/n} \cdots (b_1 \dots b_n)^{(n-k)/n},$$

which is precisely $\binom{n}{k}$ times the geometric mean of the terms on the left. Thus AM-GM shows that the terms under consideration on the left exceed those on the right; adding these inequalities over all $k$ yields the desired result.

**Third solution:** Since both sides are continuous in each $a_i$, it is sufficient to prove the claim with $a_1, \dots, a_n$ all positive (the general case follows by taking limits as some of the $a_i$ tend to zero). Put $r_i = b_i/a_i$; then the given inequality is equivalent to

$$(1+r_1)^{1/n} \cdots (1+r_n)^{1/n} \geq 1 + (r_1 \cdots r_n)^{1/n}.$$

In terms of the function

$$f(x) = \log(1+e^x)$$

and the quantities $s_i = \log r_i$, we can rewrite the desired inequality as

$$\frac{1}{n}(f(s_1) + \cdots + f(s_n)) \geq f\left( \frac{s_1 + \cdots + s_n}{n} \right).$$

This will follow from Jensen's inequality if we can verify that $f$ is a convex function; it is enough to check that $f''(x) > 0$ for all $x$. In fact,

$$f'(x) = \frac{e^x}{1+e^x} = 1 - \frac{1}{1+e^x}$$

is an increasing function of $x$, so $f''(x) > 0$ and Jensen's inequality thus yields the desired result. (As long as the $a_i$ are all positive, equality holds when $s_1 = \cdots = s_n$, i.e., when the vectors $(a_1, \dots, a_n)$ and $(b_1, \dots, b_n)$. Of course other equality cases crop up if some of the $a_i$ vanish, i.e., if $a_1 = b_1 = 0$.)

**Fourth solution:** We apply induction on $n$, the case $n = 1$ being evident. First we verify the auxiliary inequality

$$(a^n + b^n)(c^n + d^n)^{n-1} \geq (ac^{n-1} + bd^{n-1})^n$$

for $a, b, c, d \geq 0$. The left side can be written as

$$\begin{aligned} &a^n c^{n(n-1)} + b^n d^{n(n-1)} \\ &\quad + \sum_{i=1}^{n-1} \binom{n-1}{i} b^n c^{ni} d^{n(n-1-i)} \\ &\quad + \sum_{i=1}^{n-1} \binom{n-1}{i-1} a^n c^{n(i-1)} d^{n(n-i)}. \end{aligned}$$

Applying the weighted AM-GM inequality between matching terms in the two sums yields

$$\begin{aligned} (a^n + b^n)(c^n + d^n)^{n-1} &\geq a^n c^{n(n-1)} + b^n d^{n(n-1)} \\ &\quad + \sum_{i=1}^{n-1} \binom{n}{i} a^i b^{n-i} c^{(n-1)i} d^{(n-1)(n-i)}, \end{aligned}$$

proving the auxiliary inequality.

Now given the auxiliary inequality and the $n-1$ case of the desired inequality, we apply the auxiliary inequality with $a = a_1^{1/n}$, $b = b_1^{1/n}$, $c = (a_2 \cdots a_n)^{1/n(n-1)}$, $d = (b_2 \dots b_n)^{1/n(n-1)}$. The right side will be the $n$-th power of the desired inequality. The left side comes out to

$$(a_1+b_1)((a_2\cdots a_n)^{1/(n-1)} + (b_2\cdots b_n)^{1/(n-1)})^{n-1},$$

and by the induction hypothesis, the second factor is less than $(a_2+b_2)\cdots(a_n+b_n)$. This yields the desired result.

**Note:** Equality holds if and only if $a_i = b_i = 0$ for some $i$ or if the vectors $(a_1,\dots,a_n)$ and $(b_1,\dots,b_n)$ are proportional. As pointed out by Naoki Sato, the problem also appeared on the 1992 Irish Mathematical Olympiad. It is also a special case of a classical inequality, known as Hölder's inequality, which generalizes the Cauchy-Schwarz inequality (this is visible from the $n = 2$ case); the first solution above is adapted from the standard proof of Hölder's inequality. We don't know whether the declaration "Apply Hölder's inequality" by itself is considered an acceptable solution to this problem.

A3 **First solution:** Write

$$\begin{aligned} f(x) &= \sin x + \cos x + \tan x + \cot x + \sec x + \csc x \\ &= \sin x + \cos x + \frac{1}{\sin x \cos x} + \frac{\sin x + \cos x}{\sin x \cos x}. \end{aligned}$$

We can write $\sin x + \cos x = \sqrt{2}\cos(\pi/4 - x)$; this suggests making the substitution $y = \pi/4 - x$. In this new coordinate,

$$\sin x \cos x = \frac{1}{2}\sin 2x = \frac{1}{2}\cos 2y,$$

and writing $c = \sqrt{2}\cos y$, we have

$$\begin{aligned} f(y) &= (1+c)\left(1 + \frac{2}{c^2-1}\right) - 1 \\ &= c + \frac{2}{c-1}. \end{aligned}$$

We must analyze this function of $c$ in the range $[-\sqrt{2}, \sqrt{2}]$. Its value at $c = -\sqrt{2}$ is $2 - 3\sqrt{2} < -2.24$, and at $c = \sqrt{2}$ is $2 + 3\sqrt{2} > 6.24$. Its derivative is $1 - 2/(c-1)^2$, which vanishes when $(c-1)^2 = 2$, i.e., where $c = 1 \pm \sqrt{2}$. Only the value $c = 1 - \sqrt{2}$ is in bounds, at which the value of $f$ is $1 - 2\sqrt{2} > -1.83$. As for the pole at $c = 1$, we observe that $f$ decreases as $c$ approaches from below (so takes negative values for all $c < 1$) and increases as $c$ approaches from above (so takes positive values for all $c > 1$); from the data collected so far, we see that $f$ has no sign crossings, so the minimum of $|f|$ is achieved at a critical point of $f$. We conclude that the minimum of $|f|$ is $2\sqrt{2} - 1$.

Alternate derivation (due to Zuming Feng): We can also minimize $|c + 2/(c-1)|$ without calculus (or worrying about boundary conditions). For $c > 1$, we have

$$1 + (c-1) + \frac{2}{c-1} \geq 1 + 2\sqrt{2}$$

by AM-GM on the last two terms, with equality for $c - 1 = \sqrt{2}$ (which is out of range). For $c < 1$, we similarly have

$$-1 + 1 - c + \frac{2}{1-c} \geq -1 + 2\sqrt{2},$$

here with equality for $1 - c = \sqrt{2}$.

**Second solution:** Write

$$f(a,b) = a + b + \frac{1}{ab} + \frac{a+b}{ab}.$$

Then the problem is to minimize $|f(a,b)|$ subject to the constraint $a^2 + b^2 - 1 = 0$. Since the constraint region has no boundary, it is enough to check the value at each critical point and each potential discontinuity (i.e., where $ab = 0$) and select the smallest value (after checking that $f$ has no sign crossings).

We locate the critical points using the Lagrange multiplier condition: the gradient of $f$ should be parallel to that of the constraint, which is to say, to the vector $(a,b)$. Since

$$\frac{\partial f}{\partial a} = 1 - \frac{1}{a^2 b} - \frac{1}{a^2}$$

and similarly for $b$, the proportionality yields

$$a^2b^3 - a^3b^2 + a^3 - b^3 + a^2 - b^2 = 0.$$

The irreducible factors of the left side are $1 + a$, $1 + b$, $a - b$, and $ab - a - b$. So we must check what happens when any of those factors, or $a$ or $b$, vanishes.

If $1 + a = 0$, then $b = 0$, and the singularity of $f$ becomes removable when restricted to the circle. Namely, we have

$$f = a + b + \frac{1}{a} + \frac{b+1}{ab}$$

and $a^2 + b^2 - 1 = 0$ implies $(1+b)/a = a/(1-b)$. Thus we have $f = -2$; the same occurs when $1 + b = 0$.

If $a - b = 0$, then $a = b = \pm\sqrt{2}/2$ and either $f = 2 + 3\sqrt{2} > 6.24$, or $f = 2 - 3\sqrt{2} < -2.24$.

If $a = 0$, then either $b = -1$ as discussed above, or $b = 1$. In the latter case, $f$ blows up as one approaches this point, so there cannot be a global minimum there.

Finally, if $ab - a - b = 0$, then

$$a^2b^2 = (a+b)^2 = 2ab + 1$$

and so $ab = 1 \pm \sqrt{2}$. The plus sign is impossible since $|ab| \leq 1$, so $ab = 1 - \sqrt{2}$ and

$$\begin{aligned} f(a,b) &= ab + \frac{1}{ab} + 1 \\ &= 1 - 2\sqrt{2} > -1.83. \end{aligned}$$

This yields the smallest value of $|f|$ in the list (and indeed no sign crossings are possible), so $2\sqrt{2} - 1$ is the desired minimum of $|f|$.

**Note:** Instead of using the geometry of the graph of $f$ to rule out sign crossings, one can verify explicitly that $f$ cannot take the value 0. In the first solution, note that $c + 2/(c-1) = 0$ implies $c^2 - c + 2 = 0$, which has no real roots. In the second solution, we would have

$$a^2b + ab^2 + a + b = -1.$$

Squaring both sides and simplifying yields

$$2a^3b^3 + 5a^2b^2 + 4ab = 0,$$

whose only real root is $ab = 0$. But the cases with $ab = 0$ do not yield $f = 0$, as verified above.

A4 We split into three cases. Note first that $|A| \geq |a|$, by applying the condition for large $x$.

**Case 1:** $B^2 - 4AC > 0$**.** In this case $Ax^2 + Bx + C$ has two distinct real roots $r_1$ and $r_2$. The condition implies that $ax^2 + bx + c$ also vanishes at $r_1$ and $r_2$, so $b^2 - 4ac > 0$. Now

$$\begin{aligned} B^2 - 4AC &= A^2(r_1 - r_2)^2 \\ &\geq a^2(r_1 - r_2)^2 \\ &= b^2 - 4ac. \end{aligned}$$

**Case 2:** $B^2 - 4AC \leq 0$ **and** $b^2 - 4ac \leq 0$**.** Assume without loss of generality that $A \geq a > 0$, and that $B = 0$ (by shifting $x$). Then $Ax^2 + Bx + C \geq ax^2 + bx + c \geq 0$ for all $x$; in particular, $C \geq c \geq 0$. Thus

$$\begin{aligned} 4AC - B^2 &= 4AC \\ &\geq 4ac \\ &\geq 4ac - b^2. \end{aligned}$$

Alternate derivation (due to Robin Chapman): the ellipse $Ax^2 + Bxy + Cy^2 = 1$ is contained within the ellipse $ax^2 + bxy + cy^2 = 1$, and their respective enclosed areas are $\pi/(4AC - B^2)$ and $\pi/(4ac - b^2)$.

**Case 3:** $B^2 - 4AC \leq 0$ **and** $b^2 - 4ac > 0$**.** Since $Ax^2 + Bx + C$ has a graph not crossing the $x$-axis, so do $(Ax^2 + Bx + C) \pm (ax^2 + bx + c)$. Thus

$$\begin{aligned} (B-b)^2 - 4(A-a)(C-c) &\leq 0, \\ (B+b)^2 - 4(A+a)(C+c) &\leq 0 \end{aligned}$$

and adding these together yields

$$2(B^2 - 4AC) + 2(b^2 - 4ac) \leq 0.$$

Hence $b^2 - 4ac \leq 4AC - B^2$, as desired.

A5 **First solution:** We represent a Dyck $n$-path by a sequence $a_1 \cdots a_{2n}$, where each $a_i$ is either $(1,1)$ or $(1,-1)$.

Given an $(n-1)$-path $P = a_1 \cdots a_{2n-2}$, we distinguish two cases. If $P$ has no returns of even-length, then let $f(P)$ denote the $n$-path $(1,1)(1,-1)P$. Otherwise, let $a_i a_{i+1} \cdots a_j$ denote the rightmost even-length return in $P$, and let $f(P) = (1,1)a_1 a_2 \cdots a_j (1,-1) a_{j+1} \cdots a_{2n-2}$. Then $f$ clearly maps the set of Dyck $(n-1)$-paths to the set of Dyck $n$-paths having no even return.

We claim that $f$ is bijective; to see this, we simply construct the inverse mapping. Given an $n$-path $P$, let $R = a_i a_{i+1} ... a_j$ denote the leftmost return in $P$, and let $g(P)$ denote the path obtained by removing $a_1$ and $a_j$ from $P$. Then evidently $f \circ g$ and $g \circ f$ are identity maps, proving the claim.

**Second solution:** (by Dan Bernstein) Let $C_n$ be the number of Dyck paths of length $n$, let $O_n$ be the number of Dyck paths whose final return has odd length, and let $X_n$ be the number of Dyck paths with no return of even length.

We first exhibit a recursion for $O_n$; note that $O_0 = 0$. Given a Dyck $n$-path whose final return has odd length, split it just after its next-to-last return. For some $k$ (possibly zero), this yields a Dyck $k$-path, an upstep, a Dyck $(n-k-1)$-path whose odd return has even length, and a downstep. Thus for $n \geq 1$,

$$O_n = \sum_{k=0}^{n-1} C_k (C_{n-k-1} - O_{n-k-1}).$$

We next exhibit a similar recursion for $X_n$; note that $X_0 = 1$. Given a Dyck $n$-path with no even return, splitting as above yields for some $k$ a Dyck $k$-path with no even return, an upstep, a Dyck $(n-k-1)$-path whose final return has even length, then a downstep. Thus for $n \geq 1$,

$$X_n = \sum_{k=0}^{n-1} X_k (C_{n-k-1} - O_{n-k-1}).$$

To conclude, we verify that $X_n = C_{n-1}$ for $n \geq 1$, by induction on $n$. This is clear for $n = 1$ since $X_1 = C_0 = 1$. Given $X_k = C_{k-1}$ for $k < n$, we have

$$\begin{aligned} X_n &= \sum_{k=0}^{n-1} X_k (C_{n-k-1} - O_{n-k-1}) \\ &= C_{n-1} - O_{n-1} + \sum_{k=1}^{n-1} C_{k-1} (C_{n-k-1} - O_{n-k-1}) \\ &= C_{n-1} - O_{n-1} + O_{n-1} \\ &= C_{n-1}, \end{aligned}$$

as desired.

**Note:** Since the problem only asked about the *existence* of a one-to-one correspondence, we believe that any proof, bijective or not, that the two sets have the same cardinality is an acceptable solution. (Indeed, it would be highly unusual to insist on using or not using a specific proof technique!) The second solution above can also be phrased in terms of generating functions. Also, the $C_n$ are well-known to equal the Catalan numbers $\frac{1}{n+1}\binom{2n}{n}$; the problem at hand is part of a famous exercise in Richard Stanley's *Enumerative Combinatorics, Volume 1* giving 66 combinatorial interpretations of the Catalan numbers.

A6 **First solution:** Yes, such a partition is possible. To achieve it, place each integer into $A$ if it has an even number of 1s in its binary representation, and into $B$ if it has an odd number. (One discovers this by simply attempting to place the first few numbers by hand and noticing the resulting pattern.)

To show that $r_A(n) = r_B(n)$, we exhibit a bijection between the pairs $(a_1, a_2)$ of distinct elements of $A$ with $a_1 + a_2 = n$ and the pairs $(b_1, b_2)$ of distinct elements of $B$ with $b_1 + b_2 = n$. Namely, given a pair $(a_1, a_2)$ with $a_1 + a_2 = n$, write both numbers in binary and find the lowest-order place in which they differ (such a place exists because $a_1 \neq a_2$). Change both numbers in that place and call the resulting numbers $b_1, b_2$. Then $a_1 + a_2 = b_1 + b_2 = n$, but the parity of the number of 1s in $b_1$ is opposite that of $a_1$, and likewise between $b_2$ and $a_2$. This yields the desired bijection.

**Second solution:** (by Micah Smukler) Write $b(n)$ for the number of 1s in the base 2 expansion of $n$, and $f(n) = (-1)^{b(n)}$. Then the desired partition can be described as $A = f^{-1}(1)$ and $B = f^{-1}(-1)$. Since $f(2n) + f(2n+1) = 0$, we have

$$\sum_{i=0}^{n} f(n) = \begin{cases} 0 & n \text{ odd} \\ f(n) & n \text{ even.} \end{cases}$$

If $p, q$ are both in $A$, then $f(p) + f(q) = 2$; if $p, q$ are both in $B$, then $f(p) + f(q) = -2$; if $p, q$ are in different sets, then $f(p) + f(q) = 0$. In other words,

$$2(r_A(n) - r_B(n)) = \sum_{p+q=n, p<q} (f(p) + f(q))$$

and it suffices to show that the sum on the right is always zero. If $n$ is odd, that sum is visibly $\sum_{i=0}^{n} f(i) = 0$. If $n$ is even, the sum equals

$$\left(\sum_{i=0}^{n} f(i)\right) - f(n/2) = f(n) - f(n/2) = 0.$$

This yields the desired result.

**Third solution:** (by Dan Bernstein) Put $f(x) = \sum_{n \in A} x^n$ and $g(x) = \sum_{n \in B} x^n$; then the value of $r_A(n)$ (resp. $r_B(n)$) is the coefficient of $x^n$ in $f(x)^2 - f(x^2)$ (resp. $g(x)^2 - g(x^2)$). From the evident identities

$$\begin{aligned} \frac{1}{1-x} &= f(x) + g(x) \\ f(x) &= f(x^2) + xg(x^2) \\ g(x) &= g(x^2) + xf(x^2), \end{aligned}$$

we have

$$\begin{aligned} f(x) - g(x) &= f(x^2) - g(x^2) + xg(x^2) - xf(x^2) \\ &= (1-x)(f(x^2) - g(x^2)) \\ &= \frac{f(x^2) - g(x^2)}{f(x) + g(x)}. \end{aligned}$$

We deduce that $f(x)^2 - g(x)^2 = f(x^2) - g(x^2)$, yielding the desired equality.

**Note:** This partition is actually unique, up to interchanging $A$ and $B$. More precisely, the condition that $0 \in A$ and $r_A(n) = r_B(n)$ for $n = 1, \dots, m$ uniquely determines the positions of $0, \dots, m$. We see this by induction on $m$: given the result for $m-1$, switching the location of $m$ changes $r_A(m)$ by one and does not change $r_B(m)$, so it is not possible for both positions to work. Robin Chapman points out this problem is solved in D.J. Newman's *Analytic Number Theory* (Springer, 1998); in that solution, one uses generating functions to find the partition and establish its uniqueness, not just verify it.

B1 No, there do not.

**First solution:** Suppose the contrary. By setting $y = -1, 0, 1$ in succession, we see that the polynomials $1 - x + x^2, 1, 1 + x + x^2$ are linear combinations of $a(x)$ and $b(x)$. But these three polynomials are linearly independent, so cannot all be written as linear combinations of two other polynomials, contradiction.

Alternate formulation: the given equation expresses a diagonal matrix with $1, 1, 1$ and zeroes on the diagonal, which has rank 3, as the sum of two matrices of rank 1. But the rank of a sum of matrices is at most the sum of the ranks of the individual matrices.

**Second solution:** It is equivalent (by relabeling and rescaling) to show that $1 + xy + x^2y^2$ cannot be written as $a(x)d(y) - b(x)c(y)$. Write $a(x) = \sum a_i x^i$, $b(x) = \sum b_i x^i$, $c(y) = \sum c_j y^j$, $d(y) = \sum d_j y^j$. We now start comparing coefficients of $1 + xy + x^2y^2$. By comparing coefficients of $1 + xy + x^2y^2$ and $a(x)d(y) - b(x)c(y)$, we get

$$\begin{aligned} 1 &= a_i d_i - b_i c_i \qquad (i = 0, 1, 2) \\ 0 &= a_i d_j - b_i c_j \qquad (i \neq j). \end{aligned}$$

The first equation says that $a_i$ and $b_i$ cannot both vanish, and $c_i$ and $d_i$ cannot both vanish. The second equation says that $a_i/b_i = c_j/d_j$ when $i \neq j$, where both sides should be viewed in $\mathbb{R} \cup \{\infty\}$ (and neither is undetermined if $i, j \in \{0, 1, 2\}$). But then

$$a_0/b_0 = c_1/d_1 = a_2/b_2 = c_0/d_0$$

contradicting the equation $a_0d_0 - b_0c_0 = 1$.

**Third solution:** We work over the complex numbers, in which we have a primitive cube root $\omega$ of 1. We also use without further comment unique factorization for polynomials in two variables over a field. And we keep the relabeling of the second solution.

Suppose the contrary. Since $1 + xy + x^2y^2 = (1 - xy/\omega)(1 - xy/\omega^2)$, the rational function $a(\omega/y)d(y) - b(\omega/y)c(y)$ must vanish identically (that is, coefficient by coefficient). If one of the polynomials, say $a$, vanished identically, then one of $b$ or $c$ would also, and the desired inequality could not hold. So none of them vanish identically, and we can write

$$\frac{c(y)}{d(y)} = \frac{a(\omega/y)}{b(\omega/y)}.$$

Likewise,

$$\frac{c(y)}{d(y)} = \frac{a(\omega^2/y)}{b(\omega^2/y)}.$$

Put $f(x) = a(x)/b(x)$; then we have $f(\omega x) = f(x)$ identically. That is, $a(x)b(\omega x) = b(x)a(\omega x)$. Since $a$ and $b$ have no common factor (otherwise $1 + xy + x^2y^2$ would have a factor divisible only by $x$, which it doesn't since it doesn't vanish identically for any particular $x$), $a(x)$ divides $a(\omega x)$. Since they have the same degree, they are equal up to scalars. It follows that one of $a(x), xa(x), x^2a(x)$ is a polynomial in $x^3$ alone, and likewise for $b$ (with the same power of $x$).

If $xa(x)$ and $xb(x)$, or $x^2a(x)$ and $x^2b(x)$, are polynomials in $x^3$, then $a$ and $b$ are divisible by $x$, but we know $a$ and $b$ have no common factor. Hence $a(x)$ and $b(x)$ are polynomials in $x^3$. Likewise, $c(y)$ and $d(y)$ are polynomials in $y^3$. But then $1 + xy + x^2y^2 = a(x)d(y) - b(x)c(y)$ is a polynomial in $x^3$ and $y^3$, contradiction.

**Note:** The third solution only works over fields of characteristic not equal to 3, whereas the other two work over arbitrary fields. (In the first solution, one must replace $-1$ by another value if working in characteristic 2.)

B2 It is easy to see by induction that the $j$-th entry of the $k$-th sequence (where the original sequence is $k = 1$) is $\sum_{i=1}^{k} \binom{k-1}{i-1}/(2^{k-1}(i + j - 1))$, and so $x_n = \frac{1}{2^{n-1}} \sum_{i=1}^{n} \binom{n-1}{i-1}/i$. Now $\binom{n-1}{i-1}/i = \binom{n}{i}/n$; hence

$$x_n = \frac{1}{n2^{n-1}} \sum_{i=1}^{n} \binom{n}{i} = \frac{2^n - 1}{n2^{n-1}} < 2/n,$$

as desired.

B3 **First solution:** It is enough to show that for each prime $p$, the exponent of $p$ in the prime factorization of both sides is the same. On the left side, it is well-known that the exponent of $p$ in the prime factorization of $n!$ is

$$\sum_{i=1}^{n} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

(To see this, note that the $i$-th term counts the multiples of $p^i$ among $1, \dots, n$, so that a number divisible exactly by $p^i$ gets counted exactly $i$ times.) This number can be reinterpreted as the cardinality of the set $S$ of points in the plane with positive integer coordinates lying on or under the curve $y = np^{-x}$: namely, each summand is the number of points of $S$ with $x = i$.

On the right side, the exponent of $p$ in the prime factorization of $\operatorname{lcm}(1, \dots, \lfloor n/i \rfloor)$ is $\lfloor \log_p \lfloor n/i \rfloor \rfloor = \lfloor \log_p (n/i) \rfloor$. However, this is precisely the number of points of $S$ with $y = i$. Thus

$$\sum_{i=1}^{n} \lfloor \log_p \lfloor n/i \rfloor \rfloor = \sum_{i=1}^{n} \left\lfloor \frac{n}{p^i} \right\rfloor,$$

and the desired result follows.

**Second solution:** We prove the result by induction on $n$, the case $n = 1$ being obvious. What we actually show is that going from $n - 1$ to $n$ changes both sides by the same multiplicative factor, that is,

$$n = \prod_{i=1}^{n-1} \frac{\operatorname{lcm}\{1, 2, \dots, \lfloor n/i \rfloor\}}{\operatorname{lcm}\{1, 2, \dots, \lfloor (n-1)/i \rfloor\}}.$$

Note that the $i$-th term in the product is equal to 1 if $n/i$ is not an integer, i.e., if $n/i$ is not a divisor of $n$. It is also equal to 1 if $n/i$ is a divisor of $n$ but not a prime power, since any composite number divides the lcm of all smaller numbers. However, if $n/i$ is a power of $p$, then the $i$-th term is equal to $p$.

Since $n/i$ runs over all proper divisors of $n$, the product on the right side includes one factor of the prime $p$ for each factor of $p$ in the prime factorization of $n$. Thus the whole product is indeed equal to $n$, completing the induction.

B4 **First solution:** Put $g = r_1 + r_2$, $h = r_3 + r_4$, $u = r_1r_2$, $v = r_3r_4$. We are given that $g$ is rational. The following are also rational:

$$\frac{-b}{a} = g + h$$
$$\frac{c}{a} = gh + u + v$$
$$\frac{-d}{a} = gv + hu$$

From the first line, $h$ is rational. From the second line, $u + v$ is rational. From the third line, $g(u + v) - (gv + hu) = (g - h)u$ is rational. Since $g \neq h$, $u$ is rational, as desired.

**Second solution:** This solution uses some basic Galois theory. We may assume $r_1 \neq r_2$, since otherwise they are both rational and so then is $r_1r_2$.

Let $\tau$ be an automorphism of the field of algebraic numbers; then $\tau$ maps each $r_i$ to another one, and fixes the rational number $r_1+r_2$. If $\tau(r_1)$ equals one of $r_1$ or $r_2$, then $\tau(r_2)$ must equal the other one, and vice versa. Thus $\tau$ either fixes the set $\{r_1,r_2\}$ or moves it to $\{r_3,r_4\}$. But if the latter happened, we would have $r_1+r_2=r_3+r_4$, contrary to hypothesis. Thus $\tau$ fixes the set $\{r_1,r_2\}$ and in particular the number $r_1r_2$. Since this is true for any $\tau$, $r_1r_2$ must be rational.

**Note:** The conclusion fails if we allow $r_1+r_2=r_3+r_4$. For instance, take the polynomial $x^4-2$ and label its roots so that $(x-r_1)(x-r_2)=x^2-\sqrt{2}$ and $(x-r_3)(x-r_4)=x^2+\sqrt{2}$.

B5 **First solution:** Place the unit circle on the complex plane so that $A,B,C$ correspond to the complex numbers $1,\omega,\omega^2$, where $\omega=e^{2\pi i/3}$, and let $P$ correspond to the complex number $x$. The distances $a,b,c$ are then $|x-1|,|x-\omega|,|x-\omega^2|$. Now the identity

$$(x-1)+\omega(x-\omega)+\omega^2(x-\omega^2)=0$$

implies that there is a triangle whose sides, as vectors, correspond to the complex numbers $x-1,\omega(x-\omega),\omega^2(x-\omega^2)$; this triangle has sides of length $a,b,c$.

To calculate the area of this triangle, we first note a more general formula. If a triangle in the plane has vertices at 0, $v_1=s_1+it_1$, $v_2=s_2+it_2$, then it is well known that the area of the triangle is $|s_1t_2-s_2t_1|/2=|v_1\overline{v_2}-v_2\overline{v_1}|/4$. In our case, we have $v_1=x-1$ and $v_2=\omega(x-\omega)$; then

$$v_1\overline{v_2}-v_2\overline{v_1}=(\omega^2-\omega)(x\overline{x}-1)=i\sqrt{3}(|x|^2-1).$$

Hence the area of the triangle is $\sqrt{3}(1-|x|^2)/4$, which depends only on the distance $|x|$ from $P$ to $O$.

**Second solution:** (by Florian Herzig) Let $A'$, $B'$, $C'$ be the points obtained by intersecting the lines $AP$, $BP$, $CP$ with the unit circle. Let $d$ denote $OP$. Then $A'P=(1-d^2)/a$, etc., by using the power of the point $P$. As triangles $A'B'P$ and $BAP$ are similar, we get that $A'B'=AB\cdot A'P/b=\sqrt{3}(1-d^2)/(ab)$. It follows that triangle $A'B'C'$ has sides proportional to $a$, $b$, $c$, by a factor of $\sqrt{3}(1-d^2)/(abc)$. In particular, there is a triangle with sides $a$, $b$, $c$, and it has circumradius $R=(abc)/(\sqrt{3}(1-d^2))$. Its area is $abc/(4R)=\sqrt{3}(1-d^2)/4$.

**Third solution:** (by Samuel Li) Consider the rotation by the angle $\pi/3$ around $A$ carrying $B$ to $C$, and let $P_A$ be the image of $P$; define $P_B,P_C$ similarly. Let $A'$ be the intersection of the tangents to the circle at $B,C$; define $B',C'$, similarly. Put $\ell=AB=BC=CA$; we then have

$$\begin{aligned}
AB'=AC'=BC'=BA'=CA'=CB'&=\ell\\
PA=PP_A=P_AA=P_BC'=P_CA'&=a\\
PB=PP_B=P_BB=P_CA'=P_AC'&=b\\
PC=PP_C=P_CC=P_AB'=P_BA'&=c.
\end{aligned}$$

The triangle $\triangle A'B'C'$ has area four times that of $\triangle ABC$. We may dissect it into twelve triangles by first splitting it into three quadrilaterals $PAC'B$, $PBC'A,PCA'B$, then splitting each of these in four around the respective interior points $P_B,P_C,P_A$. Of the resulting twelve triangles, three have side lengths $a,b,c$, while three are equilateral triangles of respective sides lengths $a,b,c$. The other six are isomorphic to two copies each of $\triangle PAB,\triangle PBC,\triangle PCA$, so their total area is twice that of $\triangle ABC$.

It thus suffices to compute $a^2+b^2+c^2$ in terms of the radius of the circle and the distance $OP$. This can be done readily in terms of $OP$ using vectors, Cartesian coordinates, or complex numbers as in the first solution.

B6 **First solution:** (composite of solutions by Feng Xie and David Pritchard) Let $\mu$ denote Lebesgue measure on $[0,1]$. Define

$$\begin{aligned}
E_+&=\{x\in[0,1]:f(x)\geq 0\}\\
E_-&=\{x\in[0,1]:f(x)<0\};
\end{aligned}$$

then $E_+$, $E_-$ are measurable and $\mu(E_+)+\mu(E_-)=1$. Write $\mu_+$ and $\mu_-$ for $\mu(E_+)$ and $\mu(E_-)$. Also define

$$\begin{aligned}
I_+&=\int_{E_+}|f(x)|\,dx\\
I_-&=\int_{E_-}|f(x)|\,dx,
\end{aligned}$$

so that $\int_0^1|f(x)|\,dx=I_++I_-$.

From the triangle inequality $|a+b|\geq\pm(|a|-|b|)$, we have the inequality

$$\begin{aligned}
&\iint_{E_+\times E_-}|f(x)+f(y)|\,dx\,dy\\
&\geq\pm\iint_{E_+\times E_-}(|f(x)|-|f(y)|)\,dx\,dy\\
&=\pm(\mu_-I_+-\mu_+I_-),
\end{aligned}$$

and likewise with $+$ and $-$ switched. Adding these inequalities together and allowing all possible choices of the signs, we get

$$\begin{aligned}
&\iint_{(E_+\times E_-)\cup(E_-\times E_+)}|f(x)+f(y)|\,dx\,dy\\
&\geq\max\{0,2(\mu_-I_+-\mu_+I_-),2(\mu_+I_--\mu_-I_+)\}.
\end{aligned}$$

To this inequality, we add the equalities

$$\begin{aligned}
\iint_{E_+\times E_+}|f(x)+f(y)|\,dx\,dy&=2\mu_+I_+\\
\iint_{E_-\times E_-}|f(x)+f(y)|\,dx\,dy&=2\mu_-I_-\\
-\int_0^1|f(x)|\,dx&=-(\mu_++\mu_-)(I_++I_-)
\end{aligned}$$

to obtain

$$\begin{aligned}\int_0^1 \int_0^1 |f(x)+f(y)|\,dx\,dy - \int_0^1 |f(x)|\,dx \\ \geq \max\{(\mu_+ - \mu_-)(I_+ + I_-) + 2\mu_-(I_- - I_+), \\ (\mu_+ - \mu_-)(I_+ - I_-), \\ (\mu_- - \mu_+)(I_+ + I_-) + 2\mu_+(I_+ - I_-)\}.\end{aligned}$$

Now simply note that for each of the possible comparisons between $\mu_+$ and $\mu_-$, and between $I_+$ and $I_-$, one of the three terms above is manifestly nonnegative. This yields the desired result.

**Second solution:** We will show at the end that it is enough to prove a discrete analogue: if $x_1, \dots, x_n$ are real numbers, then

$$\frac{1}{n^2} \sum_{i,j=1}^n |x_i + x_j| \geq \frac{1}{n} \sum_{i=1}^n |x_i|.$$

In the meantime, we concentrate on this assertion.

Let $f(x_1, \dots, x_n)$ denote the difference between the two sides. We induct on the number of nonzero values of $|x_i|$. We leave for later the base case, where there is at most one such value. Suppose instead for now that there are two or more. Let $s$ be the smallest, and suppose without loss of generality that $x_1 = \cdots = x_a = s$, $x_{a+1} = \cdots = x_{a+b} = -s$, and for $i > a+b$, either $x_i = 0$ or $|x_i| > s$. (One of $a, b$ might be zero.)

Now consider

$$f(\overbrace{t, \cdots, t}^{a \text{ terms}}, \overbrace{-t, \cdots, -t}^{b \text{ terms}}, x_{a+b+1}, \cdots, x_n)$$

as a function of $t$. It is piecewise linear near $s$; in fact, it is linear between 0 and the smallest nonzero value among $|x_{a+b+1}|, \dots, |x_n|$ (which exists by hypothesis). Thus its minimum is achieved by one (or both) of those two endpoints. In other words, we can reduce the number of distinct nonzero absolute values among the $x_i$ without increasing $f$. This yields the induction, pending verification of the base case.

As for the base case, suppose that $x_1 = \cdots = x_a = s > 0$, $x_{a+1} = \cdots = x_{a+b} = -s$, and $x_{a+b+1} = \cdots = x_n = 0$. (Here one or even both of $a, b$ could be zero, though the latter case is trivial.) Then

$$\begin{aligned}f(x_1, \dots, x_n) &= \frac{s}{n^2}(2a^2 + 2b^2 + (a+b)(n-a-b)) \\ &\quad - \frac{s}{n}(a+b) = \frac{s}{n^2}(a^2 - 2ab + b^2) \geq 0.\end{aligned}$$

This proves the base case of the induction, completing the solution of the discrete analogue.

To deduce the original statement from the discrete analogue, approximate both integrals by equally-spaced Riemann sums and take limits. This works because given a continuous function on a product of closed intervals, any sequence of Riemann sums with mesh size tending to zero converges to the integral. (The domain is compact, so the function is uniformly continuous. Hence for any $\varepsilon > 0$ there is a cutoff below which any mesh size forces the discrepancy between the Riemann sum and the integral to be less than $\varepsilon$.)

Alternate derivation (based on a solution by Dan Bernstein): from the discrete analogue, we have

$$\sum_{1 \leq i < j \leq n} |f(x_i) + f(x_j)| \geq \frac{n-2}{2} \sum_{i=1}^n |f(x_i)|,$$

for all $x_1, \dots, x_n \in [0,1]$. Integrating both sides as $(x_1, \dots, x_n)$ runs over $[0,1]^n$ yields

$$\begin{aligned}&\frac{n(n-1)}{2} \int_0^1 \int_0^1 |f(x)+f(y)|\,dy\,dx \\ &\geq \frac{n(n-2)}{2} \int_0^1 |f(x)|\,dx,\end{aligned}$$

or

$$\int_0^1 \int_0^1 |f(x)+f(y)|\,dy\,dx \geq \frac{n-2}{n-1} \int_0^1 |f(x)|\,dx.$$

Taking the limit as $n \to \infty$ now yields the desired result.

**Third solution:** (by David Savitt) We give an argument which yields the following improved result. Let $\mu_p$ and $\mu_n$ be the measure of the sets $\{x : f(x) > 0\}$ and $\{x : f(x) < 0\}$ respectively, and let $\mu \leq 1/2$ be $\min(\mu_p, \mu_n)$. Then

$$\begin{aligned}&\int_0^1 \int_0^1 |f(x)+f(y)|\,dx\,dy \\ &\geq (1 + (1-2\mu)^2) \int_0^1 |f(x)|\,dx.\end{aligned}$$

Note that the constant can be seen to be best possible by considering a sequence of functions tending towards the step function which is 1 on $[0, \mu]$ and $-1$ on $(\mu, 1]$.

Suppose without loss of generality that $\mu = \mu_p$. As in the second solution, it suffices to prove a strengthened discrete analogue, namely

$$\frac{1}{n^2} \sum_{i,j} |a_i + a_j| \geq \left(1 + \left(1 - \frac{2p}{n}\right)^2\right) \left(\frac{1}{n} \sum_{i=1}^n |a_i|\right),$$

where $p \leq n/2$ is the number of $a_1, \dots, a_n$ which are positive. (We need only make sure to choose meshes so that $p/n \to \mu$ as $n \to \infty$.) An equivalent inequality is

$$\sum_{1 \leq i < j \leq n} |a_i + a_j| \geq \left(n - 1 - 2p + \frac{2p^2}{n}\right) \sum_{i=1}^n |a_i|.$$

Write $r_i = |a_i|$, and assume without loss of generality that $r_i \geq r_{i+1}$ for each $i$. Then for $i < j$, $|a_i + a_j| = r_i + r_j$ if $a_i$ and $a_j$ have the same sign, and is $r_i - r_j$ if they have opposite signs. The left-hand side is therefore equal to

$$\sum_{i=1}^n (n-i) r_i + \sum_{j=1}^n r_j C_j,$$

where

$$C_j = \#\{i < j \ : \mathrm{sgn}(a_i) = \mathrm{sgn}(a_j)\} \\ - \#\{i < j : \mathrm{sgn}(a_i) \neq \mathrm{sgn}(a_j)\}.$$

Consider the partial sum $P_k = \sum_{j=1}^k C_j$. If exactly $p_k$ of $a_1, \dots, a_k$ are positive, then this sum is equal to

$$\binom{p_k}{2} + \binom{k-p_k}{2} - \left[\binom{k}{2} - \binom{p_k}{2} - \binom{k-p_k}{2}\right],$$

which expands and simplifies to

$$-2p_k(k-p_k) + \binom{k}{2}.$$

For $k \leq 2p$ even, this partial sum would be minimized with $p_k = \frac{k}{2}$, and would then equal $-\frac{k}{2}$; for $k < 2p$ odd, this partial sum would be minimized with $p_k = \frac{k\pm 1}{2}$, and would then equal $-\frac{k-1}{2}$. Either way, $P_k \geq -\lfloor \frac{k}{2} \rfloor$. On the other hand, if $k > 2p$, then

$$-2p_k(k-p_k) + \binom{k}{2} \geq -2p(k-p) + \binom{k}{2}$$

since $p_k$ is at most $p$. Define $Q_k$ to be $-\lfloor \frac{k}{2} \rfloor$ if $k \leq 2p$ and $-2p(k-p) + \binom{k}{2}$ if $k \geq 2p$, so that $P_k \geq Q_k$. Note that $Q_1 = 0$.

Partial summation gives

$$\begin{aligned}\sum_{j=1}^n r_j C_j &= r_n P_n + \sum_{j=2}^n (r_{j-1} - r_j) P_{j-1} \\ &\geq r_n Q_n + \sum_{j=2}^n (r_{j-1} - r_j) Q_{j-1} \\ &= \sum_{j=2}^n r_j (Q_j - Q_{j-1}) \\ &= -r_2 - r_4 - \cdots - r_{2p} + \sum_{j=2p+1}^n (j-1-2p) r_j.\end{aligned}$$

It follows that

$$\begin{aligned}\sum_{1 \leq i < j \leq n} |a_i + a_j| &= \sum_{i=1}^n (n-i) r_i + \sum_{j=1}^n r_j C_j \\ &\geq \sum_{i=1}^{2p} (n - i - [i \text{ even}]) r_i \\ &\quad + \sum_{i=2p+1}^n (n-1-2p) r_i \\ &= (n-1-2p) \sum_{i=1}^n r_i \\ &\quad + \sum_{i=1}^{2p} (2p+1-i-[i \text{ even}]) r_i \\ &\geq (n-1-2p) \sum_{i=1}^n r_i + p \sum_{i=1}^{2p} r_i \\ &\geq (n-1-2p) \sum_{i=1}^n r_i + p \frac{2p}{n} \sum_{i=1}^n r_i,\end{aligned}$$

as desired. The next-to-last and last inequalities each follow from the monotonicity of the $r_i$'s, the former by pairing the $i^{\text{th}}$ term with the $(2p+1-i)^{\text{th}}$.

**Note:** Compare the closely related Problem 6 from the 2000 USA Mathematical Olympiad: prove that for any nonnegative real numbers $a_1, \dots, a_n, b_1, \dots, b_n$, one has

$$\sum_{i,j=1}^n \min\{a_i a_j, b_i b_j\} \leq \sum_{i,j=1}^n \min\{a_i b_j, a_j b_i\}.$$

# The 65th William Lowell Putnam Mathematical Competition
# Saturday, December 4, 2004

A1 Basketball star Shanille O'Keal's team statistician keeps track of the number, $S(N)$, of successful free throws she has made in her first $N$ attempts of the season. Early in the season, $S(N)$ was less than 80% of $N$, but by the end of the season, $S(N)$ was more than 80% of $N$. Was there necessarily a moment in between when $S(N)$ was exactly 80% of $N$?

A2 For $i = 1,2$ let $T_i$ be a triangle with side lengths $a_i, b_i, c_i$, and area $A_i$. Suppose that $a_1 \le a_2, b_1 \le b_2, c_1 \le c_2$, and that $T_2$ is an acute triangle. Does it follow that $A_1 \le A_2$?

A3 Define a sequence $\{u_n\}_{n=0}^{\infty}$ by $u_0 = u_1 = u_2 = 1$, and thereafter by the condition that

$$\det \begin{pmatrix} u_n & u_{n+1} \\ u_{n+2} & u_{n+3} \end{pmatrix} = n!$$

for all $n \ge 0$. Show that $u_n$ is an integer for all $n$. (By convention, $0! = 1$.)

A4 Show that for any positive integer $n$ there is an integer $N$ such that the product $x_1 x_2 \cdots x_n$ can be expressed identically in the form

$$x_1 x_2 \cdots x_n = \sum_{i=1}^{N} c_i (a_{i1} x_1 + a_{i2} x_2 + \cdots + a_{in} x_n)^n$$

where the $c_i$ are rational numbers and each $a_{ij}$ is one of the numbers $-1, 0, 1$.

A5 An $m \times n$ checkerboard is colored randomly: each square is independently assigned red or black with probability $1/2$. We say that two squares, $p$ and $q$, are in the same connected monochromatic region if there is a sequence of squares, all of the same color, starting at $p$ and ending at $q$, in which successive squares in the sequence share a common side. Show that the expected number of connected monochromatic regions is greater than $mn/8$.

A6 Suppose that $f(x,y)$ is a continuous real-valued function on the unit square $0 \le x \le 1, 0 \le y \le 1$. Show that

$$\int_0^1 \left( \int_0^1 f(x,y) dx \right)^2 dy + \int_0^1 \left( \int_0^1 f(x,y) dy \right)^2 dx$$
$$\le \left( \int_0^1 \int_0^1 f(x,y) dx\, dy \right)^2 + \int_0^1 \int_0^1 [f(x,y)]^2 dx\, dy.$$

B1 Let $P(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0$ be a polynomial with integer coefficients. Suppose that $r$ is a rational number such that $P(r) = 0$. Show that the $n$ numbers

$$c_n r,\ c_n r^2 + c_{n-1} r,\ c_n r^3 + c_{n-1} r^2 + c_{n-2} r,$$
$$\ldots,\ c_n r^n + c_{n-1} r^{n-1} + \cdots + c_1 r$$

are integers.

B2 Let $m$ and $n$ be positive integers. Show that

$$\frac{(m+n)!}{(m+n)^{m+n}} < \frac{m!}{m^m} \frac{n!}{n^n}.$$

B3 Determine all real numbers $a > 0$ for which there exists a nonnegative continuous function $f(x)$ defined on $[0,a]$ with the property that the region

$$R = \{(x,y); 0 \le x \le a, 0 \le y \le f(x)\}$$

has perimeter $k$ units and area $k$ square units for some real number $k$.

B4 Let $n$ be a positive integer, $n \ge 2$, and put $\theta = 2\pi/n$. Define points $P_k = (k,0)$ in the $xy$-plane, for $k = 1,2,\ldots,n$. Let $R_k$ be the map that rotates the plane counterclockwise by the angle $\theta$ about the point $P_k$. Let $R$ denote the map obtained by applying, in order, $R_1$, then $R_2, \ldots$, then $R_n$. For an arbitrary point $(x,y)$, find, and simplify, the coordinates of $R(x,y)$.

B5 Evaluate

$$\lim_{x \to 1^-} \prod_{n=0}^{\infty} \left( \frac{1 + x^{n+1}}{1 + x^n} \right)^{x^n}.$$

B6 Let $\mathscr{A}$ be a non-empty set of positive integers, and let $N(x)$ denote the number of elements of $\mathscr{A}$ not exceeding $x$. Let $\mathscr{B}$ denote the set of positive integers $b$ that can be written in the form $b = a - a'$ with $a \in \mathscr{A}$ and $a' \in \mathscr{A}$. Let $b_1 < b_2 < \cdots$ be the members of $\mathscr{B}$, listed in increasing order. Show that if the sequence $b_{i+1} - b_i$ is unbounded, then

$$\lim_{x \to \infty} N(x)/x = 0.$$

# Solutions to the 65th William Lowell Putnam Mathematical Competition
# Saturday, December 4, 2004

Kiran Kedlaya and Lenny Ng

A–1 Yes. Suppose otherwise. Then there would be an $N$ such that $S(N) < .8N$ and $S(N+1) > .8(N+1)$; that is, O'Keal's free throw percentage is under 80% at some point, and after one subsequent free throw (necessarily made), her percentage is over 80%. If she makes $m$ of her first $N$ free throws, then $m/N < 4/5$ and $(m+1)/(N+1) > 4/5$. This means that $5m < 4n < 5m+1$, which is impossible since then $4n$ is an integer between the consecutive integers $5m$ and $5m+1$.

**Remark:** This same argument works for any fraction of the form $(n-1)/n$ for some integer $n > 1$, but not for any other real number between 0 and 1.

A–2 **First solution:** (partly due to Ravi Vakil) Yes, it does follow. For $i = 1,2$, let $P_i, Q_i, R_i$ be the vertices of $T_i$ opposide the sides of length $a_i, b_i, c_i$, respectively.

We first check the case where $a_1 = a_2$ (or $b_1 = b_2$ or $c_1 = c_2$, by the same argument after relabeling). Imagine $T_2$ as being drawn with the base $Q_2R_2$ horizontal and the point $P_2$ above the line $Q_2R_2$. We may then position $T_1$ so that $Q_1 = Q_2$, $R_1 = R_2$, and $P_1$ lies above the line $Q_1R_1 = Q_2R_2$. Then $P_1$ also lies inside the region bounded by the circles through $P_2$ centered at $Q_2$ and $R_2$. Since $\angle Q_2$ and $\angle R_2$ are acute, the part of this region above the line $Q_2R_2$ lies within $T_2$. In particular, the distance from $P_1$ to the line $Q_2R_2$ is less than or equal to the distance from $P_2$ to the line $Q_2R_2$; hence $A_1 \leq A_2$.

To deduce the general case, put

$$r = \max\{a_1/a_2, b_1/b_2, c_1/c_2\}.$$

Let $T_3$ be the triangle with sides $ra_2, rb_2, rc_2$, which has area $r^2A_2$. Applying the special case to $T_1$ and $T_3$, we deduce that $A_1 \leq r^2A_2$; since $r \leq 1$ by hypothesis, we have $A_1 \leq A_2$ as desired.

**Remark:** Another geometric argument in the case $a_1 = a_2$ is that since angles $\angle Q_2$ and $\angle R_2$ are acute, the perpendicular to $Q_2R_2$ through $P_2$ separates $Q_2$ from $R_2$. If $A_1 > A_2$, then $P_1$ lies above the parallel to $Q_2R_2$ through $P_2$; if then it lies on or to the left of the vertical line through $P_2$, we have $c_1 > c_2$ because the inequality holds for both horizontal and vertical components (possibly with equality for one, but not both). Similarly, if $P_1$ lies to the right of the vertical, then $b_1 > b_2$.

**Second solution:** (attribution unknown) Retain notation as in the first paragraph of the first solution. Since the angle measures in any triangle add up to $\pi$, some angle of $T_1$ must have measure less than or equal to its counterpart in $T_2$. Without loss of generality assume that $\angle P_1 \leq \angle P_2$. Since the latter is acute (because $T_2$ is acute), we have $\sin \angle P_1 \leq \sin \angle P_2$. By the Law of Sines,

$$A_1 = \frac{1}{2} b_1 c_1 \sin \angle P_1 \leq \frac{1}{2} b_2 c_2 \sin \angle P_2 = A_2.$$

**Remark:** Many other solutions are possible; for instance, one uses Heron's formula for the area of a triangle in terms of its side lengths.

A–3 Define a sequence $v_n$ by $v_n = (n-1)(n-3)\cdots(4)(2)$ if $n$ is odd and $v_n = (n-1)(n-3)\cdots(3)(1)$ if $n$ is even; it suffices to prove that $u_n = v_n$ for all $n \geq 2$. Now $v_{n+3}v_n = (n+2)(n)(n-1)!$ and $v_{n+2}v_{n+1} = (n+1)!$, and so $v_{n+3}v_n - v_{n+2}v_{n+1} = n!$. Since we can check that $u_n = v_n$ for $n = 2,3,4$, and $u_n$ and $v_n$ satisfy the same recurrence, it follows by induction that $u_n = v_n$ for all $n \geq 2$, as desired.

A–4 It suffices to verify that

$$x_1 \cdots x_n = \frac{1}{2^n n!} \sum_{e_i \in \{-1,1\}} (e_1 \cdots e_n)(e_1x_1 + \cdots + e_nx_n)^n.$$

To check this, first note that the right side vanishes identically for $x_1 = 0$, because each term cancels the corresponding term with $e_1$ flipped. Hence the right side, as a polynomial, is divisible by $x_1$; similarly it is divisible by $x_2, \dots, x_n$. Thus the right side is equal to $x_1 \cdots x_n$ times a scalar. (Another way to see this: the right side is clearly odd as a polynomial in each individual variable, but the only degree $n$ monomial in $x_1, \dots, x_n$ with that property is $x_1 \cdots x_n$.) Since each summand contributes $\frac{1}{2^n} x_1 \cdots x_n$ to the sum, the scalar factor is 1 and we are done.

**Remark:** Several variants on the above construction are possible; for instance,

$$x_1 \cdots x_n = \frac{1}{n!} \sum_{e_i \in \{0,1\}} (-1)^{n-e_1-\cdots-e_n} (e_1x_1 + \cdots + e_nx_n)^n$$

by the same argument as above.

**Remark:** These construction work over any field of characteristic greater than $n$ (at least for $n > 1$). On the other hand, no construction is possible over a field of characteristic $p \leq n$, since the coefficient of $x_1 \cdots x_n$ in the expansion of $(e_1x_1 + \cdots + e_nx_n)^n$ is zero for any $e_i$.

**Remark:** Richard Stanley asks whether one can use fewer than $2^n$ terms, and what the smallest possible number is.

A–5 **First solution:** First recall that any graph with $n$ vertices and $e$ edges has at least $n-e$ connected components (add each edge one at a time, and note that it reduces the number of components by at most 1). Now imagine the squares of the checkerboard as a graph, whose vertices are connected if the corresponding squares share a side and are the same color. Let $A$ be the number of edges in the graph, and let $B$ be the number of 4-cycles (formed by monochromatic $2\times 2$ squares). If we remove the bottom edge of each 4-cycle, the resulting graph has the same number of connected components as the original one; hence this number is at least

$$mn - A + B.$$

By the linearity of expectation, the expected number of connected components is at least

$$mn - E(A) + E(B).$$

Moreover, we may compute $E(A)$ by summing over the individual pairs of adjacent squares, and we may compute $E(B)$ by summing over the individual $2\times 2$ squares. Thus

$$\begin{aligned} E(A) &= \frac{1}{2}(m(n-1)+(m-1)n), \\ E(B) &= \frac{1}{8}(m-1)(n-1), \end{aligned}$$

and so the expected number of components is at least

$$\begin{aligned} &mn - \frac{1}{2}(m(n-1)+(m-1)n) + \frac{1}{8}(m-1)(n-1) \\ &= \frac{mn+3m+3n+1}{8} > \frac{mn}{8}. \end{aligned}$$

**Remark:** A "dual" approach is to consider the graph whose vertices are the corners of the squares of the checkerboard, with two vertices joined if they are adjacent and the edge between then does not separate two squares of the same color. In this approach, the 4-cycles become isolated vertices, and the bound on components is replaced by a call to Euler's formula relating the vertices, edges and faces of a planar figure. (One must be careful, however, to correctly handle faces which are not simply connected.)

**Second solution:** (by Noam Elkies) Number the squares of the checkerboard $1,\dots,mn$ by numbering the first row from left to right, then the second row, and so on. We prove by induction on $i$ that if we just consider the figure formed by the first $i$ squares, its expected number of monochromatic components is at least $i/8$. For $i=1$, this is clear.

Suppose the $i$-th square does not abut the left edge or the top row of the board. Then we may divide into three cases.

- With probability $1/4$, the $i$-th square is opposite in color from the adjacent squares directly above and to the left of it. In this case adding the $i$-th square adds one component.
- With probability $1/8$, the $i$-th square is the same in color as the adjacent squares directly above and to the left of it, but opposite in color from its diagonal neighbor above and to the left. In this case, adding the $i$-th square either removes a component or leaves the number unchanged.
- In all other cases, the number of components remains unchanged upon adding the $i$-th square.

Hence adding the $i$-th square increases the expected number of components by $1/4-1/8=1/8$.

If the $i$-th square does abut the left edge of the board, the situation is even simpler: if the $i$-th square differs in color from the square above it, one component is added, otherwise the number does not change. Hence adding the $i$-th square increases the expected number of components by $1/2$; likewise if the $i$-th square abuts the top edge of the board. Thus the expected number of components is at least $i/8$ by induction, as desired.

**Remark:** Some solvers attempted to consider adding one row at a time, rather than one square; this must be handled with great care, as it is possible that the number of components can drop rather precipitously upon adding an entire row.

A–6 By approximating each integral with a Riemann sum, we may reduce to proving the discrete analogue: for $x_{ij}\in\mathbb{R}$ for $i,j=1,\dots,n$,

$$\begin{aligned} n\sum_{i=1}^n\left(\sum_{j=1}^n x_{ij}\right)^2 &+ n\sum_{j=1}^n\left(\sum_{i=1}^n x_{ij}\right)^2 \\ &\leq \left(\sum_{i=1}^n\sum_{j=1}^n x_{ij}\right)^2 + n^2\sum_{i=1}^n\sum_{j=1}^n x_{ij}^2. \end{aligned}$$

The difference between the right side and the left side is

$$\frac{1}{4}\sum_{i,j,k,l=1}^n (x_{ij}+x_{kl}-x_{il}-x_{kj})^2,$$

which is evidently nonnegative. If you prefer not to discretize, you may rewrite the original inequality as

$$\int_0^1\int_0^1\int_0^1\int_0^1 F(x,y,z,w)^2\,dx\,dy\,dz\,dw \geq 0$$

for

$$F(x,y,z,w) = f(x,y)+f(z,w)-f(x,w)-f(z,y).$$

**Remark:** (by Po-Ning Chen) The discrete inequality can be arrived at more systematically by repeatedly applying the following identity: for any real $a_1,\dots,a_n$,

$$\sum_{1\leq i<j\leq n}(x_i-x_j)^2 = n\sum_{i=1}^n x_i^2 - \left(\sum_{i=1}^n x_i\right)^2.$$

**Remark:** (by David Savitt) The discrete inequality can also be interpreted as follows. For $c,d \in \{1,\dots,n-1\}$ and $\zeta_n = e^{2\pi i/n}$, put

$$z_{c,d} = \sum_{i,j} \zeta_n^{ci+dj} x_{ij}.$$

Then the given inequality is equivalent to

$$\sum_{c,d=1}^{n-1} |z_{c,d}|^2 \geq 0.$$

B–1 Let $k$ be an integer, $0 \leq k \leq n-1$. Since $P(r)/r^k = 0$, we have

$$\begin{aligned} c_n r^{n-k} + c_{n-1} r^{n-k+1} + \cdots + c_{k+1} r \\ = -(c_k + c_{k-1} r^{-1} + \cdots + c_0 r^{-k}). \end{aligned}$$

Write $r = p/q$ where $p$ and $q$ are relatively prime. Then the left hand side of the above equation can be written as a fraction with denominator $q^{n-k}$, while the right hand side is a fraction with denominator $p^k$. Since $p$ and $q$ are relatively prime, both sides of the equation must be an integer, and the result follows.

**Remark:** If we write $r = a/b$ in lowest terms, then $P(x)$ factors as $(bx-a)Q(x)$, where the polynomial $Q$ has integer coefficients because you can either do the long division from the left and get denominators divisible only by primes dividing $b$, or do it from the right and get denominators divisible only by primes dividing $a$. The numbers given in the problem are none other than $a$ times the coefficients of $Q$. More generally, if $P(x)$ is divisible, as a polynomial over the rationals, by a polynomial $R(x)$ with integer coefficients, then $P/R$ also has integer coefficients; this is known as "Gauss's lemma" and holds in any unique factorization domain.

B–2 **First solution:** We have

$$(m+n)^{m+n} > \binom{m+n}{m} m^m n^n$$

because the binomial expansion of $(m+n)^{m+n}$ includes the term on the right as well as some others. Rearranging this inequality yields the claim.

**Remark:** One can also interpret this argument combinatorially. Suppose that we choose $m+n$ times (with replacement) uniformly randomly from a set of $m+n$ balls, of which $m$ are red and $n$ are blue. Then the probability of picking each ball exactly once is $(m+n)!/(m+n)^{m+n}$. On the other hand, if $p$ is the probability of picking exactly $m$ red balls, then $p<1$ and the probability of picking each ball exactly once is $p(m^m/m!)(n^n/n!)$.

**Second solution:** (by David Savitt) Define

$$S_k = \{i/k : i = 1,\dots,k\}$$

and rewrite the desired inequality as

$$\prod_{x \in S_m} x \prod_{y \in S_n} y > \prod_{z \in S_{m+n}} z.$$

To prove this, it suffices to check that if we sort the multiplicands on both sides into increasing order, the $i$-th term on the left side is greater than or equal to the $i$-th term on the right side. (The equality is strict already for $i=1$, so you do get a strict inequality above.)

Another way to say this is that for any $i$, the number of factors on the left side which are less than $i/(m+n)$ is less than $i$. But since $j/m < i/(m+n)$ is equivalent to $j < im/(m+n)$, that number is

$$\begin{aligned} &\left\lceil \frac{im}{m+n} \right\rceil - 1 + \left\lceil \frac{in}{m+n} \right\rceil - 1 \\ &\leq \frac{im}{m+n} + \frac{in}{m+n} - 1 = i-1. \end{aligned}$$

**Third solution:** Put $f(x) = x(\log(x+1) - \log x)$; then for $x > 0$,

$$\begin{aligned} f'(x) &= \log(1+1/x) - \frac{1}{x+1} \\ f''(x) &= -\frac{1}{x(x+1)^2}. \end{aligned}$$

Hence $f''(x) < 0$ for all $x$; since $f'(x) \to 0$ as $x \to \infty$, we have $f'(x) > 0$ for $x > 0$, so $f$ is strictly increasing.

Put $g(m) = m \log m - \log(m!)$; then $g(m+1) - g(m) = f(m)$, so $g(m+1) - g(m)$ increases with $m$. By induction, $g(m+n) - g(m)$ increases with $n$ for any positive integer $n$, so in particular

$$\begin{aligned} g(m+n) - g(m) &> g(n) - g(1) + f(m) \\ &\geq g(n) \end{aligned}$$

since $g(1) = 0$. Exponentiating yields the desired inequality.

**Fourth solution:** (by W.G. Boskoff and Bogdan Suceavă) We prove the claim by induction on $m+n$. The base case is $m=n=1$, in which case the desired inequality is obviously true: $2!/2^2 = 1/2 < 1 = (1!/1^1)(1!/1^1)$. To prove the induction step, suppose $m+n > 2$; we must then have $m > 1$ or $n > 1$ or both. Because the desired result is symmetric in $m$ and $n$, we may as well assume $n > 1$. By the induction hypothesis, we have

$$\frac{(m+n-1)!}{(m+n-1)^{m+n-1}} < \frac{m!}{m^m} \frac{(n-1)!}{(n-1)^{n-1}}.$$

To obtain the desired inequality, it will suffice to check that

$$\frac{(m+n-1)^{m+n-1}}{(m+n-1)!} \frac{(m+n)!}{(m+n)^{m+n}} < \frac{(n-1)^{n-1}}{(n-1)!} \frac{n!}{(n)^n}$$

or in other words

$$\left(1-\frac{1}{m+n}\right)^{m+n-1} < \left(1-\frac{1}{n}\right)^{n-1}.$$

To show this, we check that the function $f(x) = (1-1/x)^{x-1}$ is strictly decreasing for $x > 1$; while this can be achieved using the weighted arithmetic-geometric mean inequality, we give a simple calculus proof instead. The derivative of $\log f(x)$ is $\log(1-1/x)+1/x$, so it is enough to check that this is negative for $x > 1$. An equivalent statement is that $\log(1-x)+x < 0$ for $0 < x < 1$; this in turn holds because the function $g(x) = \log(1-x)+x$ tends to 0 as $x \to 0^+$ and has derivative $1-\frac{1}{1-x} < 0$ for $0 < x < 1$.

B–3 The answer is $\{a \,|\, a > 2\}$. If $a > 2$, then the function $f(x) = 2a/(a-2)$ has the desired property; both perimeter and area of $R$ in this case are $2a^2/(a-2)$. Now suppose that $a \leq 2$, and let $f(x)$ be a nonnegative continuous function on $[0,a]$. Let $P = (x_0, y_0)$ be a point on the graph of $f(x)$ with maximal $y$-coordinate; then the area of $R$ is at most $ay_0$ since it lies below the line $y = y_0$. On the other hand, the points $(0,0)$, $(a,0)$, and $P$ divide the boundary of $R$ into three sections. The length of the section between $(0,0)$ and $P$ is at least the distance between $(0,0)$ and $P$, which is at least $y_0$; the length of the section between $P$ and $(a,0)$ is similarly at least $y_0$; and the length of the section between $(0,0)$ and $(a,0)$ is $a$. Since $a \leq 2$, we have $2y_0 + a > ay_0$ and hence the perimeter of $R$ is strictly greater than the area of $R$.

B–4 **First solution:** Identify the $xy$-plane with the complex plane $\mathbb{C}$, so that $P_k$ is the real number $k$. If $z$ is sent to $z'$ by a counterclockwise rotation by $\theta$ about $P_k$, then $z'-k = e^{i\theta}(z-k)$; hence the rotation $R_k$ sends $z$ to $\zeta z + k(1-\zeta)$, where $\zeta = e^{2\pi i/n}$. It follows that $R_1$ followed by $R_2$ sends $z$ to $\zeta(\zeta z + (1-\zeta)) + 2(1-\zeta) = \zeta^2 z + (1-\zeta)(\zeta+2)$, and so forth; an easy induction shows that $R$ sends $z$ to

$$\zeta^n z + (1-\zeta)(\zeta^{n-1} + 2\zeta^{n-2} + \cdots + (n-1)\zeta + n).$$

Expanding the product $(1-\zeta)(\zeta^{n-1} + 2\zeta^{n-2} + \cdots + (n-1)\zeta + n)$ yields $-\zeta^n - \zeta^{n-1} - \cdots - \zeta + n = n$. Thus $R$ sends $z$ to $z+n$; in cartesian coordinates, $R(x,y) = (x+n, y)$.

**Second solution:** (by Andy Lutomirski, via Ravi Vakil) Imagine a regular $n$-gon of side length 1 placed with its top edge on the $x$-axis and the left endpoint of that edge at the origin. Then the rotations correspond to rolling this $n$-gon along the $x$-axis; after the $n$ rotations, it clearly ends up in its original rotation and translated $n$ units to the right. Hence the whole plane must do so as well.

**Third solution:** (attribution unknown) Viewing each $R_k$ as a function of a complex number $z$ as in the first solution, the function $R_n \circ R_{n-1} \circ \cdots \circ R_1(z)$ is linear in $z$ with slope $\zeta^n = 1$. It thus equals $z + T$ for some $T \in \mathbb{C}$. Since $f_1(1) = 1$, we can write $1 + T = R_n \circ \cdots \circ R_2(1)$. However, we also have

$$R_n \circ \cdots \circ R_2(1) = R_{n-1} \circ R_1(0) + 1$$

by the symmetry in how the $R_i$ are defined. Hence

$$R_n(1+T) = R_n \circ R_1(0) + R_n(1) = T + R_n(1);$$

that is, $R_n(T) = T$. Hence $T = n$, as desired.

B–5 **First solution:** By taking logarithms, we see that the desired limit is $\exp(L)$, where $L = \lim_{x\to 1^-} \sum_{n=0}^{\infty} x^n \left(\ln(1+x^{n+1}) - \ln(1+x^n)\right)$. Now

$$\begin{aligned}
&\sum_{n=0}^{N} x^n \left(\ln(1+x^{n+1}) - \ln(1+x^n)\right) \\
&= 1/x \sum_{n=0}^{N} x^{n+1} \ln(1+x^{n+1}) - \sum_{n=0}^{N} x^n \ln(1+x^n) \\
&= x^N \ln(1+x^{N+1}) - \ln 2 + (1/x-1) \sum_{n=1}^{N} x^n \ln(1+x^n);
\end{aligned}$$

since $\lim_{N\to\infty}(x^N \ln(1+x^{N+1})) = 0$ for $0 < x < 1$, we conclude that $L = -\ln 2 + \lim_{x\to 1^-} f(x)$, where

$$\begin{aligned}
f(x) &= (1/x-1) \sum_{n=1}^{\infty} x^n \ln(1+x^n) \\
&= (1/x-1) \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} (-1)^{m+1} x^{n+mn}/m.
\end{aligned}$$

This final double sum converges absolutely when $0 < x < 1$, since

$$\begin{aligned}
\sum_{n=1}^{\infty} \sum_{m=1}^{\infty} x^{n+mn}/m &= \sum_{n=1}^{\infty} x^n(-\ln(1-x^n)) \\
&< \sum_{n=1}^{\infty} x^n(-\ln(1-x)),
\end{aligned}$$

which converges. (Note that $-\ln(1-x)$ and $-\ln(1-x^n)$ are positive.) Hence we may interchange the summations in $f(x)$ to obtain

$$\begin{aligned}
f(x) &= (1/x-1) \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{(-1)^{m+1} x^{(m+1)n}}{m} \\
&= (1/x-1) \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m} \left(\frac{x^m(1-x)}{1-x^{m+1}}\right).
\end{aligned}$$

This last sum converges absolutely uniformly in $x$, so it is legitimate to take limits term by term. Since

$\lim_{x\to 1^-} \frac{x^m 1-x}{1-x^{m+1}} = \frac{1}{m+1}$ for fixed $m$, we have

$$\begin{aligned}
\lim_{x\to 1^-} f(x) &= \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m(m+1)} \\
&= \sum_{m=1}^{\infty} (-1)^{m+1} \left( \frac{1}{m} - \frac{1}{m+1} \right) \\
&= 2 \left( \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m} \right) - 1 \\
&= 2\ln 2 - 1,
\end{aligned}$$

and hence $L = \ln 2 - 1$ and the desired limit is $2/e$.

**Remark:** Note that the last series is not absolutely convergent, so the recombination must be done without rearranging terms.

**Second solution:** (by Greg Price, via Tony Zhang and Anders Kaseorg) Put $t_n(x) = \ln(1+x^n)$; we can then write $x^n = \exp(t_n(x)) - 1$, and

$$L = \lim_{x\to 1^-} \sum_{n=0}^{\infty} (t_n(x) - t_{n+1}(x))(1 - \exp(t_n(x))).$$

The expression on the right is a Riemann sum approximating the integral $\int_0^{\ln 2}(1-e^t)\,dt$, over the subdivision of $[0, \ln(2))$ given by the $t_n(x)$. As $x \to 1^-$, the maximum difference between consecutive $t_n(x)$ tends to 0, so the Riemann sum tends to the value of the integral. Hence $L = \int_0^{\ln 2}(1-e^t)\,dt = \ln 2 - 1$, as desired.

B–6 **First solution:** (based on a solution of Dan Bernstein) Note that for any $b$, the condition that $b \notin \mathscr{B}$ already forces $\limsup N(x)/x$ to be at most 1/2: pair off $2mb+n$ with $(2m+1)b+n$ for $n = 1,\dots,b$, and note that at most one member of each pair may belong to $\mathscr{A}$. The idea of the proof is to do something similar with pairs replaced by larger clumps, using long runs of excluded elements of $B$.

Suppose we have positive integers $b_0 = 1, b_1, \dots, b_n$ with the following properties:

(a) For $i = 1,\dots,n$, $c_i = b_i/(2b_{i-1})$ is an integer.

(b) For $e_i \in \{-1,0,1\}$, $|e_1 b_1 + \cdots + e_n b_n| \notin \mathscr{B}$.

Each nonnegative integer $a$ has a unique "base expansion"

$$a = a_0 b_0 + \cdots + a_{n-1} b_{n-1} + m b_n \qquad (0 \le a_i < 2c_i);$$

if two integers have expansions with the same value of $m$, and values of $a_i$ differing by at most 1 for $i = 0,\dots,n-1$, then their difference is not in $\mathscr{B}$, so at most one of them lies in $\mathscr{A}$. In particular, for any $d_i \in \{0,\dots,c_i - 1\}$, any $m_0 \in \{0, 2c_0 - 1\}$ and any $m_n$, the set

$$\{m_0 b_0 + (2d_1 + e_1) b_0 + \cdots \\ + (2d_{n-1} + e_{n-1}) b_{n-1} + (2m_n + e_n) b_n\},$$

where each $e_i$ runs over $\{0,1\}$, contains at most one element of $\mathscr{A}$; consequently, $\limsup N(x)/x \le 1/2^n$.

We now produce such $b_i$ recursively, starting with $b_0 = 1$ (and both (a) and (b) holding vacuously). Given $b_0,\dots,b_n$ satisfying (a) and (b), note that $b_0 + \cdots + b_{n-1} < b_n$ by induction on $n$. By the hypotheses of the problem, we can find a set $S_n$ of $6b_n$ consecutive integers, none of which belongs to $\mathscr{B}$. Let $b_{n+1}$ be the second-smallest multiple of $2b_n$ in $S_n$; then $b_{n+1} + x \in S_n$ for $-2b_n \le x \le 0$ clearly, and also for $0 \le x \le 2b_n$ because there are most $4b_n - 1$ elements of $S_n$ preceding $b_{n+1}$. In particular, the analogue of (b) with $n$ replaced by $n+1$ holds for $e_{n+1} \ne 0$; of course it holds for $e_{n+1} = 0$ because (b) was already known. Since the analogue of (a) holds by construction, we have completed this step of the construction and the recursion may continue.

Since we can construct $b_0,\dots,b_n$ satisfying (a) and (b) for any $n$, we have $\limsup N(x)/x \le 1/2^n$ for any $n$, yielding $\lim N(x)/x = 0$ as desired.

**Second solution:** (by Paul Pollack) Let $S$ be the set of possible values of $\limsup N(x)/x$; since $S \subseteq [0,1]$ is bounded, it has a least upper bound $L$. Suppose by way of contradiction that $L > 0$; we can then choose $\mathscr{A}, \mathscr{B}$ satisfying the conditions of the problem such that $\limsup N(x)/x > 3L/4$.

To begin with, we can certainly find some positive integer $m \notin \mathscr{B}$, so that $\mathscr{A}$ is disjoint from $\mathscr{A} + m = \{a + m : a \in \mathscr{A}\}$. Put $\mathscr{A}' = \mathscr{A} \cup (\mathscr{A} + m)$ and let $N'(x)$ be the size of $\mathscr{A}' \cap \{1,\dots,x\}$; then $\limsup N'(x)/x = 3L/2 > L$, so $\mathscr{A}'$ cannot obey the conditions of the problem statement. That is, if we let $\mathscr{B}'$ be the set of positive integers that occur as differences between elements of $\mathscr{A}'$, then there exists an integer $n$ such that among any $n$ consecutive integers, at least one lies in $\mathscr{B}'$. But

$$\mathscr{B}' \subseteq \{b + em : b \in \mathscr{B}, e \in \{-1,0,1\}\},$$

so among any $n + 2m$ consecutive integers, at least one lies in $\mathscr{B}$. This contradicts the condition of the problem statement.

We conclude that it is impossible to have $L > 0$, so $L = 0$ and $\lim N(x)/x = 0$ as desired.

**Remark:** A hybrid between these two arguments is to note that if we can produce $c_1,\dots,c_n$ such that $|c_i - c_j| \notin \mathscr{B}$ for $i,j = 1,\dots,n$, then the translates $\mathscr{A} + c_1, \dots, \mathscr{A} + c_n$ are disjoint and so $\limsup N(x)/x \le 1/n$. Given $c_1 \le \cdots \le c_n$ as above, we can then choose $c_{n+1}$ to be the largest element of a run of $c_n + 1$ consecutive integers, none of which lie in $\mathscr{B}$.

# The 66th William Lowell Putnam Mathematical Competition
# Saturday, December 3, 2005

A1 Show that every positive integer is a sum of one or more numbers of the form $2^r 3^s$, where $r$ and $s$ are nonnegative integers and no summand divides another. (For example, 23 = 9 + 8 + 6.)

A2 Let $\mathbf{S} = \{(a,b) | a = 1,2,\dots,n, b = 1,2,3\}$. A *rook tour* of $\mathbf{S}$ is a polygonal path made up of line segments connecting points $p_1, p_2, \dots, p_{3n}$ in sequence such that

(i) $p_i \in \mathbf{S}$,

(ii) $p_i$ and $p_{i+1}$ are a unit distance apart, for $1 \le i < 3n$,

(iii) for each $p \in \mathbf{S}$ there is a unique $i$ such that $p_i = p$.

How many rook tours are there that begin at $(1,1)$ and end at $(n,1)$?

(An example of such a rook tour for $n = 5$ was depicted in the original.)

A3 Let $p(z)$ be a polynomial of degree $n$ all of whose zeros have absolute value 1 in the complex plane. Put $g(z) = p(z)/z^{n/2}$. Show that all zeros of $g'(z) = 0$ have absolute value 1.

A4 Let $H$ be an $n \times n$ matrix all of whose entries are $\pm 1$ and whose rows are mutually orthogonal. Suppose $H$ has an $a \times b$ submatrix whose entries are all 1. Show that $ab \le n$.

A5 Evaluate $\int_0^1 \frac{\ln(x+1)}{x^2+1}\,dx$.

A6 Let $n$ be given, $n \ge 4$, and suppose that $P_1, P_2, \dots, P_n$ are $n$ randomly, independently and uniformly, chosen points on a circle. Consider the convex $n$-gon whose vertices are the $P_i$. What is the probability that at least one of the vertex angles of this polygon is acute?

B1 Find a nonzero polynomial $P(x,y)$ such that $P(\lfloor a \rfloor, \lfloor 2a \rfloor) = 0$ for all real numbers $a$. (Note: $\lfloor \nu \rfloor$ is the greatest integer less than or equal to $\nu$.)

B2 Find all positive integers $n, k_1, \dots, k_n$ such that $k_1 + \cdots + k_n = 5n - 4$ and

$$\frac{1}{k_1} + \cdots + \frac{1}{k_n} = 1.$$

B3 Find all differentiable functions $f : (0,\infty) \to (0,\infty)$ for which there is a positive real number $a$ such that

$$f'\left(\frac{a}{x}\right) = \frac{x}{f(x)}$$

for all $x > 0$.

B4 For positive integers $m$ and $n$, let $f(m,n)$ denote the number of $n$-tuples $(x_1, x_2, \dots, x_n)$ of integers such that $|x_1| + |x_2| + \cdots + |x_n| \le m$. Show that $f(m,n) = f(n,m)$.

B5 Let $P(x_1, \dots, x_n)$ denote a polynomial with real coefficients in the variables $x_1, \dots, x_n$, and suppose that

$$\left(\frac{\partial^2}{\partial x_1^2} + \cdots + \frac{\partial^2}{\partial x_n^2}\right) P(x_1, \dots, x_n) = 0 \quad \text{(identically)}$$

and that

$$x_1^2 + \cdots + x_n^2 \text{ divides } P(x_1, \dots, x_n).$$

Show that $P = 0$ identically.

B6 Let $S_n$ denote the set of all permutations of the numbers $1, 2, \dots, n$. For $\pi \in S_n$, let $\sigma(\pi) = 1$ if $\pi$ is an even permutation and $\sigma(\pi) = -1$ if $\pi$ is an odd permutation. Also, let $\nu(\pi)$ denote the number of fixed points of $\pi$. Show that

$$\sum_{\pi \in S_n} \frac{\sigma(\pi)}{\nu(\pi) + 1} = (-1)^{n+1} \frac{n}{n+1}.$$

# Solutions to the 66th William Lowell Putnam Mathematical Competition
# Saturday, December 3, 2005

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A–1 We proceed by induction, with base case $1 = 2^0 3^0$. Suppose all integers less than $n-1$ can be represented. If $n$ is even, then we can take a representation of $n/2$ and multiply each term by 2 to obtain a representation of $n$. If $n$ is odd, put $m = \lfloor \log_3 n \rfloor$, so that $3^m \leq n < 3^{m+1}$. If $3^m = n$, we are done. Otherwise, choose a representation $(n-3^m)/2 = s_1 + \cdots + s_k$ in the desired form. Then

$$n = 3^m + 2s_1 + \cdots + 2s_k,$$

and clearly none of the $2s_i$ divide each other or $3^m$. Moreover, since $2s_i \leq n - 3^m < 3^{m+1} - 3^m$, we have $s_i < 3^m$, so $3^m$ cannot divide $2s_i$ either. Thus $n$ has a representation of the desired form in all cases, completing the induction.

**Remarks:** This problem is originally due to Paul Erdős. Note that the representations need not be unique: for instance,

$$11 = 2 + 9 = 3 + 8.$$

A–2 We will assume $n \geq 2$ hereafter, since the answer is 0 for $n = 1$.

**First solution:** We show that the set of rook tours from $(1,1)$ to $(n,1)$ is in bijection with the set of subsets of $\{1,2,...,n\}$ that include $n$ and contain an even number of elements in total. Since the latter set evidently contains $2^{n-2}$ elements, so does the former.

We now construct the bijection. Given a rook tour $P$ from $(1,1)$ to $(n,1)$, let $S = S(P)$ denote the set of all $i \in \{1,2,\dots,n\}$ for which there is either a directed edge from $(i,1)$ to $(i,2)$ or from $(i,3)$ to $(i,2)$. It is clear that this set $S$ includes $n$ and must contain an even number of elements. Conversely, given a subset $S = \{a_1, a_2, \dots, a_{2r} = n\} \subset \{1,2,\dots,n\}$ of this type with $a_1 < a_2 < \cdots < a_{2r}$, we notice that there is a unique path $P$ containing $(a_i, 2+(-1)^i), (a_1, 2)$ for $i = 1,2,\dots,2r$. This establishes the desired bijection.

**Second solution:** Let $A_n$ denote the set of rook tours beginning at $(1,1)$ and ending at $(n,1)$, and let $B_n$ denote the set of rook tours beginning at $(1,1)$ and ending at $(n,3)$.

For $n \geq 2$, we construct a bijection between $A_n$ and $A_{n-1} \cup B_{n-1}$. Any path $P$ in $A_n$ contains either the line segment $P_1$ between $(n-1,1)$ and $(n,1)$, or the line segment $P_2$ between $(n,2)$ and $(n,1)$. In the former case, $P$ must also contain the subpath $P_1'$ which joins $(n-1,3)$, $(n,3)$, $(n,2)$, and $(n-1,2)$ consecutively; then deleting $P_1$ and $P_1'$ from $P$ and adding the line segment joining $(n-1,3)$ to $(n-1,2)$ results in a path in $A_{n-1}$. (This construction is reversible, lengthening any path in $A_{n-1}$ to a path in $A_n$.) In the latter case, $P$ contains the subpath $P_2'$ which joins $(n-1,3)$, $(n,3)$, $(n,2)$, $(n,1)$ consecutively; deleting $P_2'$ results in a path in $B_{n-1}$, and this construction is also reversible. The desired bijection follows.

Similarly, there is a bijection between $B_n$ and $A_{n-1} \cup B_{n-1}$ for $n \geq 2$. It follows by induction that for $n \geq 2$, $|A_n| = |B_n| = 2^{n-2}(|A_1| + |B_1|)$. But $|A_1| = 0$ and $|B_1| = 1$, and hence the desired answer is $|A_n| = 2^{n-2}$.

**Remarks:** Other bijective arguments are possible: for instance, Noam Elkies points out that each element of $A_n \cup B_n$ contains a different one of the possible sets of segments of the form $(i,2),(i+1,2)$ for $i = 1,\dots,n-1$. Richard Stanley provides the reference: K.L. Collins and L.B. Krompart, The number of Hamiltonian paths in a rectangular grid, *Discrete Math.* **169** (1997), 29–38. This problem is Theorem 1 of that paper; the cases of $4 \times n$ and $5 \times n$ grids are also treated. The paper can also be found online at the URL `kcollins.web.wesleyan.edu/vita.htm`.

A–3 Note that it is implicit in the problem that $p$ is nonconstant, one may take any branch of the square root, and that $z = 0$ should be ignored.

**First solution:** Write $p(z) = c\prod_{j=1}^n (z - r_j)$, so that

$$\frac{g'(z)}{g(z)} = \frac{1}{2z}\sum_{j=1}^n \frac{z+r_j}{z-r_j}.$$

Now if $z \neq r_j$ for all $j$,then

$$\frac{z+r_j}{z-r_j} = \frac{(z+r_j)(\bar{z}-\overline{r_j})}{|z-r_j|^2} = \frac{|z|^2 - 1 + 2\mathrm{Im}(\bar{z}r_j)}{|z-r_j|^2},$$

and so

$$\mathrm{Re}\,\frac{zg'(z)}{g(z)} = \frac{|z|^2-1}{2}\left(\sum_j \frac{1}{|z-r_j|^2}\right).$$

Since the quantity in parentheses is positive, $g'(z)/g(z)$ can be 0 only if $|z| = 1$. If on the other hand $z = r_j$ for some $j$, then $|z| = 1$ anyway.

**Second solution:** Write $p(z) = c\prod_{j=1}^n (z - r_j)$, so that

$$\frac{g'(z)}{g(z)} = \sum_{j=1}^n \left(\frac{1}{z-r_j} - \frac{1}{2z}\right).$$

We first check that $g'(z) \neq 0$ whenever $z$ is real and $z > 1$. In this case, for $r_j = e^{i\theta_j}$, we have $z - r_j = (z -$

$\cos(\theta_j)) + \sin(\theta_j)i$, so the real part of $\frac{1}{z-r_j} - \frac{1}{2z}$ is

$$\frac{z-\cos(\theta_j)}{z^2-2z\cos(\theta_j)+1} - \frac{1}{2z} = \frac{z^2-1}{2z(z^2-2z\cos(\theta_j)+1)} > 0.$$

Hence $g'(z)/g(z)$ has positive real part, so $g'(z)/g(z)$ and hence $g(z)$ are nonzero.

Applying the same argument after replacing $p(z)$ by $p(e^{i\theta}z)$, we deduce that $g'$ cannot have any roots outside the unit circle. Applying the same argument after replacing $p(z)$ by $z^n p(1/z)$, we also deduce that $g'$ cannot have any roots inside the unit circle. Hence all roots of $g'$ have absolute value 1, as desired.

**Third solution:** Write $p(z) = c\prod_{j=1}^n (z-r_j)$ and put $r_j = e^{2i\theta_j}$. Note that $g(e^{2i\theta})$ is equal to a nonzero constant times

$$h(\theta) = \prod_{j=1}^n \frac{e^{i(\theta+\theta_j)} - e^{-i(\theta+\theta_j)}}{2i} = \prod_{j=1}^n \sin(\theta+\theta_j).$$

Since $h$ has at least $2n$ roots (counting multiplicity) in the interval $[0,2\pi)$, $h'$ does also by repeated application of Rolle's theorem. Since $g'(e^{2i\theta}) = 2ie^{2i\theta}h'(\theta)$, $g'(z^2)$ has at least $2n$ roots on the unit circle. Since $g'(z^2)$ is equal to $z^{-n-1}$ times a polynomial of degree $2n$, $g'(z^2)$ has all roots on the unit circle, as then does $g'(z)$.

**Remarks:** The second solution imitates the proof of the Gauss-Lucas theorem: the roots of the derivative of a complex polynomial lie in the convex hull of the roots of the original polynomial. The second solution is close to problem B3 from the 2000 Putnam. A hybrid between the first and third solutions is to check that on the unit circle, $\mathrm{Re}(zg'(z)/g(z)) = 0$ while between any two roots of $p$, $\mathrm{Im}(zg'(z)/g(z))$ runs from $+\infty$ to $-\infty$ and so must have a zero crossing. (This only works when $p$ has distinct roots, but the general case follows by the continuity of the roots of a polynomial as functions of the coefficients.) One can also construct a solution using Rouché's theorem.

A–4 **First solution:** Choose a set of $a$ rows $r_1,\dots,r_a$ containing an $a\times b$ submatrix whose entries are all 1. Then for $i,j\in\{1,\dots,a\}$, we have $r_i\cdot r_j = n$ if $i=j$ and 0 otherwise. Hence

$$\sum_{i,j=1}^{a} r_i\cdot r_j = an.$$

On the other hand, the term on the left is the dot product of $r_1+\cdots+r_a$ with itself, i.e., its squared length. Since this vector has $a$ in each of its first $b$ coordinates, the dot product is at least $a^2b$. Hence $an \geq a^2b$, whence $n\geq ab$ as desired.

**Second solution:** (by Richard Stanley) Suppose without loss of generality that the $a\times b$ submatrix occupies the first $a$ rows and the first $b$ columns. Let $M$ be the submatrix occupying the first $a$ rows and the last $n-b$ columns. Then the hypothesis implies that the matrix $MM^T$ has $n-b$'s on the main diagonal and $-b$'s elsewhere. Hence the column vector $v$ of length $a$ consisting of all 1's satisfies $MM^Tv = (n-ab)v$, so $n-ab$ is an eigenvalue of $MM^T$. But $MM^T$ is semidefinite, so its eigenvalues are all nonnegative real numbers. Hence $n-ab\geq 0$.

**Remarks:** A matrix as in the problem is called a *Hadamard matrix*, because it meets the equality condition of Hadamard's inequality: any $n\times n$ matrix with $\pm1$ entries has absolute determinant at most $n^{n/2}$, with equality if and only if the rows are mutually orthogonal (from the interpretation of the determinant as the volume of a paralellepiped whose edges are parallel to the row vectors). Note that this implies that the columns are also mutually orthogonal. A generalization of this problem, with a similar proof, is known as *Lindsey's lemma*: the sum of the entries in any $a\times b$ submatrix of a Hadamard matrix is at most $\sqrt{abn}$. Stanley notes that Ryser (1981) asked for the smallest size of a Hadamard matrix containing an $r\times s$ submatrix of all 1's, and refers to the URL `www3.interscience.wiley.com/cgi-bin/abstract/110550861/ABSTRACT` for more information.

A–5 **First solution:** We make the substitution $x=\tan\theta$, rewriting the desired integral as

$$\int_0^{\pi/4} \log(\tan(\theta)+1)\,d\theta.$$

Write

$$\log(\tan(\theta)+1) = \log(\sin(\theta)+\cos(\theta)) - \log(\cos(\theta))$$

and then note that $\sin(\theta)+\cos(\theta) = \sqrt{2}\cos(\pi/4-\theta)$. We may thus rewrite the integrand as

$$\frac{1}{2}\log(2) + \log(\cos(\pi/4-\theta)) - \log(\cos(\theta)).$$

But over the interval $[0,\pi/4]$, the integrals of $\log(\cos(\theta))$ and $\log(\cos(\pi/4-\theta))$ are equal, so their contributions cancel out. The desired integral is then just the integral of $\frac{1}{2}\log(2)$ over the interval $[0,\pi/4]$, which is $\pi\log(2)/8$.

**Second solution:** (by Roger Nelsen) Let $I$ denote the desired integral. We make the substitution $x=(1-u)/(1+u)$ to obtain

$$\begin{aligned} I &= \int_0^1 \frac{(1+u)^2\log(2/(1+u))}{2(1+u^2)}\frac{2\,du}{(1+u)^2} \\ &= \int_0^1 \frac{\log(2)-\log(1+u)}{1+u^2}\,du \\ &= \log(2)\int_0^1 \frac{du}{1+u^2} - I, \end{aligned}$$

yielding

$$I = \frac{1}{2}\log(2)\int_0^1 \frac{du}{1+u^2} = \frac{\pi \log(2)}{8}.$$

**Third solution:** (attributed to Steven Sivek) Define the function

$$f(t) = \int_0^1 \frac{\log(xt+1)}{x^2+1}\,dx$$

so that $f(0) = 0$ and the desired integral is $f(1)$. Then by differentiation under the integral,

$$f'(t) = \int_0^1 \frac{x}{(xt+1)(x^2+1)}\,dx.$$

By partial fractions, we obtain

$$\begin{aligned} f'(t) &= \left.\frac{2t\arctan(x) - 2\log(tx+1) + \log(x^2+1)}{2(t^2+1)}\right|_{x=0}^{x=1} \\ &= \frac{\pi t + 2\log(2) - 4\log(t+1)}{4(t^2+1)}, \end{aligned}$$

whence

$$f(t) = \frac{\log(2)\arctan(t)}{2} + \frac{\pi\log(t^2+1)}{8} - \int_0^t \frac{\log(t+1)}{t^2+1}\,dt$$

and hence

$$f(1) = \frac{\pi\log(2)}{4} - \int_0^1 \frac{\log(t+1)}{t^2+1}\,dt.$$

But the integral on the right is again the desired integral $f(1)$, so we may move it to the left to obtain

$$2f(1) = \frac{\pi\log(2)}{4}$$

and hence $f(1) = \pi\log(2)/8$ as desired.

**Fourth solution:** (by David Rusin) We have

$$\int_0^1 \frac{\log(x+1)}{x^2+1}\,dx = \int_0^1 \left( \sum_{n=1}^{\infty} \frac{(-1)^{n-1}x^n}{n(x^2+1)} \right) dx.$$

We next justify moving the sum through the integral sign. Note that

$$\sum_{n=1}^{\infty} \int_0^1 \frac{(-1)^{n-1}x^n\,dx}{n(x^2+1)}$$

is an alternating series whose terms strictly decrease to zero, so it converges. Moreover, its partial sums alternately bound the previous integral above and below, so the sum of the series coincides with the integral.

Put

$$J_n = \int_0^1 \frac{x^n\,dx}{x^2+1};$$

then $J_0 = \arctan(1) = \frac{\pi}{4}$ and $J_1 = \frac{1}{2}\log(2)$. Moreover,

$$J_n + J_{n+2} = \int_0^1 x^n\,dx = \frac{1}{n+1}.$$

Write

$$\begin{aligned} A_m &= \sum_{i=1}^{m} \frac{(-1)^{i-1}}{2i-1} \\ B_m &= \sum_{i=1}^{m} \frac{(-1)^{i-1}}{2i}; \end{aligned}$$

then

$$\begin{aligned} J_{2n} &= (-1)^n(J_0 - A_n) \\ J_{2n+1} &= (-1)^n(J_1 - B_n). \end{aligned}$$

Now the $2N$-th partial sum of our series equals

$$\begin{aligned} &\sum_{n=1}^{N} \left[ \frac{J_{2n-1}}{2n-1} - \frac{J_{2n}}{2n} \right] \\ &= \sum_{n=1}^{N} \frac{(-1)^{n-1}}{2n-1} \left[ (J_1 - B_{n-1}) - \frac{(-1)^n}{2n}(J_0 - A_n) \right] \\ &= A_N(J_1 - B_{N-1}) + B_N(J_0 - A_N) + A_N B_N. \end{aligned}$$

As $N \to \infty$, $A_N \to J_0$ and $B_N \to J_1$, so the sum tends to $J_0 J_1 = \pi\log(2)/8$.

**Fifth solution:** (suggested by Alin Bostan) Note that

$$\log(1+x) = \int_0^1 \frac{x\,dy}{1+xy},$$

so the desired integral $I$ may be written as

$$I = \int_0^1 \int_0^1 \frac{x\,dy\,dx}{(1+xy)(1+x^2)}.$$

We may interchange $x$ and $y$ in this expression, then use Fubini's theorem to interchange the order of summation, to obtain

$$I = \int_0^1 \int_0^1 \frac{y\,dy\,dx}{(1+xy)(1+y^2)}.$$

We then add these expressions to obtain

$$\begin{aligned} 2I &= \int_0^1 \int_0^1 \left( \frac{x}{1+x^2} + \frac{y}{1+y^2} \right) \frac{dy\,dx}{1+xy} \\ &= \int_0^1 \int_0^1 \frac{x+y+xy^2+x^2y}{(1+x^2)(1+y^2)} \frac{dy\,dx}{1+xy} \\ &= \int_0^1 \int_0^1 \frac{(x+y)\,dy\,dx}{(1+x^2)(1+y^2)}. \end{aligned}$$

By another symmetry argument, we have

$$2I = 2\int_0^1 \int_0^1 \frac{x\,dy\,dx}{(1+x^2)(1+y^2)},$$

so

$$I = \left(\int_0^1 \frac{x\,dx}{1+x^2}\right)\left(\int_0^1 \frac{1}{1+y^2}\right) = \log(2)\cdot\frac{\pi}{8}.$$

**Remarks:** The first two solutions are related by the fact that if $x = \tan(\theta)$, then $1 - x/(1+x) = \tan(\pi/4 - \theta)$. The strategy of the third solution (introducing a parameter then differentiating it) was a favorite of physics Nobelist (and Putnam Fellow) Richard Feynman. The fifth solution resembles Gauss's evaluation of $\int_{-\infty}^{\infty} \exp(-x^2)\,dx$. Noam Elkies notes that this integral is number 2.491#8 in Gradshteyn and Ryzhik, *Table of integrals, series, and products*. The *Mathematica* computer algebra system (version 5.2) successfully computes this integral, but we do not know how.

A–6 **First solution:** The angle at a vertex $P$ is acute if and only if all of the other points lie on an open semicircle. We first deduce from this that if there are any two acute angles at all, they must occur consecutively. Suppose the contrary; label the vertices $Q_1,\dots,Q_n$ in counterclockwise order (starting anywhere), and suppose that the angles at $Q_1$ and $Q_i$ are acute for some $i$ with $3 \leq i \leq n-1$. Then the open semicircle starting at $Q_2$ and proceeding counterclockwise must contain all of $Q_3,\dots,Q_n$, while the open semicircle starting at $Q_i$ and proceeding counterclockwise must contain $Q_{i+1},\dots,Q_n,Q_1,\dots,Q_{i-1}$. Thus two open semicircles cover the entire circle, contradiction.

It follows that if the polygon has at least one acute angle, then it has either one acute angle or two acute angles occurring consecutively. In particular, there is a unique pair of consecutive vertices $Q_1, Q_2$ in counterclockwise order for which $\angle Q_2$ is acute and $\angle Q_1$ is not acute. Then the remaining points all lie in the arc from the antipode of $Q_1$ to $Q_1$, but $Q_2$ cannot lie in the arc, and the remaining points cannot all lie in the arc from the antipode of $Q_1$ to the antipode of $Q_2$. Given the choice of $Q_1, Q_2$, let $x$ be the measure of the counterclockwise arc from $Q_1$ to $Q_2$; then the probability that the other points fall into position is $2^{-n+2} - x^{n-2}$ if $x \leq 1/2$ and 0 otherwise.

Hence the probability that the polygon has at least one acute angle with a *given* choice of which two points will act as $Q_1$ and $Q_2$ is

$$\int_0^{1/2} (2^{-n+2} - x^{n-2})\,dx = \frac{n-2}{n-1}2^{-n+1}.$$

Since there are $n(n-1)$ choices for which two points act as $Q_1$ and $Q_2$, the probability of at least one acute angle is $n(n-2)2^{-n+1}$.

**Second solution:** (by Calvin Lin) As in the first solution, we may compute the probability that for a particular one of the points $Q_1$, the angle at $Q_1$ is not acute but the following angle is, and then multiply by $n$. Imagine picking the points by first choosing $Q_1$, then picking $n-1$ *pairs* of antipodal points and then picking one member of each pair. Let $R_2,\dots,R_n$ be the points of the pairs which lie in the semicircle, taken in order away from $Q_1$, and let $S_2,\dots,S_n$ be the antipodes of these. Then to get the desired situation, we must choose from the pairs to end up with all but one of the $S_i$, and we cannot take $R_n$ and the other $S_i$ or else $\angle Q_1$ will be acute. That gives us $(n-2)$ good choices out of $2^{n-1}$; since we could have chosen $Q_1$ to be any of the $n$ points, the probability is again $n(n-2)2^{-n+1}$.

B–1 Take $P(x,y) = (y-2x)(y-2x-1)$. To see that this works, first note that if $m = \lfloor a \rfloor$, then $2m$ is an integer less than or equal to $2a$, so $2m \leq \lfloor 2a \rfloor$. On the other hand, $m+1$ is an integer strictly greater than $a$, so $2m+2$ is an integer strictly greater than $2a$, so $\lfloor 2a \rfloor \leq 2m+1$.

B–2 By the arithmetic-harmonic mean inequality or the Cauchy-Schwarz inequality,

$$(k_1 + \cdots + k_n)\left(\frac{1}{k_1} + \cdots + \frac{1}{k_n}\right) \geq n^2.$$

We must thus have $5n - 4 \geq n^2$, so $n \leq 4$. Without loss of generality, we may suppose that $k_1 \leq \cdots \leq k_n$.

If $n = 1$, we must have $k_1 = 1$, which works. Note that hereafter we cannot have $k_1 = 1$.

If $n = 2$, we have $(k_1,k_2) \in \{(2,4),(3,3)\}$, neither of which work.

If $n = 3$, we have $k_1 + k_2 + k_3 = 11$, so $2 \leq k_1 \leq 3$. Hence

$$(k_1,k_2,k_3) \in \{(2,2,7),(2,3,6),(2,4,5),(3,3,5),(3,4,4)\},$$

and only $(2,3,6)$ works.

If $n = 4$, we must have equality in the AM-HM inequality, which only happens when $k_1 = k_2 = k_3 = k_4 = 4$.

Hence the solutions are $n = 1$ and $k_1 = 1$, $n = 3$ and $(k_1,k_2,k_3)$ is a permutation of $(2,3,6)$, and $n = 4$ and $(k_1,k_2,k_3,k_4) = (4,4,4,4)$.

**Remark:** In the cases $n = 2,3$, Greg Kuperberg suggests the alternate approach of enumerating the solutions of $1/k_1 + \cdots + 1/k_n = 1$ with $k_1 \leq \cdots \leq k_n$. This is easily done by proceeding in lexicographic order: one obtains $(2,2)$ for $n = 2$, and $(2,3,6),(2,4,4),(3,3,3)$ for $n = 3$, and only $(2,3,6)$ contributes to the final answer.

B–3 **First solution:** The functions are precisely $f(x) = cx^d$ for $c,d > 0$ arbitrary except that we must take $c = 1$ in case $d = 1$. To see that these work, note that $f'(a/x) = dc(a/x)^{d-1}$ and $x/f(x) = 1/(cx^{d-1})$, so the given equation holds if and only if $dc^2a^{d-1} = 1$. If $d \neq 1$, we may solve for $a$ no matter what $c$ is; if $d = 1$, we must have $c = 1$. (Thanks to Brad Rodgers for pointing out the $d = 1$ restriction.)

To check that these are all solutions, put $b = \log(a)$ and $y = \log(a/x)$; rewrite the given equation as

$$f(e^{b-y})f'(e^y) = e^{b-y}.$$

Put

$$g(y) = \log f(e^y);$$

then the given equation rewrites as

$$g(b-y) + \log g'(y) + g(y) - y = b - y,$$

or

$$\log g'(y) = b - g(y) - g(b-y).$$

By the symmetry of the right side, we have $g'(b-y) = g'(y)$. Hence the function $g(y) + g(b-y)$ has zero derivative and so is constant, as then is $g'(y)$. From this we deduce that $f(x) = cx^d$ for some $c,d$, both necessarily positive since $f'(x) > 0$ for all $x$.

**Second solution:** (suggested by several people) Substitute $a/x$ for $x$ in the given equation:

$$f'(x) = \frac{a}{xf(a/x)}.$$

Differentiate:

$$f''(x) = -\frac{a}{x^2 f(a/x)} + \frac{a^2 f'(a/x)}{x^3 f(a/x)^2}.$$

Now substitute to eliminate evaluations at $a/x$:

$$f''(x) = -\frac{f'(x)}{x} + \frac{f'(x)^2}{f(x)}.$$

Clear denominators:

$$xf(x)f''(x) + f(x)f'(x) = xf'(x)^2.$$

Divide through by $f(x)^2$ and rearrange:

$$0 = \frac{f'(x)}{f(x)} + \frac{xf''(x)}{f(x)} - \frac{xf'(x)^2}{f(x)^2}.$$

The right side is the derivative of $xf'(x)/f(x)$, so that quantity is constant. That is, for some $d$,

$$\frac{f'(x)}{f(x)} = \frac{d}{x}.$$

Integrating yields $f(x) = cx^d$, as desired.

B–4 **First solution:** Define $f(m,n,k)$ as the number of $n$-tuples $(x_1, x_2, \dots, x_n)$ of integers such that $|x_1| + \cdots + |x_n| \leq m$ and exactly $k$ of $x_1, \dots, x_n$ are nonzero. To choose such a tuple, we may choose the $k$ nonzero positions, the signs of those $k$ numbers, and then an ordered $k$-tuple of positive integers with sum $\leq m$. There are $\binom{n}{k}$ options for the first choice, and $2^k$ for the second. As for the third, we have $\binom{m}{k}$ options by a "stars and bars" argument: depict the $k$-tuple by drawing a number of stars for each term, separated by bars, and adding stars at the end to get a total of $m$ stars. Then each tuple corresponds to placing $k$ bars, each in a different position behind one of the $m$ fixed stars.

We conclude that

$$f(m,n,k) = 2^k \binom{m}{k} \binom{n}{k} = f(n,m,k);$$

summing over $k$ gives $f(m,n) = f(n,m)$. (One may also extract easily a bijective interpretation of the equality.)

**Second solution:** (by Greg Kuperberg) It will be convenient to extend the definition of $f(m,n)$ to $m,n \geq 0$, in which case we have $f(0,m) = f(n,0) = 1$.

Let $S_{m,n}$ be the set of $n$-tuples $(x_1, \dots, x_n)$ of integers such that $|x_1| + \cdots + |x_n| \leq m$. Then elements of $S_{m,n}$ can be classified into three types. Tuples with $|x_1| + \cdots + |x_n| < m$ also belong to $S_{m-1,n}$. Tuples with $|x_1| + \cdots + |x_n| = m$ and $x_n \geq 0$ correspond to elements of $S_{m,n-1}$ by dropping $x_n$. Tuples with $|x_1| + \cdots + |x_n| = m$ and $x_n < 0$ correspond to elements of $S_{m-1,n-1}$ by dropping $x_n$. It follows that

$$f(m,n) = f(m-1,n) + f(m,n-1) + f(m-1,n-1),$$

so $f$ satisfies a symmetric recurrence with symmetric boundary conditions $f(0,m) = f(n,0) = 1$. Hence $f$ is symmetric.

**Third solution:** (by Greg Martin) As in the second solution, it is convenient to allow $f(m,0) = f(0,n) = 1$. Define the generating function

$$G(x,y) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} f(m,n) x^m y^n.$$

As equalities of formal power series (or convergent series on, say, the region $|x|,|y| < \frac{1}{3}$), we have

$$\begin{aligned}
G(x,y) &= \sum_{m\geq 0} \sum_{n \geq 0} x^m y^n \sum_{\substack{k_1,\dots,k_n \in \mathbb{Z} \\ |k_1|+\cdots+|k_n| \leq m}} 1 \\
&= \sum_{n\geq 0} y^n \sum_{k_1,\dots,k_n \in \mathbb{Z}} \sum_{m \geq |k_1|+\cdots+|k_n|} x^m \\
&= \sum_{n\geq 0} y^n \sum_{k_1,\dots,k_n \in \mathbb{Z}} \frac{x^{|k_1|+\cdots+|k_n|}}{1-x} \\
&= \frac{1}{1-x} \sum_{n\geq 0} y^n \left( \sum_{k \in \mathbb{Z}} x^{|k|} \right)^n \\
&= \frac{1}{1-x} \sum_{n\geq 0} y^n \left( \frac{1+x}{1-x} \right)^n \\
&= \frac{1}{1-x} \cdot \frac{1}{1-y(1+x)/(1-x)} \\
&= \frac{1}{1-x-y-xy}.
\end{aligned}$$

Since $G(x,y) = G(y,x)$, it follows that $f(m,n) = f(n,m)$ for all $m,n \geq 0$.

B–5 **First solution:** Put $Q = x_1^2 + \cdots + x_n^2$. Since $Q$ is homogeneous, $P$ is divisible by $Q$ if and only if each of the homogeneous components of $P$ is divisible by $Q$. It is thus sufficient to solve the problem in case $P$ itself is homogeneous, say of degree $d$.

Suppose that we have a factorization $P = Q^m R$ for some $m > 0$, where $R$ is homogeneous of degree $d$ and not divisible by $Q$; note that the homogeneity implies that

$$\sum_{i=1}^n x_i \frac{\partial R}{\partial x_i} = dR.$$

Write $\nabla^2$ as shorthand for $\frac{\partial^2}{\partial x_1^2} + \cdots + \frac{\partial^2}{\partial x_n^2}$; then

$$\begin{aligned} 0 &= \nabla^2 P \\ &= 2mnQ^{m-1}R + Q^m \nabla^2 R + 2\sum_{i=1}^n 2mx_i Q^{m-1} \frac{\partial R}{\partial x_i} \\ &= Q^m \nabla^2 R + (2mn + 4md) Q^{m-1} R. \end{aligned}$$

Since $m > 0$, this forces $R$ to be divisible by $Q$, contradiction.

**Second solution:** (by Noam Elkies) Retain notation as in the first solution. Let $P_d$ be the set of homogeneous polynomials of degree $d$, and let $H_d$ be the subset of $P_d$ of polynomials killed by $\nabla^2$, which has dimension $\geq \dim(P_d) - \dim(P_{d-2})$; the given problem amounts to showing that this inequality is actually an equality.

Consider the operator $Q\nabla^2$ (i.e., apply $\nabla^2$ then multiply by $Q$) on $P_d$; its zero eigenspace is precisely $H_d$. By the calculation from the first solution, if $R \in P_d$, then

$$\nabla^2(QR) - Q\nabla^2 R = (2n + 4d)R.$$

Consequently, $Q^j H_{d-2j}$ is contained in the eigenspace of $Q\nabla^2$ on $P_d$ of eigenvalue

$$(2n + 4(d-2j)) + \cdots + (2n + 4(d-2)).$$

In particular, the $Q^j H^{d-2j}$ lie in distinct eigenspaces, so are linearly independent within $P_d$. But by dimension counting, their total dimension is at least that of $P_d$. Hence they exhaust $P_d$, and the zero eigenspace cannot have dimension greater than $\dim(P_d) - \dim(P_{d-2})$, as desired.

**Third solution:** (by Richard Stanley) Write $x = (x_1, \dots, x_n)$ and $\nabla = (\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_n})$. Suppose that $P(x) = Q(x)(x_1^2 + \cdots + x_n^2)$. Then

$$P(\nabla)P(x) = Q(\nabla)(\nabla^2)P(x) = 0.$$

On the other hand, if $P(x) = \sum_\alpha c_\alpha x^\alpha$ (where $\alpha = (\alpha_1, \dots, \alpha_n)$ and $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$), then the constant term of $P(\nabla)P(x)$ is seen to be $\sum_\alpha c_\alpha^2$. Hence $c_\alpha = 0$ for all $\alpha$.

**Remarks:** The first two solutions apply directly over any field of characteristic zero. (The result fails in characteristic $p > 0$ because we may take $P = (x_1^2 + \cdots + x_n^2)^p = x_1^{2p} + \cdots + x_n^{2p}$.) The third solution can be extended to complex coefficients by replacing $P(\nabla)$ by its complex conjugate, and again the result may be deduced for any field of characteristic zero. Stanley also suggests Section 5 of the arXiv e-print `math.CO/0502363` for some algebraic background for this problem.

B–6 **First solution:** Let $I$ be the identity matrix, and let $J_x$ be the matrix with $x$'s on the diagonal and 1's elsewhere. Note that $J_x - (x-1)I$, being the all 1's matrix, has rank 1 and trace $n$, so has $n-1$ eigenvalues equal to 0 and one equal to $n$. Hence $J_x$ has $n-1$ eigenvalues equal to $x-1$ and one equal to $x+n-1$, implying

$$\det J_x = (x+n-1)(x-1)^{n-1}.$$

On the other hand, we may expand the determinant as a sum indexed by permutations, in which case we get

$$\det J_x = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) x^{\nu(\pi)}.$$

Integrating both sides from 0 to 1 (and substituting $y = 1-x$) yields

$$\begin{aligned} \sum_{\pi \in S_n} \frac{\operatorname{sgn}(\pi)}{\nu(\pi)+1} &= \int_0^1 (x+n-1)(x-1)^{n-1}\,dx \\ &= \int_0^1 (-1)^{n+1}(n-y)y^{n-1}\,dy \\ &= (-1)^{n+1}\frac{n}{n+1}, \end{aligned}$$

as desired.

**Second solution:** We start by recalling a form of the principle of inclusion-exclusion: if $f$ is a function on the power set of $\{1, \dots, n\}$, then

$$f(S) = \sum_{T \supseteq S} (-1)^{|T|-|S|} \sum_{U \supseteq T} f(U).$$

In this case we take $f(S)$ to be the sum of $\sigma(\pi)$ over all permutations $\pi$ whose fixed points are exactly $S$. Then $\sum_{U \supseteq T} f(U) = 1$ if $|T| \geq n-1$ and 0 otherwise (since a permutation group on 2 or more symbols has as many even and odd permutations), so

$$f(S) = (-1)^{n-|S|}(1 - n + |S|).$$

The desired sum can thus be written, by grouping over fixed point sets, as

$$\begin{aligned} \sum_{i=0}^n \binom{n}{i} (-1)^{n-i} \frac{1-n+i}{i+1} &= \sum_{i=0}^n (-1)^{n-i}\binom{n}{i} - \sum_{i=0}^n (-1)^{n-i}\frac{n}{i+1}\binom{n}{i} \\ &= 0 - \sum_{i=0}^n (-1)^{n-i}\frac{n}{n+1}\binom{n+1}{i+1} \\ &= (-1)^{n+1}\frac{n}{n+1}. \end{aligned}$$

**Third solution:** (by Richard Stanley) The *cycle indicator* of the symmetric group $S_n$ is defined by

$$Z_n(x_1,\dots,x_n) = \sum_{\pi\in S_n} x_1^{c_1(\pi)}\cdots x_n^{c_n(\pi)},$$

where $c_i(\pi)$ is the number of cycles of $\pi$ of length $i$. Put

$$F_n = \sum_{\pi\in S_n} \sigma(\pi)x^{\nu(\pi)} = Z_n(x,-1,1,-1,1,\dots)$$

and

$$f(n) = \sum_{\pi\in S_n} \frac{\sigma(\pi)}{\nu(\pi)+1} = \int_0^1 F_n(x)\,dx.$$

A standard argument in enumerative combinatorics (the Exponential Formula) gives

$$\sum_{n=0}^{\infty} Z_n(x_1,\dots,x_n)\frac{t^n}{n!} = \exp\sum_{k=1}^{\infty} x_k\frac{t^k}{k},$$

yielding

$$\begin{aligned}\sum_{n=0}^{\infty} f(n)\frac{t^n}{n!} &= \int_0^1 \exp\left(xt - \frac{t^2}{2} + \frac{t^3}{3} - \cdots\right) dx\\ &= \int_0^1 e^{(x-1)t+\log(1+t)}\,dx\\ &= \int_0^1 (1+t)e^{(x-1)t}\,dx\\ &= \frac{1}{t}(1-e^{-t})(1+t).\end{aligned}$$

Expanding the right side as a Taylor series and comparing coefficients yields the desired result.

**Fourth solution (sketch):** (by David Savitt) We prove the identity of rational functions

$$\sum_{\pi\in S_n} \frac{\sigma(\pi)}{\nu(\pi)+x} = \frac{(-1)^{n+1}n!(x+n-1)}{x(x+1)\cdots(x+n)}$$

by induction on $n$, which for $x=1$ implies the desired result. (This can also be deduced as in the other solutions, but in this argument it is necessary to formulate the strong induction hypothesis.)

Let $R(n,x)$ be the right hand side of the above equation. It is easy to verify that

$$\begin{aligned}R(x,n) = R(x+1,n-1) + (n-1)!\frac{(-1)^{n+1}}{x}\\ + \sum_{l=2}^{n-1}(-1)^{l-1}\frac{(n-1)!}{(n-l)!}R(x,n-l),\end{aligned}$$

since the sum telescopes. To prove the desired equality, it suffices to show that the left hand side satisfies the same recurrence. This follows because we can classify each $\pi\in S_n$ as either fixing $n$, being an $n$-cycle, or having $n$ in an $l$-cycle for one of $l=2,\dots,n-1$; writing the sum over these classes gives the desired recurrence.

# The 67th William Lowell Putnam Mathematical Competition
# Saturday, December 2, 2006

A–1 Find the volume of the region of points $(x,y,z)$ such that
$$(x^2+y^2+z^2+8)^2 \leq 36(x^2+y^2).$$

A–2 Alice and Bob play a game in which they take turns removing stones from a heap that initially has $n$ stones. The number of stones removed at each turn must be one less than a prime number. The winner is the player who takes the last stone. Alice plays first. Prove that there are infinitely many $n$ such that Bob has a winning strategy. (For example, if $n = 17$, then Alice might take 6 leaving 11; then Bob might take 1 leaving 10; then Alice can take the remaining stones to win.)

A–3 Let $1,2,3,\dots,2005,2006,2007,2009,2012,2016,\dots$ be a sequence defined by $x_k = k$ for $k = 1,2,\dots,2006$ and $x_{k+1} = x_k + x_{k-2005}$ for $k \geq 2006$. Show that the sequence has 2005 consecutive terms each divisible by 2006.

A–4 Let $S = \{1,2,\dots,n\}$ for some integer $n > 1$. Say a permutation $\pi$ of $S$ has a *local maximum* at $k \in S$ if

(i) $\pi(k) > \pi(k+1)$ for $k = 1$;

(ii) $\pi(k-1) < \pi(k)$ and $\pi(k) > \pi(k+1)$ for $1 < k < n$;

(iii) $\pi(k-1) < \pi(k)$ for $k = n$.

(For example, if $n = 5$ and $\pi$ takes values at $1,2,3,4,5$ of $2,1,4,5,3$, then $\pi$ has a local maximum of 2 at $k = 1$, and a local maximum of 5 at $k = 4$.) What is the average number of local maxima of a permutation of $S$, averaging over all permutations of $S$?

A–5 Let $n$ be a positive odd integer and let $\theta$ be a real number such that $\theta/\pi$ is irrational. Set $a_k = \tan(\theta + k\pi/n)$, $k = 1,2,\dots,n$. Prove that
$$\frac{a_1+a_2+\cdots+a_n}{a_1a_2\cdots a_n}$$
is an integer, and determine its value.

A–6 Four points are chosen uniformly and independently at random in the interior of a given circle. Find the probability that they are the vertices of a convex quadrilateral.

B–1 Show that the curve $x^3+3xy+y^3 = 1$ contains only one set of three distinct points, $A$, $B$, and $C$, which are vertices of an equilateral triangle, and find its area.

B–2 Prove that, for every set $X = \{x_1,x_2,\dots,x_n\}$ of $n$ real numbers, there exists a non-empty subset $S$ of $X$ and an integer $m$ such that
$$\left| m + \sum_{s\in S} s \right| \leq \frac{1}{n+1}.$$

B–3 Let $S$ be a finite set of points in the plane. A linear partition of $S$ is an unordered pair $\{A,B\}$ of subsets of $S$ such that $A \cup B = S$, $A \cap B = \emptyset$, and $A$ and $B$ lie on opposite sides of some straight line disjoint from $S$ ($A$ or $B$ may be empty). Let $L_S$ be the number of linear partitions of $S$. For each positive integer $n$, find the maximum of $L_S$ over all sets $S$ of $n$ points.

B–4 Let $Z$ denote the set of points in $\mathbb{R}^n$ whose coordinates are 0 or 1. (Thus $Z$ has $2^n$ elements, which are the vertices of a unit hypercube in $\mathbb{R}^n$.) Given a vector subspace $V$ of $\mathbb{R}^n$, let $Z(V)$ denote the number of members of $Z$ that lie in $V$. Let $k$ be given, $0 \leq k \leq n$. Find the maximum, over all vector subspaces $V \subseteq \mathbb{R}^n$ of dimension $k$, of the number of points in $V \cap Z$. [Editorial note: the proposers probably intended to write $Z(V)$ instead of "the number of points in $V \cap Z$", but this changes nothing.]

B–5 For each continuous function $f : [0,1] \to \mathbb{R}$, let $I(f) = \int_0^1 x^2 f(x)\,dx$ and $J(x) = \int_0^1 x\,(f(x))^2\,dx$. Find the maximum value of $I(f) - J(f)$ over all such functions $f$.

B–6 Let $k$ be an integer greater than 1. Suppose $a_0 > 0$, and define
$$a_{n+1} = a_n + \frac{1}{\sqrt[k]{a_n}}$$
for $n > 0$. Evaluate
$$\lim_{n\to\infty} \frac{a_n^{k+1}}{n^k}.$$

# Solutions to the 67th William Lowell Putnam Mathematical Competition
# Saturday, December 2, 2006

Kiran Kedlaya and Lenny Ng

A–1 We change to cylindrical coordinates, i.e., we put $r = \sqrt{x^2+y^2}$. Then the given inequality is equivalent to

$$r^2+z^2+8 \leq 6r,$$

or

$$(r-3)^2+z^2 \leq 1.$$

This defines a solid of revolution (a solid torus); the area being rotated is the disc $(x-3)^2+z^2 \leq 1$ in the $xz$-plane. By Pappus's theorem, the volume of this equals the area of this disc, which is $\pi$, times the distance through which the center of mass is being rotated, which is $(2\pi)3$. That is, the total volume is $6\pi^2$.

A–2 Suppose on the contrary that the set $B$ of values of $n$ for which Bob has a winning strategy is finite; for convenience, we include $n = 0$ in $B$, and write $B = \{b_1,\dots,b_m\}$. Then for every nonnegative integer $n$ not in $B$, Alice must have some move on a heap of $n$ stones leading to a position in which the second player wins. That is, every nonnegative integer not in $B$ can be written as $b+p-1$ for some $b \in B$ and some prime $p$. However, there are numerous ways to show that this cannot happen.

**First solution:** Let $t$ be any integer bigger than all of the $b \in B$. Then it is easy to write down $t$ consecutive composite integers, e.g., $(t+1)!+2,\dots,(t+1)!+t+1$. Take $n = (t+1)!+t$; then for each $b \in B$, $n-b+1$ is one of the composite integers we just wrote down.

**Second solution:** Let $p_1,\dots,p_{2m}$ be any prime numbers; then by the Chinese remainder theorem, there exists a positive integer $x$ such that

$$\begin{aligned} x - b_1 &\equiv -1 \pmod{p_1 p_{m+1}} \\ &\cdots \\ x - b_n &\equiv -1 \pmod{p_m p_{2m}}. \end{aligned}$$

For each $b \in B$, the unique integer $p$ such that $x = b+p-1$ is divisible by at least two primes, and so cannot itself be prime.

**Third solution:** (by Catalin Zara) Put $b_1 = 0$, and take $n = (b_2-1)\cdots(b_m-1)$; then $n$ is composite because $3,8 \in B$, and for any nonzero $b \in B$, $n-b_i+1$ is divisible by but not equal to $b_i-1$. (One could also take $n = b_2\cdots b_m - 1$, so that $n-b_i+1$ is divisible by $b_i$.)

A–3 We first observe that given any sequence of integers $x_1,x_2,\dots$ satisfying a recursion

$$x_k = f(x_{k-1},\dots,x_{k-n}) \qquad (k > n),$$

where $n$ is fixed and $f$ is a fixed polynomial of $n$ variables with integer coefficients, for any positive integer $N$, the sequence modulo $N$ is eventually periodic. This is simply because there are only finitely many possible sequences of $n$ consecutive values modulo $N$, and once such a sequence is repeated, every subsequent value is repeated as well.

We next observe that if one can rewrite the same recursion as

$$x_{k-n} = g(x_{k-n+1},\dots,x_k) \qquad (k > n),$$

where $g$ is also a polynomial with integer coefficients, then the sequence extends uniquely to a doubly infinite sequence $\dots,x_{-1},x_0,x_1,\dots$ which is fully periodic modulo any $N$. That is the case in the situation at hand, because we can rewrite the given recursion as

$$x_{k-2005} = x_{k+1} - x_k.$$

It thus suffices to find 2005 consecutive terms divisible by $N$ in the doubly infinite sequence, for any fixed $N$ (so in particular for $N = 2006$). Running the recursion backwards, we easily find

$$\begin{aligned} x_1 = x_0 = \cdots = x_{-2004} &= 1 \\ x_{-2005} = \cdots = x_{-4009} &= 0, \end{aligned}$$

yielding the desired result.

A–4 **First solution:** By the linearity of expectation, the average number of local maxima is equal to the sum of the probability of having a local maximum at $k$ over $k = 1,\dots,n$. For $k = 1$, this probability is 1/2: given the pair $\{\pi(1),\pi(2)\}$, it is equally likely that $\pi(1)$ or $\pi(2)$ is bigger. Similarly, for $k = n$, the probability is 1/2. For $1 < k < n$, the probability is 1/3: given the pair $\{\pi(k-1),\pi(k),\pi(k+1)\}$, it is equally likely that any of the three is the largest. Thus the average number of local maxima is

$$2 \cdot \frac{1}{2} + (n-2)\cdot\frac{1}{3} = \frac{n+1}{3}.$$

**Second solution:** Another way to apply the linearity of expectation is to compute the probability that $i \in \{1,\dots,n\}$ occurs as a local maximum. The most efficient way to do this is to imagine the permutation as consisting of the symbols $1,\dots,n,*$ written in a circle in some order. The number $i$ occurs as a local maximum if the two symbols it is adjacent to both belong to the set $\{*,1,\dots,i-1\}$. There are $i(i-1)$ pairs of such symbols and $n(n-1)$ pairs in total, so the probability of

$i$ occurring as a local maximum is $i(i-1)/(n(n-1))$, and the average number of local maxima is

$$\begin{aligned}\sum_{i=1}^n \frac{i(i-1)}{n(n-1)} &= \frac{2}{n(n-1)} \sum_{i=1}^n \binom{i}{2} \\ &= \frac{2}{n(n-1)} \binom{n+1}{3} \\ &= \frac{n+1}{3}.\end{aligned}$$

One can obtain a similar (if slightly more intricate) solution inductively, by removing the known local maximum $n$ and splitting into two shorter sequences.

**Remark:** The usual term for a local maximum in this sense is a *peak*. The complete distribution for the number of peaks is known; Richard Stanley suggests the reference: F. N. David and D. E. Barton, *Combinatorial Chance*, Hafner, New York, 1962, p. 162 and subsequent.

A–5 Since the desired expression involves symmetric functions of $a_1, \dots, a_n$, we start by finding a polynomial with $a_1, \dots, a_n$ as roots. Note that

$$1 \pm i \tan\theta = e^{\pm i\theta} \sec\theta$$

so that

$$1 + i\tan\theta = e^{2i\theta}(1 - i\tan\theta).$$

Consequently, if we put $\omega = e^{2in\theta}$, then the polynomial

$$Q_n(x) = (1+ix)^n - \omega(1-ix)^n$$

has among its roots $a_1, \dots, a_n$. Since these are distinct and $Q_n$ has degree $n$, these must be exactly the roots.

If we write

$$Q_n(x) = c_n x^n + \cdots + c_1 x + c_0,$$

then $a_1 + \cdots + a_n = -c_{n-1}/c_n$ and $a_1 \cdots a_n = -c_0/c_n$, so the ratio we are seeking is $c_{n-1}/c_0$. By inspection,

$$\begin{aligned}c_{n-1} &= ni^{n-1} - \omega n(-i)^{n-1} = ni^{n-1}(1-\omega) \\ c_0 &= 1 - \omega\end{aligned}$$

so

$$\frac{a_1 + \cdots + a_n}{a_1 \cdots a_n} = \begin{cases} n & n \equiv 1 \pmod 4 \\ -n & n \equiv 3 \pmod 4. \end{cases}$$

**Remark:** The same argument shows that the ratio between any two *odd* elementary symmetric functions of $a_1, \dots, a_n$ is independent of $\theta$.

A–6 **First solution:** (by Daniel Kane) The probability is $1 - \frac{35}{12\pi^2}$. We start with some notation and simplifications. For simplicity, we assume without loss of generality that the circle has radius 1. Let $E$ denote the expected value of a random variable over all choices of $P, Q, R$. Write $[XYZ]$ for the area of triangle $XYZ$.

If $P, Q, R, S$ are the four points, we may ignore the case where three of them are collinear, as this occurs with probability zero. Then the only way they can fail to form the vertices of a convex quadrilateral is if one of them lies inside the triangle formed by the other three. There are four such configurations, depending on which point lies inside the triangle, and they are mutually exclusive. Hence the desired probability is 1 minus four times the probability that $S$ lies inside triangle $PQR$. That latter probability is simply $E([PQR])$ divided by the area of the disc.

Let $O$ denote the center of the circle, and let $P', Q', R'$ be the projections of $P, Q, R$ onto the circle from $O$. We can write

$$[PQR] = \pm[OPQ] \pm [OQR] \pm [ORP]$$

for a suitable choice of signs, determined as follows. If the points $P', Q', R'$ lie on no semicircle, then all of the signs are positive. If $P', Q', R'$ lie on a semicircle in that order and $Q$ lies inside the triangle $OPR$, then the sign on $[OPR]$ is positive and the others are negative. If $P', Q', R'$ lie on a semicircle in that order and $Q$ lies outside the triangle $OPR$, then the sign on $[OPR]$ is negative and the others are positive.

We first calculate

$$E([OPQ] + [OQR] + [ORP]) = 3E([OPQ]).$$

Write $r_1 = OP, r_2 = OQ, \theta = \angle POQ$, so that

$$[OPQ] = \frac{1}{2} r_1 r_2 (\sin\theta).$$

The distribution of $r_1$ is given by $2r_1$ on $[0,1]$ (e.g., by the change of variable formula to polar coordinates), and similarly for $r_2$. The distribution of $\theta$ is uniform on $[0, \pi]$. These three distributions are independent; hence

$$\begin{aligned}&E([OPQ]) \\ &= \frac{1}{2}\left(\int_0^1 2r^2\,dr\right)^2 \left(\frac{1}{\pi}\int_0^\pi \sin(\theta)\,d\theta\right) \\ &= \frac{4}{9\pi},\end{aligned}$$

and

$$E([OPQ] + [OQR] + [ORP]) = \frac{4}{3\pi}.$$

We now treat the case where $P', Q', R'$ lie on a semicircle in that order. Put $\theta_1 = \angle POQ$ and $\theta_2 = \angle QOR$; then the distribution of $\theta_1, \theta_2$ is uniform on the region

$$0 \le \theta_1, \quad 0 \le \theta_2, \quad \theta_1 + \theta_2 \le \pi.$$

In particular, the distribution on $\theta = \theta_1 + \theta_2$ is $\frac{2\theta}{\pi^2}$ on $[0, \pi]$. Put $r_P = OP, r_Q = OQ, r_R = OR$. Again, the distribution on $r_P$ is given by $2r_P$ on $[0,1]$, and similarly for $r_Q, r_R$; these are independent from each other and from the joint distribution of $\theta_1, \theta_2$. Write $E'(X)$ for the expectation of a random variable $X$ restricted to this part of the domain.

Let $\chi$ be the random variable with value 1 if $Q$ is inside triangle $OPR$ and 0 otherwise. We now compute

$$\begin{aligned}
&E'([OPR]) \\
&= \frac{1}{2}\left(\int_0^1 2r^2\,dr\right)^2 \left(\int_0^\pi \frac{2\theta}{\pi^2}\sin(\theta)\,d\theta\right) \\
&= \frac{4}{9\pi} \\
&E'(\chi[OPR]) \\
&= E'(2[OPR]^2/\theta) \\
&= \frac{1}{2}\left(\int_0^1 2r^3\,dr\right)^2 \left(\int_0^\pi \frac{2\theta}{\pi^2}\theta^{-1}\sin^2(\theta)\,d\theta\right) \\
&= \frac{1}{8\pi}.
\end{aligned}$$

Also recall that given any triangle $XYZ$, if $T$ is chosen uniformly at random inside $XYZ$, the expectation of $[TXY]$ is the area of triangle bounded by $XY$ and the centroid of $XYZ$, namely $\frac{1}{3}[XYZ]$.

Let $\chi$ be the random variable with value 1 if $Q$ is inside triangle $OPR$ and 0 otherwise. Then

$$\begin{aligned}
&E'([OPQ]+[OQR]+[ORP]-[PQR]) \\
&= 2E'(\chi([OPQ]+[OQR]) + 2E'((1-\chi)[OPR]) \\
&= 2E'(\frac{2}{3}\chi[OPR]) + 2E'([OPR]) - 2E'(\chi[OPR]) \\
&= 2E'([OPR]) - \frac{2}{3}E'(\chi[OPR]) = \frac{29}{36\pi}.
\end{aligned}$$

Finally, note that the case when $P', Q', R'$ lie on a semicircle in some order occurs with probability 3/4. (The case where they lie on a semicircle proceeding clockwise from $P'$ to its antipode has probability 1/4; this case and its two analogues are exclusive and exhaustive.) Hence

$$\begin{aligned}
&E([PQR]) \\
&= E([OPQ]+[OQR]+[ORP]) \\
&\quad -\frac{3}{4}E'([OPQ]+[OQR]+[ORP]-[PQR]) \\
&= \frac{4}{3\pi} - \frac{29}{48\pi} = \frac{35}{48\pi},
\end{aligned}$$

so the original probability is

$$1 - \frac{4E([PQR])}{\pi} = 1 - \frac{35}{12\pi^2}.$$

**Second solution:** (by David Savitt) As in the first solution, it suffices to check that for $P, Q, R$ chosen uniformly at random in the disc, $E([PQR]) = \frac{35}{48\pi}$. Draw the lines $PQ, QR, RP$, which with probability 1 divide the interior of the circle into seven regions. Put $a = [PQR]$, let $b_1, b_2, b_3$ denote the areas of the three other regions sharing a side with the triangle, and let $c_1, c_2, c_3$ denote the areas of the other three regions. Put $A = E(a)$, $B = E(b_1)$, $C = E(c_1)$, so that $A + 3B + 3C = \pi$.

Note that $c_1 + c_2 + c_3 + a$ is the area of the region in which we can choose a fourth point $S$ so that the quadrilateral $PQRS$ fails to be convex. By comparing expectations, we have $3C + A = 4A$, so $A = C$ and $4A + 3B = \pi$.

We will compute $B + 2A = B + 2C$, which is the expected area of the part of the circle cut off by a chord through two random points $D, E$, on the side of the chord not containing a third random point $F$. Let $h$ be the distance from the center $O$ of the circle to the line $DE$. We now determine the distribution of $h$.

Put $r = OD$; the distribution of $r$ is $2r$ on $[0,1]$. Without loss of generality, suppose $O$ is the origin and $D$ lies on the positive $x$-axis. For fixed $r$, the distribution of $h$ runs over $[0,r]$, and can be computed as the area of the infinitesimal region in which $E$ can be chosen so the chord through $DE$ has distance to $O$ between $h$ and $h + dh$, divided by $\pi$. This region splits into two symmetric pieces, one of which lies between chords making angles of $\arcsin(h/r)$ and $\arcsin((h+dh)/r)$ with the $x$-axis. The angle between these is $d\theta = dh/(r^2 - h^2)$. Draw the chord through $D$ at distance $h$ to $O$, and let $L_1, L_2$ be the lengths of the parts on opposite sides of $D$; then the area we are looking for is $\frac{1}{2}(L_1^2 + L_2^2)d\theta$. Since

$$\{L_1, L_2\} = \sqrt{1-h^2} \pm \sqrt{r^2-h^2},$$

the area we are seeking (after doubling) is

$$2\frac{1 + r^2 - 2h^2}{\sqrt{r^2-h^2}}.$$

Dividing by $\pi$, then integrating over $r$, we compute the distribution of $h$ to be

$$\begin{aligned}
&\frac{1}{\pi}\int_h^1 2\frac{1+r^2-2h^2}{\sqrt{r^2-h^2}}2r\,dr \\
&= \frac{16}{3\pi}(1-h^2)^{3/2}.
\end{aligned}$$

We now return to computing $B + 2A$. Let $A(h)$ denote the smaller of the two areas of the disc cut off by a chord at distance $h$. The chance that the third point is in the smaller (resp. larger) portion is $A(h)/\pi$ (resp. $1 - A(h)/\pi$), and then the area we are trying to compute is $\pi - A(h)$ (resp. $A(h)$). Using the distribution on $h$, and the fact that

$$\begin{aligned}
A(h) &= 2\int_h^1 \sqrt{1-h^2}\,dh \\
&= \frac{\pi}{2} - \arcsin(h) - h\sqrt{1-h^2},
\end{aligned}$$

we find

$$\begin{aligned} &B+2A \\ &= \frac{2}{\pi}\int_0^1 A(h)(\pi - A(h))\,\frac{16}{3\pi}(1-h^2)^{3/2}\,dh \\ &= \frac{35+24\pi^2}{72\pi}. \end{aligned}$$

Since $4A+3B=\pi$, we solve to obtain $A = \frac{35}{48\pi}$ as in the first solution.

**Third solution:** (by Noam Elkies) Again, we reduce to computing the average area of a triangle formed by three random points $A,B,C$ inside a unit circle. Let $O$ be the center of the circle, and put $c = \max\{OA, OB, OC\}$; then the probability that $c \leq r$ is $(r^2)^3$, so the distribution of $c$ is $6c^5\,dc$ on $[0,1]$.

Given $c$, the expectation of $[ABC]$ is equal to $c^2$ times $X$, the expected area of a triangle formed by two random points $P,Q$ in a circle and a fixed point $R$ on the boundary. We introduce polar coordinates centered at $R$, in which the circle is given by $r = 2\sin\theta$ for $\theta \in [0,\pi]$. The distribution of a random point in that circle is $\frac{1}{\pi} r\,dr\,d\theta$ over $\theta \in [0,\pi]$ and $r \in [0, 2\sin\theta]$. If $(r,\theta)$ and $(r',\theta')$ are the two random points, then the area is $\frac{1}{2}rr'\sin|\theta-\theta'|$.

Performing the integrals over $r$ and $r'$ first, we find

$$\begin{aligned} X &= \frac{32}{9\pi^2}\int_0^\pi\int_0^\pi \sin^3\theta\sin^3\theta'\sin|\theta-\theta'|\,d\theta'\,d\theta \\ &= \frac{64}{9\pi^2}\int_0^\pi\int_0^\theta \sin^3\theta\sin^3\theta'\sin(\theta-\theta')\,d\theta'\,d\theta. \end{aligned}$$

This integral is unpleasant but straightforward; it yields $X = 35/(36\pi)$, and $E([PQR]) = \int_0^1 6c^7X\,dc = 35/(48\pi)$, giving the desired result.

**Remark:** This is one of the oldest problems in geometric probability; it is an instance of Sylvester's four-point problem, which nowadays is usually solved using a device known as Crofton's formula. We defer to `http://mathworld.wolfram.com/` for further discussion.

B–1 The "curve" $x^3+3xy+y^3-1=0$ is actually reducible, because the left side factors as

$$(x+y-1)(x^2-xy+y^2+x+y+1).$$

Moreover, the second factor is

$$\frac{1}{2}((x+1)^2+(y+1)^2+(x-y)^2),$$

so it only vanishes at $(-1,-1)$. Thus the curve in question consists of the single point $(-1,-1)$ together with the line $x+y=1$. To form a triangle with three points on this curve, one of its vertices must be $(-1,-1)$. The other two vertices lie on the line $x+y=1$, so the length of the altitude from $(-1,-1)$ is the distance from $(-1,-1)$ to $(1/2,1/2)$, or $3\sqrt{2}/2$. The area of an equilateral triangle of height $h$ is $h^2\sqrt{3}/3$, so the desired area is $3\sqrt{3}/2$.

**Remark:** The factorization used above is a special case of the fact that

$$\begin{aligned} &x^3+y^3+z^3-3xyz \\ &= (x+y+z)(x+\omega y+\omega^2 z)(x+\omega^2 y+\omega z), \end{aligned}$$

where $\omega$ denotes a primitive cube root of unity. That fact in turn follows from the evaluation of the determinant of the *circulant matrix*

$$\begin{pmatrix} x & y & z \\ z & x & y \\ y & z & x \end{pmatrix}$$

by reading off the eigenvalues of the eigenvectors $(1,\omega^i,\omega^{2i})$ for $i=0,1,2$.

B–2 Let $\{x\} = x - \lfloor x \rfloor$ denote the fractional part of $x$. For $i=0,\dots,n$, put $s_i = x_1+\cdots+x_i$ (so that $s_0=0$). Sort the numbers $\{s_0\},\dots,\{s_n\}$ into ascending order, and call the result $t_0,\dots,t_n$. Since $0=t_0\leq\cdots\leq t_n<1$, the differences

$$t_1-t_0,\dots,t_n-t_{n-1},1-t_n$$

are nonnegative and add up to 1. Hence (as in the pigeonhole principle) one of these differences is no more than $1/(n+1)$; if it is anything other than $1-t_n$, it equals $\pm(\{s_i\}-\{s_j\})$ for some $0\leq i<j\leq n$. Put $S=\{x_{i+1},\dots,x_j\}$ and $m=\lfloor s_i\rfloor-\lfloor s_j\rfloor$; then

$$\begin{aligned} \left|m+\sum_{s\in S}s\right| &= |m+s_j-s_i| \\ &= |\{s_j\}-\{s_i\}| \\ &\leq \frac{1}{n+1}, \end{aligned}$$

as desired. In case $1-t_n\leq 1/(n+1)$, we take $S=\{x_1,\dots,x_n\}$ and $m=-\lceil s_n\rceil$, and again obtain the desired conclusion.

B–3 The maximum is $\binom{n}{2}+1$, achieved for instance by a convex $n$-gon: besides the trivial partition (in which all of the points are in one part), each linear partition occurs by drawing a line crossing a unique pair of edges.

**First solution:** We will prove that $L_S=\binom{n}{2}+1$ in any configuration in which no two of the lines joining points of $S$ are parallel. This suffices to imply the maximum in all configurations: given a maximal configuration, we may vary the points slightly to get another maximal configuration in which our hypothesis is satisfied. For convenience, we assume $n\geq 3$, as the cases $n=1,2$ are easy.

Let $P$ be the line at infinity in the real projective plane; i.e., $P$ is the set of possible directions of lines in the plane, viewed as a circle. Remove the directions corresponding to lines through two points of $S$; this leaves behind $\binom{n}{2}$ intervals.

Given a direction in one of the intervals, consider the set of linear partitions achieved by lines parallel to that direction. Note that the resulting collection of partitions depends only on the interval. Then note that the collections associated to adjacent intervals differ in only one element.

The trivial partition that puts all of $S$ on one side is in every such collection. We now observe that for any other linear partition $\{A,B\}$, the set of intervals to which $\{A,B\}$ is:

(a) a consecutive block of intervals, but

(b) not all of them.

For (a), note that if $\ell_1, \ell_2$ are nonparallel lines achieving the same partition, then we can rotate around their point of intersection to achieve all of the intermediate directions on one side or the other. For (b), the case $n = 3$ is evident; to reduce the general case to this case, take points $P,Q,R$ such that $P$ lies on the opposite side of the partition from $Q$ and $R$.

It follows now that that each linear partition, except for the trivial one, occurs in exactly one place as the partition associated to some interval but not to its immediate counterclockwise neighbor. In other words, the number of linear partitions is one more than the number of intervals, or $\binom{n}{2}+1$ as desired.

**Second solution:** We prove the upper bound by induction on $n$. Choose a point $P$ in the convex hull of $S$. Put $S' = S \setminus \{P\}$; by the induction hypothesis, there are at most $\binom{n-1}{2}+1$ linear partitions of $S'$. Note that each linear partition of $S$ restricts to a linear partition of $S'$. Moreover, if two linear partitions of $S$ restrict to the same linear partition of $S'$, then that partition of $S'$ is achieved by a line through $P$.

By rotating a line through $P$, we see that there are at most $n-1$ partitions of $S'$ achieved by lines through $P$: namely, the partition only changes when the rotating line passes through one of the points of $S$. This yields the desired result.

**Third solution:** (by Noam Elkies) We enlarge the plane to a projective plane by adding a line at infinity, then apply the polar duality map centered at one of the points $O \in S$. This turns the rest of $S$ into a set $S'$ of $n-1$ lines in the dual projective plane. Let $O'$ be the point in the dual plane corresponding to the original line at infinity; it does not lie on any of the lines in $S'$.

Let $\ell$ be a line in the original plane, corresponding to a point $P$ in the dual plane. If we form the linear partition induced by $\ell$, then the points of $S \setminus \{O\}$ lying in the same part as $O$ correspond to the lines of $S'$ which cross the segment $O'P$. If we consider the dual affine plane as being divided into regions by the lines of $S'$, then the lines of $S'$ crossing the segment $O'P$ are determined by which region $P$ lies in.

Thus our original maximum is equal to the maximum number of regions into which $n-1$ lines divide an affine plane. By induction on $n$, this number is easily seen to be $1+\binom{n}{2}$.

**Fourth solution:** (by Florian Herzig) Say that an *S-line* is a line that intersects $S$ in at least two points. We claim that the nontrivial linear partitions of $S$ are in natural bijection with pairs $(\ell,\{X,Y\})$ consisting of an $S$-line $\ell$ and a nontrivial linear partition $\{X,Y\}$ of $\ell \cap S$. Since an $S$-line $\ell$ admits precisely $|\ell \cap S| - 1 \leq \binom{|\ell \cap S|}{2}$ nontrivial linear partitions, the claim implies that $L_S \leq \binom{n}{2}+1$ with equality iff no three points of $S$ are collinear.

Let $P$ be the line at infinity in the real projective plane. Given any nontrivial linear partition $\{A,B\}$ of $S$, the set of lines inducing this partition is a proper, open, connected subset $I$ of $P$. (It is proper because it has to omit directions of $S$-lines that pass through both parts of the partition and open because we can vary the separating line. It is connected because if we have two such lines that aren't parallel, we can rotate through their point of intersection to get all intermediate directions.) Among all $S$-lines that intersect both $A$ and $B$ choose a line $\ell$ whose direction is minimal (in the clockwise direction) with respect to the interval $I$; also, pick an arbitrary line $\ell'$ that induces $\{A,B\}$. By rotating $\ell'$ clockwise to $\ell$ about their point of intersection, we see that the direction of $\ell$ is the least upper bound of $I$. (We can't hit any point of $S$ during the rotation because of the minimality property of $\ell$.) The line $\ell$ is in fact unique because if the (parallel) lines $pq$ and $rs$ are two choices for $\ell$, with $p$, $q \in A$; $r$, $s \in B$, then one of the diagonals $ps$, $qr$ would contradict the minimality property of $\ell$. To define the above bijection we send $\{A,B\}$ to $(\ell,\{A\cap\ell, B\cap\ell\})$.

Conversely, suppose that we are given an $S$-line $\ell$ and a nontrivial linear partition $\{X,Y\}$ of $\ell \cap S$. Pick any point $p \in \ell$ that induces the partition $\{X,Y\}$. If we rotate the line $\ell$ about $p$ in the counterclockwise direction by a sufficiently small amount, we get a nontrivial linear partitition of $S$ that is independent of all choices. (It is obtained from the partition of $S-\ell$ induced by $\ell$ by adjoining $X$ to one part and $Y$ to the other.) This defines a map in the other direction.

By construction these two maps are inverse to each other, and this proves the claim.

**Remark:** Given a finite set $S$ of points in $\mathbb{R}^n$, a *non-Radon partition* of $S$ is a pair $(A,B)$ of complementary subsets that can be separated by a hyperplane. *Radon's theorem* states that if $\#S \geq n+2$, then not every $(A,B)$ is a non-Radon partition. The result of this problem has been greatly extended, especially within the context of matroid theory and oriented matroid theory. Richard Stanley suggests the following references: T. H. Brylawski, A combinatorial perspective on the Radon convexity theorem, *Geom. Ded.* **5** (1976), 459-466; and T.

Zaslavsky, Extremal arrangements of hyperplanes, *Ann. N. Y. Acad. Sci.* **440** (1985), 69-87.

B–4 The maximum is $2^k$, achieved for instance by the subspace

$$\{(x_1,\dots,x_n)\in\mathbb{R}^n : x_1=\cdots=x_{n-k}=0\}.$$

**First solution:** More generally, we show that any affine $k$-dimensional plane in $\mathbb{R}^n$ can contain at most $2^k$ points in $Z$. The proof is by induction on $k+n$; the case $k=n=0$ is clearly true.

Suppose that $V$ is a $k$-plane in $\mathbb{R}^n$. Denote the hyperplanes $\{x_n=0\}$ and $\{x_n=1\}$ by $V_0$ and $V_1$, respectively. If $V\cap V_0$ and $V\cap V_1$ are each at most $(k-1)$-dimensional, then $V\cap V_0\cap Z$ and $V\cap V_1\cap Z$ each have cardinality at most $2^{k-1}$ by the induction assumption, and hence $V\cap Z$ has at most $2^k$ elements. Otherwise, if $V\cap V_0$ or $V\cap V_1$ is $k$-dimensional, then $V\subset V_0$ or $V\subset V_1$; now apply the induction hypothesis on $V$, viewed as a subset of $\mathbb{R}^{n-1}$ by dropping the last coordinate.

**Second solution:** Let $S$ be a subset of $Z$ contained in a $k$-dimensional subspace of $V$. This is equivalent to asking that any $t_1,\dots,t_{k+1}\in S$ satisfy a nontrivial linear dependence $c_1t_1+\cdots+c_{k+1}t_{k+1}=0$ with $c_1,\dots,c_{k+1}\in\mathbb{R}$. Since $t_1,\dots,t_{k+1}\in\mathbb{Q}^n$, given such a dependence we can always find another one with $c_1,\dots,c_{k+1}\in\mathbb{Q}$; then by clearing denominators, we can find one with $c_1,\dots,c_{k+1}\in\mathbb{Z}$ and not all having a common factor.

Let $\mathbb{F}_2$ denote the field of two elements, and let $\overline{S}\subseteq\mathbb{F}_2^n$ be the reductions modulo 2 of the points of $S$. Then any $t_1,\dots,t_{k+1}\in\overline{S}$ satisfy a nontrivial linear dependence, because we can take the dependence from the end of the previous paragraph and reduce modulo 2. Hence $\overline{S}$ is contained in a $k$-dimensional subspace of $\mathbb{F}_{2^n}$, and the latter has cardinality exactly $2^k$. Thus $\overline{S}$ has at most $2^k$ elements, as does $S$.

Variant (suggested by David Savitt): if $\overline{S}$ contained $k+1$ linearly independent elements, the $(k+1)\times n$ matrix formed by these would have a nonvanishing maximal minor. The lift of that minor back to $\mathbb{R}$ would also not vanish, so $S$ would contain $k+1$ linearly independent elements.

**Third solution:** (by Catalin Zara) Let $V$ be a $k$-dimensional subspace. Form the matrix whose rows are the elements of $V\cap Z$; by construction, it has row rank at most $k$. It thus also has column rank at most $k$; in particular, we can choose $k$ coordinates such that each point of $V\cap Z$ is determined by those $k$ of its coordinates. Since each coordinate of a point in $Z$ can only take two values, $V\cap Z$ can have at most $2^k$ elements.

**Remark:** The proposers probably did not realize that this problem appeared online about three months before the exam, at `http://www.artofproblemsolving.com/Forum/viewtopic.php?t=105991`. (It may very well have also appeared even earlier.)

B–5 The answer is $1/16$. We have

$$\begin{aligned}&\int_0^1 x^2 f(x)\,dx-\int_0^1 x f(x)^2\,dx\\ &=\int_0^1 (x^3/4-x(f(x)-x/2)^2)\,dx\\ &\le\int_0^1 x^3/4\,dx=1/16,\end{aligned}$$

with equality when $f(x)=x/2$.

B–6 **First solution:** We start with some easy upper and lower bounds on $a_n$. We write $O(f(n))$ and $\Omega(f(n))$ for functions $g(n)$ such that $f(n)/g(n)$ and $g(n)/f(n)$, respectively, are bounded above. Since $a_n$ is a nondecreasing sequence, $a_{n+1}-a_n$ is bounded above, so $a_n=O(n)$. That means $a_n^{-1/k}=\Omega(n^{-1/k})$, so

$$a_n=\Omega\left(\sum_{i=1}^n i^{-1/k}\right)=\Omega(n^{(k-1)/k}).$$

In fact, all we will need is that $a_n\to\infty$ as $n\to\infty$.

By Taylor's theorem with remainder, for $1<m<2$ and $x>0$,

$$|(1+x)^m-1-mx|\le\frac{m(m-1)}{2}x^2.$$

Taking $m=(k+1)/k$ and $x=a_{n+1}/a_n=1+a_n^{-(k+1)/k}$, we obtain

$$\left|a_{n+1}^{(k+1)/k}-a_n^{(k+1)/k}-\frac{k+1}{k}\right|\le\frac{k+1}{2k^2}a_n^{-(k+1)/k}.$$

In particular,

$$\lim_{n\to\infty} a_{n+1}^{(k+1)/k}-a_n^{(k+1)/k}=\frac{k+1}{k}.$$

In general, if $x_n$ is a sequence with $\lim_{n\to\infty}x_n=c$, then also

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^n x_i=c$$

by Cesaro's lemma. Explicitly, for any $\varepsilon>0$, we can find $N$ such that $|x_n-c|\le\varepsilon/2$ for $n\ge N$, and then

$$\left|c-\frac{1}{n}\sum_{i=1}^n x_i\right|\le\frac{n-N}{n}\frac{\varepsilon}{2}+\frac{N}{n}\left|\sum_{i=1}^N(c-x_i)\right|;$$

for $n$ large, the right side is smaller than $\varepsilon$.

In our case, we deduce that

$$\lim_{n\to\infty}\frac{a_n^{(k+1)/k}}{n}=\frac{k+1}{k}$$

and so

$$\lim_{n\to\infty}\frac{a_n^{k+1}}{n^k}=\left(\frac{k+1}{k}\right)^k,$$

as desired.

**Remark:** The use of Cesaro's lemma above is the special case $b_n = n$ of the *Cesaro-Stolz theorem*: if $a_n, b_n$ are sequences such that $b_n$ is positive, strictly increasing, and unbounded, and

$$\lim_{n\to\infty} \frac{a_{n+1}-a_n}{b_{n+1}-b_n} = L,$$

then

$$\lim_{n\to\infty} \frac{a_n}{b_n} = L.$$

**Second solution:** In this solution, rather than applying Taylor's theorem with remainder to $(1+x)^m$ for $1 < m < 2$ and $x > 0$, we only apply convexity to deduce that $(1+x)^m \geq 1+mx$. This gives

$$a_{n+1}^{(k+1)/k} - a_n^{(k+1)/k} \geq \frac{k+1}{k},$$

and so

$$a_n^{(k+1)/k} \geq \frac{k+1}{k} n + c$$

for some $c \in \mathbb{R}$. In particular,

$$\liminf_{n\to\infty} \frac{a_n^{(k+1)/k}}{n} \geq \frac{k+1}{k}$$

and so

$$\liminf_{n\to\infty} \frac{a_n}{n^{k/(k+1)}} \geq \left(\frac{k+1}{k}\right)^{k/(k+1)}.$$

But turning this around, the fact that

$$\begin{aligned}
&a_{n+1} - a_n \\
&= a_n^{-1/k} \\
&\leq \left(\frac{k+1}{k}\right)^{-1/(k+1)} n^{-1/(k+1)}(1+o(1)),
\end{aligned}$$

where $o(1)$ denotes a function tending to 0 as $n \to \infty$, yields

$$\begin{aligned}
&a_n \\
&\leq \left(\frac{k+1}{k}\right)^{-1/(k+1)} \sum_{i=1}^{n} i^{-1/(k+1)}(1+o(1)) \\
&= \frac{k+1}{k}\left(\frac{k+1}{k}\right)^{-1/(k+1)} n^{k/(k+1)}(1+o(1)) \\
&= \left(\frac{k+1}{k}\right)^{k/(k+1)} n^{k/(k+1)}(1+o(1)),
\end{aligned}$$

so

$$\limsup_{n\to\infty} \frac{a_n}{n^{k/(k+1)}} \leq \left(\frac{k+1}{k}\right)^{k/(k+1)}$$

and this completes the proof.

**Third solution:** We argue that $a_n \to \infty$ as in the first solution. Write $b_n = a_n - Ln^{k/(k+1)}$, for a value of $L$ to be determined later. We have

$$\begin{aligned}
&b_{n+1} \\
&= b_n + a_n^{-1/k} - L((n+1)^{k/(k+1)} - n^{k/(k+1)}) \\
&= e_1 + e_2,
\end{aligned}$$

where

$$\begin{aligned}
e_1 &= b_n + a_n^{-1/k} - L^{-1/k} n^{-1/(k+1)} \\
e_2 &= L((n+1)^{k/(k+1)} - n^{k/(k+1)}) \\
&\quad - L^{-1/k} n^{-1/(k+1)}.
\end{aligned}$$

We first estimate $e_1$. For $-1 < m < 0$, by the convexity of $(1+x)^m$ and $(1+x)^{1-m}$, we have

$$\begin{aligned}
1 + mx &\leq (1+x)^m \\
&\leq 1 + mx(1+x)^{m-1}.
\end{aligned}$$

Hence

$$\begin{aligned}
-\frac{1}{k} L^{-(k+1)/k} n^{-1} b_n &\leq e_1 - b_n \\
&\leq -\frac{1}{k} b_n a_n^{-(k+1)/k}.
\end{aligned}$$

Note that both bounds have sign opposite to $b_n$; moreover, by the bound $a_n = \Omega(n^{(k-1)/k})$, both bounds have absolutely value strictly less than that of $b_n$ for $n$ sufficiently large. Consequently, for $n$ large,

$$|e_1| \leq |b_n|.$$

We now work on $e_2$. By Taylor's theorem with remainder applied to $(1+x)^m$ for $x > 0$ and $0 < m < 1$,

$$\begin{aligned}
1 + mx &\geq (1+x)^m \\
&\geq 1 + mx + \frac{m(m-1)}{2} x^2.
\end{aligned}$$

The "main term" of $L((n+1)^{k/(k+1)} - n^{k/(k+1)})$ is $L\frac{k}{k+1} n^{-1/(k+1)}$. To make this coincide with $L^{-1/k} n^{-1/(k+1)}$, we take

$$L = \left(\frac{k+1}{k}\right)^{k/(k+1)}.$$

We then find that

$$|e_2| = O(n^{-2}),$$

and because $b_{n+1} = e_1 + e_2$, we have $|b_{n+1}| \leq |b_n| + |e_2|$. Hence

$$|b_n| = O\left(\sum_{i=1}^{n} i^{-2}\right) = O(1),$$

and so

$$\lim_{n\to\infty} \frac{a_n^{k+1}}{n^k} = L^{k+1} = \left(\frac{k+1}{k}\right)^k.$$

**Remark:** The case $k = 2$ appeared on the 2004 Romanian Olympiad (district level).

**Remark:** One can make a similar argument for any sequence given by $a_{n+1} = a_n + f(a_n)$, when $f$ is a *decreasing* function.

**Remark:** Richard Stanley suggests a heuristic for determining the asymptotic behavior of sequences of this type: replace the given recursion

$$a_{n+1} - a_n = a_n^{-1/k}$$

by the differential equation

$$y' = y^{-1/k}$$

and determine the asymptotics of the latter.

# The 68th William Lowell Putnam Mathematical Competition
# Saturday, December 1, 2007

A–1 Find all values of $\alpha$ for which the curves $y = \alpha x^2 + \alpha x + \frac{1}{24}$ and $x = \alpha y^2 + \alpha y + \frac{1}{24}$ are tangent to each other.

A–2 Find the least possible area of a convex set in the plane that intersects both branches of the hyperbola $xy = 1$ and both branches of the hyperbola $xy = -1$. (A set $S$ in the plane is called *convex* if for any two points in $S$ the line segment connecting them is contained in $S$.)

A–3 Let $k$ be a positive integer. Suppose that the integers $1, 2, 3, \dots, 3k+1$ are written down in random order. What is the probability that at no time during this process, the sum of the integers that have been written up to that time is a positive integer divisible by 3? Your answer should be in closed form, but may include factorials.

A–4 A *repunit* is a positive integer whose digits in base 10 are all ones. Find all polynomials $f$ with real coefficients such that if $n$ is a repunit, then so is $f(n)$.

A–5 Suppose that a finite group has exactly $n$ elements of order $p$, where $p$ is a prime. Prove that either $n = 0$ or $p$ divides $n+1$.

A–6 A *triangulation* $\mathcal{T}$ of a polygon $P$ is a finite collection of triangles whose union is $P$, and such that the intersection of any two triangles is either empty, or a shared vertex, or a shared side. Moreover, each side is a side of exactly one triangle in $\mathcal{T}$. Say that $\mathcal{T}$ is *admissible* if every internal vertex is shared by 6 or more triangles. For example, [figure omitted.] Prove that there is an integer $M_n$, depending only on $n$, such that any admissible triangulation of a polygon $P$ with $n$ sides has at most $M_n$ triangles.

B–1 Let $f$ be a polynomial with positive integer coefficients. Prove that if $n$ is a positive integer, then $f(n)$ divides $f(f(n)+1)$ if and only if $n = 1$. [Editor's note: one must assume $f$ is nonconstant.]

B–2 Suppose that $f : [0,1] \to \mathbb{R}$ has a continuous derivative and that $\int_0^1 f(x)\,dx = 0$. Prove that for every $\alpha \in (0,1)$,

$$\left| \int_0^\alpha f(x)\,dx \right| \leq \frac{1}{8} \max_{0 \leq x \leq 1} |f'(x)|.$$

B–3 Let $x_0 = 1$ and for $n \geq 0$, let $x_{n+1} = 3x_n + \lfloor x_n \sqrt{5} \rfloor$. In particular, $x_1 = 5$, $x_2 = 26$, $x_3 = 136$, $x_4 = 712$. Find a closed-form expression for $x_{2007}$. ($\lfloor a \rfloor$ means the largest integer $\leq a$.)

B–4 Let $n$ be a positive integer. Find the number of pairs $P, Q$ of polynomials with real coefficients such that

$$(P(X))^2 + (Q(X))^2 = X^{2n} + 1$$

and $\deg P > \deg Q$.

B–5 Let $k$ be a positive integer. Prove that there exist polynomials $P_0(n), P_1(n), \dots, P_{k-1}(n)$ (which may depend on $k$) such that for any integer $n$,

$$\left\lfloor \frac{n}{k} \right\rfloor^k = P_0(n) + P_1(n) \left\lfloor \frac{n}{k} \right\rfloor + \cdots + P_{k-1}(n) \left\lfloor \frac{n}{k} \right\rfloor^{k-1}.$$

($\lfloor a \rfloor$ means the largest integer $\leq a$.)

B–6 For each positive integer $n$, let $f(n)$ be the number of ways to make $n!$ cents using an unordered collection of coins, each worth $k!$ cents for some $k$, $1 \leq k \leq n$. Prove that for some constant $C$, independent of $n$,

$$n^{n^2/2 - Cn} e^{-n^2/4} \leq f(n) \leq n^{n^2/2 + Cn} e^{-n^2/4}.$$

# Solutions to the 68th William Lowell Putnam Mathematical Competition
# Saturday, December 1, 2007

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A–1 The only such $\alpha$ are $2/3, 3/2, (13 \pm \sqrt{601})/12$.

**First solution:** Let $C_1$ and $C_2$ be the curves $y = \alpha x^2 + \alpha x + \frac{1}{24}$ and $x = \alpha y^2 + \alpha y + \frac{1}{24}$, respectively, and let $L$ be the line $y = x$. We consider three cases.

If $C_1$ is tangent to $L$, then the point of tangency $(x,x)$ satisfies

$$2\alpha x + \alpha = 1, \qquad x = \alpha x^2 + \alpha x + \frac{1}{24};$$

by symmetry, $C_2$ is tangent to $L$ there, so $C_1$ and $C_2$ are tangent. Writing $\alpha = 1/(2x+1)$ in the first equation and substituting into the second, we must have

$$x = \frac{x^2+x}{2x+1} + \frac{1}{24},$$

which simplifies to $0 = 24x^2 - 2x - 1 = (6x+1)(4x-1)$, or $x \in \{1/4, -1/6\}$. This yields $\alpha = 1/(2x+1) \in \{2/3, 3/2\}$.

If $C_1$ does not intersect $L$, then $C_1$ and $C_2$ are separated by $L$ and so cannot be tangent.

If $C_1$ intersects $L$ in two distinct points $P_1, P_2$, then it is not tangent to $L$ at either point. Suppose at one of these points, say $P_1$, the tangent to $C_1$ is perpendicular to $L$; then by symmetry, the same will be true of $C_2$, so $C_1$ and $C_2$ will be tangent at $P_1$. In this case, the point $P_1 = (x,x)$ satisfies

$$2\alpha x + \alpha = -1, \qquad x = \alpha x^2 + \alpha x + \frac{1}{24};$$

writing $\alpha = -1/(2x+1)$ in the first equation and substituting into the second, we have

$$x = -\frac{x^2+x}{2x+1} + \frac{1}{24},$$

or $x = (-23 \pm \sqrt{601})/72$. This yields $\alpha = -1/(2x+1) = (13 \pm \sqrt{601})/12$.

If instead the tangents to $C_1$ at $P_1, P_2$ are not perpendicular to $L$, then we claim there cannot be any point where $C_1$ and $C_2$ are tangent. Indeed, if we count intersections of $C_1$ and $C_2$ (by using $C_1$ to substitute for $y$ in $C_2$, then solving for $y$), we get at most four solutions counting multiplicity. Two of these are $P_1$ and $P_2$, and any point of tangency counts for two more. However, off of $L$, any point of tangency would have a mirror image which is also a point of tangency, and there cannot be six solutions. Hence we have now found all possible $\alpha$.

**Second solution:** For any nonzero value of $\alpha$, the two conics will intersect in four points in the complex projective plane $\mathbb{P}^2(\mathbb{C})$. To determine the $y$-coordinates of these intersection points, subtract the two equations to obtain

$$(y-x) = \alpha(x-y)(x+y) + \alpha(x-y).$$

Therefore, at a point of intersection we have either $x = y$, or $x = -1/\alpha - (y+1)$. Substituting these two possible linear conditions into the second equation shows that the $y$-coordinate of a point of intersection is a root of either $Q_1(y) = \alpha y^2 + (\alpha - 1)y + 1/24$ or $Q_2(y) = \alpha y^2 + (\alpha+1)y + 25/24 + 1/\alpha$.

If two curves are tangent, then the $y$-coordinates of at least two of the intersection points will coincide; the converse is also true because one of the curves is the graph of a function in $x$. The coincidence occurs precisely when either the discriminant of at least one of $Q_1$ or $Q_2$ is zero, or there is a common root of $Q_1$ and $Q_2$. Computing the discriminants of $Q_1$ and $Q_2$ yields (up to constant factors) $f_1(\alpha) = 6\alpha^2 - 13\alpha + 6$ and $f_2(\alpha) = 6\alpha^2 - 13\alpha - 18$, respectively. If on the other hand $Q_1$ and $Q_2$ have a common root, it must be also a root of $Q_2(y) - Q_1(y) = 2y + 1 + 1/\alpha$, yielding $y = -(1+\alpha)/(2\alpha)$ and $0 = Q_1(y) = -f_2(\alpha)/(24\alpha)$.

Thus the values of $\alpha$ for which the two curves are tangent must be contained in the set of zeros of $f_1$ and $f_2$, namely $2/3$, $3/2$, and $(13 \pm \sqrt{601})/12$.

**Remark:** The fact that the two conics in $\mathbb{P}^2(\mathbb{C})$ meet in four points, counted with multiplicities, is a special case of *Bézout's theorem*: two curves in $\mathbb{P}^2(\mathbb{C})$ of degrees $m, n$ and not sharing any common component meet in exactly $mn$ points when counted with multiplicity.

Many solvers were surprised that the proposers chose the parameter $1/24$ to give two rational roots and two nonrational roots. In fact, they had no choice in the matter: attempting to make all four roots rational by replacing $1/24$ by $\beta$ amounts to asking for $\beta^2 + \beta$ and $\beta^2 + \beta + 1$ to be perfect squares. This cannot happen outside of trivial cases ($\beta = 0, -1$) ultimately because the elliptic curve 24A1 (in Cremona's notation) over $\mathbb{Q}$ has rank 0. (Thanks to Noam Elkies for providing this computation.)

However, there are choices that make the radical milder, e.g., $\beta = 1/3$ gives $\beta^2 + \beta = 4/9$ and $\beta^2 + \beta + 1 = 13/9$, while $\beta = 3/5$ gives $\beta^2 + \beta = 24/25$ and $\beta^2 + \beta + 1 = 49/25$.

A–2 The minimum is 4, achieved by the square with vertices $(\pm 1, \pm 1)$.

**First solution:** To prove that 4 is a lower bound, let $S$ be a convex set of the desired form. Choose $A,B,C,D \in S$ lying on the branches of the two hyperbolas, with $A$ in the upper right quadrant, $B$ in the upper left, $C$ in the lower left, $D$ in the lower right. Then the area of the quadrilateral $ABCD$ is a lower bound for the area of $S$.

Write $A = (a,1/a)$, $B = (-b,1/b)$, $C = (-c,-1/c)$, $D = (d,-1/d)$ with $a,b,c,d > 0$. Then the area of the quadrilateral $ABCD$ is

$$\frac{1}{2}(a/b+b/c+c/d+d/a+b/a+c/b+d/c+a/d),$$

which by the arithmetic-geometric mean inequality is at least 4.

**Second solution:** Choose $A,B,C,D$ as in the first solution. Note that both the hyperbolas and the area of the convex hull of $ABCD$ are invariant under the transformation $(x,y) \mapsto (xm,y/m)$ for any $m > 0$. For $m$ small, the counterclockwise angle from the line $AC$ to the line $BD$ approaches 0; for $m$ large, this angle approaches $\pi$. By continuity, for some $m$ this angle becomes $\pi/2$, that is, $AC$ and $BD$ become perpendicular. The area of $ABCD$ is then $AC \cdot BD$.

It thus suffices to note that $AC \geq 2\sqrt{2}$ (and similarly for $BD$). This holds because if we draw the tangent lines to the hyperbola $xy = 1$ at the points $(1,1)$ and $(-1,-1)$, then $A$ and $C$ lie outside the region between these lines. If we project the segment $AC$ orthogonally onto the line $x = y = 1$, the resulting projection has length at least $2\sqrt{2}$, so $AC$ must as well.

**Third solution:** (by Richard Stanley) Choose $A,B,C,D$ as in the first solution. Now fixing $A$ and $C$, move $B$ and $D$ to the points at which the tangents to the curve are parallel to the line $AC$. This does not increase the area of the quadrilateral $ABCD$ (even if this quadrilateral is not convex).

Note that $B$ and $D$ are now diametrically opposite; write $B = (-x,1/x)$ and $D = (x,-1/x)$. If we thus repeat the procedure, fixing $B$ and $D$ and moving $A$ and $C$ to the points where the tangents are parallel to $BD$, then $A$ and $C$ must move to $(x,1/x)$ and $(-x,-1/x)$, respectively, forming a rectangle of area 4.

**Remark:** Many geometric solutions are possible. An example suggested by David Savitt (due to Chris Brewer): note that $AD$ and $BC$ cross the positive and negative $x$-axes, respectively, so the convex hull of $ABCD$ contains $O$. Then check that the area of triangle $OAB$ is at least 1, et cetera.

A–3 Assume that we have an ordering of $1,2,\dots,3k+1$ such that no initial subsequence sums to 0 mod 3. If we omit the multiples of 3 from this ordering, then the remaining sequence mod 3 must look like $1,1,-1,1,-1,\dots$ or $-1,-1,1,-1,1,\dots$. Since there is one more integer in the ordering congruent to 1 mod 3 than to $-1$, the sequence mod 3 must look like $1,1,-1,1,-1,\dots$.

It follows that the ordering satisfies the given condition if and only if the following two conditions hold: the first element in the ordering is not divisible by 3, and the sequence mod 3 (ignoring zeroes) is of the form $1,1,-1,1,-1,\dots$. The two conditions are independent, and the probability of the first is $(2k+1)/(3k+1)$ while the probability of the second is $1/\binom{2k+1}{k}$, since there are $\binom{2k+1}{k}$ ways to order $(k+1)$ 1's and $k$ $-1$'s. Hence the desired probability is the product of these two, or $\frac{k!(k+1)!}{(3k+1)(2k)!}$.

A–4 Note that $n$ is a repunit if and only if $9n+1 = 10^m$ for some power of 10 greater than 1. Consequently, if we put

$$g(n) = 9f\left(\frac{n-1}{9}\right)+1,$$

then $f$ takes repunits to repunits if and only if $g$ takes powers of 10 greater than 1 to powers of 10 greater than 1. We will show that the only such functions $g$ are those of the form $g(n) = 10^c n^d$ for $d \geq 0$, $c \geq 1-d$ (all of which clearly work), which will mean that the desired polynomials $f$ are those of the form

$$f(n) = \frac{1}{9}(10^c(9n+1)^d - 1)$$

for the same $c,d$.

It is convenient to allow "powers of 10" to be of the form $10^k$ for any integer $k$. With this convention, it suffices to check that the polynomials $g$ taking powers of 10 greater than 1 to powers of 10 are of the form $10^c n^d$ for any integers $c,d$ with $d \geq 0$.

**First solution:** Suppose that the leading term of $g(x)$ is $ax^d$, and note that $a > 0$. As $x \to \infty$, we have $g(x)/x^d \to a$; however, for $x$ a power of 10 greater than 1, $g(x)/x^d$ is a power of 10. The set of powers of 10 has no positive limit point, so $g(x)/x^d$ must be equal to $a$ for $x = 10^k$ with $k$ sufficiently large, and we must have $a = 10^c$ for some $c$. The polynomial $g(x) - 10^c x^d$ has infinitely many roots, so must be identically zero.

**Second solution:** We proceed by induction on $d = \deg(g)$. If $d = 0$, we have $g(n) = 10^c$ for some $c$. Otherwise, $g$ has rational coefficients by Lagrange's interpolation formula (this applies to any polynomial of degree $d$ taking at least $d+1$ different rational numbers to rational numbers), so $g(0) = t$ is rational. Moreover, $g$ takes each value only finitely many times, so the sequence $g(10^0), g(10^1), \dots$ includes arbitrarily large powers of 10. Suppose that $t \neq 0$; then we can choose a positive integer $h$ such that the numerator of $t$ is not divisible by $10^h$. But for $c$ large enough, $g(10^c) - t$ has numerator divisible by $10^b$ for some $b > h$, contradiction.

Consequently, $t = 0$, and we may apply the induction hypothesis to $g(n)/n$ to deduce the claim.

**Remark:** The second solution amounts to the fact that $g$, being a polynomial with rational coefficients, is continuous for the 2-adic and 5-adic topologies on $\mathbb{Q}$. By contrast, the first solution uses the "$\infty$-adic" topology, i.e., the usual real topology.

A–5 In all solutions, let $G$ be a finite group of order $m$.

**First solution:** By Lagrange's theorem, if $m$ is not divisible by $p$, then $n = 0$. Otherwise, let $S$ be the set of $p$-tuples $(a_0, \dots, a_{p-1}) \in G^p$ such that $a_0 \cdots a_{p-1} = e$; then $S$ has cardinality $m^{p-1}$, which is divisible by $p$. Note that this set is invariant under cyclic permutation, that is, if $(a_0, \dots, a_{p-1}) \in S$, then $(a_1, \dots, a_{p-1}, a_0) \in S$ also. The fixed points under this operation are the tuples $(a, \dots, a)$ with $a^p = e$; all other tuples can be grouped into orbits under cyclic permutation, each of which has size $p$. Consequently, the number of $a \in G$ with $a^p = e$ is divisible by $p$; since that number is $n+1$ (only $e$ has order 1), this proves the claim.

**Second solution:** (by Anand Deopurkar) Assume that $n > 0$, and let $H$ be any subgroup of $G$ of order $p$. Let $S$ be the set of all elements of $G \setminus H$ of order dividing $p$, and let $H$ act on $G$ by conjugation. Each orbit has size $p$ except for those which consist of individual elements $g$ which commute with $H$. For each such $g$, $g$ and $H$ generate an elementary abelian subgroup of $G$ of order $p^2$. However, we can group these $g$ into sets of size $p^2 - p$ based on which subgroup they generate together with $H$. Hence the cardinality of $S$ is divisible by $p$; adding the $p-1$ nontrivial elements of $H$ gives $n \equiv -1 \pmod{p}$ as desired.

**Third solution:** Let $S$ be the set of elements in $G$ having order dividing $p$, and let $H$ be an elementary abelian $p$-group of maximal order in $G$. If $|H| = 1$, then we are done. So assume $|H| = p^k$ for some $k \geq 1$, and let $H$ act on $S$ by conjugation. Let $T \subset S$ denote the set of fixed points of this action. Then the size of every $H$-orbit on $S$ divides $p^k$, and so $|S| \equiv |T| \pmod{p}$. On the other hand, $H \subset T$, and if $T$ contained an element not in $H$, then that would contradict the maximality of $H$. It follows that $H = T$, and so $|S| \equiv |T| = |H| = p^k \equiv 0 \pmod{p}$, i.e., $|S| = n+1$ is a multiple of $p$.

**Remark:** This result is a theorem of Cauchy; the first solution above is due to McKay. A more general (and more difficult) result was proved by Frobenius: for any positive integer $m$, if $G$ is a finite group of order divisible by $m$, then the number of elements of $G$ of order dividing $m$ is a multiple of $m$.

A–6 For an admissible triangulation $\mathscr{T}$, number the vertices of $P$ consecutively $v_1, \dots, v_n$, and let $a_i$ be the number of edges in $\mathscr{T}$ emanating from $v_i$; note that $a_i \geq 2$ for all $i$.

We first claim that $a_1 + \cdots + a_n \leq 4n - 6$. Let $V, E, F$ denote the number of vertices, edges, and faces in $\mathscr{T}$. By Euler's Formula, $(F+1) - E + V = 2$ (one must add 1 to the face count for the region exterior to $P$). Each face has three edges, and each edge but the $n$ outside edges belongs to two faces; hence $F = 2E - n$. On the other hand, each edge has two endpoints, and each of the $V - n$ internal vertices is an endpoint of at least 6 edges; hence $a_1 + \cdots + a_n + 6(V-n) \leq 2E$. Combining this inequality with the previous two equations gives

$$\begin{aligned} a_1 + \cdots + a_n &\leq 2E + 6n - 6(1 - F + E) \\ &= 4n - 6, \end{aligned}$$

as claimed.

Now set $A_3 = 1$ and $A_n = A_{n-1} + 2n - 3$ for $n \geq 4$; we will prove by induction on $n$ that $\mathscr{T}$ has at most $A_n$ triangles. For $n = 3$, since $a_1 + a_2 + a_3 = 6$, $a_1 = a_2 = a_3 = 2$ and hence $\mathscr{T}$ consists of just one triangle.

Next assume that an admissible triangulation of an $(n-1)$-gon has at most $A_{n-1}$ triangles, and let $\mathscr{T}$ be an admissible triangulation of an $n$-gon. If any $a_i = 2$, then we can remove the triangle of $\mathscr{T}$ containing vertex $v_i$ to obtain an admissible triangulation of an $(n-1)$-gon; then the number of triangles in $\mathscr{T}$ is at most $A_{n-1} + 1 < A_n$ by induction. Otherwise, all $a_i \geq 3$. Now the average of $a_1, \dots, a_n$ is less than 4, and thus there are more $a_i = 3$ than $a_i \geq 5$. It follows that there is a sequence of $k$ consecutive vertices in $P$ whose degrees are $3, 4, 4, \dots, 4, 3$ in order, for some $k$ with $2 \leq k \leq n-1$ (possibly $k = 2$, in which case there are no degree 4 vertices separating the degree 3 vertices). If we remove from $\mathscr{T}$ the $2k-1$ triangles which contain at least one of these vertices, then we are left with an admissible triangulation of an $(n-1)$-gon. It follows that there are at most $A_{n-1} + 2k - 1 \leq A_{n-1} + 2n - 3 = A_n$ triangles in $\mathscr{T}$. This completes the induction step and the proof.

**Remark:** We can refine the bound $A_n$ somewhat. Supposing that $a_i \geq 3$ for all $i$, the fact that $a_1 + \cdots + a_n \leq 4n - 6$ implies that there are at least six more indices $i$ with $a_i = 3$ than with $a_i \geq 5$. Thus there exist six sequences with degrees $3, 4, \dots, 4, 3$, of total length at most $n + 6$. We may thus choose a sequence of length $k \leq \lfloor \frac{n}{6} \rfloor + 1$, so we may improve the upper bound to $A_n = A_{n-1} + 2\lfloor \frac{n}{6} \rfloor + 1$, or asymptotically $\frac{1}{6}n^2$.

However (as noted by Noam Elkies), a hexagonal swatch of a triangular lattice, with the boundary as close to regular as possible, achieves asymptotically $\frac{1}{6}n^2$ triangles.

B–1 The problem fails if $f$ is allowed to be constant, e.g., take $f(n) = 1$. We thus assume that $f$ is nonconstant. Write $f(n) = \sum_{i=0}^d a_i n^i$ with $a_i > 0$. Then

$$\begin{aligned} f(f(n)+1) &= \sum_{i=0}^d a_i (f(n)+1)^i \\ &\equiv f(1) \pmod{f(n)}. \end{aligned}$$

If $n = 1$, then this implies that $f(f(n)+1)$ is divisible by $f(n)$. Otherwise, $0 < f(1) < f(n)$ since $f$ is nonconstant and has positive coefficients, so $f(f(n)+1)$ cannot be divisible by $f(n)$.

B–2 Put $B = \max_{0 \leq x \leq 1} |f'(x)|$ and $g(x) = \int_0^x f(y)\,dy$. Since $g(0) = g(1) = 0$, the maximum value of $|g(x)|$ must occur at a critical point $y \in (0,1)$ satisfying $g'(y) = f(y) = 0$. We may thus take $\alpha = y$ hereafter.

Since $\int_0^\alpha f(x)\,dx = -\int_0^{1-\alpha} f(1-x)\,dx$, we may assume that $\alpha \leq 1/2$. By then substituting $-f(x)$ for $f(x)$ if needed, we may assume that $\int_0^\alpha f(x)\,dx \geq 0$. From the inequality $f'(x) \geq -B$, we deduce $f(x) \leq B(\alpha - x)$ for $0 \leq x \leq \alpha$, so

$$\begin{aligned}\int_0^\alpha f(x)\,dx &\leq \int_0^\alpha B(\alpha - x)\,dx \\ &= -\frac{1}{2}B(\alpha-x)^2\Big|_0^\alpha \\ &= \frac{\alpha^2}{2}B \leq \frac{1}{8}B\end{aligned}$$

as desired.

B–3 **First solution:** Observing that $x_2/2 = 13$, $x_3/4 = 34$, $x_4/8 = 89$, we guess that $x_n = 2^{n-1}F_{2n+3}$, where $F_k$ is the $k$-th Fibonacci number. Thus we claim that $x_n = \frac{2^{n-1}}{\sqrt{5}}(\alpha^{2n+3} - \alpha^{-(2n+3)})$, where $\alpha = \frac{1+\sqrt{5}}{2}$, to make the answer $x_{2007} = \frac{2^{2006}}{\sqrt{5}}(\alpha^{3997} - \alpha^{-3997})$.

We prove the claim by induction; the base case $x_0 = 1$ is true, and so it suffices to show that the recursion $x_{n+1} = 3x_n + \lfloor x_n\sqrt{5} \rfloor$ is satisfied for our formula for $x_n$. Indeed, since $\alpha^2 = \frac{3+\sqrt{5}}{2}$, we have

$$\begin{aligned}x_{n+1} - (3+\sqrt{5})x_n &= \frac{2^{n-1}}{\sqrt{5}}(2(\alpha^{2n+5} - \alpha^{-(2n+5)}) \\ &\quad - (3+\sqrt{5})(\alpha^{2n+3} - \alpha^{-(2n+3)})) \\ &= 2^n\alpha^{-(2n+3)}.\end{aligned}$$

Now $2^n\alpha^{-(2n+3)} = (\frac{1-\sqrt{5}}{2})^3(3-\sqrt{5})^n$ is between $-1$ and 0; the recursion follows since $x_n, x_{n+1}$ are integers.

**Second solution:** (by Catalin Zara) Since $x_n$ is rational, we have $0 < x_n\sqrt{5} - \lfloor x_n\sqrt{5} \rfloor < 1$. We now have the inequalities

$$\begin{gathered}x_{n+1} - 3x_n < x_n\sqrt{5} < x_{n+1} - 3x_n + 1 \\ (3+\sqrt{5})x_n - 1 < x_{n+1} < (3+\sqrt{5})x_n \\ 4x_n - (3-\sqrt{5}) < (3-\sqrt{5})x_{n+1} < 4x_n \\ 3x_{n+1} - 4x_n < x_{n+1}\sqrt{5} < 3x_{n+1} - 4x_n + (3-\sqrt{5}).\end{gathered}$$

Since $0 < 3 - \sqrt{5} < 1$, this yields $\lfloor x_{n+1}\sqrt{5} \rfloor = 3x_{n+1} - 4x_n$, so we can rewrite the recursion as $x_{n+1} = 6x_n - 4x_{n-1}$ for $n \geq 2$. It is routine to solve this recursion to obtain the same solution as above.

**Remark:** With an initial 1 prepended, this becomes sequence A018903 in Sloane's On-Line Encyclopedia of Integer Sequences: (`http://www.research.att.com/~njas/sequences/`). Therein, the sequence is described as the case $S(1,5)$ of the sequence $S(a_0,a_1)$ in which $a_{n+2}$ is the least integer for which $a_{n+2}/a_{n+1} > a_{n+1}/a_n$. Sloane cites D. W. Boyd, Linear recurrence relations for some generalized Pisot sequences, *Advances in Number Theory (Kingston, ON, 1991)*, Oxford Univ. Press, New York, 1993, p. 333–340.

B–4 The number of pairs is $2^{n+1}$. The degree condition forces $P$ to have degree $n$ and leading coefficient $\pm 1$; we may count pairs in which $P$ has leading coefficient 1 as long as we multiply by 2 afterward.

Factor both sides:

$$\begin{aligned}&(P(X) + Q(X)i)(P(X) - Q(X)i) \\ &= \prod_{j=0}^{n-1}(X - \exp(2\pi i(2j+1)/(4n))) \\ &\cdot \prod_{j=0}^{n-1}(X + \exp(2\pi i(2j+1)/(4n))).\end{aligned}$$

Then each choice of $P, Q$ corresponds to equating $P(X) + Q(X)i$ with the product of some $n$ factors on the right, in which we choose exactly of the two factors for each $j = 0, \dots, n-1$. (We must take exactly $n$ factors because as a polynomial in $X$ with complex coefficients, $P(X) + Q(X)i$ has degree exactly $n$. We must choose one for each $j$ to ensure that $P(X) + Q(X)i$ and $P(X) - Q(X)i$ are complex conjugates, so that $P, Q$ have real coefficients.) Thus there are $2^n$ such pairs; multiplying by 2 to allow $P$ to have leading coefficient $-1$ yields the desired result.

**Remark:** If we allow $P$ and $Q$ to have complex coefficients but still require $\deg(P) > \deg(Q)$, then the number of pairs increases to $2\binom{2n}{n}$, as we may choose any $n$ of the $2n$ factors of $X^{2n} + 1$ to use to form $P(X) + Q(X)i$.

B–5 For $n$ an integer, we have $\left\lfloor \frac{n}{k} \right\rfloor = \frac{n-j}{k}$ for $j$ the unique integer in $\{0, \dots, k-1\}$ congruent to $n$ modulo $k$; hence

$$\prod_{j=0}^{k-1}\left(\left\lfloor \frac{n}{k} \right\rfloor - \frac{n-j}{k}\right) = 0.$$

By expanding this out, we obtain the desired polynomials $P_0(n), \dots, P_{k-1}(n)$.

**Remark:** Variants of this solution are possible that construct the $P_i$ less explicitly, using Lagrange interpolation or Vandermonde determinants.

B–6 (Suggested by Oleg Golberg) Assume $n \geq 2$, or else the problem is trivially false. Throughout this proof, any $C_i$ will be a positive constant whose exact value is immaterial. As in the proof of Stirling's approximation, we estimate for any fixed $c \in \mathbb{R}$,

$$\sum_{i=1}^n (i+c)\log i = \frac{1}{2}n^2\log n - \frac{1}{4}n^2 + O(n\log n)$$

by comparing the sum to an integral. This gives

$$\begin{aligned} n^{n^2/2-C_1 n} e^{-n^2/4} &\le 1^{1+c} 2^{2+c} \cdots n^{n+c} \\ &\le n^{n^2/2+C_2 n} e^{-n^2/4}. \end{aligned}$$

We now interpret $f(n)$ as counting the number of $n$-tuples $(a_1, \dots, a_n)$ of nonnegative integers such that

$$a_1 1! + \cdots + a_n n! = n!.$$

For an upper bound on $f(n)$, we use the inequalities $0 \le a_i \le n!/i!$ to deduce that there are at most $n!/i! + 1 \le 2(n!/i!)$ choices for $a_i$. Hence

$$\begin{aligned} f(n) &\le 2^n \frac{n!}{1!} \cdots \frac{n!}{n!} \\ &= 2^n 2^1 3^2 \cdots n^{n-1} \\ &\le n^{n^2/2+C_3 n} e^{-n^2/4}. \end{aligned}$$

For a lower bound on $f(n)$, we note that if $0 \le a_i < (n-1)!/i!$ for $i = 2, \dots, n-1$ and $a_n = 0$, then $0 \le a_2 2! + \cdots + a_n n! \le n!$, so there is a unique choice of $a_1$ to complete this to a solution of $a_1 1! + \cdots + a_n n! = n!$. Hence

$$\begin{aligned} f(n) &\ge \frac{(n-1)!}{2!} \cdots \frac{(n-1)!}{(n-1)!} \\ &= 3^1 4^2 \cdots (n-1)^{n-3} \\ &\ge n^{n^2/2+C_4 n} e^{-n^2/4}. \end{aligned}$$

# The 69th William Lowell Putnam Mathematical Competition
# Saturday, December 6, 2008

A1 Let $f : \mathbb{R}^2 \to \mathbb{R}$ be a function such that $f(x,y) + f(y,z) + f(z,x) = 0$ for all real numbers $x$, $y$, and $z$. Prove that there exists a function $g : \mathbb{R} \to \mathbb{R}$ such that $f(x,y) = g(x) - g(y)$ for all real numbers $x$ and $y$.

A2 Alan and Barbara play a game in which they take turns filling entries of an initially empty $2008 \times 2008$ array. Alan plays first. At each turn, a player chooses a real number and places it in a vacant entry. The game ends when all the entries are filled. Alan wins if the determinant of the resulting matrix is nonzero; Barbara wins if it is zero. Which player has a winning strategy?

A3 Start with a finite sequence $a_1, a_2, \dots, a_n$ of positive integers. If possible, choose two indices $j < k$ such that $a_j$ does not divide $a_k$, and replace $a_j$ and $a_k$ by $\gcd(a_j, a_k)$ and $\operatorname{lcm}(a_j, a_k)$, respectively. Prove that if this process is repeated, it must eventually stop and the final sequence does not depend on the choices made. (Note: gcd means greatest common divisor and lcm means least common multiple.)

A4 Define $f : \mathbb{R} \to \mathbb{R}$ by

$$f(x) = \begin{cases} x & \text{if } x \leq e \\ x f(\ln x) & \text{if } x > e. \end{cases}$$

Does $\sum_{n=1}^{\infty} \frac{1}{f(n)}$ converge?

A5 Let $n \geq 3$ be an integer. Let $f(x)$ and $g(x)$ be polynomials with real coefficients such that the points $(f(1), g(1)), (f(2), g(2)), \dots, (f(n), g(n))$ in $\mathbb{R}^2$ are the vertices of a regular $n$-gon in counterclockwise order. Prove that at least one of $f(x)$ and $g(x)$ has degree greater than or equal to $n-1$.

A6 Prove that there exists a constant $c > 0$ such that in every nontrivial finite group $G$ there exists a sequence of length at most $c \log |G|$ with the property that each element of $G$ equals the product of some subsequence. (The elements of $G$ in the sequence are not required to be distinct. A *subsequence* of a sequence is obtained by selecting some of the terms, not necessarily consecutive, without reordering them; for example, $4, 4, 2$ is a subsequence of $2, 4, 6, 4, 2$, but $2, 2, 4$ is not.)

B1 What is the maximum number of rational points that can lie on a circle in $\mathbb{R}^2$ whose center is not a rational point? (A *rational point* is a point both of whose coordinates are rational numbers.)

B2 Let $F_0(x) = \ln x$. For $n \geq 0$ and $x > 0$, let $F_{n+1}(x) = \int_0^x F_n(t)\,dt$. Evaluate

$$\lim_{n \to \infty} \frac{n! F_n(1)}{\ln n}.$$

B3 What is the largest possible radius of a circle contained in a 4-dimensional hypercube of side length 1?

B4 Let $p$ be a prime number. Let $h(x)$ be a polynomial with integer coefficients such that $h(0), h(1), \dots, h(p^2 - 1)$ are distinct modulo $p^2$. Show that $h(0), h(1), \dots, h(p^3 - 1)$ are distinct modulo $p^3$.

B5 Find all continuously differentiable functions $f : \mathbb{R} \to \mathbb{R}$ such that for every rational number $q$, the number $f(q)$ is rational and has the same denominator as $q$. (The denominator of a rational number $q$ is the unique positive integer $b$ such that $q = a/b$ for some integer $a$ with $\gcd(a, b) = 1$.) (Note: gcd means greatest common divisor.)

B6 Let $n$ and $k$ be positive integers. Say that a permutation $\sigma$ of $\{1, 2, \dots, n\}$ is *$k$-limited* if $|\sigma(i) - i| \leq k$ for all $i$. Prove that the number of $k$-limited permutations of $\{1, 2, \dots, n\}$ is odd if and only if $n \equiv 0$ or $1 \pmod{2k+1}$.

# Solutions to the 69th William Lowell Putnam Mathematical Competition
# Saturday, December 6, 2008

Kiran Kedlaya and Lenny Ng

A–1 The function $g(x) = f(x,0)$ works. Substituting $(x,y,z) = (0,0,0)$ into the given functional equation yields $f(0,0) = 0$, whence substituting $(x,y,z) = (x,0,0)$ yields $f(x,0) + f(0,x) = 0$. Finally, substituting $(x,y,z) = (x,y,0)$ yields $f(x,y) = -f(y,0) - f(0,x) = g(x) - g(y)$.

**Remark:** A similar argument shows that the possible functions $g$ are precisely those of the form $f(x,0) + c$ for some $c$.

A–2 Barbara wins using one of the following strategies.

**First solution:** Pair each entry of the first row with the entry directly below it in the second row. If Alan ever writes a number in one of the first two rows, Barbara writes the same number in the other entry in the pair. If Alan writes a number anywhere other than the first two rows, Barbara does likewise. At the end, the resulting matrix will have two identical rows, so its determinant will be zero.

**Second solution:** (by Manjul Bhargava) Whenever Alan writes a number $x$ in an entry in some row, Barbara writes $-x$ in some other entry in the same row. At the end, the resulting matrix will have all rows summing to zero, so it cannot have full rank.

A–3 We first prove that the process stops. Note first that the product $a_1 \cdots a_n$ remains constant, because $a_j a_k = \gcd(a_j, a_k) \operatorname{lcm}(a_j, a_k)$. Moreover, the last number in the sequence can never decrease, because it is always replaced by its least common multiple with another number. Since it is bounded above (by the product of all of the numbers), the last number must eventually reach its maximum value, after which it remains constant throughout. After this happens, the next-to-last number will never decrease, so it eventually becomes constant, and so on. After finitely many steps, all of the numbers will achieve their final values, so no more steps will be possible. This only happens when $a_j$ divides $a_k$ for all pairs $j < k$.

We next check that there is only one possible final sequence. For $p$ a prime and $m$ a nonnegative integer, we claim that the number of integers in the list divisible by $p^m$ never changes. To see this, suppose we replace $a_j, a_k$ by $\gcd(a_j, a_k), \operatorname{lcm}(a_j, a_k)$. If neither of $a_j, a_k$ is divisible by $p^m$, then neither of $\gcd(a_j, a_k), \operatorname{lcm}(a_j, a_k)$ is either. If exactly one $a_j, a_k$ is divisible by $p^m$, then $\operatorname{lcm}(a_j, a_k)$ is divisible by $p^m$ but $\gcd(a_j, a_k)$ is not.

$\gcd(a_j, a_k), \operatorname{lcm}(a_j, a_k)$ are as well.

If we started out with exactly $h$ numbers not divisible by $p^m$, then in the final sequence $a'_1, \dots, a'_n$, the numbers $a'_{h+1}, \dots, a'_n$ are divisible by $p^m$ while the numbers $a'_1, \dots, a'_h$ are not. Repeating this argument for each pair $(p, m)$ such that $p^m$ divides the initial product $a_1, \dots, a_n$, we can determine the exact prime factorization of each of $a'_1, \dots, a'_n$. This proves that the final sequence is unique.

**Remark:** (by David Savitt and Noam Elkies) Here are two other ways to prove the termination. One is to observe that $\prod_j a_j^j$ is *strictly* increasing at each step, and bounded above by $(a_1 \cdots a_n)^n$. The other is to notice that $a_1$ is nonincreasing but always positive, so eventually becomes constant; then $a_2$ is nonincreasing but always positive, and so on.

**Reinterpretation:** For each $p$, consider the sequence consisting of the exponents of $p$ in the prime factorizations of $a_1, \dots, a_n$. At each step, we pick two positions $i$ and $j$ such that the exponents of some prime $p$ are in the wrong order at positions $i$ and $j$. We then sort these two position into the correct order for every prime $p$ simultaneously.

It is clear that this can only terminate with all sequences being sorted into the correct order. We must still check that the process terminates; however, since all but finitely many of the exponent sequences consist of all zeroes, and each step makes a nontrivial switch in at least one of the other exponent sequences, it is enough to check the case of a single exponent sequence. This can be done as in the first solution.

**Remark:** Abhinav Kumar suggests the following proof that the process always terminates in at most $\binom{n}{2}$ steps. (This is a variant of the worst-case analysis of the *bubble sort* algorithm.)

Consider the number of pairs $(k, l)$ with $1 \leq k < l \leq n$ such that $a_k$ does not divide $a_l$ (call these *bad pairs*). At each step, we find one bad pair $(i, j)$ and eliminate it, and we do not touch any pairs that do not involve either $i$ or $j$. If $i < k < j$, then neither of the pairs $(i, k)$ and $(k, j)$ can become bad, because $a_i$ is replaced by a divisor of itself, while $a_j$ is replaced by a multiple of itself. If $k < i$, then $(k, i)$ can only become a bad pair if $a_k$ divided $a_i$ but not $a_j$, in which case $(k, j)$ stops being bad. Similarly, if $k > j$, then $(i, k)$ and $(j, k)$ either stay the same or switch status. Hence the number of bad pairs goes down by at least 1 each time; since it is at most $\binom{n}{2}$ to begin with, this is an upper bound for the number of steps.

**Remark:** This problem is closely related to the classification theorem for finite abelian groups. Namely, if $a_1, \dots, a_n$ and $a'_1, \dots, a'_n$ are the sequences obtained at two different steps in the process, then the abelian groups $\mathbb{Z}/a_1\mathbb{Z}\times\cdots\times\mathbb{Z}/a_n\mathbb{Z}$ and $\mathbb{Z}/a_1'\mathbb{Z}\times\cdots\times\mathbb{Z}/a_n'\mathbb{Z}$ are isomorphic. The final sequence gives a canonical presentation of this group; the terms of this sequence are called the *elementary divisors* or *invariant factors* of the group.

**Remark:** (by Tom Belulovich) A *lattice* is a partially ordered set $L$ in which for any two $x,y\in L$, there is a unique minimal element $z$ with $z\geq x$ and $z\geq y$, called the *join* and denoted $x\wedge y$, and there is a unique maximal element $z$ with $z\leq x$ and $z\leq y$, called the *meet* and denoted $x\vee y$. In terms of a lattice $L$, one can pose the following generalization of the given problem. Start with $a_1,\dots,a_n\in L$. If $i<j$ but $a_i\not\leq a_j$, it is permitted to replace $a_i,a_j$ by $a_i\vee a_j, a_i\wedge a_j$, respectively. The same argument as above shows that this always terminates in at most $\binom{n}{2}$ steps. The question is, under what conditions on the lattice $L$ is the final sequence uniquely determined by the initial sequence?

It turns out that this holds if and only if $L$ is *distributive*, i.e., for any $x,y,z\in L$,

$$x\wedge(y\vee z)=(x\wedge y)\vee(x\wedge z).$$

(This is equivalent to the same axiom with the operations interchanged.) For example, if $L$ is a *Boolean algebra*, i.e., the set of subsets of a given set $S$ under inclusion, then $\wedge$ is union, $\vee$ is intersection, and the distributive law holds. Conversely, any finite distributive lattice is contained in a Boolean algebra by a theorem of Birkhoff. The correspondence takes each $x\in L$ to the set of $y\in L$ such that $x\geq y$ and $y$ cannot be written as a join of two elements of $L\setminus\{y\}$. (See for instance Birkhoff, *Lattice Theory*, Amer. Math. Soc., 1967.)

On one hand, if $L$ is distributive, it can be shown that the $j$-th term of the final sequence is equal to the meet of $a_{i_1}\wedge\cdots\wedge a_{i_j}$ over all sequences $1\leq i_1<\cdots<i_j\leq n$. For instance, this can be checked by forming the smallest subset $L'$ of $L$ containing $a_1,\dots,a_n$ and closed under meet and join, then embedding $L'$ into a Boolean algebra using Birkhoff's theorem, then checking the claim for all Boolean algebras. It can also be checked directly (as suggested by Nghi Nguyen) by showing that for $j=1,\dots,n$, the meet of all joins of $j$-element subsets of $a_1,\dots,a_n$ is invariant at each step.

On the other hand, a lattice fails to be distributive if and only if it contains five elements $a,b,c,0,1$ such that either the only relations among them are implied by

$$1\geq a,b,c\geq 0$$

(this lattice is sometimes called the *diamond*), or the only relations among them are implied by

$$1\geq a\geq b\geq 0,\qquad 1\geq c\geq 0$$

(this lattice is sometimes called the *pentagon*). (For a proof, see the Birkhoff reference given above.) For each of these examples, the initial sequence $a,b,c$ fails to determine the final sequence; for the diamond, we can end up with $0,*,1$ for any of $*=a,b,c$, whereas for the pentagon we can end up with $0,*,1$ for any of $*=a,b$.

Consequently, the final sequence is determined by the initial sequence if and only if $L$ is distributive.

A–4 The sum diverges. From the definition, $f(x)=x$ on $[1,e]$, $x\ln x$ on $(e,e^e]$, $x\ln x\ln\ln x$ on $(e^e,e^{e^e}]$, and so forth. It follows that on $[1,\infty)$, $f$ is positive, continuous, and increasing. Thus $\sum_{n=1}^\infty\frac{1}{f(n)}$, if it converges, is bounded below by $\int_1^\infty\frac{dx}{f(x)}$; it suffices to prove that the integral diverges.

Write $\ln^1 x=\ln x$ and $\ln^k x=\ln(\ln^{k-1}x)$ for $k\geq 2$; similarly write $\exp^1 x=e^x$ and $\exp^k x=e^{\exp^{k-1}x}$. If we write $y=\ln^k x$, then $x=\exp^k y$ and $dx=(\exp^k y)(\exp^{k-1}y)\cdots(\exp^1 y)dy=x(\ln^1 x)\cdots(\ln^{k-1}x)dy$. Now on $[\exp^{k-1}1,\exp^k 1]$, we have $f(x)=x(\ln^1 x)\cdots(\ln^{k-1}x)$, and thus substituting $y=\ln^k x$ yields

$$\int_{\exp^{k-1}1}^{\exp^k 1}\frac{dx}{f(x)}=\int_0^1 dy=1.$$

It follows that $\int_1^\infty\frac{dx}{f(x)}=\sum_{k=1}^\infty\int_{\exp^{k-1}1}^{\exp^k 1}\frac{dx}{f(x)}$ diverges, as desired.

A–5 Form the polynomial $P(z)=f(z)+ig(z)$ with complex coefficients. It suffices to prove that $P$ has degree at least $n-1$, as then one of $f,g$ must have degree at least $n-1$.

By replacing $P(z)$ with $aP(z)+b$ for suitable $a,b\in\mathbb{C}$, we can force the regular $n$-gon to have vertices $\zeta_n,\zeta_n^2,\dots,\zeta_n^n$ for $\zeta_n=\exp(2\pi i/n)$. It thus suffices to check that there cannot exist a polynomial $P(z)$ of degree at most $n-2$ such that $P(i)=\zeta_n^i$ for $i=1,\dots,n$.

We will prove more generally that for any complex number $t\notin\{0,1\}$, and any integer $m\geq 1$, any polynomial $Q(z)$ for which $Q(i)=t^i$ for $i=1,\dots,m$ has degree at least $m-1$. There are several ways to do this.

**First solution:** If $Q(z)$ has degree $d$ and leading coefficient $c$, then $R(z)=Q(z+1)-tQ(z)$ has degree $d$ and leading coefficient $(1-t)c$. However, by hypothesis, $R(z)$ has the distinct roots $1,2,\dots,m-1$, so we must have $d\geq m-1$.

**Second solution:** We proceed by induction on $m$. For the base case $m=1$, we have $Q(1)=t^1\neq 0$, so $Q$ must be nonzero, and so its degree is at least 0. Given the assertion for $m-1$, if $Q(i)=t^i$ for $i=1,\dots,m$, then the polynomial $R(z)=(t-1)^{-1}(Q(z+1)-Q(z))$ has degree one less than that of $Q$, and satisfies $R(i)=t^i$ for $i=1,\dots,m-1$. Since $R$ must have degree at least $m-2$ by the induction hypothesis, $Q$ must have degree at least $m-1$.

**Third solution:** We use the method of *finite differences* (as in the second solution) but without induction.

Namely, the $(m-1)$-st finite difference of $P$ evaluated at 1 equals

$$\sum_{j=0}^{m-1}(-1)^j\binom{m-1}{j}Q(m-j) = t(1-t)^{m-1} \neq 0,$$

which is impossible if $Q$ has degree less than $m-1$.

**Remark:** One can also establish the claim by computing a Vandermonde-type determinant, or by using the Lagrange interpolation formula to compute the leading coefficient of $Q$.

A–6 For notational convenience, we will interpret the problem as allowing the empty subsequence, whose product is the identity element of the group. To solve the problem in the interpretation where the empty subsequence is not allowed, simply append the identity element to the sequence given by one of the following solutions.

**First solution:** Put $n = |G|$. We will say that a sequence $S$ *produces* an element $g \in G$ if $g$ occurs as the product of some subsequence of $S$. Let $H$ be the set of elements produced by the sequence $S$.

Start with $S$ equal to the empty sequence. If at any point the set $H^{-1}H = \{h_1h_2 : h_1^{-1}, h_2 \in H\}$ fails to be all of $G$, extend $S$ by appending an element $g$ of $G$ not in $H^{-1}H$. Then $Hg \cap H$ must be empty, otherwise there would be an equation of the form $h_1 g = h_2$ with $h_1, h_2 \in G$, or $g = h_1^{-1}h_2$, a contradiction. Thus we can extend $S$ by one element and double the size of $H$.

After $k \leq \log_2 n$ steps, we must obtain a sequence $S = a_1, \dots, a_k$ for which $H^{-1}H = G$. Then the sequence $a_k^{-1}, \dots, a_1^{-1}, a_1, \dots, a_k$ produces all of $G$ and has length at most $(2/\ln 2)\ln n$.

**Second solution:**

Put $m = |H|$. We will show that we can append one element $g$ to $S$ so that the resulting sequence of $k+1$ elements will produce at least $2m - m^2/n$ elements of $G$. To see this, we compute

$$\begin{aligned}
\sum_{g\in G}|H\cup Hg| &= \sum_{g\in G}(|H| + |Hg| - |H\cap Hg|)\\
&= 2mn - \sum_{g\in G}|H\cap Hg|\\
&= 2mn - |\{(g,h)\in G^2 : h \in H\cap Hg\}|\\
&= 2mn - \sum_{h\in H}|\{g\in G : h \in Hg\}|\\
&= 2mn - \sum_{h\in H}|H^{-1}h|\\
&= 2mn - m^2.
\end{aligned}$$

By the pigeonhole principle, we have $|H\cup Hg| \geq 2m - m^2/n$ for some choice of $g$, as claimed.

In other words, by extending the sequence by one element, we can replace the ratio $s = 1 - m/n$ (i.e., the fraction of elements of $G$ not generated by $S$) by a quantity no greater than

$$1 - (2m - m^2/n)/n = s^2.$$

We start out with $k = 0$ and $s = 1 - 1/n$; after $k$ steps, we have $s \leq (1-1/n)^{2^k}$. It is enough to prove that for some $c > 0$, we can always find an integer $k \leq c \ln n$ such that

$$\left(1 - \frac{1}{n}\right)^{2^k} < \frac{1}{n},$$

as then we have $n - m < 1$ and hence $H = G$.

To obtain this last inequality, put

$$k = \lfloor 2\log_2 n\rfloor < (2/\ln 2)\ln n,$$

so that $2^{k+1} \geq n^2$. From the facts that $\ln n \leq \ln 2 + (n-2)/2 \leq n/2$ and $\ln(1-1/n) < -1/n$ for all $n \geq 2$, we have

$$2^k \ln\left(1 - \frac{1}{n}\right) < -\frac{n^2}{2n} = -\frac{n}{2} < -\ln n,$$

yielding the desired inequality.

**Remark:** An alternate approach in the second solution is to distinguish betwen the cases of $H$ small (i.e., $m < n^{1/2}$, in which case $m$ can be replaced by a value no less than $2m-1$) and $H$ large. This strategy is used in a number of recent results of Bourgain, Tao, Helfgott, and others on *small doubling* or *small tripling* of subsets of finite groups.

In the second solution, if we avoid the rather weak inequality $\ln n \leq n/2$, we instead get sequences of length $\log_2(n \ln n) = \log_2(n) + \log_2(\ln n)$. This is close to optimal: one cannot use fewer than $\log_2 n$ terms because the number of subsequences must be at least $n$.

B–1 There are at most two such points. For example, the points $(0,0)$ and $(1,0)$ lie on a circle with center $(1/2, x)$ for any real number $x$, not necessarily rational.

On the other hand, suppose $P = (a,b), Q = (c,d), R = (e,f)$ are three rational points that lie on a circle. The midpoint $M$ of the side $PQ$ is $((a+c)/2, (b+d)/2)$, which is again rational. Moreover, the slope of the line $PQ$ is $(d-b)/(c-a)$, so the slope of the line through $M$ perpendicular to $PQ$ is $(a-c)/(b-d)$, which is rational or infinite.

Similarly, if $N$ is the midpoint of $QR$, then $N$ is a rational point and the line through $N$ perpendicular to $QR$ has rational slope. The center of the circle lies on both of these lines, so its coordinates $(g,h)$ satisfy two linear equations with rational coefficients, say $Ag + Bh = C$ and $Dg + Eh = F$. Moreover, these equations have a unique solution. That solution must then be

$$\begin{aligned}
g &= (CE - BD)/(AE - BD)\\
h &= (AF - BC)/(AE - BD)
\end{aligned}$$

(by elementary algebra, or Cramer's rule), so the center of the circle is rational. This proves the desired result.

**Remark:** The above solution is deliberately more verbose than is really necessary. A shorter way to say this is that any two distinct rational points determine a *rational line* (a line of the form $ax+by+c=0$ with $a,b,c$ rational), while any two nonparallel rational lines intersect at a rational point. A similar statement holds with the rational numbers replaced by any field.

**Remark:** A more explicit argument is to show that the equation of the circle through the rational points $(x_1,y_1),(x_2,y_2),(x_3,y_3)$ is

$$0=\det\begin{pmatrix} x_1^2+y_1^2 & x_1 & y_1 & 1\\ x_2^2+y_2^2 & x_2 & y_2 & 1\\ x_3^2+y_3^2 & x_3 & y_3 & 1\\ x^2+y^2 & x & y & 1\end{pmatrix}$$

which has the form $a(x^2+y^2)+dx+ey+f=0$ for $a,d,e,f$ rational. The center of this circle is $(-d/(2a),-e/(2a))$, which is again a rational point.

B–2 We claim that $F_n(x)=(\ln x-a_n)x^n/n!$, where $a_n=\sum_{k=1}^n 1/k$. Indeed, temporarily write $G_n(x)=(\ln x-a_n)x^n/n!$ for $x>0$ and $n\geq 1$; then $\lim_{x\to 0}G_n(x)=0$ and $G_n'(x)=(\ln x-a_n+1/n)x^{n-1}/(n-1)!=G_{n-1}(x)$, and the claim follows by the Fundamental Theorem of Calculus and induction on $n$.

Given the claim, we have $F_n(1)=-a_n/n!$ and so we need to evaluate $-\lim_{n\to\infty}\frac{a_n}{\ln n}$. But since the function $1/x$ is strictly decreasing for $x$ positive, $\sum_{k=2}^n 1/k=a_n-1$ is bounded below by $\int_2^n dx/x=\ln n-\ln 2$ and above by $\int_1^n dx/x=\ln n$. It follows that $\lim_{n\to\infty}\frac{a_n}{\ln n}=1$, and the desired limit is $-1$.

B–3 The largest possible radius is $\frac{\sqrt{2}}{2}$. It will be convenient to solve the problem for a hypercube of side length 2 instead, in which case we are trying to show that the largest radius is $\sqrt{2}$.

Choose coordinates so that the interior of the hypercube is the set $H=[-1,1]^4$ in $\mathbb{R}^4$. Let $C$ be a circle centered at the point $P$. Then $C$ is contained both in $H$ and its reflection across $P$; these intersect in a rectangular parallelepiped each of whose pairs of opposite faces are at most 2 unit apart. Consequently, if we translate $C$ so that its center moves to the point $O=(0,0,0,0)$ at the center of $H$, then it remains entirely inside $H$.

This means that the answer we seek equals the largest possible radius of a circle $C$ contained in $H$ *and centered at* $O$. Let $v_1=(v_{11},\dots,v_{14})$ and $v_2=(v_{21},\dots,v_{24})$ be two points on $C$ lying on radii perpendicular to each other. Then the points of the circle can be expressed as $v_1\cos\theta+v_2\sin\theta$ for $0\leq\theta<2\pi$. Then $C$ lies in $H$ if and only if for each $i$, we have

$$|v_{1i}\cos\theta+v_{2i}\sin\theta|\leq 1\qquad(0\leq\theta<2\pi).$$

In geometric terms, the vector $(v_{1i},v_{2i})$ in $\mathbb{R}^2$ has dot product at most 1 with every unit vector. Since this holds for the unit vector in the same direction as $(v_{1i},v_{2i})$, we must have

$$v_{1i}^2+v_{2i}^2\leq 1\qquad(i=1,\dots,4).$$

Conversely, if this holds, then the Cauchy-Schwarz inequality and the above analysis imply that $C$ lies in $H$.

If $r$ is the radius of $C$, then

$$\begin{aligned}2r^2&=\sum_{i=1}^4 v_{1i}^2+\sum_{i=1}^4 v_{2i}^2\\&=\sum_{i=1}^4(v_{1i}^2+v_{2i}^2)\\&\leq 4,\end{aligned}$$

so $r\leq\sqrt{2}$. Since this is achieved by the circle through $(1,1,0,0)$ and $(0,0,1,1)$, it is the desired maximum.

**Remark:** One may similarly ask for the radius of the largest $k$-dimensional ball inside an $n$-dimensional unit hypercube; the given problem is the case $(n,k)=(4,2)$. Daniel Kane gives the following argument to show that the maximum radius in this case is $\frac{1}{2}\sqrt{\frac{n}{k}}$. (Thanks for Noam Elkies for passing this along.)

We again scale up by a factor of 2, so that we are trying to show that the maximum radius $r$ of a $k$-dimensional ball contained in the hypercube $[-1,1]^n$ is $\sqrt{\frac{n}{k}}$. Again, there is no loss of generality in centering the ball at the origin. Let $T:\mathbb{R}^k\to\mathbb{R}^n$ be a similitude carrying the unit ball to this embedded $k$-ball. Then there exists a vector $v_i\in\mathbb{R}^k$ such that for $e_1,\dots,e_n$ the standard basis of $\mathbb{R}^n$, $x\cdot v_i=T(x)\cdot e_i$ for all $x\in\mathbb{R}^k$. The condition of the problem is equivalent to requiring $|v_i|\leq 1$ for all $i$, while the radius $r$ of the embedded ball is determined by the fact that for all $x\in\mathbb{R}^k$,

$$r^2(x\cdot x)=T(x)\cdot T(x)=\sum_{i=1}^n x\cdot v_i.$$

Let $M$ be the matrix with columns $v_1,\dots,v_k$; then $MM^T=r^2I_k$, for $I_k$ the $k\times k$ identity matrix. We then have

$$\begin{aligned}kr^2&=\mathrm{Trace}(r^2I_k)=\mathrm{Trace}(MM^T)\\&=\mathrm{Trace}(M^TM)=\sum_{i=1}^n|v_i|^2\\&\leq n,\end{aligned}$$

yielding the upper bound $r\leq\sqrt{\frac{n}{k}}$.

To show that this bound is optimal, it is enough to show that one can find an orthogonal projection of $\mathbb{R}^n$ onto $\mathbb{R}^k$ so that the projections of the $e_i$ all have the same norm (one can then rescale to get the desired configuration of $v_1,\dots,v_n$). We construct such a configuration by a "smoothing" argument. Startw with any projection. Let

$w_1, \dots, w_n$ be the projections of $e_1, \dots, e_n$. If the desired condition is not achieved, we can choose $i, j$ such that

$$|w_i|^2 < \frac{1}{n}(|w_1|^2 + \cdots + |w_n|^2) < |w_j|^2.$$

By precomposing with a suitable rotation that fixes $e_h$ for $h \neq i, j$, we can vary $|w_i|, |w_j|$ without varying $|w_i|^2 + |w_j|^2$ or $|w_h|$ for $h \neq i, j$. We can thus choose such a rotation to force one of $|w_i|^2, |w_j|^2$ to become equal to $\frac{1}{n}(|w_1|^2 + \cdots + |w_n|^2)$. Repeating at most $n-1$ times gives the desired configuration.

B–4 We use the identity given by Taylor's theorem:

$$h(x+y) = \sum_{i=0}^{\deg(h)} \frac{h^{(i)}(x)}{i!} y^i.$$

In this expression, $h^{(i)}(x)/i!$ is a polynomial in $x$ with integer coefficients, so its value at an integer $x$ is an integer.

For $x = 0, \dots, p-1$, we deduce that

$$h(x+p) \equiv h(x) + ph'(x) \pmod{p^2}.$$

(This can also be deduced more directly using the binomial theorem.) Since we assumed $h(x)$ and $h(x+p)$ are distinct modulo $p^2$, we conclude that $h'(x) \not\equiv 0 \pmod{p}$. Since $h'$ is a polynomial with integer coefficients, we have $h'(x) \equiv h'(x+mp) \pmod{p}$ for any integer $m$, and so $h'(x) \not\equiv 0 \pmod{p}$ for *all* integers $x$.

Now for $x = 0, \dots, p^2 - 1$ and $y = 0, \dots, p-1$, we write

$$h(x+yp^2) \equiv h(x) + p^2 y h'(x) \pmod{p^3}.$$

Thus $h(x), h(x+p^2), \dots, h(x+(p-1)p^2)$ run over all of the residue classes modulo $p^3$ congruent to $h(x)$ modulo $p^2$. Since the $h(x)$ themselves cover all the residue classes modulo $p^2$, this proves that $h(0), \dots, h(p^3-1)$ are distinct modulo $p^3$.

**Remark:** More generally, the same proof shows that for any integers $d, e > 1$, $h$ permutes the residue classes modulo $p^d$ if and only if it permutes the residue classes modulo $p^e$. The argument used in the proof is related to a general result in number theory known as *Hensel's lemma*.

B–5 The functions $f(x) = x + n$ and $f(x) = -x + n$ for any integer $n$ clearly satisfy the condition of the problem; we claim that these are the only possible $f$.

Let $q = a/b$ be any rational number with $\gcd(a,b) = 1$ and $b > 0$. For $n$ any positive integer, we have

$$\frac{f(\frac{an+1}{bn}) - f(\frac{a}{b})}{\frac{1}{bn}} = bnf\left(\frac{an+1}{bn}\right) - nbf\left(\frac{a}{b}\right)$$

is an integer by the property of $f$. Since $f$ is differentiable at $a/b$, the left hand side has a limit. It follows that for sufficiently large $n$, both sides must be equal to some integer $c = f'(\frac{a}{b})$: $f(\frac{an+1}{bn}) = f(\frac{a}{b}) + \frac{c}{bn}$. Now $c$ cannot be 0, since otherwise $f(\frac{an+1}{bn}) = f(\frac{a}{b})$ for sufficiently large $n$ has denominator $b$ rather than $bn$. Similarly, $|c|$ cannot be greater than 1: otherwise if we take $n = k|c|$ for $k$ a sufficiently large positive integer, then $f(\frac{a}{b}) + \frac{c}{bn}$ has denominator $bk$, contradicting the fact that $f(\frac{an+1}{bn})$ has denominator $bn$. It follows that $c = f'(\frac{a}{b}) = \pm 1$.

Thus the derivative of $f$ at any rational number is $\pm 1$. Since $f$ is continuously differentiable, we conclude that $f'(x) = 1$ for all real $x$ or $f'(x) = -1$ for all real $x$. Since $f(0)$ must be an integer (a rational number with denominator 1), $f(x) = x + n$ or $f(x) = -x + n$ for some integer $n$.

**Remark:** After showing that $f'(q)$ is an integer for each $q$, one can instead argue that $f'$ is a continuous function from the rationals to the integers, so must be constant. One can then write $f(x) = ax + b$ and check that $b \in \mathbb{Z}$ by evaluation at $a = 0$, and that $a = \pm 1$ by evaluation at $x = 1/a$.

B–6 In all solutions, let $F_{n,k}$ be the number of $k$-limited permutations of $\{1, \dots, n\}$.

**First solution:** (by Jacob Tsimerman) Note that any permutation is $k$-limited if and only if its inverse is $k$-limited. Consequently, the number of $k$-limited permutations of $\{1, \dots, n\}$ is the same as the number of $k$-limited involutions (permutations equal to their inverses) of $\{1, \dots, n\}$.

We use the following fact several times: the number of involutions of $\{1, \dots, n\}$ is odd if $n = 0, 1$ and even otherwise. This follows from the fact that non-involutions come in pairs, so the number of involutions has the same parity as the number of permutations, namely $n!$.

For $n \leq k+1$, all involutions are $k$-limited. By the previous paragraph, $F_{n,k}$ is odd for $n = 0, 1$ and even for $n = 2, \dots, k+1$.

For $n > k+1$, group the $k$-limited involutions into classes based on their actions on $k+2, \dots, n$. Note that for $C$ a class and $\sigma \in C$, the set of elements of $A = \{1, \dots, k+1\}$ which map into $A$ under $\sigma$ depends only on $C$, not on $\sigma$. Call this set $S(C)$; then the size of $C$ is exactly the number of involutions of $S(C)$. Consequently, $|C|$ is even unless $S(C)$ has at most one element. However, the element 1 cannot map out of $A$ because we are looking at $k$-limited involutions. Hence if $S(C)$ has one element and $\sigma \in C$, we must have $\sigma(1) = 1$. Since $\sigma$ is $k$-limited and $\sigma(2)$ cannot belong to $A$, we must have $\sigma(2) = k+2$. By induction, for $i = 3, \dots, k+1$, we must have $\sigma(i) = k+i$.

If $n < 2k+1$, this shows that no class $C$ of odd cardinality can exist, so $F_{n,k}$ must be even. If $n \geq 2k+1$, the classes of odd cardinality are in bijection with $k$-limited involutions of $\{2k+2, \dots, n\}$, so $F_{n,k}$ has the same parity as $F_{n-2k-1,k}$. By induction on $n$, we deduce the desired result.

**Second solution:** (by Yufei Zhao) Let $M_{n,k}$ be the $n \times n$ matrix with

$$(M_{n,k})_{ij} = \begin{cases} 1 & |i-j| \leq k \\ 0 & \text{otherwise.} \end{cases}$$

Write $\det(M_{n,k})$ as the sum over permutations $\sigma$ of $\{1,\dots,n\}$ of $(M_{n,k})_{1\sigma(1)} \cdots (M_{n,k})_{n\sigma(n)}$ times the signature of $\sigma$. Then $\sigma$ contributes $\pm 1$ to $\det(M_{n,k})$ if $\sigma$ is $k$-limited and 0 otherwise. We conclude that

$$\det(M_{n,k}) \equiv F_{n,k} \pmod{2}.$$

For the rest of the solution, we interpret $M_{n,k}$ as a matrix over the field of two elements. We compute its determinant using linear algebra modulo 2.

We first show that for $n \geq 2k+1$,

$$F_{n,k} \equiv F_{n-2k-1,k} \pmod{2},$$

provided that we interpret $F_{0,k} = 1$. We do this by computing $\det(M_{n,k})$ using row and column operations. We will verbally describe these operations for general $k$, while illustrating with the example $k = 3$.

To begin with, $M_{n,k}$ has the following form.

$$\left(\begin{array}{ccccccc|c}
1 & 1 & 1 & 1 & 0 & 0 & 0 & \emptyset \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & \emptyset \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & \emptyset \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & \emptyset \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & ? \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & ? \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & ? \\
\hline
\emptyset & \emptyset & \emptyset & \emptyset & ? & ? & ? & *
\end{array}\right)$$

In this presentation, the first $2k+1$ rows and columns are shown explicitly; the remaining rows and columns are shown in a compressed format. The symbol $\emptyset$ indicates that the unseen entries are all zeroes, while the symbol ? indicates that they are not. The symbol $*$ in the lower right corner represents the matrix $F_{n-2k-1,k}$. We will preserve the unseen structure of the matrix by only adding the first $k+1$ rows or columns to any of the others.

We first add row 1 to each of rows $2,\dots,k+1$.

$$\left(\begin{array}{ccccccc|c}
1 & 1 & 1 & 1 & 0 & 0 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & \emptyset \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & ? \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & ? \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & ? \\
\hline
\emptyset & \emptyset & \emptyset & \emptyset & ? & ? & ? & *
\end{array}\right)$$

We next add column 1 to each of columns $2,\dots,k+1$.

$$\left(\begin{array}{ccccccc|c}
1 & 0 & 0 & 0 & 0 & 0 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & \emptyset \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & ? \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & ? \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & ? \\
\hline
\emptyset & \emptyset & \emptyset & \emptyset & ? & ? & ? & *
\end{array}\right)$$

For $i = 2$, for each of $j = i+1,\dots,2k+1$ for which the $(j,k+i)$-entry is nonzero, add row $i$ to row $j$.

$$\left(\begin{array}{ccccccc|c}
1 & 0 & 0 & 0 & 0 & 0 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & \emptyset \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & ? \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & ? \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & ? \\
\hline
\emptyset & \emptyset & \emptyset & \emptyset & \emptyset & ? & ? & *
\end{array}\right)$$

Repeat the previous step for $i = 3,\dots,k+1$ in succession.

$$\left(\begin{array}{ccccccc|c}
1 & 0 & 0 & 0 & 0 & 0 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & \emptyset \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & ? \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & ? \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & ? \\
\hline
\emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & *
\end{array}\right)$$

Repeat the two previous steps with the roles of the rows and columns reversed. That is, for $i = 2,\dots,k+1$, for each of $j = i+1,\dots,2k+1$ for which the $(j,k+i)$-entry is nonzero, add row $i$ to row $j$.

$$\left(\begin{array}{ccccccc|c}
1 & 0 & 0 & 0 & 0 & 0 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & \emptyset \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & \emptyset \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & \emptyset \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & \emptyset \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & \emptyset \\
\hline
\emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & \emptyset & *
\end{array}\right)$$

We now have a block diagonal matrix in which the top left block is a $(2k+1) \times (2k+1)$ matrix with nonzero determinant (it results from reordering the rows of the identity matrix), the bottom right block is $M_{n-2k-1,k}$, and the other two blocks are zero. We conclude that

$$\det(M_{n,k}) \equiv \det(M_{n-2k-1,k}) \pmod 2,$$

proving the desired congruence.

To prove the desired result, we must now check that $F_{0,k}, F_{1,k}$ are odd and $F_{2,k}, \dots, F_{2k,k}$ are even. For $n = 0, \dots, k+1$, the matrix $M_{n,k}$ consists of all ones, so its determinant is 1 if $n = 0, 1$ and 0 otherwise. (Alternatively, we have $F_{n,k} = n!$ for $n = 0, \dots, k+1$, since every permutation of $\{1, \dots, n\}$ is $k$-limited.) For $n = k+2, \dots, 2k$, observe that rows $k$ and $k+1$ of $M_{n,k}$ both consist of all ones, so $\det(M_{n,k}) = 0$ as desired.

**Third solution:** (by Tom Belulovich) Define $M_{n,k}$ as in the second solution. We prove $\det(M_{n,k})$ is odd for $n \equiv 0, 1 \pmod{2k+1}$ and even otherwise, by directly determining whether or not $M_{n,k}$ is invertible as a matrix over the field of two elements.

Let $r_i$ denote row $i$ of $M_{n,k}$. We first check that if $n \equiv 2, \dots, 2k \pmod{2k+1}$, then $M_{n,k}$ is not invertible. In this case, we can find integers $0 \leq a < b \leq k$ such that $n + a + b \equiv 0 \pmod{2k+1}$. Put $j = (n+a+b)/(2k+1)$. We can then write the all-ones vector both as

$$\sum_{i=0}^{j-1} r_{k+1-a+(2k+1)i}$$

and as

$$\sum_{i=0}^{j-1} r_{k+1-b+(2k+1)i}.$$

Hence $M_{n,k}$ is not invertible.

We next check that if $n \equiv 0, 1 \pmod{2k+1}$, then $M_{n,k}$ is invertible. Suppose that $a_1, \dots, a_n$ are scalars such that $a_1 r_1 + \cdots + a_n r_n$ is the zero vector. The $m$-th coordinate of this vector equals $a_{m-k} + \cdots + a_{m+k}$, where we regard $a_i$ as zero if $i \notin \{1, \dots, n\}$. By comparing consecutive coordinates, we obtain

$$a_{m-k} = a_{m+k+1} \qquad (1 \leq m < n).$$

In particular, the $a_i$ repeat with period $2k+1$. Taking $m = 1, \dots, k$ further yields that

$$a_{k+2} = \cdots = a_{2k+1} = 0$$

while taking $m = n-k, \dots, n-1$ yields

$$a_{n-2k} = \cdots = a_{n-1-k} = 0.$$

For $n \equiv 0 \pmod{2k+1}$, the latter can be rewritten as

$$a_1 = \cdots = a_k = 0$$

whereas for $n \equiv 1 \pmod{2k+1}$, it can be rewritten as

$$a_2 = \cdots = a_{k+1} = 0.$$

In either case, since we also have

$$a_1 + \cdots + a_{2k+1} = 0$$

from the $(k+1)$-st coordinate, we deduce that all of the $a_i$ must be zero, and so $M_{n,k}$ must be invertible.

**Remark:** The matrices $M_{n,k}$ are examples of *banded matrices*, which occur frequently in numerical applications of linear algebra. They are also examples of *Toeplitz matrices*.

# The 70th William Lowell Putnam Mathematical Competition
# Saturday, December 5, 2009

A1 Let $f$ be a real-valued function on the plane such that for every square $ABCD$ in the plane, $f(A)+f(B)+f(C)+f(D)=0$. Does it follow that $f(P)=0$ for all points $P$ in the plane?

A2 Functions $f,g,h$ are differentiable on some open interval around 0 and satisfy the equations and initial conditions

$$\begin{aligned} f' &= 2f^2gh+\frac{1}{gh}, \quad f(0)=1, \\ g' &= fg^2h+\frac{4}{fh}, \quad g(0)=1, \\ h' &= 3fgh^2+\frac{1}{fg}, \quad h(0)=1. \end{aligned}$$

Find an explicit formula for $f(x)$, valid in some open interval around 0.

A3 Let $d_n$ be the determinant of the $n\times n$ matrix whose entries, from left to right and then from top to bottom, are $\cos 1, \cos 2, \dots, \cos n^2$. (For example,

$$d_3 = \begin{vmatrix} \cos 1 & \cos 2 & \cos 3 \\ \cos 4 & \cos 5 & \cos 6 \\ \cos 7 & \cos 8 & \cos 9 \end{vmatrix}.$$

The argument of cos is always in radians, not degrees.) Evaluate $\lim_{n\to\infty} d_n$.

A4 Let $S$ be a set of rational numbers such that

(a) $0\in S$;

(b) If $x\in S$ then $x+1\in S$ and $x-1\in S$; and

(c) If $x\in S$ and $x\notin\{0,1\}$, then $\frac{1}{x(x-1)}\in S$.

Must $S$ contain all rational numbers?

A5 Is there a finite abelian group $G$ such that the product of the orders of all its elements is $2^{2009}$?

A6 Let $f:[0,1]^2\to\mathbb{R}$ be a continuous function on the closed unit square such that $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ exist and are continuous on the interior $(0,1)^2$. Let $a=\int_0^1 f(0,y)\,dy$, $b=\int_0^1 f(1,y)\,dy$, $c=\int_0^1 f(x,0)\,dx$, $d=\int_0^1 f(x,1)\,dx$. Prove or disprove: There must be a point $(x_0,y_0)$ in $(0,1)^2$ such that

$$\frac{\partial f}{\partial x}(x_0,y_0)=b-a \quad\text{and}\quad \frac{\partial f}{\partial y}(x_0,y_0)=d-c.$$

B1 Show that every positive rational number can be written as a quotient of products of factorials of (not necessarily distinct) primes. For example,

$$\frac{10}{9}=\frac{2!\cdot 5!}{3!\cdot 3!\cdot 3!}.$$

B2 A game involves jumping to the right on the real number line. If $a$ and $b$ are real numbers and $b>a$, the cost of jumping from $a$ to $b$ is $b^3-ab^2$. For what real numbers $c$ can one travel from 0 to 1 in a finite number of jumps with total cost exactly $c$?

B3 Call a subset $S$ of $\{1,2,\dots,n\}$ *mediocre* if it has the following property: Whenever $a$ and $b$ are elements of $S$ whose average is an integer, that average is also an element of $S$. Let $A(n)$ be the number of mediocre subsets of $\{1,2,\dots,n\}$. [For instance, every subset of $\{1,2,3\}$ except $\{1,3\}$ is mediocre, so $A(3)=7$.] Find all positive integers $n$ such that $A(n+2)-2A(n+1)+A(n)=1$.

B4 Say that a polynomial with real coefficients in two variables, $x,y$, is *balanced* if the average value of the polynomial on each circle centered at the origin is 0. The balanced polynomials of degree at most 2009 form a vector space $V$ over $\mathbb{R}$. Find the dimension of $V$.

B5 Let $f:(1,\infty)\to\mathbb{R}$ be a differentiable function such that

$$f'(x)=\frac{x^2-f(x)^2}{x^2(f(x)^2+1)} \qquad \text{for all } x>1.$$

Prove that $\lim_{x\to\infty} f(x)=\infty$.

B6 Prove that for every positive integer $n$, there is a sequence of integers $a_0,a_1,\dots,a_{2009}$ with $a_0=0$ and $a_{2009}=n$ such that each term after $a_0$ is either an earlier term plus $2^k$ for some nonnegative integer $k$, or of the form $b \bmod c$ for some earlier positive terms $b$ and $c$. [Here $b \bmod c$ denotes the remainder when $b$ is divided by $c$, so $0\le (b \bmod c) < c$.]

# Solutions to the 70th William Lowell Putnam Mathematical Competition
# Saturday, December 5, 2009

Kiran Kedlaya and Lenny Ng

A–1 Yes, it does follow. Let $P$ be any point in the plane. Let $ABCD$ be any square with center $P$. Let $E,F,G,H$ be the midpoints of the segments $AB,BC,CD,DA$, respectively. The function $f$ must satisfy the equations

$$\begin{aligned}
0 &= f(A)+f(B)+f(C)+f(D)\\
0 &= f(E)+f(F)+f(G)+f(H)\\
0 &= f(A)+f(E)+f(P)+f(H)\\
0 &= f(B)+f(F)+f(P)+f(E)\\
0 &= f(C)+f(G)+f(P)+f(F)\\
0 &= f(D)+f(H)+f(P)+f(G).
\end{aligned}$$

If we add the last four equations, then subtract the first equation and twice the second equation, we obtain $0 = 4f(P)$, whence $f(P) = 0$.

**Remark.** Problem 1 of the 1996 Romanian IMO team selection exam asks the same question with squares replaced by regular polygons of any (fixed) number of vertices.

A–2 Multiplying the first differential equation by $gh$, the second by $fh$, and the third by $fg$, and summing gives

$$(fgh)' = 6(fgh)^2 + 6.$$

Write $k(x) = f(x)g(x)h(x)$; then $k' = 6k^2+6$ and $k(0) = 1$. One solution for this differential equation with this initial condition is $k(x) = \tan(6x+\pi/4)$; by standard uniqueness, this must necessarily hold for $x$ in some open interval around 0. Now the first given equation becomes

$$\begin{aligned}
f'/f &= 2k(x)+1/k(x)\\
&= 2\tan(6x+\pi/4)+\cot(6x+\pi/4);
\end{aligned}$$

integrating both sides gives

$$\ln(f(x)) = \frac{-2\ln\cos(6x+\pi/4)+\ln\sin(6x+\pi/4)}{6} + c,$$

whence $f(x) = e^c\left(\frac{\sin(6x+\pi/4)}{\cos^2(6x+\pi/4)}\right)^{1/6}$. Substituting $f(0) = 1$ gives $e^c = 2^{-1/12}$ and thus $f(x) = 2^{-1/12}\left(\frac{\sin(6x+\pi/4)}{\cos^2(6x+\pi/4)}\right)^{1/6}$.

**Remark.** The answer can be put in alternate forms using trigonometric identities. One particularly simple one is

$$f(x) = (\sec 12x)^{1/12}(\sec 12x+\tan 12x)^{1/4}.$$

A–3 The limit is 0; we will show this by checking that $d_n = 0$ for all $n \geq 3$. Starting from the given matrix, add the third column to the first column; this does not change the determinant. However, thanks to the identity $\cos x+\cos y = 2\cos\frac{x+y}{2}\cos\frac{x-y}{2}$, the resulting matrix has the form

$$\begin{pmatrix}
2\cos 2\cos 1 & \cos 2 & \cdots\\
2\cos(n+2)\cos 1 & \cos(n+2) & \cdots\\
2\cos(2n+2)\cos 1 & 2\cos(2n+2) & \cdots\\
\vdots & \vdots & \ddots
\end{pmatrix}$$

with the first column being a multiple of the second. Hence $d_n = 0$.

**Remark.** Another way to draw the same conclusion is to observe that the given matrix is the sum of the two rank 1 matrices $A_{jk} = \cos(j-1)n\cos k$ and $B_{jk} = -\sin(j-1)n\sin k$, and so has rank at most 2. One can also use the matrices $A_{jk} = e^{i((j-1)n+k)}$, $B_{jk} = e^{-i(j-1)n+k}$.

A–4 The answer is no; indeed, $S = \mathbb{Q}\setminus\{n+2/5 \mid n\in\mathbb{Z}\}$ satisfies the given conditions. Clearly $S$ satisfies (a) and (b); we need only check that it satisfies (c). It suffices to show that if $x = p/q$ is a fraction with $(p,q) = 1$ and $p > 0$, then we cannot have $1/(x(x-1)) = n+2/5$ for an integer $n$. Suppose otherwise; then

$$(5n+2)p(p-q) = 5q^2.$$

Since $p$ and $q$ are relatively prime, and $p$ divides $5q^2$, we must have $p\mid 5$, so $p = 1$ or $p = 5$. On the other hand, $p-q$ and $q$ are also relatively prime, so $p-q$ divides 5 as well, and $p-q$ must be $\pm 1$ or $\pm 5$. This leads to eight possibilities for $(p,q)$: $(1,0)$, $(5,0)$, $(5,10)$, $(1,-4)$, $(1,2)$, $(1,6)$, $(5,4)$, $(5,6)$. The first three are impossible, while the final five lead to $5n+2 = 16,-20,-36,16,-36$ respectively, none of which holds for integral $n$.

**Remark.** More generally, no rational number of the form $m/n$, where $m,n$ are relatively prime and neither of $\pm m$ is a quadratic residue mod $n$, need be in $S$. If $x = p/q$ is in lowest terms and $1/(x(x-1)) = m/n+k$ for some integer $k$, then $p(p-q)$ is relatively prime to $q^2$; $q^2/(p(p-q)) = (m+kn)/n$ then implies that $m+kn = \pm q^2$ and so $\pm m$ must be a quadratic residue mod $n$.

A–5 No, there is no such group. By the structure theorem for finitely generated abelian groups, $G$ can be written as a product of cyclic groups. If any of these factors has odd order, then $G$ has an element of odd order, so the product of the orders of all of its elements cannot be a power of 2.

We may thus consider only abelian 2-groups hereafter. For such a group $G$, the product of the orders of all of its elements has the form $2^{k(G)}$ for some nonnegative integer $G$, and we must show that it is impossible to achieve $k(G) = 2009$. Again by the structure theorem, we may write

$$G \cong \prod_{i=1}^{\infty} (\mathbb{Z}/2^i\mathbb{Z})^{e_i}$$

for some nonnegative integers $e_1, e_2, \dots$, all but finitely many of which are 0.

For any nonnegative integer $m$, the elements of $G$ of order at most $2^m$ form a subgroup isomorphic to

$$\prod_{i=1}^{\infty} (\mathbb{Z}/2^{\min\{i,m\}}\mathbb{Z})^{e_i},$$

which has $2^{s_m}$ elements for $s_m = \sum_{i=1}^{\infty} \min\{i,m\} e_i$. Hence

$$k(G) = \sum_{i=1}^{\infty} i(2^{s_i} - 2^{s_{i-1}}).$$

Since $s_1 \leq s_2 \leq \cdots$, $k(G)+1$ is always divisible by $2^{s_1}$. In particular, $k(G) = 2009$ forces $s_1 \leq 1$.

However, the only cases where $s_1 \leq 1$ are where all of the $e_i$ are 0, in which case $k(G) = 0$, or where $e_i = 1$ for some $i$ and $e_j = 0$ for $j \neq i$, in which case $k(G) = (i-1)2^i + 1$. The right side is a strictly increasing function of $i$ which equals 1793 for $i = 8$ and 4097 for $i = 9$, so it can never equal 2009. This proves the claim.

**Remark.** One can also arrive at the key congruence by dividing $G$ into equivalence classes, by declaring two elements to be equivalent if they generate the same cyclic subgroup of $G$. For $h > 0$, an element of order $2^h$ belongs to an equivalence class of size $2^{h-1}$, so the products of the orders of the elements of this equivalence class is $2^j$ for $j = h2^{h-1}$. This quantity is divisible by 4 as long as $h > 1$; thus to have $k(G) \equiv 1 \pmod 4$, the number of elements of $G$ of order 2 must be congruent to 1 modulo 4. However, there are exactly $2^e - 1$ such elements, for $e$ the number of cyclic factors of $G$. Hence $e = 1$, and one concludes as in the given solution.

A–6 We disprove the assertion using the example

$$f(x,y) = 3(1+y)(2x-1)^2 - y.$$

We have $b - a = d - c = 0$ because the identity $f(x,y) = f(1-x,y)$ forces $a = b$, and because

$$c = \int_0^1 3(2x-1)^2\,dx = 1,$$
$$d = \int_0^1 (6(2x-1)^2 - 1)\,dx = 1.$$

Moreover, the partial derivatives

$$\frac{\partial f}{\partial x}(x_0,y_0) = 3(1+y_0)(8x_0 - 4)$$
$$\frac{\partial f}{\partial y}(x_0,y_0) = 3(2x_0-1)^2 - 1.$$

have no common zero in $(0,1)^2$. Namely, for the first partial to vanish, we must have $x_0 = 1/2$ since $1 + y_0$ is nowhere zero, but for $x_0 = 1/2$ the second partial cannot vanish.

**Remark.** This problem amounts to refuting a potential generalization of the Mean Value Theorem to bivariate functions. Many counterexamples are possible. Kent Merryfield suggests $y\sin(2\pi x)$, for which all four of the boundary integrals vanish; here the partial derivatives are $2\pi y\cos(2\pi x)$ and $\sin(2\pi x)$. Catalin Zara suggests $x^{1/3}y^{2/3}$. Qingchun Ren suggests $xy(1-y)$.

B–1 Every positive rational number can be uniquely written in lowest terms as $a/b$ for $a,b$ positive integers. We prove the statement in the problem by induction on the largest prime dividing either $a$ or $b$ (where this is considered to be 1 if $a = b = 1$). For the base case, we can write $1/1 = 2!/2!$. For a general $a/b$, let $p$ be the largest prime dividing either $a$ or $b$; then $a/b = p^k a'/b'$ for some $k \neq 0$ and positive integers $a', b'$ whose largest prime factors are strictly less than $p$. We now have $a/b = (p!)^k \frac{a'}{(p-1)!^k b'}$, and all prime factors of $a'$ and $(p-1)!^k b'$ are strictly less than $p$. By the induction assumption, $\frac{a'}{(p-1)!^k b'}$ can be written as a quotient of products of prime factorials, and so $a/b = (p!)^k \frac{a'}{(p-1)!^k b'}$ can as well. This completes the induction.

**Remark.** Noam Elkies points out that the representations are unique up to rearranging and canceling common factors.

B–2 The desired real numbers $c$ are precisely those for which $1/3 < c \leq 1$. For any positive integer $m$ and any sequence $0 = x_0 < x_1 < \cdots < x_m = 1$, the cost of jumping along this sequence is $\sum_{i=1}^m (x_i - x_{i-1})x_i^2$. Since

$$\begin{aligned} 1 = \sum_{i=1}^m (x_i - x_{i-1}) &\geq \sum_{i=1}^m (x_i - x_{i-1})x_i^2 \\ &> \sum_{i=1}^m \int_{x_i}^{x_{i-1}} t^2\,dt \\ &= \int_0^1 t^2\,dt = \frac{1}{3}, \end{aligned}$$

we can only achieve costs $c$ for which $1/3 < c \leq 1$.

It remains to check that any such $c$ can be achieved. Suppose $0 = x_0 < \cdots < x_m = 1$ is a sequence with $m \geq 1$. For $i = 1, \dots, m$, let $c_i$ be the cost of the sequence $0, x_i, x_{i+1}, \dots, x_m$. For $i > 1$ and $0 < y \leq x_{i-1}$, the cost of the sequence $0, y, x_i, \dots, x_m$ is

$$c_i + y^3 + (x_i - y)x_i^2 - x_i^3 = c_i - y(x_i^2 - y^2),$$

which is less than $c_i$ but approaches $c_i$ as $y \to 0$. By continuity, for $i = 2, \dots, m$, every value in the interval $[c_{i-1}, c_i)$ can be achieved, as can $c_m = 1$ by the sequence $0, 1$.

To show that all costs $c$ with $1/3 < c \leq 1$ can be achieved, it now suffices to check that for every $\varepsilon > 0$, there exists a sequence with cost at most $1/3 + \varepsilon$. For instance, if we take $x_i = i/m$ for $i = 0, \dots, m$, the cost becomes

$$\frac{1}{m^3}(1^2 + \cdots + m^2) = \frac{(m+1)(2m+1)}{6m^2},$$

which converges to $1/3$ as $m \to +\infty$.

**Reinterpretation.** The cost of jumping along a particular sequence is an upper Riemann sum of the function $t^2$. The fact that this function admits a Riemann integral implies that for any $\varepsilon > 0$, there exists $\delta_0$ such that the cost of the sequence $x_0, \dots, x_m$ is at most $1/3 + \varepsilon$ as long as $\max_i \{x_i - x_{i-1}\} < \varepsilon$. (The computation of the integral using the sequence $x_i = i/m$ was already known to Archimedes.)

B–3 The answer is $n = 2^k - 1$ for some integer $k \geq 1$. There is a bijection between mediocre subsets of $\{1, \dots, n\}$ and mediocre subsets of $\{2, \dots, n+1\}$ given by adding 1 to each element of the subset; thus $A(n+1) - A(n)$ is the number of mediocre subsets of $\{1, \dots, n+1\}$ that contain 1. It follows that $A(n+2) - 2A(n+1) + A_n = (A(n+2) - A(n+1)) - (A(n+1) - A(n))$ is the difference between the number of mediocre subsets of $\{1, \dots, n+2\}$ containing 1 and the number of mediocre subsets of $\{1, \dots, n+1\}$ containing 1. This difference is precisely the number of mediocre subsets of $\{1, \dots, n+2\}$ containing both 1 and $n+2$, which we term "mediocre subsets containing the endpoints." Since $\{1, \dots, n+2\}$ itself is a mediocre subset of itself containing the endpoints, it suffices to prove that this is the only mediocre subset of $\{1, \dots, n+2\}$ containing the endpoints if and only if $n = 2^k - 1$ for some $k$.

If $n$ is not of the form $2^k - 1$, then we can write $n + 1 = 2^a b$ for odd $b > 1$. In this case, the set $\{1 + mb \,|\, 0 \leq m \leq 2^a\}$ is a mediocre subset of $\{1, \dots, n+2\}$ containing the endpoints: the average of $1 + m_1 b$ and $1 + m_2 b$, namely $1 + \frac{m_1+m_2}{2} b$, is an integer if and only if $m_1 + m_2$ is even, in which case this average lies in the set.

It remains to show that if $n = 2^k - 1$, then the only mediocre subset of $\{1, \dots, n+2\}$ containing the endpoints is itself. This is readily seen by induction on $k$. For $k = 1$, the statement is obvious. For general $k$, any mediocre subset $S$ of $\{1, \dots, n+2 = 2^k + 1\}$ containing 1 and $2^k + 1$ must also contain their average, $2^{k-1} + 1$. By the induction assumption, the only mediocre subset of $\{1, \dots, 2^{k-1} + 1\}$ containing the endpoints is itself, and so $S$ must contain all integers between 1 and $2^{k-1} + 1$. Similarly, a mediocre subset of $\{2^{k-1} + 1, \dots, 2^k + 1\}$ containing the endpoints gives a mediocre subset of $\{1, \dots, 2^{k-1} + 1\}$ containing the endpoints by subtracting $2^{k-1}$ from each element. By the induction assumption again, it follows that $S$ must contain all integers between $2^{k-1} + 1$ and $2^k + 1$. Thus $S = \{1, \dots, 2^k + 1\}$ and the induction is complete.

**Remark.** One can also proceed by checking that a nonempty subset of $\{1, \dots, n\}$ is mediocre if and only if it is an arithmetic progression with odd common difference. Given this fact, the number of mediocre subsets of $\{1, \dots, n+2\}$ containing the endpoints is seen to be the number of odd factors of $n+1$, from which the desired result is evident. (The sequence $A(n)$ appears as sequence A124197 in the Encyclopedia of Integer Sequences.)

B–4 Any polynomial $P(x,y)$ of degree at most 2009 can be written uniquely as a sum $\sum_{i=0}^{2009} P_i(x,y)$ in which $P_i(x,y)$ is a homogeneous polynomial of degree $i$. For $r > 0$, let $C_r$ be the path $(r\cos\theta, r\sin\theta)$ for $0 \leq \theta \leq 2\pi$. Put $\lambda(P_i) = \oint_{C_1} P_i$; then for $r > 0$,

$$\oint_{C_r} P = \sum_{i=0}^{2009} r^i \lambda(P_i).$$

For fixed $P$, the right side is a polynomial in $r$, which vanishes for all $r > 0$ if and only if its coefficients vanish. In other words, $P$ is balanced if and only if $\lambda(P_i) = 0$ for $i = 0, \dots, 2009$.

For $i$ odd, we have $P_i(-x,-y) = -P_i(x,y)$. Hence $\lambda(P_i) = 0$, e.g., because the contributions to the integral from $\theta$ and $\theta + \pi$ cancel.

For $i$ even, $\lambda(P_i)$ is a linear function of the coefficients of $P_i$. This function is not identically zero, e.g., because for $P_i = (x^2 + y^2)^{i/2}$, the integrand is always positive and so $\lambda(P_i) > 0$. The kernel of $\lambda$ on the space of homogeneous polynomials of degree $i$ is thus a subspace of codimension 1.

It follows that the dimension of $V$ is

$$(1 + \cdots + 2010) - 1005 = (2011 - 1) \times 1005 = 2020050.$$

B–5 **First solution.** If $f(x) \geq x$ for all $x > 1$, then the desired conclusion clearly holds. We may thus assume hereafter that there exists $x_0 > 1$ for which $f(x_0) < x_0$.

Rewrite the original differential equation as

$$f'(x) = 1 - \frac{x^2+1}{x^2} \frac{f(x)^2}{1 + f(x)^2}.$$

Put $c_0 = \min\{0, f(x_0) - 1/x_0\}$. For all $x \geq x_0$, we have $f'(x) > -1/x^2$ and so

$$f(x) \geq f(x_0) - \int_{x_0}^{x} dt/t^2 > c_0.$$

In the other direction, we claim that $f(x) < x$ for all $x \geq x_0$. To see this, suppose the contrary; then by continuity, there is a least $x \geq x_0$ for which $f(x) \geq x$, and this least value satisfies $f(x) = x$. However, this forces $f'(x) = 0 < 1$ and so $f(x-\varepsilon) > x-\varepsilon$ for $\varepsilon > 0$ small, contradicting the choice of $x$.

Put $x_1 = \max\{x_0, -c_0\}$. For $x \geq x_1$, we have $|f(x)| < x$ and so $f'(x) > 0$. In particular, the limit $\lim_{x\to+\infty} f(x) = L$ exists.

Suppose that $L < +\infty$; then $\lim_{x\to+\infty} f'(x) = 1/(1+L^2) > 0$. Hence for any sufficiently small $\varepsilon > 0$, we can choose $x_2 \geq x_1$ so that $f'(x) \geq \varepsilon$ for $x \geq x_2$. But then $f(x) \geq f(x_2) + \varepsilon(x - x_2)$, which contradicts $L < +\infty$. Hence $L = +\infty$, as desired.

**Variant.** (by Leonid Shteyman) One obtains a similar argument by writing

$$f'(x) = \frac{1}{1+f(x)^2} - \frac{f(x)^2}{x^2(1+f(x)^2)},$$

so that

$$-\frac{1}{x^2} \leq f'(x) - \frac{1}{1+f(x)^2} \leq 0.$$

Hence $f'(x) - 1/(1+f(x)^2)$ tends to 0 as $x \to +\infty$, so $f(x)$ is bounded below, and tends to $+\infty$ if and only if the improper integral $\int dx/(1+f(x)^2)$ diverges. However, if the integral were to converge, then as $x \to +\infty$ we would have $1/(1+f(x)^2) \to 0$; however, since $f$ is bounded below, this again forces $f(x) \to +\infty$.

**Second solution.** (by Catalin Zara) The function $g(x) = f(x) + x$ satisfies the differential equation

$$g'(x) = 1 + \frac{1-(g(x)/x-1)^2}{1+x^2(g(x)/x-1)^2}.$$

This implies that $g'(x) > 0$ for all $x > 1$, so the limit $L_1 = \lim_{x\to+\infty} g(x)$ exists. In addition, we cannot have $L_1 < +\infty$, or else we would have $\lim_{x\to+\infty} g'(x) = 0$ whereas the differential equation forces this limit to be 1. Hence $g(x) \to +\infty$ as $x \to +\infty$.

Similarly, the function $h(x) = -f(x) + x$ satisfies the differential equation

$$h'(x) = 1 - \frac{1-(h(x)/x-1)^2}{1+x^2(h(x)/x-1)^2}.$$

This implies that $h'(x) \geq 0$ for all $x$, so the limit $L_2 = \lim_{x\to+\infty} h(x)$ exists. In addition, we cannot have $L_2 < +\infty$, or else we would have $\lim_{x\to+\infty} h'(x) = 0$ whereas the differential equation forces this limit to be 1. Hence $h(x) \to +\infty$ as $x \to +\infty$.

For some $x_1 > 1$, we must have $g(x), h(x) > 0$ for all $x \geq x_1$. For $x \geq x_1$, we have $|f(x)| < x$ and hence $f'(x) > 0$, so the limit $L = \lim_{x\to+\infty} f(x)$ exists. Once again, we cannot have $L < +\infty$, or else we would have $\lim_{x\to+\infty} f'(x) = 0$ whereas the original differential equation (e.g., in the form given in the first solution) forces this limit to be $1/(1+L^2) > 0$. Hence $f(x) \to +\infty$ as $x \to \infty$, as desired.

**Third solution.** (by Noam Elkies) Consider the function $g(x) = f(x) + \frac{1}{3}f(x)^3$, for which

$$g'(x) = f'(x)(1+f(x)^2) = 1 - \frac{f(x)^2}{x^2}$$

for $x > 1$. Since evidently $g'(x) < 1$, $g(x) - x$ is bounded above for $x$ large. As in the first solution, $f(x)$ is bounded below for $x$ large, so $\frac{1}{3}f(x)^3 - x$ is bounded above by some $c > 0$. For $x \geq c$, we obtain $f(x) \leq (6x)^{1/3}$.

Since $f(x)/x \to 0$ as $x \to +\infty$, $g'(x) \to 1$ and so $g(x)/x \to 1$. Since $g(x)$ tends to $+\infty$, so does $f(x)$. (With a tiny bit of extra work, one shows that in fact $f(x)/(3x)^{1/3} \to 1$ as $x \to +\infty$.)

B–6 **First solution.** (based on work of Yufei Zhao) Since any sequence of the desired form remains of the desired form upon multiplying each term by 2, we may reduce to the case where $n$ is odd. In this case, take $x = 2^h$ for some positive integer $h$ for which $x \geq n$, and set

$$\begin{aligned}
a_0 &= 0\\
a_1 &= 1\\
a_2 &= 2x+1 = a_1 + 2x\\
a_3 &= (x+1)^2 = a_2 + x^2\\
a_4 &= x^n + 1 = a_1 + x^n\\
a_5 &= n(x+1) = a_4 \mod a_3\\
a_6 &= x\\
a_7 &= n = a_5 \mod a_6.
\end{aligned}$$

We may pad the sequence to the desired length by taking $a_8 = \cdots = a_{2009} = n$.

**Second solution.** (by James Merryfield) Suppose first that $n$ is not divisible by 3. Recall that since 2 is a primitive root modulo $3^2$, it is also a primitive root modulo $3^h$ for any positive integer $h$. In particular, if we choose $h$ so that $3^{2h} > n$, then there exists a positive integer $c$ for which $2^c \mod 3^{2h} = n$. We now take $b$ to be a positive integer for which $2^b > 3^{2h}$, and then put

$$\begin{aligned}
a_0 &= 0\\
a_1 &= 1\\
a_2 &= 3 = a_1 + 2\\
a_3 &= 3 + 2^b\\
a_4 &= 2^{2hb}\\
a_5 &= 3^{2h} = a_4 \mod a_3\\
a_6 &= 2^c\\
a_7 &= n = a_6 \mod a_5.
\end{aligned}$$

If $n$ is divisible by 3, we can force $a_7 = n-1$ as in the above construction, then put $a_8 = a_7 + 1 = n$. In both cases, we then pad the sequence as in the first solution.

**Remark.** Hendrik Lenstra, Ronald van Luijk, and Gabriele Della Torre suggest the following variant of the first solution requiring only 6 steps. For $n$ odd and $x$ as in the first solution, set

$$\begin{aligned}
a_0 &= 0 \\
a_1 &= 1 \\
a_2 &= x+1 = a_1 + x \\
a_3 &= x^n + x + 1 = a_2 + x^n \\
a_4 &= x^{(n-1)(\phi(a_3)-1)} \\
a_5 &= \frac{x^n+1}{x+1} = a_4 \mod a_3 \\
a_6 &= n = a_5 \mod a_2.
\end{aligned}$$

It seems unlikely that a shorter solution can be constructed without relying on any deep number-theoretic conjectures.

# The 71st William Lowell Putnam Mathematical Competition
# Saturday, December 4, 2010

A1 Given a positive integer $n$, what is the largest $k$ such that the numbers $1,2,\dots,n$ can be put into $k$ boxes so that the sum of the numbers in each box is the same? [When $n=8$, the example $\{1,2,3,6\},\{4,8\},\{5,7\}$ shows that the largest $k$ is *at least* 3.]

A2 Find all differentiable functions $f:\mathbb{R}\to\mathbb{R}$ such that

$$f'(x)=\frac{f(x+n)-f(x)}{n}$$

for all real numbers $x$ and all positive integers $n$.

A3 Suppose that the function $h:\mathbb{R}^2\to\mathbb{R}$ has continuous partial derivatives and satisfies the equation

$$h(x,y)=a\frac{\partial h}{\partial x}(x,y)+b\frac{\partial h}{\partial y}(x,y)$$

for some constants $a,b$. Prove that if there is a constant $M$ such that $|h(x,y)|\le M$ for all $(x,y)\in\mathbb{R}^2$, then $h$ is identically zero.

A4 Prove that for each positive integer $n$, the number $10^{10^{10^n}}+10^{10^n}+10^n-1$ is not prime.

A5 Let $G$ be a group, with operation $*$. Suppose that

(i) $G$ is a subset of $\mathbb{R}^3$ (but $*$ need not be related to addition of vectors);

(ii) For each $\mathbf{a},\mathbf{b}\in G$, either $\mathbf{a}\times\mathbf{b}=\mathbf{a}*\mathbf{b}$ or $\mathbf{a}\times\mathbf{b}=0$ (or both), where $\times$ is the usual cross product in $\mathbb{R}^3$.

Prove that $\mathbf{a}\times\mathbf{b}=0$ for all $\mathbf{a},\mathbf{b}\in G$.

A6 Let $f:[0,\infty)\to\mathbb{R}$ be a strictly decreasing continuous function such that $\lim_{x\to\infty}f(x)=0$. Prove that $\int_0^\infty \frac{f(x)-f(x+1)}{f(x)}\,dx$ diverges.

B1 Is there an infinite sequence of real numbers $a_1,a_2,a_3,\dots$ such that

$$a_1^m+a_2^m+a_3^m+\cdots=m$$

for every positive integer $m$?

B2 Given that $A$, $B$, and $C$ are noncollinear points in the plane with integer coordinates such that the distances $AB$, $AC$, and $BC$ are integers, what is the smallest possible value of $AB$?

B3 There are 2010 boxes labeled $B_1,B_2,\dots,B_{2010}$, and $2010n$ balls have been distributed among them, for some positive integer $n$. You may redistribute the balls by a sequence of moves, each of which consists of choosing an $i$ and moving *exactly* $i$ balls from box $B_i$ into any one other box. For which values of $n$ is it possible to reach the distribution with exactly $n$ balls in each box, regardless of the initial distribution of balls?

B4 Find all pairs of polynomials $p(x)$ and $q(x)$ with real coefficients for which

$$p(x)q(x+1)-p(x+1)q(x)=1.$$

B5 Is there a strictly increasing function $f:\mathbb{R}\to\mathbb{R}$ such that $f'(x)=f(f(x))$ for all $x$?

B6 Let $A$ be an $n\times n$ matrix of real numbers for some $n\ge 1$. For each positive integer $k$, let $A^{[k]}$ be the matrix obtained by raising each entry to the $k$th power. Show that if $A^k=A^{[k]}$ for $k=1,2,\dots,n+1$, then $A^k=A^{[k]}$ for all $k\ge 1$.

# Solutions to the 71st William Lowell Putnam Mathematical Competition
# Saturday, December 4, 2010

Kiran Kedlaya and Lenny Ng

A–1 The largest such $k$ is $\lfloor \frac{n+1}{2} \rfloor = \lceil \frac{n}{2} \rceil$. For $n$ even, this value is achieved by the partition

$$\{1,n\},\{2,n-1\},\dots;$$

for $n$ odd, it is achieved by the partition

$$\{n\},\{1,n-1\},\{2,n-2\},\dots.$$

One way to see that this is optimal is to note that the common sum can never be less than $n$, since $n$ itself belongs to one of the boxes. This implies that $k \leq (1+\cdots+n)/n = (n+1)/2$. Another argument is that if $k > (n+1)/2$, then there would have to be two boxes with one number each (by the pigeonhole principle), but such boxes could not have the same sum.

**Remark.** A much subtler question would be to find the smallest $k$ (as a function of $n$) for which no such arrangement exists.

A–2 The only such functions are those of the form $f(x) = cx+d$ for some real numbers $c,d$ (for which the property is obviously satisfied). To see this, suppose that $f$ has the desired property. Then for any $x \in \mathbb{R}$,

$$\begin{aligned}
2f'(x) &= f(x+2)-f(x) \\
&= (f(x+2)-f(x+1)) + (f(x+1)-f(x)) \\
&= f'(x+1) + f'(x).
\end{aligned}$$

Consequently, $f'(x+1) = f'(x)$.

Define the function $g: \mathbb{R} \to \mathbb{R}$ by $g(x) = f(x+1)-f(x)$, and put $c = g(0)$, $d = f(0)$. For all $x \in \mathbb{R}$, $g'(x) = f'(x+1) - f'(x) = 0$, so $g(x) = c$ identically, and $f'(x) = f(x+1)-f(x) = g(x) = c$, so $f(x) = cx+d$ identically as desired.

A–3 If $a = b = 0$, then the desired result holds trivially, so we assume that at least one of $a,b$ is nonzero. Pick any point $(a_0,b_0) \in \mathbb{R}^2$, and let $L$ be the line given by the parametric equation $L(t) = (a_0,b_0) + (a,b)t$ for $t \in \mathbb{R}$. By the chain rule and the given equation, we have $\frac{d}{dt}(h \circ L) = h \circ L$. If we write $f = h \circ L: \mathbb{R} \to \mathbb{R}$, then $f'(t) = f(t)$ for all $t$. It follows that $f(t) = Ce^t$ for some constant $C$. Since $|f(t)| \leq M$ for all $t$, we must have $C = 0$. It follows that $h(a_0,b_0) = 0$; since $(a_0,b_0)$ was an arbitrary point, $h$ is identically 0 over all of $\mathbb{R}^2$.

A–4 Put

$$N = 10^{10^{10^n}} + 10^{10^n} + 10^n - 1.$$

Write $n = 2^m k$ with $m$ a nonnegative integer and $k$ a positive odd integer. For any nonnegative integer $j$,

$$10^{2^m j} \equiv (-1)^j \pmod{10^{2^m}+1}.$$

Since $10^n \geq n \geq 2^m \geq m+1$, $10^n$ is divisible by $2^n$ and hence by $2^{m+1}$, and similarly $10^{10^n}$ is divisible by $2^{10^n}$ and hence by $2^{m+1}$. It follows that

$$N \equiv 1+1+(-1)+(-1) \equiv 0 \pmod{10^{2^m}+1}.$$

Since $N \geq 10^{10^n} > 10^n + 1 \geq 10^{2^m}+1$, it follows that $N$ is composite.

A–5 We start with three lemmas.

**Lemma 1.** *If $\mathbf{x},\mathbf{y} \in G$ are nonzero orthogonal vectors, then $\mathbf{x}*\mathbf{x}$ is parallel to $\mathbf{y}$.*

*Proof.* Put $\mathbf{z} = \mathbf{x} \times \mathbf{y} \neq 0$, so that $\mathbf{x},\mathbf{y}$, and $\mathbf{z} = \mathbf{x}*\mathbf{y}$ are nonzero and mutually orthogonal. Then $\mathbf{w} = \mathbf{x} \times \mathbf{z} \neq 0$, so $\mathbf{w} = \mathbf{x}*\mathbf{z}$ is nonzero and orthogonal to $\mathbf{x}$ and $\mathbf{z}$. However, if $(\mathbf{x}*\mathbf{x}) \times \mathbf{y} \neq 0$, then $\mathbf{w} = \mathbf{x}*(\mathbf{x}*\mathbf{y}) = (\mathbf{x}*\mathbf{x})*\mathbf{y} = (\mathbf{x}*\mathbf{x}) \times \mathbf{y}$ is also orthogonal to $\mathbf{y}$, a contradiction. $\square$

**Lemma 2.** *If $\mathbf{x} \in G$ is nonzero, and there exists $\mathbf{y} \in G$ nonzero and orthogonal to $\mathbf{x}$, then $\mathbf{x}*\mathbf{x} = 0$.*

*Proof.* Lemma 1 implies that $\mathbf{x}*\mathbf{x}$ is parallel to both $\mathbf{y}$ and $\mathbf{x} \times \mathbf{y}$, so it must be zero. $\square$

**Lemma 3.** *If $\mathbf{x},\mathbf{y} \in G$ commute, then $\mathbf{x} \times \mathbf{y} = 0$.*

*Proof.* If $\mathbf{x} \times \mathbf{y} \neq 0$, then $\mathbf{y} \times \mathbf{x}$ is nonzero and distinct from $\mathbf{x} \times \mathbf{y}$. Consequently, $\mathbf{x}*\mathbf{y} = \mathbf{x} \times \mathbf{y}$ and $\mathbf{y}*\mathbf{x} = \mathbf{y} \times \mathbf{x} \neq \mathbf{x}*\mathbf{y}$. $\square$

We proceed now to the proof. Assume by way of contradiction that there exist $\mathbf{a},\mathbf{b} \in G$ with $\mathbf{a} \times \mathbf{b} \neq 0$. Put $\mathbf{c} = \mathbf{a} \times \mathbf{b} = \mathbf{a}*\mathbf{b}$, so that $\mathbf{a},\mathbf{b},\mathbf{c}$ are nonzero and linearly independent. Let $\mathbf{e}$ be the identity element of $G$. Since $\mathbf{e}$ commutes with $\mathbf{a},\mathbf{b},\mathbf{c}$, by Lemma 3 we have $\mathbf{e} \times \mathbf{a} = \mathbf{e} \times \mathbf{b} = \mathbf{e} \times \mathbf{c} = 0$. Since $\mathbf{a},\mathbf{b},\mathbf{c}$ span $\mathbb{R}^3$, $\mathbf{e} \times \mathbf{x} = 0$ for all $\mathbf{x} \in \mathbb{R}^3$, so $\mathbf{e} = 0$.

Since $\mathbf{b},\mathbf{c}$, and $\mathbf{b} \times \mathbf{c} = \mathbf{b}*\mathbf{c}$ are nonzero and mutually orthogonal, Lemma 2 implies

$$\mathbf{b}*\mathbf{b} = \mathbf{c}*\mathbf{c} = (\mathbf{b}*\mathbf{c})*(\mathbf{b}*\mathbf{c}) = 0 = \mathbf{e}.$$

Hence $\mathbf{b}*\mathbf{c} = \mathbf{c}*\mathbf{b}$, contradicting Lemma 3 because $\mathbf{b} \times \mathbf{c} \neq 0$. The desired result follows.

A–6 **First solution.** Note that the hypotheses on $f$ imply that $f(x) > 0$ for all $x \in [0,+\infty)$, so the integrand is a continuous function of $f$ and the integral makes sense. Rewrite the integral as

$$\int_0^\infty \left(1 - \frac{f(x+1)}{f(x)}\right)dx,$$

and suppose by way of contradiction that it converges to a finite limit $L$. For $n \geq 0$, define the Lebesgue measurable set

$$I_n = \{x \in [0,1] : 1 - \frac{f(x+n+1)}{f(x+n)} \leq 1/2\}.$$

Then $L \geq \sum_{n=0}^{\infty} \frac{1}{2}(1-\mu(I_n))$, so the latter sum converges. In particular, there exists a nonnegative integer $N$ for which $\sum_{n=N}^{\infty}(1-\mu(I_n)) < 1$; the intersection

$$I = \bigcup_{n=N}^{\infty} I_n = [0,1] - \bigcap_{n=N}^{\infty}([0,1]-I_n)$$

then has positive Lebesgue measure.

By Taylor's theorem with remainder, for $t \in [0,1/2]$,

$$\begin{aligned} -\log(1-t) &\leq t + \frac{t^2}{2} \sup_{t\in[0,1/2]} \left\{ \frac{1}{(1-t)^2} \right\} \\ &= t + 2t^2 \leq 2t. \end{aligned}$$

For each nonnegative integer $n \geq N$, we then have

$$\begin{aligned} L &\geq \int_N^n \left(1 - \frac{f(x+1)}{f(x)}\right) dx \\ &= \sum_{i=N}^{n-1} \int_0^1 \left(1 - \frac{f(x+i+1)}{f(x+i)}\right) dx \\ &\geq \sum_{i=N}^{n-1} \int_I \left(1 - \frac{f(x+i+1)}{f(x+i)}\right) dx \\ &\geq \frac{1}{2} \sum_{i=N}^{n-1} \int_I \log \frac{f(x+i)}{f(x+i+1)}\, dx \\ &= \frac{1}{2} \int_I \left( \sum_{i=N}^{n-1} \log \frac{f(x+i)}{f(x+i+1)} \right) dx \\ &= \frac{1}{2} \int_I \log \frac{f(x+N)}{f(x+n)}\, dx. \end{aligned}$$

For each $x \in I$, $\log f(x+N)/f(x+n)$ is a strictly increasing unbounded function of $n$. By the monotone convergence theorem, the integral $\int_I \log(f(x+N)/f(x+n))\,dx$ grows without bound as $n \to +\infty$, a contradiction. Thus the original integral diverges, as desired.

**Remark.** This solution is motivated by the commonly-used fact that an infinite product $(1+x_1)(1+x_2)\cdots$ converges absolutely if and only if the sum $x_1+x_2+\cdots$ converges absolutely. The additional measure-theoretic argument at the beginning is needed because one cannot bound $-\log(1-t)$ by a fixed multiple of $t$ uniformly for all $t \in [0,1)$.

Greg Martin suggests a variant solution that avoids use of Lebesgue measure. Note first that if $f(y) > 2f(y+1)$, then either $f(y) > \sqrt{2}f(y+1/2)$ or $f(y+1/2) > \sqrt{2}f(y+1)$, and in either case we deduce that

$$\int_{y-1/2}^{y+1/2} \frac{f(x)-f(x+1)}{f(x)}\, dx > \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right) > \frac{1}{7}.$$

If there exist arbitrarily large values of $y$ for which $f(y) > 2f(y+1)$, we deduce that the original integral is greater than any multiple of $1/7$, and so diverges. Otherwise, for $x$ large we may argue that

$$\frac{f(x)-f(x+1)}{f(x)} > \frac{3}{5} \log \frac{f(x)}{f(x+1)}$$

as in the above solution, and again get divergence using a telescoping sum.

**Second solution.** (Communicated by Paul Allen.) Let $b > a$ be nonnegative integers. Then

$$\begin{aligned} \int_a^b \frac{f(x)-f(x+1)}{f(x)} dx &= \sum_{k=a}^{b-1} \int_0^1 \frac{f(x+k)-f(x+k+1)}{f(x+k)} dx \\ &= \int_0^1 \sum_{k=a}^{b-1} \frac{f(x+k)-f(x+k+1)}{f(x+k)} dx \\ &\geq \int_0^1 \sum_{k=a}^{b-1} \frac{f(x+k)-f(x+k+1)}{f(x+a)} dx \\ &= \int_0^1 \frac{f(x+a)-f(x+b)}{f(x+a)} dx. \end{aligned}$$

Now since $f(x) \to 0$, given $a$, we can choose an integer $l(a) > a$ for which $f(l(a)) < f(a+1)/2$; then $\frac{f(x+a)-f(x+l(a))}{f(x+a)} \geq 1 - \frac{f(l(a))}{f(a+1)} > 1/2$ for all $x \in [0,1]$. Thus if we define a sequence of integers $a_n$ by $a_0 = 0$, $a_{n+1} = l(a_n)$, then

$$\begin{aligned} \int_0^{\infty} \frac{f(x)-f(x+1)}{f(x)} dx &= \sum_{n=0}^{\infty} \int_{a_n}^{a_{n+1}} \frac{f(x)-f(x+1)}{f(x)} dx \\ &> \sum_{n=0}^{\infty} \int_0^1 (1/2) dx, \end{aligned}$$

and the final sum clearly diverges.

**Third solution.** (By Joshua Rosenberg, communicated by Catalin Zara.) If the original integral converges, then on one hand the integrand $(f(x)-f(x+1))/f(x) = 1 - f(x+1)/f(x)$ cannot tend to 1 as $x \to \infty$. On the other hand, for any $a \geq 0$,

$$\begin{aligned} 0 &< \frac{f(a+1)}{f(a)} \\ &< \frac{1}{f(a)} \int_a^{a+1} f(x)\, dx \\ &= \frac{1}{f(a)} \int_a^{\infty} (f(x)-f(x+1))\, dx \\ &\leq \int_a^{\infty} \frac{f(x)-f(x+1)}{f(x)}\, dx, \end{aligned}$$

and the last expression tends to 0 as $a \to \infty$. Hence by the squeeze theorem, $f(a+1)/f(a) \to 0$ as $a \to \infty$, a contradiction.

B–1 **First solution.** No such sequence exists. If it did, then the Cauchy-Schwartz inequality would imply

$$\begin{aligned} 8 &= (a_1^2 + a_2^2 + \cdots)(a_1^4 + a_2^4 + \cdots) \\ &\geq (a_1^3 + a_2^3 + \cdots)^2 = 9, \end{aligned}$$

contradiction.

**Second solution.** (Communicated by Catalin Zara.) Suppose that such a sequence exists. If $a_k^2 \in [0,1]$ for all $k$, then $a_k^4 \leq a_k^2$ for all $k$, and so

$$4 = a_1^4 + a_2^4 + \cdots \leq a_1^2 + a_2^2 + \cdots = 2,$$

contradiction. There thus exists a positive integer $k$ for which $a_k^2 \geq 1$. However, in this case, for $m$ large, $a_k^{2m} > 2m$ and so $a_1^{2m} + a_2^{2m} + \cdots \neq 2m$.

**Third solution.** We generalize the second solution to show that for any positive integer $k$, it is impossible for a sequence $a_1, a_2, \dots$ of complex numbers to satisfy the given conditions in case the series $a_1^k + a_2^k + \cdots$ converges absolutely. This includes the original problem by taking $k = 2$, in which case the series $a_1^2 + a_2^2 + \cdots$ consists of nonnegative real numbers and so converges absolutely if it converges at all.

Since the sum $\sum_{i=1}^\infty |a_i|^k$ converges by hypothesis, we can find a positive integer $n$ such that $\sum_{i=n+1}^\infty |a_i|^k < 1$. For each positive integer $d$, we then have

$$\left| kd - \sum_{i=1}^n a_i^{kd} \right| \leq \sum_{i=n+1}^\infty |a_i|^{kd} < 1.$$

We thus cannot have $|a_1|, \dots, |a_n| \leq 1$, or else the sum $\sum_{i=1}^n a_i^{kd}$ would be bounded in absolute value by $n$ independently of $d$. But if we put $r = \max\{|a_1|, \dots, |a_n|\} > 1$, we obtain another contradiction because for any $\varepsilon > 0$,

$$\limsup_{d \to \infty} (r - \varepsilon)^{-kd} \left| \sum_{i=1}^n a_i^{kd} \right| > 0.$$

For instance, this follows from applying the root test to the rational function

$$\sum_{i=1}^n \frac{1}{1 - a_i^k z} = \sum_{d=0}^\infty \left( \sum_{i=1}^n a_i^{kd} \right) z^d,$$

which has a pole within the circle $|z| \leq r^{-1/k}$. (An elementary proof is also possible.)

**Fourth solution.** (Communicated by Noam Elkies.) Since $\sum_k a_k^2 = 2$, for each positive integer $k$ we have $a_k^2 \leq 2$ and so $a_k^4 \leq 2a_k^2$, with equality only for $a_k^2 \in \{0, 2\}$. Thus to have $\sum_k a_k^4 = 4$, there must be a single index $k$ for which $a_k^2 = 2$, and the other $a_k$ must all equal 0. But then $\sum_k a_k^{2m} = 2^m \neq 2m$ for any positive integer $m > 2$.

**Remark.** Manjul Bhargava points out it is easy to construct sequences of complex numbers with the desired property if we drop the condition of absolute convergence. Here is an inductive construction (of which several variants are possible). For $n = 1, 2, \dots$ and $z \in \mathbb{C}$, define the finite sequence

$$s_{n,z} = \left( \frac{1}{z} e^{2\pi i j/n} : j = 0, \dots, n-1 \right).$$

This sequence has the property that for any positive integer $j$, the sum of the $j$-th powers of the terms of $s_{n,z}$ equals $1/z^j$ if $j$ is divisible by $n$ and 0 otherwise. Moreover, any partial sum of $j$-th powers is bounded in absolute value by $n/|z|^j$.

The desired sequence will be constructed as follows. Suppose that we have a finite sequence which has the correct sum of $j$-th powers for $j = 1, \dots, m$. (For instance, for $m = 1$, we may start with the singleton sequence 1.) We may then extend it to a new sequence which has the correct sum of $j$-th powers for $j = 1, \dots, m+1$, by appending $k$ copies of $s_{m+1,z}$ for suitable choices of a positive integer $k$ and a complex number $z$ with $|z| < m^{-2}$. This last restriction ensures that the resulting infinite sequence $a_1, a_2, \dots$ is such that for each positive integer $m$, the series $a_1^m + a_2^m + \cdots$ is convergent (though not absolutely convergent). Its partial sums include a subsequence equal to the constant value $m$, so the sum of the series must equal $m$ as desired.

B–2 The smallest distance is 3, achieved by $A = (0,0)$, $B = (3,0)$, $C = (0,4)$. To check this, it suffices to check that $AB$ cannot equal 1 or 2. (It cannot equal 0 because if two of the points were to coincide, the three points would be collinear.)

The triangle inequality implies that $|AC - BC| \leq AB$, with equality if and only if $A, B, C$ are collinear. If $AB = 1$, we may assume without loss of generality that $A = (0,0)$, $B = (1,0)$. To avoid collinearity, we must have $AC = BC$, but this forces $C = (1/2, y)$ for some $y \in \mathbb{R}$, a contradiction. (One can also treat this case by scaling by a factor of 2 to reduce to the case $AB = 2$, treated in the next paragraph.)

If $AB = 2$, then we may assume without loss of generality that $A = (0,0), B = (2,0)$. The triangle inequality implies $|AC - BC| \in \{0, 1\}$. Also, for $C = (x,y)$, $AC^2 = x^2 + y^2$ and $BC^2 = (2-x)^2 + y^2$ have the same parity; it follows that $AC = BC$. Hence $c = (1, y)$ for some $y \in \mathbb{R}$, so $y^2$ and $y^2 + 1 = BC^2$ are consecutive perfect squares. This can only happen for $y = 0$, but then $A, B, C$ are collinear, a contradiction again.

**Remark.** Manjul Bhargava points out that more generally, a *Heronian triangle* (a triangle with integer sides and rational area) cannot have a side of length 1 or 2 (and again it is enough to treat the case of length 2). The original problem follows from this because a triangle whose vertices have integer coordinates has area equal to half an integer (by Pick's formula or the explicit formula for the area as a determinant).

B–3 It is possible if and only if $n \geq 1005$. Since

$$1+\cdots+2009 = \frac{2009 \times 2010}{2} = 2010 \times 1004.5,$$

for $n \leq 1004$, we can start with an initial distribution in which each box $B_i$ starts with at most $i-1$ balls (so in particular $B_1$ is empty). From such a distribution, no moves are possible, so we cannot reach the desired final distribution.

Suppose now that $n \geq 1005$. By the pigeonhole principle, at any time, there exists at least one index $i$ for which the box $B_i$ contains at least $i$ balls. We will describe any such index as being *eligible*. The following sequence of operations then has the desired effect.

(a) Find the largest eligible index $i$. If $i = 1$, proceed to (b). Otherwise, move $i$ balls from $B_i$ to $B_1$, then repeat (a).

(b) At this point, only the index $i = 1$ can be eligible (so it must be). Find the largest index $j$ for which $B_j$ is nonempty. If $j = 1$, proceed to (c). Otherwise, move 1 ball from $B_1$ to $B_j$; in case this makes $j$ eligible, move $j$ balls from $B_j$ to $B_1$. Then repeat (b).

(c) At this point, all of the balls are in $B_1$. For $i = 2,\dots,2010$, move one ball from $B_1$ to $B_i$ $n$ times.

After these operations, we have the desired distribution.

B–4 **First solution.** The pairs $(p,q)$ satisfying the given equation are those of the form $p(x) = ax+b, q(x) = cx+d$ for $a,b,c,d \in \mathbb{R}$ such that $bc-ad = 1$. We will see later that these indeed give solutions.

Suppose $p$ and $q$ satisfy the given equation; note that neither $p$ nor $q$ can be identically zero. By subtracting the equations

$$\begin{aligned} p(x)q(x+1)-p(x+1)q(x) &= 1 \\ p(x-1)q(x)-p(x)q(x-1) &= 1, \end{aligned}$$

we obtain the equation

$$p(x)(q(x+1)+q(x-1)) = q(x)(p(x+1)+p(x-1)).$$

The original equation implies that $p(x)$ and $q(x)$ have no common nonconstant factor, so $p(x)$ divides $p(x+1)+p(x-1)$. Since each of $p(x+1)$ and $p(x-1)$ has the same degree and leading coefficient as $p$, we must have

$$p(x+1)+p(x-1) = 2p(x).$$

If we define the polynomials $r(x) = p(x+1)-p(x)$, $s(x) = q(x+1)-q(x)$, we have $r(x+1) = r(x)$, and similarly $s(x+1) = s(x)$. Put

$$a = r(0), b = p(0), c = s(0), d = q(0).$$

Then $r(x) = a, s(x) = c$ for all $x \in \mathbb{Z}$, and hence identically; consequently, $p(x) = ax+b, q(x) = cx+d$ for all $x \in \mathbb{Z}$, and hence identically. For $p$ and $q$ of this form,

$$p(x)q(x+1)-p(x+1)q(x) = bc-ad,$$

so we get a solution if and only if $bc-ad = 1$, as claimed.

**Second solution.** (Communicated by Catalin Zara.) Again, note that $p$ and $q$ must be nonzero. Write

$$\begin{aligned} p(x) &= p_0+p_1x+\cdots+p_mx^m \\ q(x) &= q_0+q_1x+\cdots+q_nx^n \end{aligned}$$

with $p_m, q_n \neq 0$, so that $m = \deg(p), n = \deg(q)$. It is enough to derive a contradiction assuming that $\max\{m,n\} > 1$, the remaining cases being treated as in the first solution.

Put $R(x) = p(x)q(x+1)-p(x+1)q(x)$. Since $m+n \geq 2$ by assumption, the coefficient of $x^{m+n-1}$ in $R(x)$ must vanish. By easy algebra, this coefficient equals $(m-n)p_mq_n$, so we must have $m = n > 1$.

For $k = 1,\dots,2m-2$, the coefficient of $x^k$ in $R(x)$ is

$$\sum_{i+j>k,\, j>i} \left( \binom{j}{k-i} - \binom{i}{k-j} \right) (p_iq_j - p_jq_i)$$

and must vanish. For $k = 2m-2$, the only summand is for $(i,j) = (m-1,m)$, so $p_{m-1}q_m = p_mq_{m-1}$.

Suppose now that $h \geq 1$ and that $p_iq_j = p_jq_i$ is known to vanish whenever $j > i \geq h$. (By the previous paragraph, we initially have this for $h = m-1$.) Take $k = m+h-2$ and note that the conditions $i+j > h, j \leq m$ force $i \geq h-1$. Using the hypothesis, we see that the only possible nonzero contribution to the coefficient of $x^k$ in $R(x)$ is from $(i,j) = (h-1,m)$. Hence $p_{h-1}q_m = p_mq_{h-1}$; since $p_m, q_m \neq 0$, this implies $p_{h-1}q_j = p_jq_{h-1}$ whenever $j > h-1$.

By descending induction, we deduce that $p_iq_j = p_jq_i$ whenever $j > i \geq 0$. Consequently, $p(x)$ and $q(x)$ are scalar multiples of each other, forcing $R(x) = 0$, a contradiction.

**Third solution.** (Communicated by David Feldman.) As in the second solution, we note that there are no solutions where $m = \deg(p), n = \deg(q)$ are distinct and $m+n \geq 2$. Suppose $p,q$ form a solution with $m = n \geq 2$. The desired identity asserts that the matrix

$$\begin{pmatrix} p(x) & p(x+1) \\ q(x) & q(x+1) \end{pmatrix}$$

has determinant 1. This condition is preserved by replacing $q(x)$ with $q(x)-tp(x)$ for any real number $t$. In particular, we can choose $t$ so that $\deg(q(x)-tp(x)) < m$; we then obtain a contradiction.

B–5 **First solution.** The answer is no. Suppose otherwise. For the condition to make sense, $f$ must be differentiable. Since $f$ is strictly increasing, we must have $f'(x) \geq 0$ for all $x$. Also, the function $f'(x)$ is strictly increasing: if $y > x$ then $f'(y) = f(f(y)) > f(f(x)) = f'(x)$. In particular, $f'(y) > 0$ for all $y \in \mathbb{R}$.

For any $x_0 \geq -1$, if $f(x_0) = b$ and $f'(x_0) = a > 0$, then $f'(x) > a$ for $x > x_0$ and thus $f(x) \geq a(x - x_0) + b$ for $x \geq x_0$. Then either $b < x_0$ or $a = f'(x_0) = f(f(x_0)) = f(b) \geq a(b - x_0) + b$. In the latter case, $b \leq a(x_0 + 1)/(a+1) \leq x_0 + 1$. We conclude in either case that $f(x_0) \leq x_0 + 1$ for all $x_0 \geq -1$.

It must then be the case that $f(f(x)) = f'(x) \leq 1$ for all $x$, since otherwise $f(x) > x + 1$ for large $x$. Now by the above reasoning, if $f(0) = b_0$ and $f'(0) = a_0 > 0$, then $f(x) > a_0 x + b_0$ for $x > 0$. Thus for $x > \max\{0, -b_0/a_0\}$, we have $f(x) > 0$ and $f(f(x)) > a_0 x + b_0$. But then $f(f(x)) > 1$ for sufficiently large $x$, a contradiction.

**Second solution.** (Communicated by Catalin Zara.) Suppose such a function exists. Since $f$ is strictly increasing and differentiable, so is $f \circ f = f'$. In particular, $f$ is twice differentiable; also, $f''(x) = f'(f(x))f'(x)$ is the product of two strictly increasing nonnegative functions, so it is also strictly increasing and nonnegative. In particular, we can choose $\alpha > 0$ and $M \in \mathbb{R}$ such that $f''(x) > 4\alpha$ for all $x \geq M$. Then for all $x \geq M$,

$$f(x) \geq f(M) + f'(M)(x - M) + 2\alpha(x - M)^2.$$

In particular, for some $M' > M$, we have $f(x) \geq \alpha x^2$ for all $x \geq M'$.

Pick $T > 0$ so that $\alpha T^2 > M'$. Then for $x \geq T$, $f(x) > M'$ and so $f'(x) = f(f(x)) \geq \alpha f(x)^2$. Now

$$\frac{1}{f(T)} - \frac{1}{f(2T)} = \int_T^{2T} \frac{f'(t)}{f(t)^2}\,dt \geq \int_T^{2T} \alpha\,dt;$$

however, as $T \to \infty$, the left side of this inequality tends to 0 while the right side tends to $+\infty$, a contradiction.

**Third solution.** (Communicated by Noam Elkies.) Since $f$ is strictly increasing, for some $y_0$, we can define the inverse function $g(y)$ of $f$ for $y \geq y_0$. Then $x = g(f(x))$, and we may differentiate to find that $1 = g'(f(x))f'(x) = g'(f(x))f(f(x))$. It follows that $g'(y) = 1/f(y)$ for $y \geq y_0$; since $g$ takes arbitrarily large values, the integral $\int_{y_0}^{\infty} dy/f(y)$ must diverge. One then gets a contradiction from any reasonable lower bound on $f(y)$ for $y$ large, e.g., the bound $f(x) \geq \alpha x^2$ from the second solution. (One can also start with a linear lower bound $f(x) \geq \beta x$, then use the integral expression for $g$ to deduce that $g(x) \leq \gamma \log x$, which in turn forces $f(x)$ to grow exponentially.)

B–6 For any polynomial $p(x)$, let $[p(x)]A$ denote the $n \times n$ matrix obtained by replacing each entry $A_{ij}$ of $A$ by $p(A_{ij})$; thus $A^{[k]} = [x^k]A$. Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ denote the characteristic polynomial of $A$. By the Cayley-Hamilton theorem,

$$\begin{aligned}
0 &= A \cdot P(A) \\
&= A^{n+1} + a_{n-1}A^n + \cdots + a_0 A \\
&= A^{[n+1]} + a_{n-1}A^{[n]} + \cdots + a_0 A^{[1]} \\
&= [xp(x)]A.
\end{aligned}$$

Thus each entry of $A$ is a root of the polynomial $xp(x)$.

Now suppose $m \geq n+1$. Then

$$\begin{aligned}
0 &= [x^{m+1-n}P(x)]A \\
&= A^{[m+1]} + a_{n-1}A^{[m]} + \cdots + a_0 A^{[m+1-n]}
\end{aligned}$$

since each entry of $A$ is a root of $x^{m+1-n}P(x)$. On the other hand,

$$\begin{aligned}
0 &= A^{m+1-n} \cdot P(A) \\
&= A^{m+1} + a_{n-1}A^m + \cdots + a_0 A^{m+1-n}.
\end{aligned}$$

Therefore if $A^k = A^{[k]}$ for $m + 1 - n \leq k \leq m$, then $A^{m+1} = A^{[m+1]}$. The desired result follows by induction on $m$.

**Remark.** David Feldman points out that the result is best possible in the following sense: there exist examples of $n \times n$ matrices $A$ for which $A^k = A^{[k]}$ for $k = 1, \ldots, n$ but $A^{n+1} \neq A^{[n+1]}$.

# The 72nd William Lowell Putnam Mathematical Competition
## Saturday, December 3, 2011

A1 Define a *growing spiral* in the plane to be a sequence of points with integer coordinates $P_0 = (0,0), P_1, \dots, P_n$ such that $n \ge 2$ and:

- the directed line segments $P_0P_1, P_1P_2, \dots, P_{n-1}P_n$ are in the successive coordinate directions east (for $P_0P_1$), north, west, south, east, etc.;
- the lengths of these line segments are positive and strictly increasing.

[Picture omitted.] How many of the points $(x,y)$ with integer coordinates $0 \le x \le 2011, 0 \le y \le 2011$ *cannot* be the last point, $P_n$ of any growing spiral?

A2 Let $a_1, a_2, \dots$ and $b_1, b_2, \dots$ be sequences of positive real numbers such that $a_1 = b_1 = 1$ and $b_n = b_{n-1}a_n - 2$ for $n = 2, 3, \dots$. Assume that the sequence $(b_j)$ is bounded. Prove that

$$S = \sum_{n=1}^{\infty} \frac{1}{a_1 \dots a_n}$$

converges, and evaluate $S$.

A3 Find a real number $c$ and a positive number $L$ for which

$$\lim_{r\to\infty} \frac{r^c \int_0^{\pi/2} x^r \sin x\, dx}{\int_0^{\pi/2} x^r \cos x\, dx} = L.$$

A4 For which positive integers $n$ is there an $n \times n$ matrix with integer entries such that every dot product of a row with itself is even, while every dot product of two different rows is odd?

A5 Let $F : \mathbb{R}^2 \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ be twice continuously differentiable functions with the following properties:

- $F(u,u) = 0$ for every $u \in \mathbb{R}$;
- for every $x \in \mathbb{R}$, $g(x) > 0$ and $x^2 g(x) \le 1$;
- for every $(u,v) \in \mathbb{R}^2$, the vector $\nabla F(u,v)$ is either $\mathbf{0}$ or parallel to the vector $\langle g(u), -g(v) \rangle$.

Prove that there exists a constant $C$ such that for every $n \ge 2$ and any $x_1, \dots, x_{n+1} \in \mathbb{R}$, we have

$$\min_{i \ne j} |F(x_i, x_j)| \le \frac{C}{n}.$$

A6 Let $G$ be an abelian group with $n$ elements, and let

$$\{g_1 = e, g_2, \dots, g_k\} \subsetneqq G$$

be a (not necessarily minimal) set of distinct generators of $G$. A special die, which randomly selects one of the elements $g_1, g_2, \dots, g_k$ with equal probability, is rolled $m$ times and the selected elements are multiplied to produce an element $g \in G$. Prove that there exists a real number $b \in (0,1)$ such that

$$\lim_{m\to\infty} \frac{1}{b^{2m}} \sum_{x \in G} \left( \mathrm{Prob}(g = x) - \frac{1}{n} \right)^2$$

is positive and finite.

B1 Let $h$ and $k$ be positive integers. Prove that for every $\varepsilon > 0$, there are positive integers $m$ and $n$ such that

$$\varepsilon < |h\sqrt{m} - k\sqrt{n}| < 2\varepsilon.$$

B2 Let $S$ be the set of all ordered triples $(p,q,r)$ of prime numbers for which at least one rational number $x$ satisfies $px^2 + qx + r = 0$. Which primes appear in seven or more elements of $S$?

B3 Let $f$ and $g$ be (real-valued) functions defined on an open interval containing 0, with $g$ nonzero and continuous at 0. If $fg$ and $f/g$ are differentiable at 0, must $f$ be differentiable at 0?

B4 In a tournament, 2011 players meet 2011 times to play a multiplayer game. Every game is played by all 2011 players together and ends with each of the players either winning or losing. The standings are kept in two $2011 \times 2011$ matrices, $T = (T_{hk})$ and $W = (W_{hk})$. Initially, $T = W = 0$. After every game, for every $(h,k)$ (including for $h = k$), if players $h$ and $k$ tied (that is, both won or both lost), the entry $T_{hk}$ is increased by 1, while if player $h$ won and player $k$ lost, the entry $W_{hk}$ is increased by 1 and $W_{kh}$ is decreased by 1.

Prove that at the end of the tournament, $\det(T + iW)$ is a non-negative integer divisible by $2^{2010}$.

B5 Let $a_1, a_2, \dots$ be real numbers. Suppose that there is a constant $A$ such that for all $n$,

$$\int_{-\infty}^{\infty} \left( \sum_{i=1}^{n} \frac{1}{1 + (x - a_i)^2} \right)^2 dx \le An.$$

Prove there is a constant $B > 0$ such that for all $n$,

$$\sum_{i,j=1}^{n} (1 + (a_i - a_j)^2) \ge Bn^3.$$

B6 Let $p$ be an odd prime. Show that for at least $(p+1)/2$ values of $n$ in $\{0, 1, 2, \dots, p-1\}$,

$$\sum_{k=0}^{p-1} k! n^k \qquad \text{is not divisible by } p.$$

# Solutions to the 72nd William Lowell Putnam Mathematical Competition
# Saturday, December 3, 2011

Kiran Kedlaya and Lenny Ng

A1 We claim that the set of points with $0 \leq x \leq 2011$ and $0 \leq y \leq 2011$ that cannot be the last point of a growing spiral are as follows: $(0,y)$ for $0 \leq y \leq 2011$; $(x,0)$ and $(x,1)$ for $1 \leq x \leq 2011$; $(x,2)$ for $2 \leq x \leq 2011$; and $(x,3)$ for $3 \leq x \leq 2011$. This gives a total of

$$2012 + 2011 + 2011 + 2010 + 2009 = 10053$$

excluded points.

The complement of this set is the set of $(x,y)$ with $0 < x < y$, along with $(x,y)$ with $x \geq y \geq 4$. Clearly the former set is achievable as $P_2$ in a growing spiral, while a point $(x,y)$ in the latter set is $P_6$ in a growing spiral with successive lengths 1, 2, 3, $x+1$, $x+2$, and $x+y-1$.

We now need to rule out the other cases. Write $x_1 < y_1 < x_2 < y_2 < \dots$ for the lengths of the line segments in the spiral in order, so that $P_1 = (x_1,0)$, $P_2 = (x_1,y_1)$, $P_3 = (x_1 - x_2, y_1)$, and so forth. Any point beyond $P_0$ has $x$-coordinate of the form $x_1 - x_2 + \cdots + (-1)^{n-1} x_n$ for $n \geq 1$; if $n$ is odd, we can write this as $x_1 + (-x_2 + x_3) + \cdots + (-x_{n-1} + x_n) > 0$, while if $n$ is even, we can write this as $(x_1 - x_2) + \cdots + (x_{n-1} - x_n) < 0$. Thus no point beyond $P_0$ can have $x$-coordinate 0, and we have ruled out $(0,y)$ for $0 \leq y \leq 2011$.

Next we claim that any point beyond $P_3$ must have $y$-coordinate either negative or $\geq 4$. Indeed, each such point has $y$-coordinate of the form $y_1 - y_2 + \cdots + (-1)^{n-1} y_n$ for $n \geq 2$, which we can write as $(y_1 - y_2) + \cdots + (y_{n-1} - y_n) < 0$ if $n$ is even, and

$$y_1 + (-y_2 + y_3) + \cdots + (-y_{n-1} + y_n) \geq y_1 + 2 \geq 4$$

if $n \geq 3$ is odd. Thus to rule out the rest of the forbidden points, it suffices to check that they cannot be $P_2$ or $P_3$ for any growing spiral. But none of them can be $P_3 = (x_1 - x_2, y_1)$ since $x_1 - x_2 < 0$, and none of them can be $P_2 = (x_1, y_1)$ since they all have $y$-coordinate at most equal to their $x$-coordinate.

A2 For $m \geq 1$, write

$$S_m = \frac{3}{2}\left(1 - \frac{b_1 \cdots b_m}{(b_1+2)\cdots(b_m+2)}\right).$$

Then $S_1 = 1 = 1/a_1$ and a quick calculation yields

$$S_m - S_{m-1} = \frac{b_1 \cdots b_{m-1}}{(b_2+2)\cdots(b_m+2)} = \frac{1}{a_1 \cdots a_m}$$

for $m \geq 2$, since $a_j = (b_j+2)/b_{j-1}$ for $j \geq 2$. It follows that $S_m = \sum_{n=1}^m 1/(a_1 \cdots a_n)$.

Now if $(b_j)$ is bounded above by $B$, then $\frac{b_j}{b_j+2} \leq \frac{B}{B+2}$ for all $j$, and so $3/2 > S_m \geq 3/2(1 - (\frac{B}{B+2})^m)$. Since $\frac{B}{B+2} < 1$, it follows that the sequence $(S_m)$ converges to $S = 3/2$.

A3 We claim that $(c,L) = (-1, 2/\pi)$ works. Write $f(r) = \int_0^{\pi/2} x^r \sin x\,dx$. Then

$$f(r) < \int_0^{\pi/2} x^r\,dx = \frac{(\pi/2)^{r+1}}{r+1}$$

while since $\sin x \geq 2x/\pi$ for $x \leq \pi/2$,

$$f(r) > \int_0^{\pi/2} \frac{2x^{r+1}}{\pi}\,dx = \frac{(\pi/2)^{r+1}}{r+2}.$$

It follows that

$$\lim_{r\to\infty} r \left(\frac{2}{\pi}\right)^{r+1} f(r) = 1,$$

whence

$$\lim_{r\to\infty} \frac{f(r)}{f(r+1)} = \lim_{r\to\infty} \frac{r(2/\pi)^{r+1} f(r)}{(r+1)(2/\pi)^{r+2} f(r+1)} \cdot \frac{2(r+1)}{\pi r} = \frac{2}{\pi}.$$

Now by integration by parts, we have

$$\int_0^{\pi/2} x^r \cos x\,dx = \frac{1}{r+1}\int_0^{\pi/2} x^{r+1} \sin x\,dx = \frac{f(r+1)}{r+1}.$$

Thus setting $c = -1$ in the given limit yields

$$\lim_{r\to\infty} \frac{(r+1) f(r)}{r f(r+1)} = \frac{2}{\pi},$$

as desired.

A4 The answer is $n$ odd. Let $I$ denote the $n \times n$ identity matrix, and let $A$ denote the $n \times n$ matrix all of whose entries are 1. If $n$ is odd, then the matrix $A - I$ satisfies the conditions of the problem: the dot product of any row with itself is $n-1$, and the dot product of any two distinct rows is $n-2$.

Conversely, suppose $n$ is even, and suppose that the matrix $M$ satisfied the conditions of the problem. Consider all matrices and vectors mod 2. Since the dot product of a row with itself is equal mod 2 to the sum of the entries of the row, we have $Mv = 0$ where $v$ is the vector $(1,1,\dots,1)$, and so $M$ is singular. On the other hand, $MM^T = A - I$; since

$$(A-I)^2 = A^2 - 2A + I = (n-2)A + I = I,$$

we have $(\det M)^2 = \det(A-I) = 1$ and $\det M = 1$, contradicting the fact that $M$ is singular.

A5 (by Abhinav Kumar) Define $G:\mathbb{R}\to\mathbb{R}$ by $G(x) = \int_0^x g(t)\,dt$. By assumption, $G$ is a strictly increasing, thrice continuously differentiable function. It is also bounded: for $x>1$, we have

$$0 < G(x)-G(1) = \int_1^x g(t)\,dt \leq \int_1^x dt/t^2 = 1,$$

and similarly, for $x<-1$, we have $0 > G(x)-G(-1) \geq -1$. It follows that the image of $G$ is some open interval $(A,B)$ and that $G^{-1}:(A,B)\to\mathbb{R}$ is also thrice continuously differentiable.

Define $H:(A,B)\times(A,B)\to\mathbb{R}$ by $H(x,y) = F(G^{-1}(x),G^{-1}(y))$; it is twice continuously differentiable since $F$ and $G^{-1}$ are. By our assumptions about $F$,

$$\begin{aligned}\frac{\partial H}{\partial x}+\frac{\partial H}{\partial y} &= \frac{\partial F}{\partial x}(G^{-1}(x),G^{-1}(y))\cdot\frac{1}{g(G^{-1}(x))}\\ &\quad+\frac{\partial F}{\partial y}(G^{-1}(x),G^{-1}(y))\cdot\frac{1}{g(G^{-1}(y))} = 0.\end{aligned}$$

Therefore $H$ is constant along any line parallel to the vector $(1,1)$, or equivalently, $H(x,y)$ depends only on $x-y$. We may thus write $H(x,y) = h(x-y)$ for some function $h$ on $(-(B-A),B-A)$, and we then have $F(x,y) = h(G(x)-G(y))$. Since $F(u,u)=0$, we have $h(0)=0$. Also, $h$ is twice continuously differentiable (since it can be written as $h(x) = H((A+B+x)/2,(A+B-x)/2)$), so $|h'|$ is bounded on the closed interval $[-(B-A)/2,(B-A)/2]$, say by $M$.

Given $x_1,\dots,x_{n+1}\in\mathbb{R}$ for some $n\geq 2$, the numbers $G(x_1),\dots,G(x_{n+1})$ all belong to $(A,B)$, so we can choose indices $i$ and $j$ so that $|G(x_i)-G(x_j)| \leq (B-A)/n \leq (B-A)/2$. By the mean value theorem,

$$|F(x_i,x_j)| = |h(G(x_i)-G(x_j))| \leq M\frac{B-A}{n},$$

so the claim holds with $C = M(B-A)$.

A6 Choose some ordering $h_1,\dots,h_n$ of the elements of $G$ with $h_1 = e$. Define an $n\times n$ matrix $M$ by settting $M_{ij} = 1/k$ if $h_j = h_i g$ for some $g\in\{g_1,\dots,g_k\}$ and $M_{ij}=0$ otherwise. Let $v$ denote the column vector $(1,0,\dots,0)$. The probability that the product of $m$ random elements of $\{g_1,\dots,g_k\}$ equals $h_i$ can then be interpreted as the $i$-th component of the vector $M^m v$.

Let $\hat{G}$ denote the dual group of $G$, i.e., the group of complex-valued characters of $G$. Let $\hat{e}\in\hat{G}$ denote the trivial character. For each $\chi\in\hat{G}$, the vector $v_\chi = (\chi(h_i))_{i=1}^n$ is an eigenvector of $M$ with eigenvalue $\lambda_\chi = (\chi(g_1)+\cdots+\chi(g_k))/k$. In particular, $v_{\hat{e}}$ is the all-ones vector and $\lambda_{\hat{e}} = 1$. Put

$$b = \max\{|\lambda_\chi| : \chi\in\hat{G}-\{\hat{e}\}\};$$

we show that $b\in(0,1)$ as follows. First suppose $b=0$; then

$$1 = \sum_{\chi\in\hat{G}}\lambda_\chi = \frac{1}{k}\sum_{i=1}^k\sum_{\chi\in\hat{G}}\chi(g_i) = \frac{n}{k}$$

because $\sum_{\chi\in\hat{(G)}}\chi(g_i)$ equals $n$ for $i=1$ and 0 otherwise. However, this contradicts the hypothesis that $\{g_1,\dots,g_k\}$ is not all of $G$. Hence $b>0$. Next suppose $b=1$, and choose $\chi\in\hat{G}-\{\hat{e}\}$ with $|\lambda_\chi|=1$. Since each of $\chi(g_1),\dots,\chi(g_k)$ is a complex number of norm 1, the triangle inequality forces them all to be equal. Since $\chi(g_1) = \chi(e) = 1$, $\chi$ must map each of $g_1,\dots,g_k$ to 1, but this is impossible because $\chi$ is a nontrivial character and $g_1,\dots,g_k$ form a set of generators of $G$. This contradiction yields $b<1$.

Since $v = \frac{1}{n}\sum_{\chi\in\hat{G}} v_\chi$ and $Mv_\chi = \lambda_\chi v_\chi$, we have

$$M^m v - \frac{1}{n}v_{\hat{e}} = \frac{1}{n}\sum_{\chi\in\hat{G}-\{\hat{e}\}}\lambda_\chi^m v_\chi.$$

Since the vectors $v_\chi$ are pairwise orthogonal, the limit we are interested in can be written as

$$\lim_{m\to\infty}\frac{1}{b^{2m}}(M^m v - \frac{1}{n}v_{\hat{e}})\cdot(M^m v - \frac{1}{n}v_{\hat{e}}).$$

and then rewritten as

$$\lim_{m\to\infty}\frac{1}{b^{2m}}\sum_{\chi\in\hat{G}-\{\hat{e}\}}|\lambda_\chi|^{2m} = \#\{\chi\in\hat{G} : |\lambda_\chi| = b\}.$$

By construction, this last quantity is nonzero and finite.

**Remark.** It is easy to see that the result fails if we do not assume $g_1 = e$: take $G = \mathbb{Z}/2\mathbb{Z}$, $n=1$, and $g_1 = 1$.

**Remark.** Harm Derksen points out that a similar argument applies even if $G$ is not assumed to be abelian, provided that the operator $g_1+\cdots+g_k$ in the group algebra $\mathbb{Z}[G]$ is *normal*, i.e., it commutes with the operator $g_1^{-1}+\cdots+g_k^{-1}$. This includes the cases where the set $\{g_1,\dots,g_k\}$ is closed under taking inverses and where it is a union of conjugacy classes (which in turn includes the case of $G$ abelian).

**Remark**. The matrix $M$ used above has nonnegative entries with row sums equal to 1 (i.e., it corresponds to a Markov chain), and there exists a positive integer $m$ such that $M^m$ has positive entries. For any such matrix, the Perron-Frobenius theorem implies that the sequence of vectors $M^m v$ converges to a limit $w$, and there exists $b\in[0,1)$ such that

$$\limsup_{m\to\infty}\frac{1}{b^{2m}}\sum_{i=1}^n((M^m v - w)_i)^2$$

is nonzero and finite. (The intended interpretation in case $b=0$ is that $M^m v = w$ for all large $m$.) However, the limit need not exist in general.

B1 Since the rational numbers are dense in the reals, we can find positive integers $a,b$ such that

$$\frac{3\varepsilon}{hk} < \frac{b}{a} < \frac{4\varepsilon}{hk}.$$

By multiplying $a$ and $b$ by a suitably large positive integer, we can also ensure that $3a^2 > b$. We then have

$$\frac{\varepsilon}{hk} < \frac{b}{3a} < \frac{b}{\sqrt{a^2+b}+a} = \sqrt{a^2+b}-a$$

and

$$\sqrt{a^2+b}-a = \frac{b}{\sqrt{a^2+b}+a} \leq \frac{b}{2a} < 2\frac{\varepsilon}{hk}.$$

We may then take $m = k^2(a^2+b), n = h^2a^2$.

B2 Only the primes 2 and 5 appear seven or more times. The fact that these primes appear is demonstrated by the examples

$$(2,5,2),(2,5,3),(2,7,5),(2,11,5)$$

and their reversals.

It remains to show that if either $\ell = 3$ or $\ell$ is a prime greater than 5, then $\ell$ occurs at most six times as an element of a triple in $S$. Note that $(p,q,r) \in S$ if and only if $q^2 - 4pr = a^2$ for some integer $a$; in particular, since $4pr \geq 16$, this forces $q \geq 5$. In particular, $q$ is odd, as then is $a$, and so $q^2 \equiv a^2 \equiv 1 \pmod 8$; consequently, one of $p,r$ must equal 2. If $r = 2$, then $8p = q^2 - a^2 = (q+a)(q-a)$; since both factors are of the same sign and their sum is the positive number $2q$, both factors are positive. Since they are also both even, we have $q+a \in \{2,4,2p,4p\}$ and so $q \in \{2p+1, p+2\}$. Similarly, if $p = 2$, then $q \in \{2r+1, r+2\}$. Consequently, $\ell$ occurs at most twice as many times as there are prime numbers in the list

$$2\ell+1, \ell+2, \frac{\ell-1}{2}, \ell-2.$$

For $\ell = 3, \ell-2 = 1$ is not prime. For $\ell \geq 7$, the numbers $\ell-2, \ell, \ell+2$ cannot all be prime, since one of them is always a nontrivial multiple of 3.

**Remark.** The above argument shows that the cases listed for 5 are the only ones that can occur. By contrast, there are infinitely many cases where 2 occurs if either the twin prime conjecture holds or there are infinitely many Sophie Germain primes (both of which are expected to be true).

B3 Yes, it follows that $f$ is differentiable.

**First solution.** Note first that at 0, $f/g$ and $g$ are both continuous, as then is their product $f$. If $f(0) \neq 0$, then in some neighborhood of 0, $f$ is either always positive or always negative. We can thus choose $\varepsilon \in \{\pm 1\}$ so that $\varepsilon f$ is the composition of the differentiable function $(fg)\cdot(f/g)$ with the square root function. By the chain rule, $f$ is differentiable at 0.

If $f(0) = 0$, then $(f/g)(0) = 0$, so we have

$$(f/g)'(0) = \lim_{x\to 0} \frac{f(x)}{xg(x)}.$$

Since $g$ is continuous at 0, we may multiply limits to deduce that $\lim_{x\to 0} f(x)/x$ exists.

**Second solution.** Choose a neighborhood $N$ of 0 on which $g(x) \neq 0$. Define the following functions on $N \setminus \{0\}$: $h_1(x) = \frac{f(x)g(x)-f(0)g(0)}{x}$; $h_2(x) = \frac{f(x)g(0)-f(0)g(x)}{xg(0)g(x)}$; $h_3(x) = g(0)g(x)$; $h_4(x) = \frac{1}{g(x)+g(0)}$. Then by assumption, $h_1,h_2,h_3,h_4$ all have limits as $x \to 0$. On the other hand,

$$\frac{f(x)-f(0)}{x} = (h_1(x)+h_2(x)h_3(x))h_4(x),$$

and it follows that $\lim_{x\to 0} \frac{f(x)-f(0)}{x}$ exists, as desired.

B4 Number the games $1,\dots,2011$, and let $A = (a_{jk})$ be the $2011 \times 2011$ matrix whose $jk$ entry is 1 if player $k$ wins game $j$ and $i = \sqrt{-1}$ if player $k$ loses game $j$. Then $\overline{a_{hj}}a_{jk}$ is 1 if players $h$ and $k$ tie in game $j$; $i$ if player $h$ wins and player $k$ loses in game $j$; and $-i$ if $h$ loses and $k$ wins. It follows that $T + iW = \overline{A}^T A$.

Now the determinant of $A$ is unchanged if we subtract the first row of $A$ from each of the other rows, producing a matrix whose rows, besides the first one, are $(1-i)$ times a row of integers. Thus we can write $\det A = (1-i)^{2010}(a+bi)$ for some integers $a,b$. But then $\det(T+iW) = \det(\overline{A}^T A) = 2^{2010}(a^2+b^2)$ is a nonnegative integer multiple of $2^{2010}$, as desired.

B5 Define the function

$$f(y) = \int_{-\infty}^{\infty} \frac{dx}{(1+x^2)(1+(x+y)^2)}.$$

For $y \geq 0$, in the range $-1 \leq x \leq 0$, we have

$$\begin{aligned}(1+x^2)(1+(x+y)^2) &\leq (1+1)(1+(1+y)^2) = 2y^2+4y+4 \\ &\leq 2y^2+4+2(y^2+1) \leq 6+6y^2.\end{aligned}$$

We thus have the lower bound

$$f(y) \geq \frac{1}{6(1+y^2)};$$

the same bound is valid for $y \leq 0$ because $f(y) = f(-y)$.

The original hypothesis can be written as

$$\sum_{i,j=1}^{n} f(a_i - a_j) \leq An$$

and thus implies that

$$\sum_{i,j=1}^{n} \frac{1}{1+(a_i-a_j)^2} \leq 6An.$$

By the Cauchy-Schwarz inequality, this implies

$$\sum_{i,j=1}^{n}(1+(a_i-a_j)^2)\geq Bn^3$$

for $B=1/(6A)$.

**Remark.** One can also compute explicitly (using partial fractions, Fourier transforms, or contour integration) that $f(y)=\frac{2\pi}{4+y^2}$.

**Remark.** Praveen Venkataramana points out that the lower bound can be improved to $Bn^4$ as follows. For each $z\in\mathbb{Z}$, put $Q_{z,n}=\{i\in\{1,\ldots,n\}:a_i\in[z,z+1)\}$ and $q_{z,n}=\#Q_{z,n}$. Then $\sum_z q_{z,n}=n$ and

$$6An\geq\sum_{i,j=1}^{n}\frac{1}{1+(a_i-a_j)^2}\geq\sum_{z\in\mathbb{Z}}\frac{1}{2}q_{z,n}^2.$$

If exactly $k$ of the $q_{z,n}$ are nonzero, then $\sum_{z\in\mathbb{Z}}q_{z,n}^2\geq n^2/k$ by Jensen's inequality (or various other methods), so we must have $k\geq n/(6A)$. Then

$$\begin{aligned}\sum_{i,j=1}^{n}(1+(a_i-a_j)^2)&\geq n^2+\sum_{i,j=1}^{k}\max\{0,(|i-j|-1)^2\}\\&\geq n^2+\frac{k^4}{6}-\frac{2k^3}{3}+\frac{5k^2}{6}-\frac{k}{3}.\end{aligned}$$

This is bounded below by $Bn^4$ for some $B>0$.

In the opposite direction, one can weaken the initial upper bound to $An^{4/3}$ and still derive a lower bound of $Bn^3$. The argument is similar.

B6 In order to interpret the problem statement, one must choose a convention for the value of $0^0$; we will take it to equal 1. (If one takes $0^0$ to be 0, then the problem fails for $p=3$.)

**First solution.** By Wilson's theorem,

$$k!(p-1-k)!\equiv(-1)^k(p-1)!\equiv(-1)^{k+1}\pmod{p},$$

so we have a congruence of Laurent polynomials

$$\begin{aligned}\sum_{k=0}^{p-1}k!x^k&\equiv\sum_{k=0}^{p-1}\frac{(-1)^{k+1}x^k}{(p-1-k)!}\pmod{p}\\&\equiv -x^{p-1}\sum_{k=0}^{p-1}\frac{(-x)^{-k}}{k!}\pmod{p}.\end{aligned}$$

Replacing $x$ with $-1/x$, we reduce the original problem to showing that the polynomial

$$g(x)=\sum_{k=0}^{p-1}\frac{x^k}{k!}$$

over $\mathbb{F}_p$ has at most $(p-1)/2$ nonzero roots in $\mathbb{F}_p$. To see this, write

$$h(x)=x^p-x+g(x)$$

and note that by Wilson's theorem again,

$$h'(x)=1+\sum_{k=1}^{p-1}\frac{x^{k-1}}{(k-1)!}=x^{p-1}-1+g(x).$$

If $z\in\mathbb{F}_p$ is such that $g(z)=0$, then $z\neq 0$ because $g(0)=1$. Therefore, $z^{p-1}=1$, so $h(z)=h'(z)=0$ and so $z$ is at least a double root of $h$. Since $h$ is a polynomial of degree $p$, there can be at most $(p-1)/2$ zeroes of $g$ in $\mathbb{F}_p$, as desired.

**Second solution.** (By Noam Elkies) Define the polynomial $f$ over $\mathbb{F}_p$ by

$$f(x)=\sum_{k=0}^{p-1}k!x^k.$$

Put $t=(p-1)/2$; the problem statement is that $f$ has at most $t$ roots modulo $p$. Suppose the contrary; since $f(0)=1$, this means that $f(x)$ is nonzero for at most $t-1$ values of $x\in\mathbb{F}_p^*$. Denote these values by $x_1,\ldots,x_m$, where by assumption $m<t$, and define the polynomial $Q$ over $\mathbb{F}_p$ by

$$Q(x)=\prod_{k=1}^{m}(x-x_m)=\sum_{k=0}^{t-1}Q_kx^k.$$

Then we can write

$$f(x)=\frac{P(x)}{Q(x)}(1-x^{p-1})$$

where $P(x)$ is some polynomial of degree at most $m$. This means that the power series expansions of $f(x)$ and $P(x)/Q(x)$ coincide modulo $x^{p-1}$, so the coefficients of $x^t,\ldots,x^{2t-1}$ in $f(x)Q(x)$ vanish. In other words, the product of the square matrix

$$A=((i+j+1)!)_{i,j=0}^{t-1}$$

with the nonzero column vector $(Q_{t-1},\ldots,Q_0)$ is zero. However, by the following lemma, $\det(A)$ is nonzero modulo $p$, a contradiction.

**Lemma 1.** *For any nonnegative integer $m$ and any integer $n$,*

$$\det((i+j+n)!)_{i,j=0}^{m}=\prod_{k=0}^{m}k!(k+n)!.$$

*Proof.* Define the $(m+1)\times(m+1)$ matrix $A_{m,n}$ by $(A_{m,n})_{i,j}=\binom{i+j+n}{i}$; the desired result is then that $\det(A_{m,n})=1$. Note that

$$(A_{m,n-1})_{ij}=\begin{cases}(A_{m,n})_{ij} & i=0\\(A_{m,n})_{ij}-(A_{m,n})_{(i-1)j} & i>0;\end{cases}$$

that is, $A_{m,n-1}$ can be obtained from $A_{m,n}$ by elementary row operations. Therefore, $\det(A_{m,n})=\det(A_{m,n-1})$, so $\det(A_{m,n})$ depends only on $m$. The claim now follows by observing that $A_{0,0}$ is the $1\times 1$ matrix with entry 1 and that $A_{m,-1}$ has the block representation $\begin{pmatrix}1 & *\\0 & A_{m-1,0}\end{pmatrix}$. $\square$

**Remark.** Elkies has given a more detailed discussion of the origins of this solution in the theory of orthogonal polynomials; see `http://mathoverflow.net/questions/82648`.

# The 73rd William Lowell Putnam Mathematical Competition
## Saturday, December 1, 2012

A1 Let $d_1, d_2, \dots, d_{12}$ be real numbers in the open interval $(1, 12)$. Show that there exist distinct indices $i, j, k$ such that $d_i, d_j, d_k$ are the side lengths of an acute triangle.

A2 Let $*$ be a commutative and associative binary operation on a set $S$. Assume that for every $x$ and $y$ in $S$, there exists $z$ in $S$ such that $x * z = y$. (This $z$ may depend on $x$ and $y$.) Show that if $a, b, c$ are in $S$ and $a * c = b * c$, then $a = b$.

A3 Let $f : [-1, 1] \to \mathbb{R}$ be a continuous function such that

(i) $f(x) = \frac{2-x^2}{2} f\left(\frac{x^2}{2-x^2}\right)$ for every $x$ in $[-1, 1]$,

(ii) $f(0) = 1$, and

(iii) $\lim_{x \to 1^-} \frac{f(x)}{\sqrt{1-x}}$ exists and is finite.

Prove that $f$ is unique, and express $f(x)$ in closed form.

A4 Let $q$ and $r$ be integers with $q > 0$, and let $A$ and $B$ be intervals on the real line. Let $T$ be the set of all $b + mq$ where $b$ and $m$ are integers with $b$ in $B$, and let $S$ be the set of all integers $a$ in $A$ such that $ra$ is in $T$. Show that if the product of the lengths of $A$ and $B$ is less than $q$, then $S$ is the intersection of $A$ with some arithmetic progression.

A5 Let $\mathbb{F}_p$ denote the field of integers modulo a prime $p$, and let $n$ be a positive integer. Let $v$ be a fixed vector in $\mathbb{F}_p^n$, let $M$ be an $n \times n$ matrix with entries of $\mathbb{F}_p$, and define $G : \mathbb{F}_p^n \to \mathbb{F}_p^n$ by $G(x) = v + Mx$. Let $G^{(k)}$ denote the $k$-fold composition of $G$ with itself, that is, $G^{(1)}(x) = G(x)$ and $G^{(k+1)}(x) = G(G^{(k)}(x))$. Determine all pairs $p, n$ for which there exist $v$ and $M$ such that the $p^n$ vectors $G^{(k)}(0)$, $k = 1, 2, \dots, p^n$ are distinct.

A6 Let $f(x, y)$ be a continuous, real-valued function on $\mathbb{R}^2$. Suppose that, for every rectangular region $R$ of area 1, the double integral of $f(x, y)$ over $R$ equals 0. Must $f(x, y)$ be identically 0?

B1 Let $S$ be a class of functions from $[0, \infty)$ to $[0, \infty)$ that satisfies:

(i) The functions $f_1(x) = e^x - 1$ and $f_2(x) = \ln(x + 1)$ are in $S$;

(ii) If $f(x)$ and $g(x)$ are in $S$, the functions $f(x) + g(x)$ and $f(g(x))$ are in $S$;

(iii) If $f(x)$ and $g(x)$ are in $S$ and $f(x) \geq g(x)$ for all $x \geq 0$, then the function $f(x) - g(x)$ is in $S$.

Prove that if $f(x)$ and $g(x)$ are in $S$, then the function $f(x)g(x)$ is also in $S$.

B2 Let $P$ be a given (non-degenerate) polyhedron. Prove that there is a constant $c(P) > 0$ with the following property: If a collection of $n$ balls whose volumes sum to $V$ contains the entire surface of $P$, then $n > c(P)/V^2$.

B3 A round-robin tournament of $2n$ teams lasted for $2n - 1$ days, as follows. On each day, every team played one game against another team, with one team winning and one team losing in each of the $n$ games. Over the course of the tournament, each team played every other team exactly once. Can one necessarily choose one winning team from each day without choosing any team more than once?

B4 Suppose that $a_0 = 1$ and that $a_{n+1} = a_n + e^{-a_n}$ for $n = 0, 1, 2, \dots$. Does $a_n - \log n$ have a finite limit as $n \to \infty$? (Here $\log n = \log_e n = \ln n$.)

B5 Prove that, for any two bounded functions $g_1, g_2 : \mathbb{R} \to [1, \infty)$, there exist functions $h_1, h_2 : \mathbb{R} \to \mathbb{R}$ such that, for every $x \in \mathbb{R}$,

$$\sup_{s \in \mathbb{R}} (g_1(s)^x g_2(s)) = \max_{t \in \mathbb{R}} (x h_1(t) + h_2(t)).$$

B6 Let $p$ be an odd prime number such that $p \equiv 2 \pmod 3$. Define a permutation $\pi$ of the residue classes modulo $p$ by $\pi(x) \equiv x^3 \pmod p$. Show that $\pi$ is an even permutation if and only if $p \equiv 3 \pmod 4$.

# Solutions to the 73rd William Lowell Putnam Mathematical Competition
# Saturday, December 1, 2012

Kiran Kedlaya and Lenny Ng

A1 Without loss of generality, assume $d_1 \leq d_2 \leq \cdots \leq d_{12}$. If $d_{i+2}^2 < d_i^2 + d_{i+1}^2$ for some $i \leq 10$, then $d_i, d_{i+1}, d_{i+2}$ are the side lengths of an acute triangle, since in this case $d_i^2 < d_{i+1}^2 + d_{i+2}^2$ and $d_{i+1}^2 < d_i^2 + d_{i+2}^2$ as well. Thus we may assume $d_{i+2}^2 \geq d_i^2 + d_{i+1}^2$ for all $i$. But then by induction, $d_i^2 \geq F_i d_1^2$ for all $i$, where $F_i$ is the $i$-th Fibonacci number (with $F_1 = F_2 = 1$): $i = 1$ is clear, $i = 2$ follows from $d_2 \geq d_1$, and the induction step follows from the assumed inequality. Setting $i = 12$ now gives $d_{12}^2 \geq 144 d_1^2$, contradicting $d_1 > 1$ and $d_{12} < 12$.

**Remark.** A materially equivalent problem appeared on the 2012 USA Mathematical Olympiad and USA Junior Mathematical Olympiad.

A2 Write $d$ for $a * c = b * c \in S$. For some $e \in S$, $d * e = a$, and thus for $f = c * e$, $a * f = a * c * e = d * e = a$ and $b * f = b * c * e = d * e = a$. Let $g \in S$ satisfy $g * a = b$; then $b = g * a = g * (a * f) = (g * a) * f = b * f = a$, as desired.

**Remark.** With slightly more work, one can show that $S$ forms an abelian group with the operation $*$.

A3 We will prove that $f(x) = \sqrt{1 - x^2}$ for all $x \in [-1, 1]$. Define $g : (-1, 1) \to \mathbb{R}$ by $g(x) = f(x)/\sqrt{1 - x^2}$. Plugging $f(x) = g(x)\sqrt{1 - x^2}$ into equation (i) and simplifying yields

$$g(x) = g\left(\frac{x^2}{2 - x^2}\right) \tag{1}$$

for all $x \in (-1, 1)$. Now fix $x \in (-1, 1)$ and define a sequence $\{a_n\}_{n=1}^{\infty}$ by $a_1 = x$ and $a_{n+1} = \frac{a_n^2}{2 - a_n^2}$. Then $a_n \in (-1, 1)$ and thus $|a_{n+1}| \leq |a_n|^2$ for all $n$. It follows that $\{|a_n|\}$ is a decreasing sequence with $|a_n| \leq |x|^n$ for all $n$, and so $\lim_{n \to \infty} a_n = 0$. Since $g(a_n) = g(x)$ for all $n$ by (1) and $g$ is continuous at 0, we conclude that $g(x) = g(0) = f(0) = 1$. This holds for all $x \in (-1, 1)$ and thus for $x = \pm 1$ as well by continuity. The result follows.

**Remark.** As pointed out by Noam Elkies, condition (iii) is unnecessary. However, one can use it to derive a slightly different solution by running the recursion in the opposite direction.

A4 We begin with an easy lemma.

**Lemma.** *Let $S$ be a finite set of integers with the following property: for all $a, b, c \in S$ with $a \leq b \leq c$, we also have $a + c - b \in S$. Then $S$ is an arithmetic progression.*

*Proof.* We may assume $\#S \geq 3$, as otherwise $S$ is trivially an arithmetic progression. Let $a_1, a_2$ be the smallest and second-smallest elements of $S$, respectively, and put $d = a_2 - a_1$. Let $m$ be the smallest positive integer such that $a_1 + md \notin S$. Suppose that there exists an integer $n$ contained in $S$ but not in $\{a_1, a_1 + d, \ldots, a_1 + (m-1)d\}$, and choose the least such $n$. By the hypothesis applied with $(a, b, c) = (a_1, a_2, n)$, we see that $n - d$ also has the property, a contradiction. $\square$

We now return to the original problem. By dividing $B, q, r$ by $\gcd(q, r)$ if necessary, we may reduce to the case where $\gcd(q, r) = 1$. We may assume $\#S \geq 3$, as otherwise $S$ is trivially an arithmetic progression. Let $a_1, a_2, a_3$ be any three distinct elements of $S$, labeled so that $a_1 < a_2 < a_3$, and write $ra_i = b_i + m_i q$ with $b_i, m_i \in \mathbb{Z}$ and $b_i \in B$. Note that $b_1, b_2, b_3$ must also be distinct, so the differences $b_2 - b_1, b_3 - b_1, b_3 - b_2$ are all nonzero; consequently, two of them have the same sign. If $b_i - b_j$ and $b_k - b_l$ have the same sign, then we must have

$$(a_i - a_j)(b_k - b_l) = (b_i - b_j)(a_k - a_l)$$

because both sides are of the same sign, of absolute value less than $q$, and congruent to each other modulo $q$. In other words, the points $(a_1, b_1), (a_2, b_2), (a_3, b_3)$ in $\mathbb{R}^2$ are collinear. It follows that $a_4 = a_1 + a_3 - a_2$ also belongs to $S$ (by taking $b_4 = b_1 + b_3 - b_2$), so $S$ satisfies the conditions of the lemma. It is therefore an arithmetic progression.

**Reinterpretations.** One can also interpret this argument geometrically using cross products (suggested by Noam Elkies), or directly in terms of congruences (suggested by Karl Mahlburg).

**Remark.** The problem phrasing is somewhat confusing: to say that "$S$ is the intersection of [the interval] $A$ with an arithmetic progression" is the same thing as saying that "$S$ is the empty set or an arithmetic progression" unless it is implied that arithmetic progressions are necessarily infinite. Under that interpretation, however, the problem becomes false; for instance, for

$$q = 5, r = 1, A = [1, 3], B = [0, 2],$$

we have

$$T = \{\cdots, 0, 1, 2, 5, 6, 7, \ldots\}, S = \{1, 2\}.$$

A5 The pairs $(p, n)$ with the specified property are those pairs with $n = 1$, together with the single pair $(2, 2)$. We first check that these do work. For $n = 1$, it is clear that taking $v = (1)$ and $M = (0)$ has the desired effect.

For $(p,n)=(2,2)$, we take $v=\begin{pmatrix}0 & 1\end{pmatrix}$ and $M=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and then observe that

$$G^{(k)}(0)=\begin{pmatrix}0\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix}, k=0,1,2,3.$$

We next check that no other pairs work, keeping in mind that the desired condition means that $G$ acts on $\mathbb{F}_p^n$ as a cyclic permutation. Assume by way of contradiction that $(p,n)$ has the desired property but does not appear in our list. In particular, we have $n\geq 2$.

Let $I$ be the $n\times n$ identity matrix over $\mathbb{F}_p$. Decompose $\mathbb{F}_p^n$ as a direct sum of two subspaces $V,W$ such that $M-I$ is nilpotent on $V$ and invertible on $W$. Suppose that $W\neq 0$. Split $v$ as $v_1+v_2$ with $v_1\in V$, $v_2\in W$. Since $M-I$ is invertible on $W$, there exists a unique $w\in W$ such that $(M-I)w=-v_2$. Then $G^{(k)}(w)-w\in V$ for all nonnegative integers $k$. Let $k$ be the least positive integer such that $G^{(k)}(w)=w$; then $k$ is at most the cardinality of $V$, which is strictly less than $p^n$ because $W\neq 0$. This gives a contradiction and thus forces $W=0$.

In other words, the matrix $N=M-I$ is nilpotent; consequently, $N^n=0$. For any positive integer $k$, we have

$$\begin{aligned}G^{(k)}(0)&=v+Mv+\cdots+M^{k-1}v\\&=\sum_{j=0}^{k-1}\sum_{i=0}^{n-1}\binom{j}{i}N^iv\\&=\sum_{i=0}^{n-1}\binom{k}{i+1}N^iv.\end{aligned}$$

If $n\geq 2$ and $(p,n)\neq(2,2)$, then $p^{n-1}>n$ and so $G^k(0)=0$ for $k=p^{n-1}$ (because all of the binomial coefficients are divisible by $p$). This contradiction completes the proof.

A6 **First solution.** Yes, $f(x,y)$ must be identically 0. We proceed using a series of lemmas.

**Lemma 1.** *Let $R$ be a rectangular region of area 1 with corners $A,B,C,D$ labeled in counterclockwise order. Then $f(A)+f(C)=f(B)+f(D)$.*

*Proof.* We may choose coordinates so that for some $c>0$,

$$A=(0,0),B=(c,0),C=(c,1/c),D=(0,1/c).$$

Define the functions

$$\begin{aligned}g(x,y)&=\int_x^{x+c}f(t,y)\,dt\\h(x,y)&=\int_0^y g(x,u)\,du.\end{aligned}$$

For any $x,y\in\mathbb{R}$,

$$h(x,y+1/c)-h(x,y)=\int_x^{x+c}\int_y^{y+1/c}f(t,u)\,dt\,du=0$$

by hypothesis, so $h(x,y+1/c)=h(x,y)$. By the fundamental theorem of calculus, we may differentiate both sides of this identity with respect to $y$ to deduce that $g(x,y+1/c)=g(x,y)$. Differentiating this new identity with respect to $x$ yields the desired equality. $\square$

**Lemma 2.** *Let $C$ be a circle whose diameter $d$ is at least $\sqrt{2}$, and let $AB$ and $A'B'$ be two diameters of $C$. Then $f(A)+f(B)=f(A')+f(B')$.*

*Proof.* By continuity, it suffices to check the case where $\alpha=\arcsin\frac{2}{d^2}$ is an irrational multiple of $2\pi$. Let $\beta$ be the radian measure of the counterclockwise arc from $A$ to $A'$. By Lemma 1, the claim holds when $\beta=\alpha$. By induction, the claim also holds when $\beta\equiv n\alpha \pmod{2\pi}$ for any positive integer $n$. Since $\alpha$ is an irrational multiple of $2\pi$, the positive multiples of $\alpha$ fill out a dense subset of the real numbers modulo $2\pi$, so by continuity the claim holds for all $\beta$. $\square$

**Lemma 3.** *Let $R$ be a rectangular region of arbitrary (positive) area with corners $A,B,C,D$ labeled in counterclockwise order. Then $f(A)+f(C)=f(B)+f(D)$.*

*Proof.* Let $EF$ be a segment such that $AEFD$ and $BEFC$ are rectangles whose diagonals have length at least $\sqrt{2}$. By Lemma 2,

$$\begin{aligned}f(A)+f(F)&=f(D)+f(E)\\f(C)+f(E)&=f(B)+f(F),\end{aligned}$$

yielding the claim. $\square$

**Lemma 4.** *The restriction of $f$ to any straight line is constant.*

*Proof.* We may choose coordinates so that the line in question is the $x$-axis. Define the function $g(y)$ by

$$g(y)=f(0,y)-f(0,0).$$

By Lemma 3, for all $x\in\mathbb{R}$,

$$f(x,y)=f(x,0)+g(y).$$

For any $c>0$, by the original hypothesis we have

$$\begin{aligned}0&=\int_x^{x+c}\int_y^{y+1/c}f(u,v)\,du\,dv\\&=\int_x^{x+c}\int_y^{y+1/c}(f(u,0)+g(v))\,du\,dv\\&=\frac{1}{c}\int_x^{x+c}f(u,0)\,du+c\int_y^{y+1/c}g(v)\,dv.\end{aligned}$$

In particular, the function $F(x)=\int_x^{x+c}f(u,0)\,du$ is constant. By the fundamental theorem of calculus, we may differentiate to conclude that $f(x+c,0)=f(x,0)$ for all $x\in\mathbb{R}$. Since $c$ was also arbitrary, we deduce the claim. $\square$

To complete the proof, note that since any two points in $\mathbb{R}^2$ are joined by a straight line, Lemma 4 implies that $f$ is constant. This constant equals the integral of $f$ over any rectangular region of area 1, and hence must be 0 as desired.

**Second solution** (by Eric Larson, communicated by Noam Elkies). In this solution, we fix coordinates and assume only that the double integral vanishes on each rectangular region of area 1 with sides parallel to the coordinate axes, and still conclude that $f$ must be identically 0.

**Lemma.** *Let $R$ be a rectangular region of area 1 with sides parallel to the coordinate axes. Then the averages of $f$ over any two adjacent sides of $R$ are equal.*

*Proof.* Without loss of generality, we may take $R$ to have corners $(0,0),(c,0),(c,1/c),(0,1/c)$ and consider the two sides adjacent to $(c,1/c)$. Differentiate the equality

$$0=\int_x^{x+c}\int_y^{y+1/c} f(u,v)\,du\,dv$$

with respect to $c$ to obtain

$$0=\int_y^{y+1/c} f(x+c,v)\,dv-\frac{1}{c^2}\int_x^{x+c} f(u,y+1/c)\,du.$$

Rearranging yields

$$c\int_y^{y+1/c} f(x+c,v)\,dv=\frac{1}{c}\int_x^{x+c} f(u,y+1/c)\,du,$$

which asserts the desired result. □

Returning to the original problem, given any $c>0$, we can tile the plane with rectangles of area 1 whose vertices lie in the lattice $\{(mc,n/c): m,n\in\mathbb{Z}\}$. By repeated application of the lemma, we deduce that for any positive integer $n$,

$$\int_0^c f(u,0)\,du=\int_{nc}^{(n+1)c} f(u,0)\,du.$$

Replacing $c$ with $c/n$, we obtain

$$\int_0^{c/n} f(u,0)\,du=\int_c^{c+1/n} f(u,0)\,du.$$

Fixing $c$ and taking the limit as $n\to\infty$ yields $f(0,0)=f(c,0)$. By similar reasoning, $f$ is constant on any horizontal line and on any vertical line, and as in the first solution the constant value is forced to equal 0.

**Third solution.** (by Sergei Artamoshin) We retain the weaker hypothesis of the second solution. Assume by way of contradiction that $f$ is not identically zero.

We first exhibit a vertical segment $PQ$ with $f(P)>0$ and $f(Q)<0$. It cannot be the case that $f(P)\le 0$ for all $P$, as otherwise the vanishing of the zero over any rectangle would force $f$ to vanish identically. By continuity, there must exist an open disc $U$ such that $f(P)>0$ for all $P\in U$. Choose a rectangle $R$ of area 1 with sides parallel to the coordinate axes with one horizontal edge contained in $U$. Since the integral of $f$ over $R$ is zero, there must exist a point $Q\in R$ such that $f(Q)<0$. Take $P$ to be the vertical projection of $Q$ onto the edge of $R$ contained in $U$.

By translating coordinates, we may assume that $P=(0,0)$ and $Q=(0,a)$ for some $a>0$. For $s$ sufficiently small, $f$ is positive on the square of side length $2s$ centered at $P$, which we call $S$, and negative on the square of side length $2s$ centered at $Q$, which we call $S'$. Since the ratio $2s/(1-4s^2)$ tends to 0 as $s$ does, we can choose $s$ so that $2s/(1-4s^2)=a/n$ for some positive integer $n$.

For $i\in\mathbb{Z}$, let $A_i$ be the rectangle

$$\Big\{(x,y): s\le x\le s+\frac{1-4s^2}{2s},\quad -s+i\frac{2s}{1-4s^2}\le y\le s+i\frac{2s}{1-4s^2}\Big\}$$

and let $B_i$ be the rectangle

$$\Big\{(x,y): s\le x\le s+\frac{1-4s^2}{2s},\quad s+i\frac{2s}{1-4s^2}\le y\le -s+(i+1)\frac{2s}{1-4s^2}\Big\}.$$

Then for all $i\in\mathbb{Z}$,

$$S\cup A_0, A_n\cup S', A_i\cup B_i, B_i\cup A_{i+1}$$

are all rectangles of area 1 with sides parallel to the coordinate axes, so the integral over $f$ over each of these rectangles is zero. Since the integral over $S$ is positive, the integral over $A_0$ must be negative; by induction, for all $i\in\mathbb{Z}$ the integral over $A_i$ is negative and the integral over $B_i$ is positive. But this forces the integral over $S'$ to be positive whereas $f$ is negative everywhere on $S'$, a contradiction.

B1 Each of the following functions belongs to $S$ for the reasons indicated.

| | |
|---|---|
| $f(x),g(x)$ | given |
| $\ln(x+1)$ | (i) |
| $\ln(f(x)+1),\ln(g(x)+1)$ | (ii) plus two previous lines |
| $\ln(f(x)+1)+\ln(g(x)+1)$ | (ii) |
| $e^x-1$ | (i) |
| $(f(x)+1)(g(x)+1)-1$ | (ii) plus two previous lines |
| $f(x)g(x)+f(x)+g(x)$ | previous line |
| $f(x)+g(x)$ | (ii) plus first line |
| $f(x)g(x)$ | (iii) plus two previous lines |

B2 Fix a face $F$ of the polyhedron with area $A$. Suppose $F$ is completely covered by balls of radii $r_1,\dots,r_n$ whose volumes sum to $V$. Then on one hand,

$$\sum_{i=1}^{n} \frac{4}{3}\pi r_i^3 = V.$$

On the other hand, the intersection of a ball of radius $r$ with the plane containing $F$ is a disc of radius at most $r$, which covers a piece of $F$ of area at most $\pi r^2$; therefore

$$\sum_{i=1}^{n} \pi r_i^2 \geq A.$$

By writing $n$ as $\sum_{i=1}^{n} 1$ and applying Hölder's inequality, we obtain

$$nV^2 \geq \left(\sum_{i=1}^{n}\left(\frac{4}{3}\pi r_i^3\right)^{2/3}\right)^3 \geq \frac{16}{9\pi}A^3.$$

Consequently, any value of $c(P)$ less than $\frac{16}{9\pi}A^3$ works.

B3 The answer is yes. We first note that for any collection of $m$ days with $1 \leq m \leq 2n-1$, there are at least $m$ distinct teams that won a game on at least one of those days. If not, then any of the teams that lost games on all of those days must in particular have lost to $m$ other teams, a contradiction.

If we now construct a bipartite graph whose vertices are the $2n$ teams and the $2n-1$ days, with an edge linking a day to a team if that team won their game on that day, then any collection of $m$ days is connected to a total of at least $m$ teams. It follows from Hall's Marriage Theorem that one can match the $2n-1$ days with $2n-1$ distinct teams that won on their respective days, as desired.

B4 **First solution.** We will show that the answer is yes. First note that for all $x > -1$, $e^x \geq 1+x$ and thus

$$x \geq \log(1+x). \tag{2}$$

We next claim that $a_n > \log(n+1)$ (and in particular that $a_n - \log n > 0$) for all $n$, by induction on $n$. For $n=0$ this follows from $a_0 = 1$. Now suppose that $a_n > \log(n+1)$, and define $f(x) = x + e^{-x}$, which is an increasing function in $x > 0$; then

$$\begin{aligned} a_{n+1} &= f(a_n) > f(\log(n+1)) \\ &= \log(n+1) + 1/(n+1) \geq \log(n+2), \end{aligned}$$

where the last inequality is (2) with $x = 1/(n+1)$. This completes the induction step.

It follows that $a_n - \log n$ is a decreasing function in $n$: we have

$$\begin{aligned} &(a_{n+1} - \log(n+1)) - (a_n - \log n) \\ &= e^{-a_n} + \log(n/(n+1)) \\ &< 1/(n+1) + \log(n/(n+1)) \leq 0, \end{aligned}$$

where the final inequality is (2) with $x = -1/(n+1)$. Thus $\{a_n - \log n\}_{n=0}^{\infty}$ is a decreasing sequence of positive numbers, and so it has a limit as $n \to \infty$.

**Second solution.** Put $b_n = e^{a_n}$, so that $b_{n+1} = b_n e^{1/b_n}$. In terms of the $b_n$, the problem is to prove that $b_n/n$ has a limit as $n \to \infty$; we will show that the limit is in fact equal to 1.

Expanding $e^{1/b_n}$ as a Taylor series in $1/b_n$, we have

$$b_{n+1} = b_n + 1 + R_n$$

where $0 \leq R_n \leq c/b_n$ for some absolute constant $c > 0$. By writing

$$b_n = n + e + \sum_{i=0}^{n-1} R_i,$$

we see first that $b_n \geq n + e$. We then see that

$$\begin{aligned} 0 &\leq \frac{b_n}{n} - 1 \\ &\leq \frac{e}{n} + \sum_{i=0}^{n-1} \frac{R_i}{n} \\ &\leq \frac{e}{n} + \sum_{i=0}^{n-1} \frac{c}{nb_i} \\ &\leq \frac{e}{n} + \sum_{i=0}^{n-1} \frac{c}{n(i+e)} \\ &\leq \frac{e}{n} + \frac{c\log n}{n}. \end{aligned}$$

It follows that $b_n/n \to 1$ as $n \to \infty$.

**Remark.** This problem is an example of the general principle that one can often predict the asymptotic behavior of a recursive sequence by studying solutions of a sufficiently similar-looking differential equation. In this case, we start with the equation $a_{n+1} - a_n = e^{-a_n}$, then replace $a_n$ with a function $y(x)$ and replace the difference $a_{n+1} - a_n$ with the derivative $y'(x)$ to obtain the differential equation $y' = e^{-y}$, which indeed has the solution $y = \log x$.

B5 Define the function

$$f(x) = \sup_{s\in\mathbb{R}} \{x \log g_1(s) + \log g_2(s)\}.$$

As a function of $x$, $f$ is the supremum of a collection of affine functions, so it is convex. The function $e^{f(x)}$ is then also convex, as may be checked directly from the definition: for $x_1, x_2 \in \mathbb{R}$ and $t \in [0,1]$, by the weighted AM-GM inequality

$$\begin{aligned} te^{f(x_1)} + (1-t)e^{f(x_2)} &\geq e^{tf(x_1)+(1-t)f(x_2)} \\ &\geq e^{f(tx_1+(1-t)x_2)}. \end{aligned}$$

For each $t \in \mathbb{R}$, draw a supporting line to the graph of $e^{f(x)}$ at $x = t$; it has the form $y = xh_1(t) + h_2(t)$ for some $h_1(t), h_2(t) \in \mathbb{R}$. For all $x$, we then have

$$\sup_{s\in\mathbb{R}} \{g_1(s)^x g_2(s)\} \geq xh_1(t) + h_2(t)$$

with equality for $x=t$. This proves the desired equality (including the fact that the maximum on the right side is achieved).

**Remark.** This problem demonstrates an example of *duality* for convex functions.

B6 **First solution.** Since fixed points do not affect the signature of a permutation, we may ignore the residue class of 0 and consider $\pi$ as a permutation on the nonzero residue classes modulo $p$. These form a cyclic group of order $p-1$, so the signature of $\pi$ is also the signature of multiplication by 3 as a permutation $\sigma$ of the residue classes modulo $p-1$. If we identify these classes with the integers $0,\dots,p-2$, then the signature equals the parity of the number of *inversions*: these are the pairs $(i,j)$ with $0 \leq i < j \leq p-2$ for which $\sigma(i) > \sigma(j)$. We may write

$$\sigma(i) = 3i - (p-1)\left\lfloor \frac{3i}{p-1} \right\rfloor$$

from which we see that $(i,j)$ cannot be an inversion unless $\lfloor \frac{3j}{p-1} \rfloor > \lfloor \frac{3i}{p-1} \rfloor$. In particular, we only obtain inversions when $i < 2(p-1)/3$.

If $i < (p-1)/3$, the elements $j$ of $\{0,\dots,p-2\}$ for which $(i,j)$ is an inversion correspond to the elements of $\{0,\dots,3i\}$ which are not multiples of 3, which are $2i$ in number. This contributes a total of $0+2+\cdots+2(p-2)/3 = (p-2)(p+1)/9$ inversions.

If $(p-1)/3 < i < 2(p-1)/3$, the elements $j$ of $\{0,\dots,p-2\}$ for which $(i,j)$ is an inversion correspond to the elements of $\{0,\dots,3i-p+1\}$ congruent to 1 modulo 3, which are $(3i-p+2)/3 = i-(p-2)/3$ in number. This contributes a total of $1+\cdots+(p-2)/3 = (p-2)(p+1)/18$ inversions.

Summing up, the total number of inversions is $(p-2)(p+1)/6$, which is even if and only if $p \equiv 3 \pmod 4$. This proves the claim.

**Second solution** (by Noam Elkies). Recall that the sign of $\pi$ (which is $+1$ if $\pi$ is even and $-1$ if $\pi$ is odd) can be computed as

$$\prod_{0 \leq x < y < p} \frac{\pi(x)-\pi(y)}{x-y}$$

(because composing $\pi$ with a transposition changes the sign of the product). Reducing modulo $p$, we get a congruence with

$$\prod_{0 \leq x < y < p} \frac{x^3-y^3}{x-y} = \prod_{0 \leq x < y < p} (x^2+xy+y^2).$$

It thus suffices to count the number of times each possible value of $x^2+xy+y^2$ occurs. Each nonzero value $c$ modulo $p$ occurs $p+1$ times as $x^2+xy+y^2$ with $0 \leq x,y < p$ and hence $(p+\chi(c/3))/2$ times with $0 \leq x < y < p$, where $\chi$ denotes the quadratic character modulo $p$. Since $p \equiv 2 \pmod 3$, by the law of quadratic reciprocity we have $\chi(-3) = +1$, so $\chi(c/3) = \chi(-c)$. It thus remains to evaluate the product $\prod_{c=1}^{p-1} c^{(p+\chi(-c))/2}$ modulo $p$.

If $p \equiv 3 \pmod 4$, this is easy: each factor is a quadratic residue (this is clear if $c$ is a residue, and otherwise $\chi(-c) = +1$ so $p+\chi(-c)$ is divisible by 4) and $-1$ is not, so we must get $+1$ modulo $p$.

If $p \equiv 1 \pmod 4$, we must do more work: we choose a primitive root $g$ modulo $p$ and rewrite the product as

$$\prod_{i=0}^{p-2} g^{i(p+(-1)^i)/2}.$$

The sum of the exponents, split into sums over $i$ odd and $i$ even, gives

$$\sum_{j=0}^{(p-3)/2} \left( j(p+1) + \frac{(2j+1)(p-1)}{2} \right)$$

which simplifies to

$$\frac{(p-3)(p-1)(p+1)}{8} + \frac{(p-1)^3}{8} = \frac{p-1}{2}\left(\frac{p^2-1}{2} - p\right).$$

Hence the product we are trying to evaluate is congruent to $g^{(p-1)/2} \equiv -1$ modulo $p$.

**Third solution** (by Mark van Hoeij). We compute the parity of $\pi$ as the parity of the number of cycles of even length in the cycle decomposition of $\pi$. For $x$ a nonzero residue class modulo $p$ of multiplicative order $d$, the elements of the orbit of $x$ under $\pi$ also have order $d$ (because $d$ divides $p-1$ and hence is coprime to 3). Since the group of nonzero residue classes modulo $p$ is cyclic of order $p-1$, the elements of order $d$ fall into $\varphi(d)/f(d)$ orbits under $\pi$, where $\varphi$ is the Euler phi function and $f(d)$ is the multiplicative order of 3 modulo $d$. The parity of $\pi$ is then the parity of the sum of $\varphi(d)/f(d)$ over all divisors $d$ of $p-1$ for which $f(d)$ is even.

If $d$ is odd, then $\varphi(d)/f(d) = \varphi(2d)/f(2d)$, so the summands corresponding to $d$ and $2d$ coincide. It thus suffices to consider those $d$ divisible by 4. If $p \equiv 3 \pmod 4$, then there are no such summands, so the sum is trivially even.

If $p \equiv 1 \pmod 4$, then $d=4$ contributes a summand of $\varphi(4)/f(4) = 2/2 = 1$. For each $d$ which is a larger multiple of 4, the group $(\mathbb{Z}/d\mathbb{Z})^*$ is isomorphic to the product of $\mathbb{Z}/2\mathbb{Z}$ with another group of even order, so the maximal power of 2 dividing $f(d)$ is strictly smaller than the maximal power of 2 dividing $d$. Hence $\varphi(d)/f(d)$ is even, and so the overall sum is odd.

**Remark.** Note that the second proof uses quadratic reciprocity, whereas the first and third proofs are similar to several classical proofs of quadratic reciprocity. Abhinav Kumar notes that the problem itself is a special case of the Duke-Hopkins quadratic reciprocity law for abelian groups (Quadratic reciprocity in a finite group, *Amer. Math. Monthly* **112** (2005), 251–256; see also `http://math.uga.edu/~pete/morequadrec.pdf`).

# The 74th William Lowell Putnam Mathematical Competition
# Saturday, December 7, 2013

A1 Recall that a regular icosahedron is a convex polyhedron having 12 vertices and 20 faces; the faces are congruent equilateral triangles. On each face of a regular icosahedron is written a nonnegative integer such that the sum of all 20 integers is 39. Show that there are two faces that share a vertex and have the same integer written on them.

A2 Let $S$ be the set of all positive integers that are *not* perfect squares. For $n$ in $S$, consider choices of integers $a_1, a_2, \dots, a_r$ such that $n < a_1 < a_2 < \cdots < a_r$ and $n \cdot a_1 \cdot a_2 \cdots a_r$ is a perfect square, and let $f(n)$ be the minumum of $a_r$ over all such choices. For example, $2 \cdot 3 \cdot 6$ is a perfect square, while $2 \cdot 3$, $2 \cdot 4$, $2 \cdot 5$, $2 \cdot 3 \cdot 4$, $2 \cdot 3 \cdot 5$, $2 \cdot 4 \cdot 5$, and $2 \cdot 3 \cdot 4 \cdot 5$ are not, and so $f(2) = 6$. Show that the function $f$ from $S$ to the integers is one-to-one.

A3 Suppose that the real numbers $a_0, a_1, \dots, a_n$ and $x$, with $0 < x < 1$, satisfy

$$\frac{a_0}{1-x} + \frac{a_1}{1-x^2} + \cdots + \frac{a_n}{1-x^{n+1}} = 0.$$

Prove that there exists a real number $y$ with $0 < y < 1$ such that

$$a_0 + a_1 y + \cdots + a_n y^n = 0.$$

A4 A finite collection of digits 0 and 1 is written around a circle. An *arc* of length $L \ge 0$ consists of $L$ consecutive digits around the circle. For each arc $w$, let $Z(w)$ and $N(w)$ denote the number of 0's in $w$ and the number of 1's in $w$, respectively. Assume that $|Z(w) - Z(w')| \le 1$ for any two arcs $w, w'$ of the same length. Suppose that some arcs $w_1, \dots, w_k$ have the property that

$$Z = \frac{1}{k} \sum_{j=1}^{k} Z(w_j) \text{ and } N = \frac{1}{k} \sum_{j=1}^{k} N(w_j)$$

are both integers. Prove that there exists an arc $w$ with $Z(w) = Z$ and $N(w) = N$.

A5 For $m \ge 3$, a list of $\binom{m}{3}$ real numbers $a_{ijk}$ $(1 \le i << j < k \le m)$ is said to be *area definite* for $\mathbb{R}^n$ if the inequality

$$\sum_{1 \le i < j < k \le m} a_{ijk} \cdot \text{Area}(\Delta A_i A_j A_k) \ge 0$$

holds for every choice of $m$ points $A_1, \dots, A_m$ in $\mathbb{R}^n$. For example, the list of four numbers $a_{123} = a_{124} = a_{134} = 1$, $a_{234} = -1$ is area definite for $\mathbb{R}^2$. Prove that if a list of $\binom{m}{3}$ numbers is area definite for $\mathbb{R}^2$, then it is area definite for $\mathbb{R}^3$.

A6 Define a function $w : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ as follows. For $|a|, |b| \le 2$, let $w(a,b)$ be as in the table shown; otherwise, let $w(a,b) = 0$.

| $w(a,b)$ | | $b$ | | | | |
|---|---|---|---|---|---|---|
| | | -2 | -1 | 0 | 1 | 2 |
| | -2 | -1 | -2 | 2 | -2 | -1 |
| | -1 | -2 | 4 | -4 | 4 | -2 |
| $a$ | 0 | 2 | -4 | 12 | -4 | 2 |
| | 1 | -2 | 4 | -4 | 4 | -2 |
| | 2 | -1 | -2 | 2 | -2 | -1 |

For every finite subset $S$ of $\mathbb{Z} \times \mathbb{Z}$, define

$$A(S) = \sum_{(\mathbf{s}, \mathbf{s}') \in S \times S} w(\mathbf{s} - \mathbf{s}').$$

Prove that if $S$ is any finite nonempty subset of $\mathbb{Z} \times \mathbb{Z}$, then $A(S) > 0$. (For example, if $S = \{(0,1), (0,2), (2,0), (3,1)\}$, then the terms in $A(S)$ are $12, 12, 12, 12, 4, 4, 0, 0, 0, 0, -1, -1, -2, -2, -4, -4$.)

B1 For positive integers $n$, let the numbers $c(n)$ be determined by the rules $c(1) = 1$, $c(2n) = c(n)$, and $c(2n+1) = (-1)^n c(n)$. Find the value of

$$\sum_{n=1}^{2013} c(n) c(n+2).$$

B2 Let $C = \bigcup_{N=1}^{\infty} C_N$, where $C_N$ denotes the set of those 'cosine polynomials' of the form

$$f(x) = 1 + \sum_{n=1}^{N} a_n \cos(2\pi n x)$$

for which:

(i) $f(x) \ge 0$ for all real $x$, and

(ii) $a_n = 0$ whenever $n$ is a multiple of 3.

Determine the maximum value of $f(0)$ as $f$ ranges through $C$, and prove that this maximum is attained.

B3 Let $\mathscr{P}$ be a nonempty collection of subsets of $\{1, \dots, n\}$ such that:

(i) if $S, S' \in \mathscr{P}$, then $S \cup S' \in \mathscr{P}$ and $S \cap S' \in \mathscr{P}$, and

(ii) if $S \in \mathscr{P}$ and $S \neq \emptyset$, then there is a subset $T \subset S$ such that $T \in \mathscr{P}$ and $T$ contains exactly one fewer element than $S$.

Suppose that $f : \mathscr{P} \to \mathbb{R}$ is a function such that $f(\emptyset) = 0$ and

$$f(S \cup S') = f(S) + f(S') - f(S \cap S') \text{ for all } S, S' \in \mathscr{P}.$$

Must there exist real numbers $f_1, \dots, f_n$ such that

$$f(S) = \sum_{i \in S} f_i$$

for every $S \in \mathscr{P}$?

B4 For any continuous real-valued function $f$ defined on the interval $[0,1]$, let

$$\mu(f)=\int_0^1 f(x)\,dx,\ \mathrm{Var}(f)=\int_0^1 (f(x)-\mu(f))^2\,dx,$$
$$M(f)=\max_{0\le x\le 1}|f(x)|.$$

Show that if $f$ and $g$ are continuous real-valued functions defined on the interval $[0,1]$, then

$$\mathrm{Var}(fg)\le 2\mathrm{Var}(f)M(g)^2+2\mathrm{Var}(g)M(f)^2.$$

B5 Let $X=\{1,2,\ldots,n\}$, and let $k\in X$. Show that there are exactly $k\cdot n^{n-1}$ functions $f:X\to X$ such that for every $x\in X$ there is a $j\ge 0$ such that $f^{(j)}(x)\le k$. [Here $f^{(j)}$ denotes the $j^{\text{th}}$ iterate of $f$, so that $f^{(0)}(x)=x$ and $f^{(j+1)}(x)=f(f^{(j)}(x))$.]

B6 Let $n\ge 1$ be an odd integer. Alice and Bob play the following game, taking alternating turns, with Alice playing first. The playing area consists of $n$ spaces, arranged in a line. Initially all spaces are empty. At each turn, a player either

- places a stone in an empty space, or
- removes a stone from a nonempty space $s$, places a stone in the nearest empty space to the left of $s$ (if such a space exists), and places a stone in the nearest empty space to the right of $s$ (if such a space exists).

Furthermore, a move is permitted only if the resulting position has not occurred previously in the game. A player loses if he or she is unable to move. Assuming that both players play optimally throughout the game, what moves may Alice make on her first turn?

# Solutions to the 74th William Lowell Putnam Mathematical Competition
# Saturday, December 7, 2013

Kiran Kedlaya and Lenny Ng

A1 Suppose otherwise. Then each vertex $v$ is a vertex for five faces, all of which have different labels, and so the sum of the labels of the five faces incident to $v$ is at least $0+1+2+3+4=10$. Adding this sum over all vertices $v$ gives $3\times 39=117$, since each face's label is counted three times. Since there are 12 vertices, we conclude that $10\times 12\leq 117$, contradiction.

**Remark:** One can also obtain the desired result by showing that any collection of five faces must contain two faces that share a vertex; it then follows that each label can appear at most 4 times, and so the sum of all labels is at least $4(0+1+2+3+4)=40>39$, contradiction.

A2 Suppose to the contrary that $f(n)=f(m)$ with $n<m$, and let $n\cdot a_1\cdots a_r$, $m\cdot b_1\cdots b_s$ be perfect squares where $n<a_1<\cdots<a_r$, $m<b_1<\cdots<b_s$, $a_r,b_s$ are minimal and $a_r=b_s$. Then $(n\cdot a_1\cdots a_r)\cdot(m\cdot b_1\cdots b_s)$ is also a perfect square. Now eliminate any factor in this product that appears twice (i.e., if $a_i=b_j$ for some $i,j$, then delete $a_i$ and $b_j$ from this product). The product of what remains must also be a perfect square, but this is now a product of distinct integers, the smallest of which is $n$ and the largest of which is strictly smaller than $a_r=b_s$. This contradicts the minimality of $a_r$.

**Remark:** Sequences whose product is a perfect square occur naturally in the *quadratic sieve* algorithm for factoring large integers. However, the behavior of the function $f(n)$ seems to be somewhat erratic. Karl Mahlburg points out the upper bound $f(n)\leq 2n$ for $n\geq 5$, which holds because the interval $(n,2n)$ contains an integer of the form $2m^2$. A trivial lower bound is $f(n)\geq n+p$ where $p$ is the least prime factor of $n$. For $n=p$ prime, the bounds agree and we have $f(p)=2p$. For more discussion, see `https://oeis.org/A006255`.

A3 Suppose on the contrary that $a_0+a_1y+\cdots+a_ny^n$ is nonzero for $0<y<1$. By the intermediate value theorem, this is only possible if $a_0+a_1y+\cdots+a_ny^n$ has the same sign for $0<y<1$; without loss of generality, we may assume that $a_0+a_1y+\cdots+a_ny^n>0$ for $0<y<1$. For the given value of $x$, we then have

$$a_0x^m+a_1x^{2m}+\cdots+a_nx^{(n+1)m}\geq 0$$

for $m=0,1,\dots$, with strict inequality for $m>0$. Taking the sum over all $m$ is absolutely convergent and hence valid; this yields

$$\frac{a_0}{1-x}+\frac{a_1}{1-x^2}+\cdots+\frac{a_n}{1-x^{n+1}}>0,$$

a contradiction.

A4 Let $w_1',\dots,w_k'$ be arcs such that: $w_j'$ has the same length as $w_j$; $w_1'$ is the same as $w_1$; and $w_{j+1}'$ is adjacent to $w_j'$ (i.e., the last digit of $w_j'$ comes right before the first digit of $w_{j+1}'$). Since $w_j$ has length $Z(w_j)+N(w_j)$, the sum of the lengths of $w_1,\dots,w_k$ is $k(Z+N)$, and so the concatenation of $w_1',\dots,w_k'$ is a string of $k(Z+N)$ consecutive digits around the circle. (This string may wrap around the circle, in which case some of these digits may appear more than once in the string.) Break this string into $k$ arcs $w_1'',\dots,w_k''$ each of length $Z+N$, each adjacent to the previous one. (Note that if the number of digits around the circle is $m$, then $Z+N\leq m$ since $Z(w_j)+N(w_j)\leq m$ for all $j$, and thus each of $w_1'',\dots,w_k''$ is indeed an arc.)

We claim that for some $j=1,\dots,k$, $Z(w_j'')=Z$ and $N(w_j'')=N$ (where the second equation follows from the first since $Z(w_j'')+N(w_j'')=Z+N$). Otherwise, since all of the $Z(w_j'')$ differ by at most 1, either $Z(w_j'')\leq Z-1$ for all $j$ or $Z(w_j'')\geq Z+1$ for all $j$. In either case, $|kZ-\sum_j Z(w_j')|=|kZ-\sum_j Z(w_j'')|\geq k$. But since $w_1=w_1'$, we have $|kZ-\sum_j Z(w_j')|=|\sum_{j=1}^k(Z(w_j)-Z(w_j'))|=|\sum_{j=2}^k(Z(w_j)-Z(w_j'))|\leq\sum_{j=2}^k|Z(w_j)-Z(w_j')|\leq k-1$, contradiction.

A5 Let $A_1,\dots,A_m$ be points in $\mathbb{R}^3$, and let $\hat{n}_{ijk}$ denote a unit vector normal to $\Delta A_iA_jA_k$ (unless $A_i,A_j,A_k$ are collinear, there are two possible choices for $\hat{n}_{ijk}$). If $\hat{n}$ is a unit vector in $\mathbb{R}^3$, and $\Pi_{\hat{n}}$ is a plane perpendicular to $\hat{n}$, then the area of the orthogonal projection of $\Delta A_iA_jA_k$ onto $\Pi_{\hat{n}}$ is $\mathrm{Area}(\Delta A_iA_jA_k)|\hat{n}_{ijk}\cdot\hat{n}|$. Thus if $\{a_{ijk}\}$ is area definite for $\mathbb{R}^2$, then for any $\hat{n}$,

$$\sum a_{ijk}\mathrm{Area}(\Delta A_iA_jA_k)|\hat{n}_{ijk}\cdot\hat{n}|\geq 0.$$

Note that integrating $|\hat{n}_{ijk}\cdot\hat{n}|$ over $\hat{n}\in S^2$, the unit sphere in $\mathbb{R}^3$, with respect to the natural measure on $S^2$ gives a positive number $c$, which is independent of $\hat{n}_{ijk}$ since the measure on $S^2$ is rotation-independent. Thus integrating the above inequality over $\hat{n}$ gives $c\sum a_{ijk}\mathrm{Area}(\Delta A_iA_jA_k)\geq 0$. It follows that $\{a_{ijk}\}$ is area definite for $\mathbb{R}^3$, as desired.

**Remark:** It is not hard to check (e.g., by integration in spherical coordinates) that the constant $c$ occurring above is equal to $2\pi$. It follows that for any convex body $C$ in $\mathbb{R}^3$, the average over $\hat{n}$ of the area of the projection of $C$ onto $\Pi_{\hat{n}}$ equals $1/4$ of the surface area of $C$.

More generally, let $C$ be a convex body in $\mathbb{R}^n$. For $\hat{n}$ a unit vector, let $\Pi_{\hat{n}}$ denote the hyperplane through the origin perpendicular to $\hat{n}$. Then the average over $\hat{n}$ of the volume of the projection of $C$ onto $\Pi_{\hat{n}}$ equals a constant (depending only on $n$) times the $(n-1)$-dimensional surface area of $C$.

Statements of this form inhabit the field of *inverse problems*, in which one attempts to reconstruct information about a geometric object from low-dimensional samples. This field has important applications in imaging and tomography.

A6 (by Harm Derksen) Consider the generating functions

$$f(x,y) = \sum_{(a,b)\in S} x^a y^b,$$
$$g(x,y) = \sum_{(a,b)\in\mathbb{Z}^2} w(a,b)x^a y^b.$$

Then $A(S)$ is the constant coefficient of the Laurent polynomial $h(x,y) = f(x,y)f(x^{-1},y^{-1})g(x,y)$. We may compute this coefficient by averaging over unit circles:

$$\begin{aligned}(2\pi)^2 A(S) &= \int_0^{2\pi}\int_0^{2\pi} h(e^{is},e^{it})\,dt\,ds \\ &= \int_0^{2\pi}\int_0^{2\pi} \left|f(e^{is},e^{it})\right|^2 g(e^{is},e^{it})\,dt\,ds.\end{aligned}$$

Consequently, it is enough to check that $g(e^{is},e^{it})$ is a nonnegative real number for all $s,t\in\mathbb{R}$. But $g(e^{is},e^{it}) = 16G(\cos s,\cos t)$ for

$$G(z,w) = zw + z^2 + w^2 - z^2 w - zw^2 - z^2 w^2.$$

If $z,w\in[-1,1]$ and $zw \geq 0$, then

$$G(z,w) = zw(1-zw) + z^2(1-w) + w^2(1-z) \geq 0.$$

If $z,w\in[-1,1]$ and $zw \leq 0$, then

$$G(z,w) = (z+w)^2 - zw(1+z)(1+w) \geq 0.$$

Hence $g(e^{is},e^{it}) \geq 0$ as desired.

B1 Note that

$$\begin{aligned}c(2k+1)c(2k+3) &= (-1)^k c(k)(-1)^{k+1}c(k+1) \\ &= -c(k)c(k+1) \\ &= -c(2k)c(2k+2).\end{aligned}$$

It follows that $\sum_{n=2}^{2013} c(n)c(n+2) = \sum_{k=1}^{1006}(c(2k)c(2k+2) + c(2k+1)c(2k+3)) = 0$, and so the desired sum is $c(1)c(3) = -1$.

**Remark**: Karl Mahlburg points out the general formula $c(n) = (-1)^{b_0b_1+b_1b_2+\cdots+b_{k-1}b_k}$ for $n$ having binary representation $b_k\cdots b_0$.

B2 We claim that the maximum value of $f(0)$ is 3. This is attained for $N=2$, $a_1 = \frac{4}{3}$, $a_2 = \frac{2}{3}$: in this case $f(x) = 1 + \frac{4}{3}\cos(2\pi x) + \frac{2}{3}\cos(4\pi x) = 1 + \frac{4}{3}\cos(2\pi x) + \frac{2}{3}(2\cos^2(2\pi x) - 1) = \frac{1}{3}(2\cos(2\pi x)+1)^2$ is always nonnegative.

Now suppose that $f = 1 + \sum_{n=1}^N a_n\cos(2\pi nx) \in C$. When $n$ is an integer, $\cos(2\pi n/3)$ equals 0 if $3|n$ and $-1/2$ otherwise. Thus $a_n\cos(2\pi n/3) = -a_n/2$ for all $n$, and $f(1/3) = 1 - \sum_{n=1}^N (a_n/2)$. Since $f(1/3)\geq 0$, $\sum_{n=1}^N a_n \leq 2$, whence $f(0) = 1 + \sum_{n=1}^N a_n \leq 3$.

B3 Yes, such numbers must exist. To define them, we make the following observations.

**Lemma 1.** *For any $i\in\{1,\dots,n\}$, if there exists any $S\in P$ containing i, then there exist $S,T\in P$ such that $S$ is the disjoint union of $T$ with $\{i\}$.*

*Proof.* Let $S$ be an element of $P$ containing $i$ of minimum cardinality. By (ii), there must be a subset $T\subset S$ containing $P$ with exactly one fewer element than $S$. These sets have the desired form. □

**Lemma 2.** *Suppose $S_1,S_2,T_1,T_2\in P$ have the property that for some $i\in\{1,\dots,n\}$, $S_1$ is the disjoint union of $T_1$ with $\{i\}$ and $S_2$ is the disjoint union of $T_2$ with $\{i\}$. Then*

$$f(S_1) - f(T_1) = f(S_2) - f(T_2).$$

*Proof.* By (i) we have

$$\begin{aligned}f(T_1\cup T_2\cup\{i\}) &= f(S_1) + f(T_2) - f(T_1\cap T_2) \\ f(T_1\cup T_2\cup\{i\}) &= f(T_1) + f(S_2) - f(T_1\cap T_2),\end{aligned}$$

from which the claim follows immediately. □

We now define $f_1,\dots,f_n$ as follows. If $i$ does not appear in any element of $P$, we put $f_i = 0$. Otherwise, by Lemma 1, we can find $S,T\in P$ such that $S$ is the disjoint union of $T$ with $\{i\}$. We then set $f_i = f(S) - f(T)$; by Lemma 2, this does not depend on the choice of $S,T$.

To check that $f(S) = \sum_{i\in S} f_i$ for $S\in P$, note first that $\emptyset\in P$ by repeated application of (ii) and that $f(\emptyset) = 0$ by hypothesis. This provides the base case for an induction on the cardinality of $S$; for any nonempty $S\in P$, we may apply (ii) to find $T\subset S$ such that $S$ is the disjoint union of $T$ and some singleton set $\{j\}$. By construction and the induction hypothesis, we have $f(S) = f(T) + f_j = j + \sum_{i\in T} f_i = \sum_{i\in S} f_i$ as desired.

B4 Write $f_0(x) = f(x) - \mu(f)$ and $g_0(x) = g(x) - \mu(g)$, so that $\int_0^1 f_0(x)^2\,dx = \mathrm{Var}(f)$, $\int_0^1 g_0(x)^2\,dx = \mathrm{Var}(g)$, and $\int_0^1 f_0(x)\,dx = \int_0^1 g_0(x)\,dx = 0$. Now since $|g(x)| \leq M(g)$ for all $x$, $0 \leq \int_0^1 f_0(x)^2(M(g)^2 - g(x)^2)\,dx = \mathrm{Var}(f)M(g)^2 - \int_0^1 f_0(x)^2 g(x)^2\,dx$, and similarly $0 \leq \mathrm{Var}(g)M(f)^2 - \int_0^1 f(x)^2 g_0(x)^2\,dx$. Summing gives

$$\mathrm{Var}(f)M(g)^2 + \mathrm{Var}(g)M(f)^2 \geq \int_0^1 (f_0(x)^2 g(x)^2 + f(x)^2 g_0(x)^2)\,dx. \tag{1}$$

Now

$$\begin{aligned}&\int_0^1 (f_0(x)^2 g(x)^2 + f(x)^2 g_0(x)^2)\,dx - \mathrm{Var}(fg) \\ &= \int_0^1 (f_0(x)^2 g(x)^2 + f(x)^2 g_0(x)^2 - (f(x)g(x) - \int_0^1 f(y)g(y)\,dy)^2)\,dx;\end{aligned}$$

substituting $f_0(x)+\mu(f)$ for $f(x)$ everywhere and $g_0(x)+\mu(g)$ for $g(x)$ everywhere, and using the fact that $\int_0^1 f_0(x)\,dx = \int_0^1 g_0(x)\,dx = 0$, we can expand and simplify the right hand side of this equation to obtain

$$\begin{aligned}
&\int_0^1 (f_0(x)^2 g(x)^2 + f(x)^2 g_0(x)^2)\,dx - \mathrm{Var}(fg)\\
&= \int_0^1 f_0(x)^2 g_0(x)^2\,dx\\
&- 2\mu(f)\mu(g)\int_0^1 f_0(x)g_0(x)\,dx + (\int_0^1 f_0(x)g_0(x)\,dx)^2\\
&\geq -2\mu(f)\mu(g)\int_0^1 f_0(x)g_0(x)\,dx.
\end{aligned}$$

Because of (1), it thus suffices to show that

$$2\mu(f)\mu(g)\int_0^1 f_0(x)g_0(x)\,dx \leq \mathrm{Var}(f)M(g)^2 + \mathrm{Var}(g)M(f)^2. \tag{2}$$

Now since $(\mu(g)f_0(x)-\mu(f)g_0(x))^2 \geq 0$ for all $x$, we have

$$\begin{aligned}
2\mu(f)\mu(g)\int_0^1 f_0(x)g_0(x)\,dx &\leq \int_0^1 (\mu(g)^2 f_0(x)^2 + \mu(f)^2 g_0(x)^2)dx\\
&= \mathrm{Var}(f)\mu(g)^2 + \mathrm{Var}(g)\mu(f)^2\\
&\leq \mathrm{Var}(f)M(g)^2 + \mathrm{Var}(g)M(f)^2,
\end{aligned}$$

establishing (2) and completing the proof.

B5 **First solution:** We assume $n \geq 1$ unless otherwise specified. For $T$ a set and $S_1, S_2$ two subsets of $T$, we say that a function $f: T \to T$ *iterates $S_1$ into $S_2$* if for each $x \in S_1$, there is a $j \geq 0$ such that $f^{(j)}(x) \in S_2$.

**Lemma 1.** *Fix $k \in X$. Let $f, g: X \to X$ be two functions such that $f$ iterates $X$ into $\{1,\dots,k\}$ and $f(x) = g(x)$ for $x \in \{k+1,\dots,n\}$. Then $g$ also iterates $X$ into $\{1,\dots,k\}$.*

*Proof.* For $x \in X$, by hypothesis there exists a nonnegative integer $j$ such that $f^{(j)}(x) \in \{1,\dots,k\}$. Choose the integer $j$ as small as possible; then $f^{(i)}(x) \in \{k+1,\dots,n\}$ for $0 \leq i < j$. By induction on $i$, we have $f^{(i)}(x) = g^{(i)}(x)$ for $i = 0,\dots,j$, so in particular $g^{(j)}(x) \in \{1,\dots,k\}$. This proves the claim. □

We proceed by induction on $n-k$, the case $n-k=0$ being trivial. For the induction step, we need only confirm that the number $x$ of functions $f: X \to X$ which iterate $X$ into $\{1,\dots,k+1\}$ but not into $\{1,\dots,k\}$ is equal to $n^{n-1}$. These are precisely the functions for which there is a unique cycle $C$ containing only numbers in $\{k+1,\dots,n\}$ and said cycle contains $k+1$. Suppose $C$ has length $\ell \in \{1,\dots,n-k\}$. For a fixed choice of $\ell$, we may choose the underlying set of $C$ in $\binom{n-k-1}{\ell-1}$ ways and the cycle structure in $(\ell-1)!$ ways. Given $C$, the functions $f$ we want are the ones that act on $C$ as specified and iterate $X$ into $\{1,\dots,k\}\cup C$. By Lemma 1, the number of such functions is $n^{-\ell}$ times the total number of functions that iterate $X$ into $\{1,\dots,k\}\cup C$. By the induction hypothesis, we compute the number of functions which iterate $X$ into $\{1,\dots,k+1\}$ but not into $\{1,\dots,k\}$ to be

$$\sum_{\ell=1}^{n-k}(n-k-1)\cdots(n-k-\ell+1)(k+\ell)n^{n-\ell-1}$$

By rewriting this as a telescoping sum, we get

$$\begin{aligned}
&\sum_{\ell=1}^{n-k}(n-k-1)\cdots(n-k-\ell+1)(n)n^{n-\ell-1}\\
&-\sum_{\ell=1}^{n-k}(n-k-1)\cdots(n-k-\ell+1)(n-k-\ell)n^{n-\ell-1}\\
&=\sum_{\ell=0}^{n-k-1}(n-k-1)\cdots(n-k-\ell)n^{n-\ell-1}\\
&-\sum_{\ell=1}^{n-k}(n-k-1)\cdots(n-k-\ell)n^{n-\ell-1}\\
&= n^{n-1}.
\end{aligned}$$

as desired.

**Second solution:** For $T$ a set, $f: T \to T$ a function, and $S$ a subset of $T$, we define the *contraction* of $f$ at $S$ as the function $g: \{*\}\cup(T-S) \to \{*\}\cup(T-S)$ given by

$$g(x) = \begin{cases} * & x = * \\ * & x \neq *, f(x) \in S \\ f(x) & x \neq *, f(x) \notin S. \end{cases}$$

**Lemma 2.** *For $S \subseteq X$ of cardinality $\ell \geq 0$, there are $\ell n^{n-\ell-1}$ functions $f: \{*\}\cup X \to \{*\}\cup X$ with $f^{-1}(*) = \{*\}\cup S$ which iterate $X$ into $\{*\}$.*

*Proof.* We induct on $n$. If $\ell = n$ then there is nothing to check. Otherwise, put $T = f^{-1}(S)$, which must be nonempty. The contraction $g$ of $f$ at $\{*\}\cup S$ is then a function on $\{*\}\cup(X-S)$ with $f^{-1}(*) = \{*\}\cup T$ which iterates $X-S$ into $\{*\}$. Moreover, for given $T$, each such $g$ arises from $\ell^{\#T}$ functions of the desired form. Summing over $T$ and invoking the induction hypothesis, we see that the number of functions $f$ is

$$\begin{aligned}
&\sum_{k=1}^{n-\ell}\binom{n-\ell}{k}\ell^k \cdot k(n-\ell)^{n-\ell-k-1}\\
&= \sum_{k=1}^{n-\ell}\binom{n-\ell-1}{k-1}\ell^k(n-\ell)^{n-\ell-k} = \ell n^{n-\ell-1}
\end{aligned}$$

as claimed. □

We now count functions $f: X \to X$ which iterate $X$ into $\{1,\dots,k\}$ as follows. By Lemma 1 of the first solution, this count equals $n^k$ times the number of functions with $f(1) = \cdots = f(k) = 1$ which iterate $X$ into $\{1,\dots,k\}$. For such a function $f$, put $S = \{k+1,\dots,n\}\cap f^{-1}(\{1,\dots,k\})$ and let $g$ be the contraction of $f$ at $\{1,\dots,k\}$; then $g^{-1}(*) = *\cup\{S\}$ and $g$ iterates its domain into $*$. By Lemma 2, for $\ell = \#S$, there are $\ell(n-k)^{n-k-\ell-1}$ such functions $g$. For given $S$, each such $g$ gives rise to $k^\ell$ functions $f$ with $f(1) = \cdots = f(k) = 1$ which iterate $X$ into $\{1,\dots,k\}$. Thus the number of such functions $f$ is

$$\begin{aligned}
&\sum_{\ell=0}^{n-k} \binom{n-k}{\ell} k^\ell \ell (n-k)^{n-k-\ell-1} \\
&= \sum_{\ell=0}^{n-k} \binom{n-k-1}{\ell-1} k^\ell (n-k)^{n-k-\ell} \\
&= kn^{n-k-1}.
\end{aligned}$$

The desired count is this times $n^k$, or $kn^{n-1}$ as desired.

**Remark:** Functions of the sort counted in Lemma 2 can be identified with rooted trees on the vertex set $\{*\} \cup X$ with root $*$. Such trees can be counted using *Cayley's formula*, a special case of *Kirchoff's matrix tree theorem*. The matrix tree theorem can also be used to show directly that the number of rooted forests on $n$ vertices with $k$ fixed roots is $kn^{n-k-1}$; the desired count follows immediately from this formula plus Lemma 1. (One can also use Prüfer sequences for a more combinatorial interpretation.)

B6 We show that the only winning first move for Alice is to place a stone in the central space. We start with some terminology.

By a *block* of stones, we mean a (possibly empty) sequence of stones occupying consecutive spaces. By the *extremal blocks*, we mean the (possibly empty) maximal blocks adjacent to the left and right ends of the playing area.

We refer to a legal move consisting of placing a stone in an empty space as a move of *type 1*, and any other legal move as being of *type 2*. For $i = 0,\dots,n$, let $P_i$ be the collection of positions containing $i$ stones. Define the *end zone* as the union $Z = P_{n-1} \cup P_n$. In this language, we make the following observations.

- Any move of type 1 from $P_i$ ends in $P_{i+1}$.
- Any move of type 2 from $P_n$ ends in $P_{n-1}$.
- For $i < n$, any move of type 2 from $P_i$ ends in $P_i \cup P_{i+1}$.
- At this point, we see that the number of stones cannot decrease until we reach the end zone.
- For $i < n-1$, if we start at a position in $P_i$ where the extremal blocks have length $a,b$, then the only possible moves to $P_i$ decrease one of $a,b$ while leaving the other unchanged (because they are separated by at least two empty spaces). In particular, no repetition is possible within $P_i$, so the number of stones must eventually increase to $i+1$.
- From any position in the end zone, the legal moves are precisely to the other positions in the end zone which have not previously occurred. Consequently, after the first move into the end zone, the rest of the game consists of enumerating all positions in the end zone in some order.
- At this point, we may change the rules without affecting the outcome by eliminating the rule on repetitions and declaring that the first player to move into the end zone loses (because $\#Z = n+1$ is even).

To determine who wins in each position, number the spaces of the board $1,\dots,n$ from left to right. Define the *weight* of a position to be the sum of the labels of the occupied spaces, reduced modulo $n+1$. For any given position outside of the end zone, for each $s = 1,\dots,n$ there is a unique move that adds $s$ to the weight: if $s$ is empty that a move of type 1 there does the job. Otherwise, $s$ inhabits a block running from $i+1$ to $j-1$ with $i$ and $j$ empty (or equal to 0 or $n+1$), so the type 2 move at $i+j-s$ (which belongs to the same block) does the job.

We now verify that a position of weight $s$ outside of the end zone is a win for the player to move if and only if $s \neq (n+1)/2$. We check this for positions in $P_i$ for $i = n-2,\dots,0$ by descending induction. For positions in $P_{n-2}$, the only safe moves are in the extremal blocks; we may thus analyze these positions as two-pile Nim with pile sizes equal to the lengths of the extremal blocks. In particular, a position is a win for the player to move if and only if the extremal blocks are unequal, in which case the winning move is to equalize the blocks. In other words, a position is a win for the player to move unless the empty spaces are at $s$ and $n+1-s$ for some $s \in \{1,\dots,(n-1)/2\}$, and indeed these are precisely the positions for which the weight equals $(1+\cdots+n) - (n+1) \equiv (n+1)/2 \pmod{n+1}$. Given the analysis of positions in $P_{i+1}$ for some $i$, it is clear that if a position in $P_i$ has weight $s \neq (n+1)/2$, there is a winning move of weight $t$ where $s+t \equiv (n+1)/2 \pmod{n}$, whereas if $s = (n+1)/2$ then no move leads to a winning position.

It thus follows that the unique winning move for Alice at her first turn is to move at the central space, as claimed.

**Remark:** Despite the existence of a simple description of the winning positions, it is nonetheless necessary to go through the preliminary analysis in order to establish the nature of the end zone and to ensure that the repetition clause does not affect the availability of moves outside of the end zone. However, it is not strictly necessary to study $P_{n-2}$ separately: none of the positions in $P_{n-1}$ has weight $(n+1)/2$, so following the strategy of forcing the weight to equal $(n+1)/2$ cannot force a first move into the end zone.

**Remark:** It is easy to see that Alice's winning strategy is to ensure that after each of her moves, the stones are placed symmetrically and the central space is occupied.

However, it is somewhat more complicated to describe Bob's winning strategy without the modular interpretation.

**Remark:** To resolve a mild ambiguity in the problem statement, it should be clarified that the initial position (with no stones placed) should be treated as having occurred previously once the first move has been made. This only affects the case $n = 1$.

**Remark:** For the analogous problem with $n$ even, David Savitt has conjectured (based on the cases $n = 2$ and $n = 4$) that Alice has a winning strategy, and her possible winning moves at her first turn are to place a stone in one of the two central spaces. We give a partial analysis based on an argument from Art of Problem Solving user `gnayijoag`, with some clarification from Savitt.

We first revise the endgame analysis from the original solution. Define the sets $P_i$ and the end zone $Z$ as before. The first six observations from the previous solution remain correct; however, now the number of positions in $Z$ is odd, so the first player to move into $Z$ wins. That is, every position in $P_{n-2}$ is a winning position for the player to move. Consequently, the positions in $P_{n-3}$ can be identified with two-player Nim on the extremal blocks (the subdivision between the two internal blocks being immaterial).

This suggests that if we want to introduce a numerical invariant that detects the difference between winning and losing positions for the player to move, we must consider a formula that selectively discards some information about some of the stones. To this end, for a position $x \in P_{n-k}$ for $k \geq 2$ with vacant spaces at $a_0 > \cdots > a_{k-1}$ (or $a_0(x) > \cdots > a_{k-1}(x)$ if this needs to be clarified), define

$$\begin{aligned} A(x) &= a_0 + \cdots + a_{k-1} \\ f(x,t) &= A - a_t - t(n+1) \quad (t = 0, \ldots, k-1); \end{aligned}$$

note that $f(x,0) > \cdots > f(x,k-1)$. We say that $x$ is *balanced* if $f(x,t) = 0$ for some (necessarily unique) choice of $t$, in which case we refer to $a_t$ as the *balance point* of $x$; otherwise, we say that $x$ is *unbalanced*. This definition then has the following properties.

- The property of being balanced is invariant under left-right symmetry. This will permit some simplification in the following arguments.
- Every position in $P_{n-2}$ is unbalanced, because $a_0 < a_0 + a_1 < a_1 + (n+1)$.
- For a position $x \in P_1$ to be balanced, in order to have $f(x,t) \equiv 0 \pmod{n+1}$ for some $t$, the unique occupied space must be $n+1-t$. We must then have $A(x) - t = 1 + \cdots + n - (n+1) = (n/2-1)(n+1)$, so $x$ is balanced if and only if $f(x, n/2-1) = 0$. This occurs if and only if the occupied space is $n/2$ or $n/2+1$.
- From every balanced position $x \in P_{n-k}$ for $k \geq 3$, every move leads to an unbalanced position. To check this, we need only consider moves at or to the left of the balance point $a_t$ of $x$. Let $y$ be the result of a move from $x$. If the move is at $a_t$, then

$$f(y,t') \equiv f(x,t) - a_{t'}(y) = -a_{t'}(y) \pmod{n+1}$$

  and the latter is not a nonzero residue because $a_{t'} \in \{1, \ldots, n\}$. For a move to the left of $a_t$, the vacant spaces to the right of $a_t$ remain at $a_0, \ldots, a_{t-1}$ and $0 < A(x) - A(y) < a_t$; consequently,

$$\begin{aligned} f(y,t-1) &= f(x,t-1) - (A(x) - A(y)) \\ &\geq (f(x,t) + a_t - a_{t-1} + (n+1)) - (a_t - 1) \\ &= n + 2 - a_{t-1} > 0. \end{aligned}$$

  Meanwhile, either $a_t$ remains vacant, or $a_t$ and $a_{t+1}$ are filled while some space $b$ in between becomes vacant; in either case, we have $f(y,t) < f(x,t) = 0$. Since $f(y,t) < 0 < f(y,t-1)$, $y$ is unbalanced.

To complete the analysis, one would need to show that from every unbalanced position in $P_{n-k}$ for $k \geq 3$, there is a move to some balanced position; this would then show that a position in the game is a win for the player to move if and only if it is unbalanced, from which the conjecture of Savitt would follow.

# The 75th William Lowell Putnam Mathematical Competition
# Saturday, December 6, 2014

A1 Prove that every nonzero coefficient of the Taylor series of

$$(1-x+x^2)e^x$$

about $x=0$ is a rational number whose numerator (in lowest terms) is either 1 or a prime number.

A2 Let $A$ be the $n \times n$ matrix whose entry in the $i$-th row and $j$-th column is

$$\frac{1}{\min(i,j)}$$

for $1 \le i,j \le n$. Compute $\det(A)$.

A3 Let $a_0 = 5/2$ and $a_k = a_{k-1}^2 - 2$ for $k \ge 1$. Compute

$$\prod_{k=0}^{\infty}\left(1-\frac{1}{a_k}\right)$$

in closed form.

A4 Suppose $X$ is a random variable that takes on only nonnegative integer values, with $E[X]=1$, $E\left[X^2\right]=2$, and $E\left[X^3\right]=5$. (Here $E[y]$ denotes the expectation of the random variable $Y$.) Determine the smallest possible value of the probability of the event $X=0$.

A5 Let

$$P_n(x) = 1+2x+3x^2+\cdots+nx^{n-1}.$$

Prove that the polynomials $P_j(x)$ and $P_k(x)$ are relatively prime for all positive integers $j$ and $k$ with $j \ne k$.

A6 Let $n$ be a positive integer. What is the largest $k$ for which there exist $n \times n$ matrices $M_1,\dots,M_k$ and $N_1,\dots,N_k$ with real entries such that for all $i$ and $j$, the matrix product $M_iN_j$ has a zero entry somewhere on its diagonal if and only if $i \ne j$?

B1 A *base* 10 *over-expansion* of a positive integer $N$ is an expression of the form

$$N = d_k 10^k + d_{k-1}10^{k-1} + \cdots + d_0 10^0$$

with $d_k \ne 0$ and $d_i \in \{0,1,2,\dots,10\}$ for all $i$. For instance, the integer $N=10$ has two base 10 over-expansions: $10 = 10\cdot 10^0$ and the usual base 10 expansion $10 = 1\cdot 10^1 + 0\cdot 10^0$. Which positive integers have a unique base 10 over-expansion?

B2 Suppose that $f$ is a function on the interval $[1,3]$ such that $-1 \le f(x) \le 1$ for all $x$ and $\int_1^3 f(x)\,dx = 0$. How large can $\int_1^3 \frac{f(x)}{x}\,dx$ be?

B3 Let $A$ be an $m \times n$ matrix with rational entries. Suppose that there are at least $m+n$ distinct prime numbers among the absolute values of the entries of $A$. Show that the rank of $A$ is at least 2.

B4 Show that for each positive integer $n$, all the roots of the polynomial

$$\sum_{k=0}^{n} 2^{k(n-k)}x^k$$

are real numbers.

B5 In the 75th annual Putnam Games, participants compete at mathematical games. Patniss and Keeta play a game in which they take turns choosing an element from the group of invertible $n \times n$ matrices with entries in the field $\mathbb{Z}/p\mathbb{Z}$ of integers modulo $p$, where $n$ is a fixed positive integer and $p$ is a fixed prime number. The rules of the game are:

(1) A player cannot choose an element that has been chosen by either player on any previous turn.

(2) A player can only choose an element that commutes with all previously chosen elements.

(3) A player who cannot choose an element on his/her turn loses the game.

Patniss takes the first turn. Which player has a winning strategy? (Your answer may depend on $n$ and $p$.)

B6 Let $f:[0,1]\to\mathbb{R}$ be a function for which there exists a constant $K>0$ such that $|f(x)-f(y)| \le K|x-y|$ for all $x,y \in [0,1]$. Suppose also that for each rational number $r \in [0,1]$, there exist integers $a$ and $b$ such that $f(r) = a+br$. Prove that there exist finitely many intervals $I_1,\dots,I_n$ such that $f$ is a linear function on each $I_i$ and $[0,1] = \bigcup_{i=1}^{n} I_i$.

# Solutions to the 75th William Lowell Putnam Mathematical Competition
## Saturday, December 6, 2014

Kiran Kedlaya and Lenny Ng

A1 The coefficient of $x^n$ in the Taylor series of $(1-x+x^2)e^x$ for $n=0,1,2$ is $1,0,\frac{1}{2}$, respectively. For $n\geq 3$, the coefficient of $x^n$ is

$$\begin{aligned} \frac{1}{n!}-\frac{1}{(n-1)!}+\frac{1}{(n-2)!} &= \frac{1-n+n(n-1)}{n!} \\ &= \frac{n-1}{n(n-2)!}. \end{aligned}$$

If $n-1$ is prime, then the lowest-terms numerator is clearly either 1 or the prime $n-1$ (and in fact the latter, since $n-1$ is relatively prime to $n$ and to $(n-2)!$). If $n-1$ is composite, either it can be written as $ab$ for some $a\neq b$, in which case both $a$ and $b$ appear separately in $(n-2)!$ and so the numerator is 1, or $n-1=p^2$ for some prime $p$, in which case $p$ appears in $(n-2)!$ and so the numerator is either 1 or $p$. (In the latter case, the numerator is actually 1 unless $p=2$, as in all other cases both $p$ and $2p$ appear in $(n-2)!$.)

A2 Let $v_1,\dots,v_n$ denote the rows of $A$. The determinant is unchanged if we replace $v_n$ by $v_n-v_{n-1}$, and then $v_{n-1}$ by $v_{n-1}-v_{n-2}$, and so forth, eventually replacing $v_k$ by $v_k-v_{k-1}$ for $k\geq 2$. Since $v_{k-1}$ and $v_k$ agree in their first $k-1$ entries, and the $k$-th entry of $v_k-v_{k-1}$ is $\frac{1}{k}-\frac{1}{k-1}$, the result of these row operations is an upper triangular matrix with diagonal entries $1,\frac{1}{2}-1,\frac{1}{3}-\frac{1}{2},\dots,\frac{1}{n}-\frac{1}{n-1}$. The determinant is then

$$\begin{aligned} \prod_{k=2}^{n}\left(\frac{1}{k}-\frac{1}{k-1}\right) &= \prod_{k=2}^{n}\left(\frac{-1}{k(k-1)}\right) \\ &= \frac{(-1)^{n-1}}{(n-1)!n!}. \end{aligned}$$

Note that a similar calculation can be made whenever $A$ has the form $A_{ij}=\min\{a_i,a_j\}$ for any monotone sequence $a_1,\dots,a_n$. Note also that the standard Gaussian elimination algorithm leads to the same upper triangular matrix, but the nonstandard order of operations used here makes the computations somewhat easier.

**Remark:** The inverse of $A$ can be identified explicitly: for $n\geq 2$, it is the matrix $B$ given by

$$B_{ij}=\begin{cases} -1 & i=j=1 \\ -2i^2 & 1<i=j<n \\ -(n-1)n & i=j=n \\ ij & |i-j|=1 \\ 0 & \text{otherwise.} \end{cases}$$

For example, for $n=5$,

$$B=\begin{pmatrix} -1 & 2 & 0 & 0 & 0 \\ 2 & -8 & 6 & 0 & 0 \\ 0 & 6 & -18 & 12 & 0 \\ 0 & 0 & 12 & -32 & 20 \\ 0 & 0 & 0 & 20 & -20 \end{pmatrix}.$$

Let $C$ denote the matrix obtained from $B$ by replacing the bottom-right entry with $-2n^2$ (for consistency with the rest of the diagonal). Expanding in minors along the bottom row produces a second-order recursion for $\det(C)$ solving to $\det(C)=(-1)^n(n!)^2$; a similar expansion then yields $\det(B)=(-1)^{n-1}n!(n-1)!$.

**Remark:** This problem and solution are due to one of us (Kedlaya). The statement appears in the comments on sequence A010790 (i.e., the sequence $(n-1)!n!$) in the On-Line Encyclopedia of Integer Sequences (`http://oeis.org`), attributed to Benoit Cloitre in 2002.

A3 **First solution:** Using the identity

$$(x+x^{-1})^2-2=x^2+x^{-2},$$

we may check by induction on $k$ that $a_k=2^{2^k}+2^{-2^k}$; in particular, the product is absolutely convergent. Using the identities

$$\begin{aligned} \frac{x^2+1+x^{-2}}{x+1+x^{-1}} &= x-1+x^{-1}, \\ \frac{x^2-x^{-2}}{x-x^{-1}} &= x+x^{-1}, \end{aligned}$$

we may telescope the product to obtain

$$\begin{aligned} \prod_{k=0}^{\infty}\left(1-\frac{1}{a_k}\right) &= \prod_{k=0}^{\infty}\frac{2^{2^k}-1+2^{-2^k}}{2^{2^k}+2^{-2^k}} \\ &= \prod_{k=0}^{\infty}\frac{2^{2^{k+1}}+1+2^{-2^{k+1}}}{2^{2^k}+1+2^{-2^k}}\cdot\frac{2^{2^k}-2^{-2^k}}{2^{2^{k+1}}-2^{2^{-k-1}}} \\ &= \frac{2^{2^0}-2^{-2^0}}{2^{2^0}+1+2^{-2^0}}=\frac{3}{7}. \end{aligned}$$

**Second solution:** (by Catalin Zara) In this solution, we do not use the explicit formula for $a_k$. We instead note first that the $a_k$ form an increasing sequence which cannot approach a finite limit (since the equation $L=L^2-2$ has no real solution $L>2$), and is thus unbounded. Using the identity

$$a_{k+1}+1=(a_k-1)(a_k+1),$$

one checks by induction on $n$ that

$$\prod_{k=0}^{n}\left(1-\frac{1}{a_k}\right)=\frac{2}{7}\frac{a_{n+1}+1}{a_0a_1\cdots a_n}.$$

Using the identity

$$a_{n+2}^2-4=a_{n+1}^4-4a_{n+1}^2,$$

one also checks by induction on $n$ that

$$a_0a_1\cdots a_n=\frac{2}{3}\sqrt{a_{n+1}^2-4}.$$

Hence

$$\prod_{k=0}^{n}\left(1-\frac{1}{a_k}\right)=\frac{3}{7}\frac{a_{n+1}+1}{\sqrt{a_{n+1}^2-4}}$$

tends to $\frac{3}{7}$ as $a_{n+1}$ tends to infinity, hence as $n$ tends to infinity.

A4 The answer is $\frac{1}{3}$.

**First solution:** Let $a_n=P(X=n)$; we want the minimum value for $a_0$. If we write $S_k=\sum_{n=1}^{\infty}n^ka_n$, then the given expectation values imply that $S_1=1$, $S_2=2$, $S_3=5$. Now define $f(n)=11n-6n^2+n^3$, and note that $f(0)=0$, $f(1)=f(2)=f(3)=6$, and $f(n)>6$ for $n\geq 4$; thus $4=11S_1-6S_2+S_3=\sum_{n=1}^{\infty}f(n)a_n\geq 6\sum_{n=1}^{\infty}a_n$. Since $\sum_{n=0}^{\infty}a_n=1$, it follows that $a_0\geq\frac{1}{3}$. Equality is achieved when $a_0=\frac{1}{3}$, $a_1=\frac{1}{2}$, $a_3=\frac{1}{6}$, and $a_n=0$ for all other $n$, and so the answer is $\frac{1}{3}$.

**Second solution:** (by Tony Qiao) Define the *probability generating function* of $P$ as the power series

$$G(z)=\sum_{n=0}^{\infty}P(x=n)z^n.$$

We compute that $G(1)=G'(1)=G''(1)=G'''(1)=1$. By Taylor's theorem with remainder, for any $x\in[0,1]$, there exists $c\in[x,1]$ such that

$$G(x)=1+(x-1)+\frac{(x-1)^2}{2!}+\frac{(x-1)^3}{3!}+\frac{G''''(c)}{4!}(x-1)^4.$$

In particular, $G(0)=\frac{1}{3}+\frac{1}{24}G''''(c)$ for some $c\in[0,1]$. However, since $G$ has nonnegative coefficients and $c\geq 0$, we must have $G''''(c)\geq 0$, and so $G(0)\geq\frac{1}{3}$. As in the first solution, we see that this bound is best possible.

A5 **First solution:** Suppose to the contrary that there exist positive integers $i\neq j$ and a complex number $z$ such that $P_i(z)=P_j(z)=0$. Note that $z$ cannot be a nonnegative real number or else $P_i(z),P_j(z)>0$; we may put $w=z^{-1}\neq 0,1$. For $n\in\{i+1,j+1\}$ we compute that

$$w^n=nw-n+1,\qquad \overline{w}^n=n\overline{w}-n+1;$$

note crucially that these equations also hold for $n\in\{0,1\}$. Therefore, the function $f:[0,+\infty)\to\mathbb{R}$ given by

$$f(t)=|w|^{2t}-t^2|w|^2+2t(t-1)\mathrm{Re}(w)-(t-1)^2$$

satisfies $f(t)=0$ for $t\in\{0,1,i+1,j+1\}$. On the other hand, for all $t\geq 0$ we have

$$f'''(t)=(2\log|w|)^3|w|^{2t}>0,$$

so by Rolle's theorem, the equation $f^{(3-k)}(t)=0$ has at most $k$ distinct solutions for $k=0,1,2,3$. This yields the desired contradiction.

**Remark:** By similar reasoning, an equation of the form $e^x=P(x)$ in which $P$ is a real polynomial of degree $d$ has at most $d+1$ real solutions. This turns out to be closely related to a concept in mathematical logic known as *o-minimality*, which in turn has deep consequences for the solution of Diophantine equations.

**Second solution:** (by Noam Elkies) We recall a result commonly known as the *Eneström-Kakeya theorem*.

**Lemma 1.** *Let*

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

*be a polynomial with real coefficients such that* $0<a_0\leq a_1\leq\cdots\leq a_n$. *Then every root* $z\in\mathbb{C}$ *of* $f$ *satisfies* $|z|\leq 1$.

*Proof.* If $f(z)=0$, then we may rearrange the equality $0=f(z)(z-1)$ to obtain

$$a_nz^{n+1}=(a_n-a_{n-1})z^n+\cdots+(a_1-a_0)z+a_0.$$

But if $|z|>1$, then

$$|a_nz^{n+1}|\leq(|a_n-a_{n-1}|+\cdots+|a_1-a_0|)|z|^n\leq|a_nz^n|,$$

contradiction. □

**Corollary 2.** *Let*

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

*be a polynomial with positive real coefficients. Then every root* $z\in\mathbb{C}$ *of* $f$ *satisfies* $r\leq|z|\leq R$ *for*

$$r=\min\{a_0/a_1,\ldots,a_{n-1}/a_n\}$$
$$R=\max\{a_0/a_1,\ldots,a_{n-1}/a_n\}.$$

*Proof.* The bound $|z|\leq R$ follows by applying the lemma to the polynomial $f(x/R)$. The bound $|z|\geq r$ follows by applying the lemma to the reverse of the polynomial $f(x/r)$. □

Suppose now that $P_i(z)=P_j(z)=0$ for some $z\in\mathbb{C}$ and some integers $i<j$. We clearly cannot have $j=i+1$, as then $P_i(0)\neq 0$ and so $P_j(z)-P_i(z)=(i+1)z^i\neq 0$; we thus have $j-i\geq 2$. By applying Corollary 2 to $P_i(x)$, we see that $|z|\leq 1-\frac{1}{i}$. On the other hand, by applying

Corollary 2 to $(P_j(x) - P_i(x))/x^{i-1}$, we see that $|z| \geq 1 - \frac{1}{i+2}$, contradiction.

**Remark:** Elkies also reports that this problem is his submission, dating back to 2005 and arising from work of Joe Harris. It dates back further to Example 3.7 in: Hajime Kaji, On the tangentially degenerate curves, *J. London Math. Soc. (2)* **33** (1986), 430–440, in which the second solution is given.

**Remark:** Elkies points out a mild generalization which may be treated using the first solution but not the second: for integers $a < b < c < d$ and $z \in \mathbb{C}$ which is neither zero nor a root of unity, the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ z^a & z^b & z^c & z^d \end{pmatrix}$$

has rank 3 (the problem at hand being the case $a = 0, b = 1, c = i+1, d = j+1$).

**Remark:** It seems likely that the individual polynomials $P_k(x)$ are all irreducible, but this appears difficult to prove.

**Third solution:** (by David Feldman) Note that

$$P_n(x)(1-x) = 1 + x + \cdots + x^{n-1} - nx^n.$$

If $|z| \geq 1$, then

$$n|z|^n \geq |z|^{n-1} + \cdots + 1 \geq |z^{n-1} + \cdots + 1|,$$

with the first equality occurring only if $|z| = 1$ and the second equality occurring only if $z$ is a positive real number. Hence the equation $P_n(z)(1-z) = 0$ has no solutions with $|z| \geq 1$ other than the trivial solution $z = 1$. Since

$$P_n(x)(1-x)^2 = 1 - (n+1)x^n + nx^{n+1},$$

it now suffices to check that the curves

$$C_n = \{z \in \mathbb{C} : 0 < |z| < 1, |z|^n \, |n+1-zn| = 1\}$$

are pairwise disjoint as $n$ varies over positive integers.

Write $z = u + iv$; we may assume without loss of generality that $v \geq 0$. Define the function

$$E_z(n) = n \log|z| + \log|n+1-zn|.$$

One computes that for $n \in \mathbb{R}$, $E_z''(n) < 0$ if and only if

$$\frac{u-v-1}{(1-u)^2+v^2} < n < \frac{u+v-1}{(1-u)^2+v^2}.$$

In addition, $E_z(0) = 0$ and

$$E_z'(0) = \frac{1}{2}\log(u^2+v^2) + (1-u) \geq \log(u) + 1 - u \geq 0$$

since $\log(u)$ is concave. From this, it follows that the equation $E_z(n) = 0$ can have at most one solution with $n > 0$.

**Remark:** The reader may notice a strong similarity between this solution and the first solution. The primary difference is we compute that $E_z'(0) \geq 0$ instead of discovering that $E_z(-1) = 0$.

**Remark:** It is also possible to solve this problem using a $p$-adic valuation on the field of algebraic numbers in place of the complex absolute value; however, this leads to a substantially more complicated solution. In lieu of including such a solution here, we refer to the approach described by Victor Wang here: `http://www.artofproblemsolving.com/Forum/viewtopic.php?f=80&t=616731`.

A6 The largest such $k$ is $n^n$. We first show that this value can be achieved by an explicit construction. Let $e_1, \dots, e_n$ be the standard basis of $\mathbb{R}^n$. For $i_1, \dots, i_n \in \{1, \dots, n\}$, let $M_{i_1,\dots,i_n}$ be the matrix with row vectors $e_{i_1}, \dots, e_{i_n}$, and let $N_{i_1,\dots,i_n}$ be the transpose of $M_{i_1,\dots,i_n}$. Then $M_{i_1,\dots,i_n} N_{j_1,\dots,j_n}$ has $k$-th diagonal entry $e_{i_k} \cdot e_{j_k}$, proving the claim.

We next show that for any families of matrices $M_i, N_j$ as described, we must have $k \leq n^n$. Let $V$ be the *n-fold tensor product* of $\mathbb{R}^n$, i.e., the vector space with orthonormal basis $e_{i_1} \otimes \cdots \otimes e_{i_n}$ for $i_1, \dots, i_n \in \{1, \dots, n\}$. Let $m_i$ be the tensor product of the rows of $M_i$; that is,

$$m_i = \sum_{i_1,\dots,i_n=1}^{n} (M_i)_{1,i_1} \cdots (M_i)_{n,i_n} e_{i_1} \otimes \cdots \otimes e_{i_n}.$$

Similarly, let $n_j$ be the tensor product of the columns of $N_j$. One computes easily that $m_i \cdot n_j$ equals the product of the diagonal entries of $M_i N_j$, and so vanishes if and only if $i \neq j$. For any $c_i \in \mathbb{R}$ such that $\sum_i c_i m_i = 0$, for each $j$ we have

$$0 = \left(\sum_i c_i m_i\right) \cdot n_j = \sum_i c_i (m_i \cdot n_j) = c_j.$$

Therefore the vectors $m_1, \dots, m_k$ in $V$ are linearly independent, implying $k \leq n^n$ as desired.

**Remark:** Noam Elkies points out that similar argument may be made in the case that the $M_i$ are $m \times n$ matrices and the $N_j$ are $n \times m$ matrices.

B1 These are the integers with no 0's in their usual base 10 expansion. If the usual base 10 expansion of $N$ is $d_k 10^k + \cdots + d_0 10^0$ and one of the digits is 0, then there exists an $i \leq k-1$ such that $d_i = 0$ and $d_{i+1} > 0$; then we can replace $d_{i+1} 10^{i+1} + (0) 10^i$ by $(d_{i+1} - 1) 10^{i+1} + (10) 10^i$ to obtain a second base 10 over-expansion.

We claim conversely that if $N$ has no 0's in its usual base 10 expansion, then this standard form is the unique base 10 over-expansion for $N$. This holds by induction on the number of digits of $N$: if $1 \leq N \leq 9$, then the result is clear. Otherwise, any base 10 over-expansion $N = d_k 10^k + \cdots + d_1 10 + d_0 10^0$ must have $d_0 \equiv N \pmod{10}$, which uniquely determines $d_0$ since

$N$ is not a multiple of 10; then $(N-d_0)/10$ inherits the base 10 over-expansion $d_k 10^{k-1}+\cdots+d_1 10^0$, which must be unique by the induction hypothesis.

**Remark:** Karl Mahlburg suggests an alternate proof of uniqueness (due to Shawn Williams): write the usual expansion $N = d_k 10^k + \cdots + d_0 10^0$ and suppose $d_i \neq 0$ for all $i$. Let $M = c_l 10^l + \cdots + c_0 10^0$ be an over-expansion with at least one 10. To have $M = N$, we must have $l \leq k$; we may pad the expansion of $M$ with zeroes to force $l = k$. Now define $e_i = c_i - d_i$; since $1 \leq d_i \leq 9$ and $0 \leq c_i \leq 10$, we have $0 \leq |e_i| \leq 9$. Moreover, there exists at least one index $i$ with $e_i \neq 0$, since any index for which $c_i = 10$ has this property. But if $i$ is the largest such index, we have

$$\begin{aligned} 10^i \leq \left|e_i 10^i\right| &= \left|-\sum_{j=0}^{i-1} e_i 10^i\right| \\ &\leq \sum_{j=0}^{i-1} \left|e_i\right|10^i\right| \leq 9\cdot 10^{i-1}+\cdots+9\cdot 10^0, \end{aligned}$$

a contradiction.

B2 In all solutions, we assume that the function $f$ is integrable.

**First solution:** Let $g(x)$ be 1 for $1 \leq x \leq 2$ and $-1$ for $2 < x \leq 3$, and define $h(x) = g(x) - f(x)$. Then $\int_1^3 h(x)\,dx = 0$ and $h(x) \geq 0$ for $1 \leq x \leq 2$, $h(x) \leq 0$ for $2 < x \leq 3$. Now

$$\begin{aligned} \int_1^3 \frac{h(x)}{x}\,dx &= \int_1^2 \frac{|h(x)|}{x}\,dx - \int_2^3 \frac{|h(x)|}{x}\,dx \\ &\geq \int_1^2 \frac{|h(x)|}{2}\,dx - \int_2^3 \frac{|h(x)|}{2}\,dx = 0, \end{aligned}$$

and thus $\int_1^3 \frac{f(x)}{x}\,dx \leq \int_1^3 \frac{g(x)}{x}\,dx = 2\log 2 - \log 3 = \log \frac{4}{3}$. Since $g(x)$ achieves the upper bound, the answer is $\log \frac{4}{3}$.

**Reformulation:** (by Karl Mahlburg and Karthik Adimurthi) Since $f$ is integrable, it can be expressed in terms of the Hadamard basis

$$\begin{aligned} H_0(x) &= \begin{cases} 1 & x \in [1,2) \\ -1 & x \in [2,3] \\ 0 & x \notin [1,3] \end{cases} \\ H_{n+1}(x) &= H_n(2(x-1)+1) + H_n(2(x-2)+1). \end{aligned}$$

More precisely, we have $f(x) = \sum_n c_n H_n(x)$ for some $c_n$ with $|c_0| + |c_1| + |\cdots| \leq 1$. Let $g_n = \int_1^3 (H_n(x)/x)\,dx$; it is easy to show that the $g_n$ are strictly decreasing in $n$. Thus

$$\int_1^3 (f(x)/x)dx = c_0 g_0 + c_1 g_1 + \cdots \leq 1 \cdot g_0 = \log \frac{4}{3}.$$

**Second solution:** (Art of Problem Solving, user `libra_gold`) Define the function $F(x) = \int_1^x f(t)\,dt$ for $1 \leq x \leq 3$; then $F(1) = F(3) = 0$ and $F(x) \leq \min\{x-1, 3-x\}$. Using integration by parts, we obtain

$$\begin{aligned} \int_1^3 \frac{f(x)}{x}\,dx &= \int_1^3 \frac{F(x)}{x^2}\,dx \\ &\leq \int_1^2 \frac{x-1}{x^2}\,dx + \int_2^3 \frac{3-x}{x^2}\,dx \\ &= \log \frac{4}{3}. \end{aligned}$$

(Some minor adjustment is needed to make this completely rigorous, e.g., approximating $f$ uniformly by continuous functions.)

B3 **First solution:** Assume by way of contradiction that $A$ has rank at most 1; in this case, we can find rational numbers $a_1, \dots, a_m$, $b_1, \dots, b_n$ such that $A_{ij} = a_i b_j$ for all $i, j$. By deleting rows or columns, we may reduce to the case where the $a_i$'s and $b_j$'s are all nonzero.

Recall that any nonzero rational number $q$ has a unique prime factorization

$$q = \pm 2^{c_1} 3^{c_2} 5^{c_3} \cdots$$

with exponents in $\mathbb{Z}$. Set

$$c(q) = (c_1, c_2, c_3, \dots).$$

Note that $|a_i b_j|$ is prime if and only if $c(a_i) + c(b_j)$ has one entry equal to 1 and all others equal to 0. The condition that $m+n$ distinct primes appear in the matrix implies that the vector space

$$\left\{ \sum_i x_i c(a_i) + \sum_j y_i c(b_j) : x_i, y_j \in \mathbb{R}, \sum_i x_i = \sum_j y_j \right\}$$

contains a linearly independent set of size $m+n$. But that space evidently has dimension at most $m+n-1$, contradiction.

**Second solution:** In this solution, we use standard terminology of graph theory, considering only simple undirected graphs (with no self-loops or multiple edges). We first recall the quick induction proof that that a graph on $k$ vertices with no cycles contains at most $k-1$ edges: for $k = 1$, the claim is trivially true because there can be no edges. For $k > 1$, choose any vertex $v$ and let $d$ be its degree. Removing the vertex $v$ and the edges incident to it leaves a disjoint union of $d$ different graphs, each having no cycles. If the numbers of vertices in these graphs are $k_1, \dots, k_d$, by induction the total number of edges in the original graph is at most $(k_1 - 1) + \cdots + (k_d - 1) + d = k - 1$.

Returning to the original problem, suppose that $A$ has rank at most 1. Draw a bipartite graph whose vertices correspond to the rows and columns of $A$, with an edge joining a particular row and column if the entry where they intersect has prime absolute value. By the previous paragraph, this graph must contain a cycle. Since the graph is bipartite, this cycle must be of length $2k$ for some integer $k \geq 2$ (we cannot have $k=1$ because the graph has no repeated edges). Without loss of generality, we may assume that the cycle consists of row 1, column 1, row 2, column 2, and so on. There must then exist distinct prime numbers $p_1,\dots,p_{2k}$ such that

$$|A_{11}| = p_1, |A_{21}| = p_2, \dots, |A_{kk}| = p_{2k-1}, |A_{1k}| = p_{2k}.$$

However, since $A$ has rank 1, the $2\times 2$ minor $A_{11}A_{ij} - A_{i1}A_{1j}$ must vanish for all $i,j$. If we put $r_i = |A_{i1}|$ and $c_j = \left|A_{ij}/A_{11}\right|$, we have

$$\begin{aligned} p_1 \cdots p_{2k} &= (r_1c_1)(r_2c_1)\cdots(r_kc_k)(r_1c_k) \\ &= (r_1c_1\cdots r_kc_k)^2, \end{aligned}$$

which contradicts the existence of unique prime factorizations for positive rational numbers: the prime $p_1$ occurs with exponent 1 on the left, but with some even exponent on the right. This contradiction completes the proof.

B4 Define the polynomial $f_n(x) = \sum_{k=0}^n 2^{k(n-k)}x^k$. Since

$$f_1(x) = 1+x, f_2(x) = 1+2x+x^2 = (1+x)^2,$$

the claim holds for for $n=1,2$. For $n\geq 3$, we show that the quantities

$$f_n(-2^{-n}), f_n(-2^{-n+2}), \dots, f_n(-2^n)$$

alternate in sign; by the intermediate value theorem, this will imply that $f_n$ has a root in each of the $n$ intervals $(-2^{-n},-2^{-n+2}),\dots,(-2^{n-2},-2^n)$, forcing $f_n$ to have as many distinct real roots as its degree.

For $j\in\{0,\dots,n\}$, group the terms of $f_n(x)$ as

$$\begin{aligned} &\cdots \\ &+2^{(j-5)(n-j+5)}x^{j-5} + 2^{(j-4)(n-j+4)}x^{j-4} \\ &+2^{(j-3)(n-j+3)}x^{j-3} + 2^{(j-2)(n-j+2)}x^{j-2} \\ &+2^{(j-1)(n-j+1)}x^{j-1} + 2^{j(n-j)}x^j + 2^{(j+1)(n-j-1)}x^{j+1} \\ &+2^{(j+2)(n-j-2)}x^{j+2} + 2^{(j+3)(n-j-3)}x^{j+3} \\ &+2^{(j+4)(n-j-4)}x^{j+4} + 2^{(j+5)(n-j-5)}x^{j+5} \\ &\cdots. \end{aligned}$$

Depending on the parity of $j$ and of $n-j$, there may be a single monomial left on each end. When evaluating at $x=-2^{-n+2j}$, the trinomial evaluates to 0. In the binomials preceding the trinomial, the right-hand term dominates, so each of these binomials contributes with the sign of $x^{j-2k}$, which is $(-1)^j$. In the binomials following the trinomial, the left-hand term dominates, so again the contribution has sign $(-1)^j$.

Any monomials which are left over on the ends also contribute with sign $(-1)^j$. Since $n\geq 3$, there exists at least one contribution other than the trinomial, so $f_n(-2^{-n+2j})$ has overall sign $(-1)^j$, proving the claimed alternation.

**Remark:** Karl Mahlburg suggests an alternate interpretation of the preceding algebra: write $2^{-j^2}f_n(2^{-n+2j})$ as

$$\begin{aligned} &2^{-j^2} - 2^{-(j-1)^2} + \cdots + (-1)^{j-1}2^{-1} + (-1)^j 2^{-1} \\ &+(-1)^j 2^{-1} + (-1)^{j+1}2^{-1} + (-1)^{j+2}2^{-2} + \cdots, \end{aligned}$$

where the two central terms $(-1)^j 2^{-1}$ arise from splitting the term arising from $x^j$. Then each row is an alternating series whose sum carries the sign of $(-1)^j$ unless it has only two terms. Since $n\geq 3$, one of the two sums is forced to be nonzero.

**Remark:** One of us (Kedlaya) received this problem and solution from David Speyer in 2009 and submitted it to the problem committee.

B5 We show that Patniss wins if $p=2$ and Keeta wins if $p>2$ (for all $n$). We first analyze the analogous game played using an arbitrary finite group $G$. Recall that for any subset $S$ of $G$, the set of elements $g\in G$ which commute with all elements of $S$ forms a subgroup $Z(S)$ of $G$, called the *centralizer* (or *commutant*) of $S$. At any given point in the game, the set $S$ of previously chosen elements is contained in $Z(S)$. Initially $S=\emptyset$ and $Z(S)=G$; after each turn, $S$ is increased by one element and $Z(S)$ is replaced by a subgroup. In particular, if the order of $Z(S)$ is odd at some point, it remains odd thereafter; conversely, if $S$ contains an element of even order, then the order of $Z(S)$ remains even thereafter. Therefore, any element $g\in G$ for which $Z(\{g\})$ has odd order is a winning first move for Patniss, while any other first move by Patniss loses if Keeta responds with some $h\in Z(\{g\})$ of even order (e.g., an element of a 2-Sylow subgroup of $Z(\{g\})$). In both cases, the win is guaranteed no matter what moves follow.

Now let $G$ be the group of invertible $n\times n$ matrices with entries in $\mathbb{Z}/p\mathbb{Z}$. If $p>2$, then $Z(S)$ will always contain the scalar matrix $-1$ of order 2, so the win for Keeta is guaranteed. (An explicit winning strategy is to answer any move $g$ with the move $-g$.)

If $p=2$, we establish the existence of $g\in G$ such that $Z(\{g\})$ has odd order using the existence of an irreducible polynomial $P(x)$ of degree $n$ over $\mathbb{Z}/p\mathbb{Z}$ (see remark). We construct an $n\times n$ matrix over $\mathbb{Z}/p\mathbb{Z}$ with characteristic polynomial $P(x)$ by taking the *companion matrix* of $P(x)$: write $P(x) = x^n + P_{n-1}x^{n-1} + \cdots + P_0$ and set

$$g = \begin{pmatrix} 0 & 0 & \cdots & 0 & -P_0 \\ 1 & 0 & \cdots & 0 & -P_1 \\ 0 & 1 & \cdots & 0 & -P_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -P_{n-1} \end{pmatrix}.$$

In particular, $\det(g) = (-1)^n P_0 \neq 0$, so $g\in G$. Over an algebraic closure of $\mathbb{Z}/p\mathbb{Z}$, $g$ becomes diagonalizable with distinct eigenvalues, so any matrix commuting with $g$ must also be diagonalizable, and hence of odd order. In particular, $Z(\{g\})$ is of odd order, so Patniss has a winning strategy.

**Remark:** It can be shown that in the case $p = 2$, the only elements $g \in G$ for which $Z(\{g\})$ has odd order are those for which $g$ has distinct eigenvalues: in any other case, $Z(\{g\})$ contains a subgroup isomorphic to the group of $k \times k$ invertible matrices over $\mathbb{Z}/2\mathbb{Z}$ for some $k > 1$, and this group has order $(2^k - 1)(2^k - 2) \cdots (2^k - 2^{k-1})$.

**Remark:** We sketch two ways to verify the existence of an irreducible polynomial of degree $n$ over $\mathbb{Z}/p\mathbb{Z}$ for any positive integer $n$ and any prime number $p$. One is to use Möbius inversion to count the number of irreducible polynomials of degree $n$ over $\mathbb{Z}/p\mathbb{Z}$ and then give a positive lower bound for this count. The other is to first establish the existence of a finite field $\mathbb{F}$ of cardinality $p^n$, e.g., as the set of roots of the polynomial $x^{p^n} - 1$ inside a splitting field, and then take the minimal polynomial of a nonzero element of $\mathbb{F}$ over $\mathbb{Z}/p\mathbb{Z}$ which is a primitive $(p^n - 1)$-st root of unity in $\mathbb{F}$ (which exist because the multiplicative group of $\mathbb{F}$ contains at most one cyclic subgroup of any given order). One might be tempted to apply the primitive element theorem for $\mathbb{F}$ over $\mathbb{Z}/p\mathbb{Z}$, but in fact one of the preceding techniques is needed in order to verify this result for finite fields, as the standard argument that "most" elements of the upper field are primitive breaks down for finite fields.

One may also describe the preceding analysis in terms of an identification of $\mathbb{F}$ as a $\mathbb{Z}/p\mathbb{Z}$-vector space with the space of column vectors of length $n$. Under such an identification, if we take $g$ to be an element of $\mathbb{F} - \{0\}$ generating this group, then any element of $Z(\{g\})$ commutes with all of $\mathbb{F} - \{0\}$ and hence must define an $\mathbb{F}$-linear endomorphism of $\mathbb{F}$. Any such endomorphism is itself multiplication by an element of $\mathbb{F}$, so $Z(\{g\})$ is identified with the multiplicative group of $\mathbb{F}$, whose order is the odd number $2^n - 1$.

B6 Let us say that a linear function $g$ on an interval is *integral* if it has the form $g(x) = a + bx$ for some $a, b \in \mathbb{Z}$, and that a piecewise linear function is *integral* if on every interval where it is linear, it is also integral.

For each positive integer $n$, define the $n$-th *Farey sequence* $F_n$ as the sequence of rational numbers in $[0,1]$ with denominators at most $n$. It is easily shown by induction on $n$ that any two consecutive elements $\frac{r}{s}, \frac{r'}{s'}$ of $F_n$, written in lowest terms, satisfy $\gcd(s,s') = 1$, $s + s' > n$, and $r's - rs' = 1$. Namely, this is obvious for $n = 1$ because $F_1 = \frac{0}{1}, \frac{1}{1}$. To deduce the claim for $F_n$ from the claim for $F_{n-1}$, let $\frac{r}{s}, \frac{r'}{s'}$ be consecutive elements of $F_{n-1}$. If $s + s' = n$, then for $m = r + r'$ we have $\frac{r}{s} < \frac{m}{n} < \frac{r'}{s'}$ and the pairs $\frac{r}{s}, \frac{m}{n}$ and $\frac{m}{n}, \frac{r'}{s'}$ satisfy the desired conditions. Conversely, if $s + s' > n$, then we cannot have $\frac{r}{s} < \frac{m}{n} < \frac{r'}{s'}$ for $a \in \mathbb{Z}$, as this yields the contradiction

$$n = (ms - nr)s' + (r'n - ms') \geq s + s' > n;$$

hence $\frac{r}{s}, \frac{r'}{s'}$ remain consecutive in $F_n$.

Let $f_n : [0,1] \to \mathbb{R}$ be the piecewise linear function which agrees with $f$ at each element of $F_n$ and is linear between any two consecutive elements of $F_n$. Between any two consecutive elements $\frac{r}{s}, \frac{r'}{s'}$ of $F_n$, $f_n$ coincides with some linear function $a + bx$. Since $sf(\frac{r}{s}), s'f(\frac{r'}{s'}) \in \mathbb{Z}$, we deduce first that

$$b = ss'(f(\frac{r'}{s'}) - f(\frac{r}{s}))$$

is an integer of absolute value at most $K$, and second that both $as = sf(\frac{r}{s}) - br$ and $as' = s'f(\frac{r'}{s'}) - br'$ are integral. It follows that $f_n$ is integral.

We now check that if $n > 2K$, then $f_n = f_{n-1}$. For this, it suffices to check that for any consecutive elements $\frac{r}{s}, \frac{m}{n}, \frac{r'}{s'}$ in $F_n$, the linear function $a_0 + b_0 x$ matching $f_{n-1}$ from $\frac{r}{s}$ to $\frac{r'}{s'}$ has the property that $f(\frac{m}{n}) = a_0 + b_0 \frac{m}{n}$. Define the integer $t = nf(\frac{m}{n}) - a_0 n - b_0 m$. We then compute that the slope of $f_n$ from $\frac{r}{s}$ to $\frac{m}{n}$ is $b_0 + st$, while the slope of $f_n$ from $\frac{m}{n}$ to $\frac{r'}{s'}$ is at most $b_0 - s't$. In order to have $|b_0 + st|, |b_0 - s't| \leq K$, we must have $(s + s')\,|t| \leq 2K$; since $s + s' = n > 2K$, this is only possible if $t = 0$. Hence $f_n = f_{n-1}$, as claimed.

It follows that for any $n > 2K$, we must have $f_n = f_{n+1} = \cdots$. Since the condition on $f$ and $K$ implies that $f$ is continuous, we must also have $f_n = f$, completing the proof.

**Remark:** The condition on $f$ and $K$ is called *Lipschitz continuity*.

**Remark:** An alternate approach is to prove that for each $x \in [0,1)$, there exists $\varepsilon \in (0, 1-x)$ such that the restriction of $f$ to $[x, x+\varepsilon)$ is linear; one may then deduce the claim using the compactness of $[0,1]$. In this approach, the role of the Farey sequence may also be played by the convergents of the continued fraction of $x$ (at least in the case where $x$ is irrational).

**Remark:** This problem and solution are due to one of us (Kedlaya). Some related results can be proved with the Lipschitz continuity condition replaced by suitable convexity conditions. See for example: Kiran S. Kedlaya and Philip Tynan, Detecting integral polyhedral functions, *Confluentes Mathematici* **1** (2009), 87–109. Such results arise in the theory of $p$-adic differential equations; see for example: Kiran S. Kedlaya and Liang Xiao, Differential modules on $p$-adic polyannuli, *J. Inst. Math. Jusssieu* **9** (2010), 155–201 (errata, *ibid.*, 669–671).

# The 76th William Lowell Putnam Mathematical Competition
# Saturday, December 5, 2015

A1 Let $A$ and $B$ be points on the same branch of the hyperbola $xy = 1$. Suppose that $P$ is a point lying between $A$ and $B$ on this hyperbola, such that the area of the triangle $APB$ is as large as possible. Show that the region bounded by the hyperbola and the chord $AP$ has the same area as the region bounded by the hyperbola and the chord $PB$.

A2 Let $a_0 = 1$, $a_1 = 2$, and $a_n = 4a_{n-1} - a_{n-2}$ for $n \geq 2$. Find an odd prime factor of $a_{2015}$.

A3 Compute

$$\log_2\left(\prod_{a=1}^{2015}\prod_{b=1}^{2015}(1+e^{2\pi iab/2015})\right)$$

Here $i$ is the imaginary unit (that is, $i^2 = -1$).

A4 For each real number $x$, let

$$f(x) = \sum_{n\in S_x}\frac{1}{2^n},$$

where $S_x$ is the set of positive integers $n$ for which $\lfloor nx \rfloor$ is even. What is the largest real number $L$ such that $f(x) \geq L$ for all $x \in [0,1)$? (As usual, $\lfloor z \rfloor$ denotes the greatest integer less than or equal to $z$.)

A5 Let $q$ be an odd positive integer, and let $N_q$ denote the number of integers $a$ such that $0 < a < q/4$ and $\gcd(a,q) = 1$. Show that $N_q$ is odd if and only if $q$ is of the form $p^k$ with $k$ a positive integer and $p$ a prime congruent to 5 or 7 modulo 8.

A6 Let $n$ be a positive integer. Suppose that $A$, $B$, and $M$ are $n\times n$ matrices with real entries such that $AM = MB$, and such that $A$ and $B$ have the same characteristic polynomial. Prove that $\det(A - MX) = \det(B - XM)$ for every $n \times n$ matrix $X$ with real entries.

B1 Let $f$ be a three times differentiable function (defined on $\mathbb{R}$ and real-valued) such that $f$ has at least five distinct real zeros. Prove that $f + 6f' + 12f'' + 8f'''$ has at least two distinct real zeros.

B2 Given a list of the positive integers $1,2,3,4,\ldots$, take the first three numbers $1,2,3$ and their sum 6 and cross all four numbers off the list. Repeat with the three smallest remaining numbers $4,5,7$ and their sum 16. Continue in this way, crossing off the three smallest remaining numbers and their sum, and consider the sequence of sums produced: $6,16,27,36,\ldots$. Prove or disprove that there is some number in the sequence whose base 10 representation ends with 2015.

B3 Let $S$ be the set of all $2\times 2$ real matrices

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

whose entries $a,b,c,d$ (in that order) form an arithmetic progression. Find all matrices $M$ in $S$ for which there is some integer $k > 1$ such that $M^k$ is also in $S$.

B4 Let $T$ be the set of all triples $(a,b,c)$ of positive integers for which there exist triangles with side lengths $a,b,c$. Express

$$\sum_{(a,b,c)\in T}\frac{2^a}{3^b5^c}$$

as a rational number in lowest terms.

B5 Let $P_n$ be the number of permutations $\pi$ of $\{1,2,\ldots,n\}$ such that

$$|i-j| = 1 \text{ implies } |\pi(i) - \pi(j)| \leq 2$$

for all $i,j$ in $\{1,2,\ldots,n\}$. Show that for $n \geq 2$, the quantity

$$P_{n+5} - P_{n+4} - P_{n+3} + P_n$$

does not depend on $n$, and find its value.

B6 For each positive integer $k$, let $A(k)$ be the number of odd divisors of $k$ in the interval $[1,\sqrt{2k})$. Evaluate

$$\sum_{k=1}^{\infty}(-1)^{k-1}\frac{A(k)}{k}.$$

# Solutions to the 76th William Lowell Putnam Mathematical Competition
## Saturday, December 5, 2015

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A1 **First solution:** Without loss of generality, assume that $A$ and $B$ lie in the first quadrant with $A = (t_1, 1/t_1)$, $B = (t_2, 1/t_2)$, and $t_1 < t_2$. If $P = (t, 1/t)$ with $t_1 \leq t \leq t_2$, then the area of triangle $APB$ is

$$\frac{1}{2}\begin{vmatrix} 1 & 1 & 1 \\ t_1 & t & t_2 \\ 1/t_1 & 1/t & 1/t_2 \end{vmatrix} = \frac{t_2 - t_1}{2t_1 t_2}(t_1 + t_2 - t - t_1 t_2/t).$$

When $t_1, t_2$ are fixed, this is maximized when $t + t_1 t_2/t$ is minimized, which by AM-GM exactly holds when $t = \sqrt{t_1 t_2}$.

The line $AP$ is given by $y = \frac{t_1 + t - x}{t t_1}$, and so the area of the region bounded by the hyperbola and $AP$ is

$$\int_{t_1}^{t} \left( \frac{t_1 + t - x}{t t_1} - \frac{1}{x} \right) dx = \frac{t}{2t_1} - \frac{t_1}{2t} - \log\left(\frac{t}{t_1}\right),$$

which at $t = \sqrt{t_1 t_2}$ is equal to $\frac{t_2 - t_1}{2\sqrt{t_1 t_2}} - \log(\sqrt{t_2/t_1})$. Similarly, the area of the region bounded by the hyperbola and $PB$ is $\frac{t_2}{2t} - \frac{t}{2t_2} - \log\frac{t_2}{t}$, which at $t = \sqrt{t_1 t_2}$ is also $\frac{t_2 - t_1}{2\sqrt{t_1 t_2}} - \log(\sqrt{t_2/t_1})$, as desired.

**Second solution:** For any $\lambda > 0$, the map $(x, y) \mapsto (\lambda x, \lambda^{-1} y)$ preserves both areas and the hyperbola $xy = 1$. We may thus rescale the picture so that $A, B$ are symmetric across the line $y = x$, with $A$ above the line. As $P$ moves from $A$ to $B$, the area of $APB$ increases until $P$ passes through the point $(1,1)$, then decreases. Consequently, $P = (1,1)$ achieves the maximum area, and the desired equality is obvious by symmetry. Alternatively, since the hyperbola is convex, the maximum is uniquely achieved at the point where the tangent line is parallel to $AB$, and by symmetry that point is $P$.

A2 **First solution:** One possible answer is 181. By induction, we have $a_n = ((2+\sqrt{3})^n + (2-\sqrt{3})^n)/2 = (\alpha^n + \beta^n)/2$ for all $n$, where $\alpha = 2 + \sqrt{3}$ and $\beta = 2 - \sqrt{3}$. Now note that if $k$ is an odd positive integer and $a_n \neq 0$, then $\frac{a_{kn}}{a_n} = \frac{\alpha^{kn} + \beta^{kn}}{\alpha^n + \beta^n} = \alpha^{(k-1)n} - \alpha^{(k-2)n}\beta^n + \cdots - \alpha^n \beta^{(k-2)n} + \beta^{(k-1)n}$. This expression is both rational (because $a_n$ and $a_{kn}$ are integers) and of the form $a + b\sqrt{3}$ for some integers $a, b$ by the expressions for $\alpha, \beta$; it follows that it must be an integer, and so $a_{kn}$ is divisible by $a_n$. Applying this to $n = 5$ and $k = 403$, we find that $a_{2015}$ is divisible by $a_5 = 362$ and thus by 181.

**Second solution:** By rewriting the formula for $a_n$ as $a_{n-2} = 4a_{n-1} - a_n$, we may extend the sequence backwards to define $a_n$ for all integers $n$. Since $a_{-1} = 2$, we may see by induction that $a_{-n} = a_n$ for all $n$. For any integer $m$ and any prime $p$ dividing $a_m$, $p$ also divides $a_{-m}$; on the other hand, $p$ cannot divide $a_{-m+1}$, as otherwise $p$ would also divide $a_{-m+2}, \dots, a_0 = 1$, a contradiction. We can thus find an integer $k$ such that $a_{m+1} \equiv k a_{-m+1} \pmod{p}$; by induction on $n$, we see that $a_n \equiv k a_{n-2m} \pmod{p}$ for all $n$. In particular, if $k$ is odd, then $p$ also divides $a_{km}$; we thus conclude (again) that $a_{2015}$ is divisible by $a_5 = 362$ and thus by 181.

**Remark:** Although it was not needed in the solution, we note in passing that if $a_n \equiv 0 \pmod{p}$, then $a_{2n+k} \equiv -a_k \pmod{p}$ for all $k$.

**Remark:** One can find other odd prime factors of $a_{2015}$ in the same manner. For example, $a_{2015}$ is divisible by each of the following quantities. (The prime factorizations were computed using the `Magma` computer algebra system.)

$$\begin{aligned}
a_{13} &= 2 \times 6811741 \\
a_{31} &= 2 \times 373 \times 360250962984637 \\
a_{5\cdot 13} &= 2 \times 181 \times 6811741 \\
&\quad \times 30450462746793166547613561 61 \\
a_{5\cdot 31} &= 1215497709121 \times 28572709494917432101 \\
&\quad \times 1327736055550617981699782712637588158 1 \\
a_{13\cdot 31} &= 2 \times 373 \times 193441 \times 6811741 \times 360250962984637 \\
&\quad \times 16866100753000669 \\
&\quad \times 7998838799247065691659453196 1 \times p_{156}
\end{aligned}$$

where $p_{156}$ is a prime of 156 decimal digits. Dividing $a_{2015}$ by the product of the primes appearing in this list yields a number $N$ of 824 decimal digits which is definitely not prime, because $2^N \not\equiv 2 \pmod{N}$, but whose prime factorization we have been unable to establish. Note that $N$ is larger than a 2048-bit RSA modulus, so the difficulty of factoring it is not surprising.

One thing we can show is that each prime factor of $N$ is congruent to 1 modulo $6 \times 2015 = 12090$, thanks to the following lemma.

**Lemma.** *Let $n$ be an odd integer. Then any odd prime factor $p$ of $a_n$ which does not divide $a_m$ for any divisor $m$ of $n$ is congruent to 1 modulo $\mathrm{lcm}(6, n)$. (By either solution of the original problem, $p$ also does not divide $a_m$ for any positive integer $m < n$.)*

*Proof.* We first check that $p \equiv 1 \pmod{3}$. In $\mathbb{F}_q = \mathbb{F}_p(\sqrt{3})$ we have $(\alpha/\beta)^n \equiv -1$. If $p \equiv 2 \pmod{3}$, then $q = p^2$ and $\alpha$ and $\beta$ are conjugate in $p$; consequently, the equality $\alpha^n = -\beta^n$ in $\mathbb{F}_{q^2}$ means that $\alpha^n = c\sqrt{3}$, $\beta^n = -c\sqrt{3}$ for some $c \in \mathbb{F}_p$. But then $-3c^2 = \alpha^n \beta^n = 1$ in $\mathbb{F}_q$ and hence in $\mathbb{F}_p$, which contradicts $p \equiv 2 \pmod{3}$ by quadratic reciprocity.

By the previous paragraph, $\alpha$ and $\beta$ may be identified with elements of $\mathbb{F}_p$, and we have $(\alpha/\beta)^n \equiv -1$, but the same does not hold with $n$ replaced by any smaller value. Since $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, this forces $p \equiv 1 \pmod{n}$ as claimed. $\square$

A3 The answer is 13725. We first claim that if $n$ is odd, then $\prod_{b=1}^n (1+e^{2\pi iab/n}) = 2^{\gcd(a,n)}$. To see this, write $d = \gcd(a,n)$ and $a = da_1$, $n = dn_1$ with $\gcd(a_1,n_1) = 1$. Then $a_1, 2a_1, \dots, n_1a_1$ modulo $n_1$ is a permutation of $1,2,\dots,n_1$ modulo $n_1$, and so $\omega^{a_1}, \omega^{2a_1}, \dots, \omega^{n_1a_1}$ is a permutation of $\omega, \omega^2, \dots, \omega^{n_1}$; it follows that for $\omega = e^{2\pi i/n_1}$,

$$\prod_{b=1}^{n_1} (1+e^{2\pi iab/n}) = \prod_{b=1}^{n_1} (1+e^{2\pi ia_1b/n_1}) = \prod_{b=1}^{n_1} (1+\omega^b).$$

Now since the roots of $z^{n_1}-1$ are $\omega, \omega^2, \dots, \omega^{n_1}$, it follows that $z^{n_1}-1 = \prod_{b=1}^{n_1}(z-\omega^b)$. Setting $z=-1$ and using the fact that $n_1$ is odd gives $\prod_{b=1}^{n_1}(1+\omega^b) = 2$.

Finally, $\prod_{b=1}^n (1+e^{2\pi iab/n}) = (\prod_{b=1}^{n_1}(1+e^{2\pi iab/n}))^d = 2^d$, and we have proven the claim.

From the claim, we find that

$$\begin{aligned}
&\log_2 \left( \prod_{a=1}^{2015} \prod_{b=1}^{2015} (1+e^{2\pi iab/2015}) \right) \\
&= \sum_{a=1}^{2015} \log_2 \left( \prod_{b=1}^{2015} (1+e^{2\pi iab/2015}) \right) \\
&= \sum_{a=1}^{2015} \gcd(a, 2015).
\end{aligned}$$

Now for each divisor $d$ of 2015, there are $\phi(2015/d)$ integers between 1 and 2015 inclusive whose gcd with 2015 is $d$. Thus

$$\sum_{a=1}^{2015} \gcd(a,2015) = \sum_{d|2015} d \cdot \phi(2015/d).$$

We factor $2015 = pqr$ with $p=5$, $q=13$, and $r=31$, and calculate

$$\begin{aligned}
&\sum_{d|pqr} d \cdot \phi(pqr/d) \\
&= 1 \cdot (p-1)(q-1)(r-1) + p \cdot (q-1)(r-1) \\
&\quad + q \cdot (p-1)(r-1) + r \cdot (p-1)(q-1) + pq \cdot (r-1) \\
&\quad + pr \cdot (q-1) + qr \cdot (p-1) + pqr \cdot 1 \\
&= (2p-1)(2q-1)(2r-1).
\end{aligned}$$

When $(p,q,r) = (5,13,31)$, this is equal to 13725.

**Remark:** Noam Elkies suggests the following similar but shorter derivation of the equality $\prod_{b=1}^{n_1}(1+\omega^b) = 2$: write

$$\prod_{b=1}^{n_1-1} (1+\omega^b) = \frac{\prod_{b=1}^{n_1-1}(1-\omega^{2b})}{\prod_{b=1}^{n_1-1}(1-\omega^b)}$$

and note (as above) that $\omega^2, \omega^4, \dots, \omega^{2(n_1-1)}$ is a permutation of $\omega, \dots, \omega^{n_1-1}$, so the two products in the fraction are equal.

**Remark:** The function $f(n) = \sum_{d|n} d \cdot \phi(n/d)$ is multiplicative: for any two coprime positive integers $m,n$, we have $f(mn) = f(m)f(n)$. This follows from the fact that $f(n)$ is the convolution of the two multiplicative functions $n \mapsto n$ and $n \mapsto \phi(n)$; it can also be seen directly using the Chinese remainder theorem.

A4 The answer is $L = 4/7$. For $S \subset \mathbb{N}$, let $F(S) = \sum_{n \in S} 1/2^n$, so that $f(x) = F(S_x)$. Note that for $T = \{1,4,7,10,\dots\}$, we have $F(T) = 4/7$.

We first show by contradiction that for any $x \in [0,1)$, $f(x) \geq 4/7$. Since each term in the geometric series $\sum_n 1/2^n$ is equal to the sum of all subsequent terms, if $S, S'$ are different subsets of $\mathbb{N}$ and the smallest positive integer in one of $S, S'$ but not in the other is in $S$, then $F(S) \geq F(S')$. Assume $f(x) < 4/7$; then the smallest integer in one of $S_x, T$ but not in the other is in $T$. Now $1 \in S_x$ for any $x \in [0,1)$, and we conclude that there are three consecutive integers $n, n+1, n+2$ that are not in $S_x$: that is, $\lfloor nx \rfloor$, $\lfloor (n+1)x \rfloor$, $\lfloor (n+2)x \rfloor$ are all odd. Since the difference between consecutive terms in $nx$, $(n+1)x$, $(n+2)x$ is $x < 1$, we conclude that $\lfloor nx \rfloor = \lfloor (n+1)x \rfloor = \lfloor (n+2)x \rfloor$ and so $x < 1/2$. But then $2 \in S_x$ and so $f(x) \geq 3/4$, contradicting our assumption.

It remains to show that $4/7$ is the greatest lower bound for $f(x)$, $x \in [0,1)$. For any $n$, choose $x = 2/3 - \varepsilon$ with $0 < \varepsilon < 1/(9n)$; then for $1 \leq k \leq n$, we have $0 < m\varepsilon < 1/3$ for $m \leq 3n$, and so

$$\begin{aligned}
\lfloor (3k-2)x \rfloor &= \lfloor (2k-2) + 2/3 - (3k-2)\varepsilon \rfloor = 2k-2 \\
\lfloor (3k-1)x \rfloor &= \lfloor (2k-1) + 1/3 - (3k-1)\varepsilon \rfloor = 2k-1 \\
\lfloor (3k)x \rfloor &= \lfloor (2k-1) + 1 - 3k\varepsilon \rfloor = 2k-1.
\end{aligned}$$

It follows that $S_x$ is a subset of $S = \{1,4,7,\dots,3n-2,3n+1,3n+2,3n+3,\dots\}$, and so $f(x) = F(S_x) \leq f(S) = (1/2 + 1/2^4 + \cdots + 1/2^{3n+1}) + 1/2^{3n+1}$. This last expression tends to $4/7$ as $n \to \infty$, and so no number greater than $4/7$ can be a lower bound for $f(x)$ for all $x \in [0,1)$.

A5 **First solution:** By inclusion-exclusion, we have

$$\begin{aligned}
N_q &= \sum_{d|q} \mu(d) \left\lfloor \frac{\lfloor q/4 \rfloor}{d} \right\rfloor \\
&= \sum_{d|q} \mu(d) \left\lfloor \frac{q/d}{4} \right\rfloor \\
&\equiv \sum_{d|q \text{ squarefree}} \left\lfloor \frac{q/d}{4} \right\rfloor \pmod{2},
\end{aligned}$$

where $\mu$ is the Möbius function. Now

$$\left\lfloor \frac{q/d}{4} \right\rfloor \equiv \begin{cases} 0 \pmod{2} & \text{if } q/d \equiv 1,3 \pmod{8} \\ 1 \pmod{2} & \text{if } q/d \equiv 5,7 \pmod{8}. \end{cases}$$

So $N_q$ is odd if and only if $q$ has an odd number of squarefree factors $q/d$ congruent to 5 or 7 (mod 8).

If $q$ has a prime factor $p$ congruent to 1 or 3 (mod 8), then the squarefree factors $d$ of $q$ occur in pairs $c, pc$, which are either both 1 or 3 (mod 8) or both 5 or 7 (mod 8). Hence $q$ must have an even number of factors that are congruent to 5 or 7 (mod 8), and so $N_q$ is even in this case.

If $q$ has two prime factors $p_1$ and $p_2$, each congruent to either 5 or 7 (mod 8), then the squarefree factors $d$ of $q$ occur in quadruples $d, p_1d, q_1d, p_1q_1d$, which are then congruent respectively to some permutation of 1,3,5,7 (mod 8) (if $p_1$ and $p_2$ are distinct mod 8) or are congruent respectively to $d, p_1d, p_1d, d$ (mod 8). Either way, we see that exactly two of the four residues are congruent to 5 or 7 (mod 8). Thus again $q$ must have an even number of factors that are 5 or 7 (mod 8), and so $N_q$ is even in this case as well.

If $q = 1$, then $N_q = 0$ is even. The only case that remains is that $q = p^k$ is a positive power of a prime $p$ congruent to 5 or 7 (mod 8). In this case, $q$ has two squarefree factors, 1 and $p$, of which exactly one is congruent to 5 or 7 (mod 8). We conclude that $N_q$ is odd in this case, as desired.

**Second solution:**

Consider the set $S$ of all integers in $\{1,\dots,q-1\}$ that are even and relatively prime to $q$. Then the product of all elements in $S$ is

$$2^{\phi(q)/2} \prod_{\substack{1\leq a\leq (q-1)/2\\ (a,q)=1}} a.$$

On the other hand, we can rewrite the set of elements in $S \pmod q$ as a set $T$ of residues in the interval $[-(q-1)/2,(q-1)/2]$. Then for each $1 \leq a \leq (q-1)/2$ with $(a,q) = 1$, $T$ contains exactly one element from $\{a,-a\}$: if $-2r \equiv 2s \pmod q$ for some $r,s \in \{1,\dots,(q-1)/2\}$, then $r \equiv -s \pmod q$, which is impossible given the ranges of $r$ and $s$. Thus the product of all elements in $T$ is

$$(-1)^n \prod_{\substack{1\leq a\leq (q-1)/2\\ (a,q)=1}} a,$$

where $n$ denotes the number of elements of $S$ greater than $(q-1)/2$. We conclude that $(-1)^n \equiv 2^{\phi(q)/2} \pmod q$.

However, note that the number of elements of $S$ less than $(q-1)/2$ is equal to $N_q$, since dividing these numbers by 2 gives exactly the numbers counted by $N_q$. Hence the total cardinality of $S$ is $N_q + n$; however, this cardinality also equals $\phi(q)/2$ because the numbers in $\{1,\dots,q-1\}$ relatively prime to $q$ come in pairs $\{a, q-a\}$ in each of which exactly one member is even. We thus obtain

$$\begin{aligned}(-1)^{N_q} &= (-1)^{\phi(q)/2+n} \\ &\equiv (-1)^{\phi(q)/2}2^{\phi(q)/2} = (-2)^{\phi(q)/2} \pmod q.\end{aligned}$$

If $q = 1$, then $N_q$ is even. If $q$ has more than one prime factor, then the group $(\mathbb{Z}/q\mathbb{Z})^\times$ has exponent dividing $\phi(q)/2$, so $(-1)^{N_q} \equiv (-2)^{\phi(q)/2} \equiv 1 \pmod q$, and thus $N_q$ must be even in this case as well. Finally, suppose that $q$ is a prime power $p^k$ with $p$ odd and $k$ positive. Since $(\mathbb{Z}/q\mathbb{Z})^\times$ is a cyclic group of order $\phi(q) = p^{k-1}(p-1)$, in which the only square roots of unity are $\pm 1$, it follows that $(-2)^{\phi(q)/2} \equiv \pm 1 \pmod q$ in accordance with whether $(-2)^{(p-1)/2} \equiv \pm 1 \pmod p$, i.e., whether $-2$ is a quadratic residue or nonresidue. But recall that $-2$ is a quadratic residue modulo $p$ if and only if $p \equiv 1,3 \pmod 8$. Thus $N_q$ is odd in this case if and only if $p \equiv 5$ or $7 \pmod 8$.

We conclude that for any odd integer $q \geq 1$, the quantity $N_q$ is odd if and only if $q = p^k$ with $k$ positive and $p$ a prime that is 5 or 7 (mod 8).

**Remark:** The combination of the two solutions recovers Gauss's criterion for when $-2$ is a quadratic residue modulo $p$, with essentially the original proof.

A6 **First solution:** (by Noam Elkies) Using row and column operations, we may construct invertible matrices $U,V$ such that $U^{-1}MV$ is a block diagonal matrix of the form

$$\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$

Put $A' = U^{-1}AU, M' = U^{-1}MV, B' = V^{-1}BV,\ X' = V^{-1}XU$, so that $A'M' = M'B'$, $\det(A-MX) = \det(U^{-1}(A-MX)U) = \det(A'-M'X')$, and $\det(B-XM) = \det(V^{-1}(B-XM)V) = \det(B'-X'M')$. Form the corresponding block decompositions

$$A' = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}, B' = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}, X' = \begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix}.$$

We then have

$$A'M' = \begin{pmatrix} A_{11} & 0 \\ A_{21} & 0 \end{pmatrix}, \qquad M'B' = \begin{pmatrix} B_{11} & B_{12} \\ 0 & 0 \end{pmatrix},$$

so we must have $A_{11} = B_{11}$ and $A_{21} = B_{12} = 0$; in particular, the characteristic polynomial of $A$ is the product of the characteristic polynomials of $A_{11}$ and $A_{22}$, and the characteristic polynomial of $B$ is the product of the characteristic polynomials of $B_{11}$ and $B_{22}$. Since $A_{11} = B_{11}$, it follows that $A_{22}$ and $B_{22}$ have the same characteristic polynomial. Since

$$X'M' = \begin{pmatrix} X_{11} & 0 \\ X_{21} & 0 \end{pmatrix}, \qquad M'X' = \begin{pmatrix} X_{11} & X_{12} \\ 0 & 0 \end{pmatrix},$$

we conclude that

$$\begin{aligned}\det(A-MX) &= \det(A'-M'X') \\ &= \det\begin{pmatrix} A_{11}-X_{11} & A_{12}-X_{12} \\ 0 & A_{22}\end{pmatrix} \\ &= \det(A_{11}-X_{11})\det(A_{22}) \\ &= \det(B_{11}-X_{11})\det(B_{22}) \\ &= \det\begin{pmatrix} B_{11}-X_{11} & 0 \\ B_{21}-X_{21} & B_{22}\end{pmatrix} \\ &= \det(B'-X'M') \\ &= \det(B-XM),\end{aligned}$$

as desired. (By similar arguments, $A-MX$ and $B-XM$ have the same characteristic polynomial.)

**Second solution:** We prove directly that $A-MX$ and $B-XM$ have the same characteristic polynomial, i.e., for any $t \in \mathbb{R}$, writing $A_t = A-tI$, $B_t = B-tI$, we have

$$\det(A_t - MX) = \det(B_t - XM).$$

For fixed $A,B,M$, the stated result is a polynomial identity in $t$ and the entries of $X$. It thus suffices to check it assuming that $A_t, B_t, X$ are all invertible. Since $AM = MB$, we also have $A_tM = MB_t$, so $A_tMB_t^{-1} = M$. Since $\det(A_t) = \det(B_t)$ by hypothesis,

$$\begin{aligned}\det(A_t-MX) &= \det(A_t - A_tMB_t^{-1}X) \\ &= \det(A_t)\det(1-MB_t^{-1}X) \\ &= \det(A_t)\det(X)\det(B_t)^{-1}\det(X^{-1}B_t - M) \\ &= \det(X)\det(X^{-1}B_t-M) \\ &= \det(B_t - XM).\end{aligned}$$

**Remark:** One can also assert directly that $\det(1-MB_t^{-1}X) = \det(1-XMB_t^{-1})$ using the fact that for any square matrices $U$ and $V$, $UV$ and $VU$ have the same characteristic polynomial; the latter is again proved by reducing to the case where one of the two matrices is invertible, in which case the two matrices are similar.

**Third solution:** (by Lev Borisov) We will check that for each positive integer $k$,

$$\mathrm{Trace}((A-MX)^k) = \mathrm{Trace}((B-XM)^k).$$

This will imply that $A-MX$ and $B-XM$ have the same characteristic polynomial, yielding the desired result.

We establish the claim by expanding both sides and comparing individual terms. By hypothesis, $A^k$ and $B^k$ have the same characteristic polynomial, so $\mathrm{Trace}(A^k) = \mathrm{Trace}(B^k)$. To compare the other terms, it suffices to check that for any sequence $i_1, i_2, \dots, i_m$ of nonnegative integers,

$$\begin{aligned}&\mathrm{Trace}(A^{i_1}MXA^{i_2}MX\cdots A^{i_{m-1}}MXA^{i_m}) \\ &\quad = \mathrm{Trace}(B^{i_1}XMB^{i_2}XM\cdots B^{i_{m-1}}XMB^{i_m}).\end{aligned}$$

To establish this equality, first apply the remark following the previous solution to write

$$\begin{aligned}&\mathrm{Trace}(A^{i_1}MXA^{i_2}MX\cdots A^{i_{m-1}}MXA^{i_m}) \\ &\quad = \mathrm{Trace}(A^{i_m+i_1}MXA^{i_2}MX\cdots A^{i_{m-1}}MX).\end{aligned}$$

Then apply the relation $AM = MB$ repeatedly to commute $M$ past $A$, to obtain

$$\mathrm{Trace}(MB^{i_m+i_1}XMB^{i_2}XM\cdots XMB^{i_{m-1}}X).$$

Finally, apply the remark again to shift $MB^{i_m}$ from the left end to the right end.

**Remark:** The conclusion holds with $\mathbb{R}$ replaced by an arbitrary field. In the second solution, one must reduce to the case of an infinite field, e.g., by replacing the original field with an algebraic closure. The third solution only applies to fields of characteristic 0 or positive characteristic greater than $n$.

**Remark:** It is tempting to try to reduce to the case where $M$ is invertible, as in this case $A-MX$ and $B-XM$ are in fact similar. However, it is not clear how to make such an argument work.

B1 Let $g(x) = e^{x/2}f(x)$. Then $g$ has at least 5 distinct real zeroes, and by repeated applications of Rolle's theorem, $g', g'', g'''$ have at least $4,3,2$ distinct real zeroes, respectively. But

$$g'''(x) = \frac{1}{8}e^{x/2}(f(x) + 6f'(x) + 12f''(x) + 8f'''(x))$$

and $e^{x/2}$ is never zero, so we obtain the desired result.

B2 We will prove that 42015 is such a number in the sequence. Label the sequence of sums $s_0, s_1, \dots,$ and let $a_n, b_n, c_n$ be the summands of $s_n$ in ascending order. We prove the following two statements for each nonnegative integer $n$:

$(\mathrm{a})_n$ The sequence

$$a_{3n}, b_{3n}, c_{3n}, a_{3n+1}, b_{3n+1}, c_{3n+1}, a_{3n+2}, b_{3n+2}, c_{3n+2}$$

is obtained from the sequence $10n+1, \dots, 10n+10$ by removing one of $10n+5, 10n+6, 10n+7$.

$(\mathrm{b})_n$ We have

$$\begin{aligned}s_{3n} &= 30n+6, \\ s_{3n+1} &\in \{30n+15, 30n+16, 30n+17\}, \\ s_{3n+2} &= 30n+27.\end{aligned}$$

These statements follow by induction from the following simple observations:

– by computing the table of values

| $n$ | $a_n$ | $b_n$ | $c_n$ | $s_n$ |
|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 6 |
| 1 | 4 | 5 | 7 | 16 |
| 2 | 8 | 9 | 10 | 27 |

we see that $(\mathrm{a})_0$ holds;

– $(a)_n$ implies $(b)_n$;

– $(a)_n$ and $(b)_1, \dots, (b)_n$ together imply $(a)_{n+1}$.

To produce a value of $n$ for which $s_n \equiv 2015 \pmod{10000}$, we take $n = 3m+1$ for some nonnegative integer $m$ for which $s_{3m+1} = 30m+15$. We must also have $30m \equiv 2000 \pmod{10000}$, or equivalently $m \equiv 400 \pmod{1000}$. By taking $m = 1400$, we ensure that $m \equiv 2 \pmod 3$, so $s_m = 10m+7$; this ensures that $s_n$ does indeed equal $30m+15 = 42015$, as desired.

**Remark:** With a bit more work, we can give a complete description of $s_n$, and in particular find the first term in the sequence whose decimal expansion ends in 2015. Define the function on nonnegative integers

$$f(n) = s_{3n+1} - (30n+16)$$

which takes values in $\{-1,0,1\}$; we then have

$$f(n) = \begin{cases} 0 & n \equiv 0 \pmod 3 \\ -f((n-1)/3) & n \equiv 1 \pmod 3 \\ -1 & n \equiv 2 \pmod 3. \end{cases}$$

Consequently, if we write $n$ in base 3, then $f(n) = 0$ unless the expansion ends with 2 followed by a string of 1s of length $k \geq 0$, in which case $f(n) = (-1)^{k+1}$.

In this notation, we have $s_n \equiv 2015 \pmod{10000}$ if and only if $n = 3m+1$ for some nonnegative integer $m$ for which $m \equiv 400 \pmod{1000}$ and $f(m) = -1$. Since $400 = 112211_{(3)}$, the first such term in the sequence is in fact $s_{1201} = 12015$.

B3 **First solution:** Any element of $S$ can be written as $M = \alpha A + \beta B$, where $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} -3 & -1 \\ 1 & 3 \end{smallmatrix}\right)$, and $\alpha, \beta \in \mathbb{R}$. Note that $A^2 = \left(\begin{smallmatrix} 4 & 4 \\ 4 & 4 \end{smallmatrix}\right)$ and $B^3 = \left(\begin{smallmatrix} -24 & -8 \\ 8 & 24 \end{smallmatrix}\right)$ are both in $S$, and so any matrix of the form $\alpha A$ or $\beta B$, $\alpha, \beta \in \mathbb{R}$, satisfies the given condition.

We claim that these are also the only matrices in $S$ satisfying the given condition. Indeed, suppose $M = \alpha A + \beta B$ where $\alpha, \beta \neq 0$. Let $C = \left(\begin{smallmatrix} 1 & 1/\sqrt{2} \\ -1 & 1/\sqrt{2} \end{smallmatrix}\right)$ with inverse $C^{-1} = \left(\begin{smallmatrix} 1/2 & -1/2 \\ 1/\sqrt{2} & 1/\sqrt{2} \end{smallmatrix}\right)$. If we define $D = C^{-1}MC$, then $D = 2\alpha \left(\begin{smallmatrix} 0 & \gamma \\ \gamma & 1 \end{smallmatrix}\right)$ where $\gamma = -\frac{\beta\sqrt{2}}{\alpha}$. Now suppose that $M^k$ is in $S$ with $k \geq 2$. Since $\left(\begin{smallmatrix} 1 & -1 \end{smallmatrix}\right) A \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & -1 \end{smallmatrix}\right) B \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right) = 0$, we have $\left(\begin{smallmatrix} 1 & -1 \end{smallmatrix}\right) M^k \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right) = 0$, and so the upper left entry of $C^{-1}M^kC = D^k$ is 0. On the other hand, from the expression for $D$, an easy induction on $k$ shows that $D^k = (2\alpha)^k \left(\begin{smallmatrix} \gamma^2 p_{k-1} & \gamma p_k \\ \gamma p_k & p_{k+1} \end{smallmatrix}\right)$, where $p_k$ is defined inductively by $p_0 = 0$, $p_1 = 1$, $p_{k+2} = \gamma^2 p_k + p_{k+1}$. In particular, it follows from the inductive definition that $p_k > 0$ when $k \geq 1$, whence the upper left entry of $D^k$ is nonzero when $k \geq 2$, a contradiction.

**Remark:** A variant of this solution can be obtained by diagonalizing the matrix $M$.

**Second solution:** If $a,b,c,d$ are in arithmetic progression, then we may write

$$a = r-3s, b = r-s, c = r+s, d = r+3s$$

for some $r,s$. If $s = 0$, then clearly all powers of $M$ are in $xS$. Also, if $r = 0$, then one easily checks that $M^3$ is in $S$.

We now assume $rs \neq 0$, and show that in that case $M$ cannot be in $S$. First, note that the characteristic polynomial of $M$ is $x^2 - 2rx - 8s^2$, and since $M$ is nonsingular (as $s \neq 0$), this is also the minimal polynomial of $M$ by the Cayley-Hamilton theorem. By repeatedly using the relation $M^2 = 2rM + 8s^2I$, we see that for each positive integer, we have $M^k = t_kM + u_kI$ for unique real constants $t_k, u_k$ (uniqueness follows from the independence of $M$ and $I$). Since $M$ is in $S$, we see that $M^k$ lies in $S$ only if $u_k = 0$.

On the other hand, we claim that if $k > 1$, then $rt_k > 0$ and $u_k > 0$ if $k$ is even, and $t_k > 0$ and $ru_k > 0$ if $k$ is odd (in particular, $u_k$ can never be zero). The claim is true for $k = 2$ by the relation $M^2 = 2rM + 8s^2I$. Assuming the claim for $k$, and multiplying both sides of the relation $M^k = t_kM + u_kI$ by $M$, yields

$$M^{k+1} = t_k(2rM + 8s^2I) + u_kM = (2rt_k + u_k)M + 8s^2t_kI,$$

implying the claim for $k+1$.

**Remark:** (from `artofproblemsolving.com`, user `hoeij`) Once one has $u_k = 0$, one can also finish using the relation $M \cdot M^k = M^k \cdot M$.

B4 **First solution:** The answer is $17/21$. For fixed $b,c$, there is a triangle of side lengths $a,b,c$ if and only if $|b-c| < a < b+c$. It follows that the desired sum is

$$S = \sum_{b,c} \frac{1}{3^b5^c} \left( \sum_{a=|b-c|+1}^{b+c-1} 2^a \right) = \sum_{b,c} \frac{2^{b+c} - 2^{|b-c|+1}}{3^b5^c}.$$

We write this as $S = S_1 + S_2$ where $S_1$ sums over positive integers $b,c$ with $b \leq c$ and $S_2$ sums over $b > c$. Then

$$\begin{aligned} S_1 &= \sum_{b=1}^\infty \sum_{c=b}^\infty \frac{2^{b+c} - 2^{c-b+1}}{3^b5^c} \\ &= \sum_{b=1}^\infty \left( \left( \left(\frac{2}{3}\right)^b - \frac{2}{6^b} \right) \sum_{c=b}^\infty \left(\frac{2}{5}\right)^c \right) \\ &= \sum_{b=1}^\infty \left( \left(\frac{2}{3}\right)^b - \frac{2}{6^b} \right) \frac{5}{3} \left(\frac{2}{5}\right)^b \\ &= \sum_{b=1}^\infty \left( \frac{5}{3} \left(\frac{4}{15}\right)^b - \frac{10}{3} \left(\frac{1}{15}\right)^b \right) \\ &= \frac{85}{231}. \end{aligned}$$

Similarly,

$$\begin{aligned}
S_2 &= \sum_{c=1}^{\infty}\sum_{b=c+1}^{\infty}\frac{2^{b+c}-2^{b-c+1}}{3^b5^c}\\
&= \sum_{c=1}^{\infty}\left(\left(\left(\frac{2}{5}\right)^c-\frac{2}{10^c}\right)\sum_{b=c+1}^{\infty}\left(\frac{2}{3}\right)^b\right)\\
&= \sum_{c=1}^{\infty}\left(\left(\frac{2}{5}\right)^c-\frac{2}{10^c}\right)3\left(\frac{2}{3}\right)^{c+1}\\
&= \sum_{c=1}^{\infty}\left(2\left(\frac{4}{15}\right)^c-4\left(\frac{1}{15}\right)^c\right)\\
&= \frac{34}{77}.
\end{aligned}$$

We conclude that $S = S_1 + S_2 = \frac{17}{21}$.

**Second solution:** Recall that the real numbers $a,b,c$ form the side lengths of a triangle if and only if

$$s-a, s-b, s-c > 0 \qquad s = \frac{a+b+c}{2},$$

and that if we put $x = 2(s-a), y = 2(s-b), z = 2(s-c)$,

$$a = \frac{y+z}{2}, b = \frac{z+x}{2}, c = \frac{x+y}{2}.$$

To generate all *integer* triples $(a,b,c)$ which form the side lengths of a triangle, we must also assume that $x,y,z$ are either all even or all odd. We may therefore write the original sum as

$$\sum_{x,y,z>0 \text{ odd}}\frac{2^{(y+z)/2}}{3^{(z+x)/2}5^{(x+y)/2}} + \sum_{x,y,z>0 \text{ even}}\frac{2^{(y+z)/2}}{3^{(z+x)/2}5^{(x+y)/2}}.$$

To unify the two sums, we substitute in the first case $x = 2u+1, y = 2v+1, z = 2w+1$ and in the second case $x = 2u+2, y = 2v+2, z = 2w+2$ to obtain

$$\begin{aligned}
\sum_{(a,b,c)\in T}\frac{2^a}{3^b5^c} &= \sum_{u,v,w=1}^{\infty}\frac{2^{v+w}}{3^{w+u}5^{u+v}}\left(1+\frac{2^{-1}}{3^{-1}5^{-1}}\right)\\
&= \frac{17}{2}\sum_{u=1}^{\infty}\left(\frac{1}{15}\right)^u\sum_{v=1}^{\infty}\left(\frac{2}{5}\right)^v\sum_{w=1}^{\infty}\left(\frac{2}{3}\right)^w\\
&= \frac{17}{2}\frac{1/15}{1-1/15}\frac{2/5}{1-2/5}\frac{2/3}{1-2/3}\\
&= \frac{17}{21}.
\end{aligned}$$

B5 The answer is 4.

Assume $n \geq 3$ for the moment. We write the permutations $\pi$ counted by $P_n$ as sequences $\pi(1),\pi(2),\dots,\pi(n)$. Let $U_n$ be the number of permutations counted by $P_n$ that end with $n-1,n$; let $V_n$ be the number ending in $n,n-1$; let $W_n$ be the number starting with $n-1$ and ending in $n-2,n$; let $T_n$ be the number ending in $n-2,n$ but not starting with $n-1$; and let $S_n$ be the number which has $n-1,n$ consecutively in that order, but not at the beginning or end. It is clear that every permutation $\pi$ counted by $P_n$ either lies in exactly one of the sets counted by $U_n,V_n,W_n,T_n,S_n$, or is the reverse of such a permutation. Therefore

$$P_n = 2(U_n+V_n+W_n+T_n+S_n).$$

By examining how each of the elements in the sets counted by $U_{n+1},V_{n+1},W_{n+1},T_{n+1},S_{n+1}$ can be obtained from a (unique) element in one of the sets counted by $U_n,V_n,W_n,T_n,S_n$ by suitably inserting the element $n+1$, we obtain the recurrence relations

$$\begin{aligned}
U_{n+1} &= U_n + W_n + T_n,\\
V_{n+1} &= U_n,\\
W_{n+1} &= W_n,\\
T_{n+1} &= V_n,\\
S_{n+1} &= S_n + V_n.
\end{aligned}$$

Also, it is clear that $W_n = 1$ for all $n$.

So far we have assumed $n \geq 3$, but it is straightforward to extrapolate the sequences $P_n,U_n,V_n,W_n,T_n,S_n$ back to $n = 2$ to preserve the preceding identities. Hence for all $n \geq 2$,

$$\begin{aligned}
P_{n+5} &= 2(U_{n+5}+V_{n+5}+W_{n+5}+T_{n+5}+S_{n+5})\\
&= 2((U_{n+4}+W_{n+4}+T_{n+4})+U_{n+4}\\
&\qquad +W_{n+4}+V_{n+4}+(S_{n+4}+V_{n+4}))\\
&= P_{n+4}+2(U_{n+4}+W_{n+4}+V_{n+4})\\
&= P_{n+4}+2((U_{n+3}+W_{n+3}+T_{n+3})+W_{n+3}+U_{n+3})\\
&= P_{n+4}+P_{n+3}+2(U_{n+3}-V_{n+3}+W_{n+3}-S_{n+3})\\
&= P_{n+4}+P_{n+3}+2((U_{n+2}+W_{n+2}+T_{n+2})-U_{n+2}\\
&\qquad +W_{n+2}-(S_{n+2}-V_{n+2}))\\
&= P_{n+4}+P_{n+3}+2(2W_{n+2}+T_{n+2}-S_{n+2}-V_{n+2})\\
&= P_{n+4}+P_{n+3}+2(2W_{n+1}+V_{n+1}\\
&\qquad -(S_{n+1}+V_{n+1})-U_{n+1})\\
&= P_{n+4}+P_{n+3}+2(2W_n+U_n-(S_n+V_n)-U_n\\
&\qquad -(U_n+W_n+T_n))\\
&= P_{n+4}+P_{n+3}-P_n+4,
\end{aligned}$$

as desired.

**Remark:** There are many possible variants of the above solution obtained by dividing the permutations up according to different features. For example, Karl Mahlburg suggests writing

$$P_n = 2P'_n, \qquad P'_n = Q'_n + R'_n$$

where $P'_n$ counts those permutations counted by $P_n$ for which 1 occurs before 2, and $Q'_n$ counts those permutations counted by $P'_n$ for which $\pi(1) = 1$. One then has the recursion

$$Q'_n = Q'_{n-1} + Q'_{n-3} + 1$$

corresponding to the cases where $\pi(1),\pi(2) = 1,2$; where $\pi(1),\pi(2),\pi(3) = 1,3,2$; and the unique case $1,3,5,\dots,6,4,2$. Meanwhile, one has

$$R'_n = R'_{n-1} + Q'_{n-2}$$

corresponding to the cases containing $3,1,2,4$ (where removing 1 and reversing gives a permutation counted by $R'_{n-1}$); and where 4 occurs before $3,1,2$ (where removing $1,2$ and reversing gives a permutation counted by $Q'_{n-2}$).

**Remark:** The permutations counted by $P_n$ are known as *key permutations*, and have been studied by E.S. Page, Systematic generation of ordered sequences using recurrence relations, *The Computer Journal* **14** (1971), no. 2, 150–153. We have used the same notation for consistency with the literature. The sequence of the $P_n$ also appears as entry A003274 in the On-line Encyclopedia of Integer Sequences (`http://oeis.org`).

B6 (from `artofproblemsolving.com`) We will prove that the sum converges to $\pi^2/16$. Note first that the sum does not converge absolutely, so we are not free to rearrange it arbitrarily. For that matter, the standard alternating sum test does not apply because the absolute values of the terms does not decrease to 0, so even the convergence of the sum must be established by hand.

Setting these issues aside momentarily, note that the elements of the set counted by $A(k)$ are those odd positive integers $d$ for which $m = k/d$ is also an integer and $d < \sqrt{2dm}$; if we write $d = 2\ell - 1$, then the condition on $m$ reduces to $m \geq \ell$. In other words, the original sum equals

$$S_1 := \sum_{k=1}^{\infty} \sum_{\substack{\ell \geq 1, m \geq \ell \\ k = m(2\ell-1)}} \frac{(-1)^{m-1}}{m(2\ell-1)},$$

and we would like to rearrange this to

$$S_2 := \sum_{\ell=1}^{\infty} \frac{1}{2\ell-1} \sum_{m=\ell}^{\infty} \frac{(-1)^{m-1}}{m},$$

in which both sums converge by the alternating sum test. In fact a bit more is true: we have

$$\left| \sum_{m=\ell}^{\infty} \frac{(-1)^{m-1}}{m} \right| < \frac{1}{\ell},$$

so the outer sum converges absolutely. In particular, $S_2$ is the limit of the truncated sums

$$S_{2,n} = \sum_{\ell(2\ell-1) \leq n} \frac{1}{2\ell-1} \sum_{m=\ell}^{\infty} \frac{(-1)^{m-1}}{m}.$$

To see that $S_1$ converges to the same value as $S_2$, write

$$S_{2,n} - \sum_{k=1}^{n} (-1)^{k-1} \frac{A(k)}{k} = \sum_{\ell(2\ell-1) \leq n} \frac{1}{2\ell-1} \sum_{m=\lfloor \frac{n}{2\ell-1}+1 \rfloor}^{\infty} \frac{(-1)^{m-1}}{m}.$$

The expression on the right is bounded above in absolute value by the sum $\sum_{\ell(2\ell-1)\leq n} \frac{1}{n}$, in which the number of summands is at most $\sqrt{n}$ (since $\sqrt{n}(2\sqrt{n}-1) \geq n$), and so the total is bounded above by $1/\sqrt{n}$. Hence the difference converges to zero as $n \to \infty$; that is, $S_1$ converges and equals $S_2$.

We may thus focus hereafter on computing $S_2$. We begin by writing

$$S_2 = \sum_{\ell=1}^{\infty} \frac{1}{2\ell-1} \sum_{m=\ell}^{\infty} (-1)^{m-1} \int_0^1 t^{m-1}\,dt.$$

Our next step will be to interchange the inner sum and the integral, but again this requires some justification.

**Lemma 1.** *Let $f_0, f_1, \dots$ be a sequence of continuous functions on $[0,1]$ such that for each $x \in [0,1]$, we have*

$$f_0(x) \geq f_1(x) \geq \cdots \geq 0.$$

*Then*

$$\sum_{n=0}^{\infty} (-1)^n \int_0^1 f_n(t)\,dt = \int_0^1 \left( \sum_{n=0}^{\infty} (-1)^n f_n(t) \right) dt$$

*provided that both sums converge.*

*Proof.* Put $g_n(t) = f_{2n}(t) - f_{2n+1}(t) \geq 0$; we may then rewrite the desired equality as

$$\sum_{n=0}^{\infty} \int_0^1 g_n(t)\,dt = \int_0^1 \left( \sum_{n=0}^{\infty} g_n(t) \right) dt,$$

which is a case of the Lebesgue monotone convergence theorem. □

By Lemma 1, we have

$$\begin{aligned} S_2 &= \sum_{\ell=1}^{\infty} \frac{1}{2\ell-1} \int_0^1 \left( \sum_{m=\ell}^{\infty} (-1)^{m-1} t^{m-1} \right) dt \\ &= \sum_{\ell=1}^{\infty} \frac{1}{2\ell-1} \int_0^1 \frac{(-t)^{\ell-1}}{1+t}\,dt. \end{aligned}$$

Since the outer sum is absolutely convergent, we may freely interchange it with the integral:

$$\begin{aligned} S_2 &= \int_0^1 \left( \sum_{\ell=1}^{\infty} \frac{1}{2\ell-1} \frac{(-t)^{\ell-1}}{1+t} \right) dt \\ &= \int_0^1 \frac{1}{\sqrt{t}(1+t)} \left( \sum_{\ell=1}^{\infty} \frac{(-1)^{\ell-1} t^{\ell-1/2}}{2\ell-1} \right) dt \\ &= \int_0^1 \frac{1}{\sqrt{t}(1+t)} \arctan(\sqrt{t})\,dt \\ &= \int_0^1 \frac{2}{1+u^2} \arctan(u)\,du \qquad (u = \sqrt{t}) \\ &= \arctan(1)^2 - \arctan(0)^2 = \frac{\pi^2}{16}. \end{aligned}$$

# The 77th William Lowell Putnam Mathematical Competition
# Saturday, December 3, 2016

A1 Find the smallest positive integer $j$ such that for every polynomial $p(x)$ with integer coefficients and for every integer $k$, the integer

$$p^{(j)}(k) = \left. \frac{d^j}{dx^j} p(x) \right|_{x=k}$$

(the $j$-th derivative of $p(x)$ at $k$) is divisible by 2016.

A2 Given a positive integer $n$, let $M(n)$ be the largest integer $m$ such that

$$\binom{m}{n-1} > \binom{m-1}{n}.$$

Evaluate

$$\lim_{n\to\infty} \frac{M(n)}{n}.$$

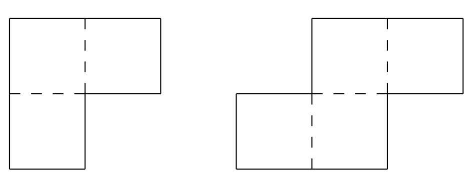
A3 Suppose that $f$ is a function from $\mathbb{R}$ to $\mathbb{R}$ such that

$$f(x) + f\left(1 - \frac{1}{x}\right) = \arctan x$$

for all real $x \neq 0$. (As usual, $y = \arctan x$ means $-\pi/2 < y < \pi/2$ and $\tan y = x$.) Find

$$\int_0^1 f(x)\,dx.$$

A4 Consider a $(2m-1)\times(2n-1)$ rectangular region, where $m$ and $n$ are integers such that $m,n \geq 4$. This region is to be tiled using tiles of the two types shown:



(The dotted lines divide the tiles into $1\times 1$ squares.) The tiles may be rotated and reflected, as long as their sides are parallel to the sides of the rectangular region. They must all fit within the region, and they must cover it completely without overlapping.

What is the minimum number of tiles required to tile the region?

A5 Suppose that $G$ is a finite group generated by the two elements $g$ and $h$, where the order of $g$ is odd. Show that every element of $G$ can be written in the form

$$g^{m_1} h^{n_1} g^{m_2} h^{n_2} \cdots g^{m_r} h^{n_r}$$

with $1 \leq r \leq |G|$ and $m_1, n_1, m_2, n_2, \ldots, m_r, n_r \in \{-1, 1\}$. (Here $|G|$ is the number of elements of $G$.)

A6 Find the smallest constant $C$ such that for every real polynomial $P(x)$ of degree 3 that has a root in the interval $[0,1]$,

$$\int_0^1 |P(x)|\,dx \leq C \max_{x\in[0,1]} |P(x)|.$$

B1 Let $x_0, x_1, x_2, \ldots$ be the sequence such that $x_0 = 1$ and for $n \geq 0$,

$$x_{n+1} = \ln(e^{x_n} - x_n)$$

(as usual, the function ln is the natural logarithm). Show that the infinite series

$$x_0 + x_1 + x_2 + \cdots$$

converges and find its sum.

B2 Define a positive integer $n$ to be *squarish* if either $n$ is itself a perfect square or the distance from $n$ to the nearest perfect square is a perfect square. For example, 2016 is squarish, because the nearest perfect square to 2016 is $45^2 = 2025$ and $2025 - 2016 = 9$ is a perfect square. (Of the positive integers between 1 and 10, only 6 and 7 are not squarish.)

For a positive integer $N$, let $S(N)$ be the number of squarish integers between 1 and $N$, inclusive. Find positive constants $\alpha$ and $\beta$ such that

$$\lim_{N\to\infty} \frac{S(N)}{N^\alpha} = \beta,$$

or show that no such constants exist.

B3 Suppose that $S$ is a finite set of points in the plane such that the area of triangle $\triangle ABC$ is at most 1 whenever $A$, $B$, and $C$ are in $S$. Show that there exists a triangle of area 4 that (together with its interior) covers the set $S$.

B4 Let $A$ be a $2n\times 2n$ matrix, with entries chosen independently at random. Every entry is chosen to be 0 or 1, each with probability $1/2$. Find the expected value of $\det(A - A^t)$ (as a function of $n$), where $A^t$ is the transpose of $A$.

B5 Find all functions $f$ from the interval $(1,\infty)$ to $(1,\infty)$ with the following property: if $x, y \in (1,\infty)$ and $x^2 \leq y \leq x^3$, then $(f(x))^2 \leq f(y) \leq (f(x))^3$.

B6 Evaluate

$$\sum_{k=1}^\infty \frac{(-1)^{k-1}}{k} \sum_{n=0}^\infty \frac{1}{k2^n + 1}.$$

# Solutions to the 77th William Lowell Putnam Mathematical Competition
# Saturday, December 3, 2016

Kiran Kedlaya and Lenny Ng

A1 The answer is $j = 8$. First suppose that $j$ satisfies the given condition. For $p(x) = x^j$, we have $p^{(j)}(x) = j!$ and thus $j!$ is divisible by 2016. Since 2016 is divisible by $2^5$ and $7!$ is not, it follows that $j \geq 8$. Conversely, we claim that $j = 8$ works. Indeed, let $p(x) = \sum_{m=0}^n a_m x^m$ be a polynomial with integer coefficients; then if $k$ is any integer,

$$\begin{aligned} p^{(8)}(k) &= \sum_{m=8}^n m(m-1)\cdots(m-7)a_m k^{m-8} \\ &= \sum_{m=8}^n \binom{m}{8} 8! a_m k^{m-8} \end{aligned}$$

is divisible by $8! = 20 \cdot 2016$, and so $p^{(8)}(k)$ is divisible by 2016.

**Remark:** By the same reasoning, if one replaces 2016 in the problem by a general integer $N$, then the minimum value of $j$ is the smallest one for which $N$ divides $j!$. This can be deduced from Pólya's observation that the set of integer-valued polynomials is the free $\mathbb{Z}$-module generated by the binomial polynomials $\binom{x}{n}$ for $n = 0, 1, \dots$. That statement can be extended to polynomials evaluated on a subset of a Dedekind domain using Bhargava's method of *P-orderings*; we do not know if this generalization can be adapted to the analogue of this problem, where one considers polynomials whose $j$-th derivatives take integral values on a prescribed subset.

A2 The answer is $\frac{3+\sqrt{5}}{2}$. Note that for $m > n+1$, both binomial coefficients are nonzero and their ratio is

$$\begin{aligned} \binom{m}{n-1} \Big/ \binom{m-1}{n} &= \frac{m!n!(m-n-1)!}{(m-1)!(n-1)!(m-n+1)!} \\ &= \frac{mn}{(m-n+1)(m-n)}. \end{aligned}$$

Thus the condition $\binom{m}{n-1} > \binom{m-1}{n}$ is equivalent to $(m-n+1)(m-n) - mn < 0$. The left hand side of this last inequality is a quadratic function of $m$ with roots

$$\begin{aligned} \alpha(n) &= \frac{3n-1+\sqrt{5n^2-2n+1}}{2}, \\ \beta(n) &= \frac{3n-1-\sqrt{5n^2-2n+1}}{2}, \end{aligned}$$

both of which are real since $5n^2-2n+1 = 4n^2+(n-1)^2 > 0$; it follows that $m$ satisfies the given inequality if and only if $\beta(n) < m < \alpha(n)$. (Note in particular that since $\alpha(n) - \beta(n) = \sqrt{5n^2-2n+1} > 1$, there is always some integer $m$ between $\beta(n)$ and $\alpha(n)$.)

We conclude that $M(n)$ is the greatest integer strictly less than $\alpha(n)$, and thus that $\alpha(n) - 1 \leq M(n) < \alpha(n)$. Now

$$\lim_{n\to\infty} \frac{\alpha(n)}{n} = \lim_{n\to\infty} \frac{3 - \frac{1}{n} + \sqrt{5 - \frac{2}{n} + \frac{1}{n^2}}}{2} = \frac{3+\sqrt{5}}{2}$$

and similarly $\lim_{n\to\infty} \frac{\alpha(n)-1}{n} = \frac{3+\sqrt{5}}{2}$, and so by the sandwich theorem, $\lim_{n\to\infty} \frac{M(n)}{n} = \frac{3+\sqrt{5}}{2}$.

A3 The given functional equation, along with the same equation but with $x$ replaced by $\frac{x-1}{x}$ and $\frac{1}{1-x}$ respectively, yields:

$$\begin{aligned} f(x) + f\left(1 - \frac{1}{x}\right) &= \tan^{-1}(x) \\ f\left(\frac{x-1}{x}\right) + f\left(\frac{1}{1-x}\right) &= \tan^{-1}\left(\frac{x-1}{x}\right) \\ f\left(\frac{1}{1-x}\right) + f(x) &= \tan^{-1}\left(\frac{1}{1-x}\right). \end{aligned}$$

Adding the first and third equations and subtracting the second gives:

$$2f(x) = \tan^{-1}(x) + \tan^{-1}\left(\frac{1}{1-x}\right) - \tan^{-1}\left(\frac{x-1}{x}\right).$$

Now $\tan^{-1}(t) + \tan^{-1}(1/t)$ is equal to $\pi/2$ if $t > 0$ and $-\pi/2$ if $t < 0$; it follows that for $x \in (0,1)$,

$$\begin{aligned} 2(f(x) + f(1-x)) &= \left(\tan^{-1}(x) + \tan^{-1}(1/x)\right) \\ &\quad + \left(\tan^{-1}(1-x) + \tan^{-1}\left(\frac{1}{1-x}\right)\right) \\ &\quad - \left(\tan^{-1}\left(\frac{x-1}{x}\right) + \tan^{-1}\left(\frac{x}{x-1}\right)\right) \\ &= \frac{\pi}{2} + \frac{\pi}{2} + \frac{\pi}{2} \\ &= \frac{3\pi}{2}. \end{aligned}$$

Thus

$$4\int_0^1 f(x)\,dx = 2\int_0^1 (f(x) + f(1-x))dx = \frac{3\pi}{2}$$

and finally $\int_0^1 f(x)\,dx = \frac{3\pi}{8}$.

**Remark:** Once one has the formula for $f(x)$, one can also (with some effort) directly evaluate the integral of each summand over $[0,1]$ to obtain the same result. A much cleaner variant of this approach (suggested on AoPS, user `henrikjb`) is to write

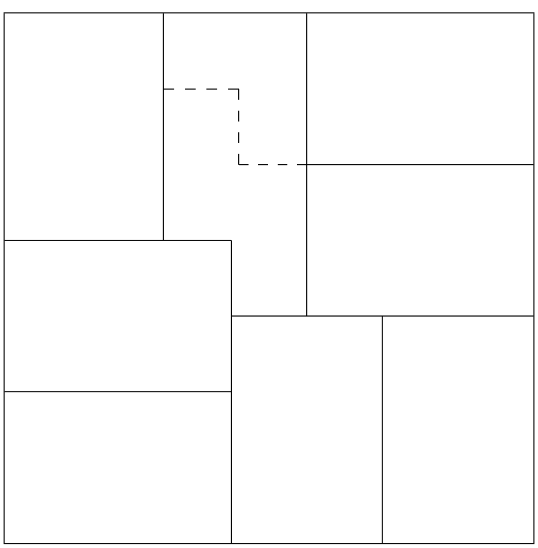
$$\tan^{-1}(x) = \int_0^y \frac{1}{1+y^2}\,dy$$

and do a change of variable on the resulting double integral.

A4 The minimum number of tiles is $mn$. To see that this many are required, label the squares $(i,j)$ with $1 \le i \le 2m-1$ and $1 \le j \le 2n-1$, and for each square with $i,j$ both odd, color the square red; then no tile can cover more than one red square, and there are $mn$ red squares.

It remains to show that we can cover any $(2m-1) \times (2n-1)$ rectangle with $mn$ tiles when $m,n \ge 4$. First note that we can tile any $2 \times (2k-1)$ rectangle with $k \ge 3$ by $k$ tiles: one of the first type, then $k-2$ of the second type, and finally one of the first type. Thus if we can cover a $7 \times 7$ square with 16 tiles, then we can do the general $(2m-1) \times (2n-1)$ rectangle, by decomposing this rectangle into a $7 \times 7$ square in the lower left corner, along with $m-4$ $(2 \times 7)$ rectangles to the right of the square, and $n-4$ $((2m-1) \times 2)$ rectangles above, and tiling each of these rectangles separately, for a total of $16+4(m-4)+m(n-4) = mn$ tiles.

To cover the $7 \times 7$ square, note that the tiling must consist of 15 tiles of the first type and 1 of the second type, and that any $2 \times 3$ rectangle can be covered using 2 tiles of the first type. We may thus construct a suitable covering by covering all but the center square with eight $2 \times 3$ rectangles, in such a way that we can attach the center square to one of these rectangles to get a shape that can be covered by two tiles. An example of such a covering, with the remaining $2 \times 3$ rectangles left intact for visual clarity, is depicted below. (Many other solutions are possible.)



A5 **First solution:** For $s \in G$ and $r$ a positive integer, define a *representation of $s$ of length $r$* to be a sequence of values $m_1, n_1, \dots, m_r, n_r \in \{-1, 1\}$ for which

$$s = g^{m_1} h^{n_1} \cdots g^{m_r} h^{n_r}.$$

We first check that every $s \in G$ admits at least one representation of some length; this is equivalent to saying that the set $S$ of $s \in G$ which admit representations of some length is equal to $G$ itself. Since $S$ is closed under the group operation and $G$ is finite, $S$ is also closed under formation of inverses and contains the identity element; that is, $S$ is a subgroup of $G$. In particular, $S$ contains not only $gh$ but also its inverse $h^{-1}g^{-1}$; since $S$ also contains $g^{-1}h$, we deduce that $S$ contains $g^{-2}$. Since $g$ is of odd order in $G$, $g^{-2}$ is also a generator of the cyclic subgroup containing $g$; it follows that $g \in S$ and hence $h \in S$. Since we assumed that $g,h$ generate $G$, we now conclude that $S = G$, as claimed.

To complete the proof, we must now check that for each $s \in G$, the smallest possible length of a representation of $s$ cannot exceed $|G|$. Suppose the contrary, and let

$$s = g^{m_1} h^{n_1} \cdots g^{m_r} h^{n_r}$$

be a representation of the smallest possible length. Set

$$s_i = g^{m_1} h^{n_1} \cdots g^{m_i} h^{n_i} \qquad (i = 0, \dots, r-1),$$

interpreting $s_0$ as $e$; since $r > |G|$ by hypothesis, by the pigeonhole principle there must exist indices $0 \le i < j \le r-1$ such that $s_i = s_j$. Then

$$s = g^{m_1} h^{n_1} \cdots g^{m_i} h^{n_i} g^{m_{j+1}} h^{n_{j+1}} \cdots g^{m_r} h^{n_r}$$

is another representation of $s$ of length strictly less than $r$, a contradiction.

**Remark:** If one considers $s_1, \dots, s_r$ instead of $s_0, \dots, s_{r-1}$, then the case $s = e$ must be handled separately: otherwise, one might end up with a representation of length 0 which is disallowed by the problem statement.

**Reinterpretation:** Note that the elements $gh, gh^{-1}, g^{-1}h, g^{-1}h^{-1}$ generate $gh(g^{-1}h)^{-1} = g^2$ and hence all of $G$ (again using the hypothesis that $g$ has odd order, as above). Form the Cayley digraph on the set $G$, i.e., the directed graph with an edge from $s_1$ to $s_2$ whenever $s_2 = s_1 *$ for $* \in \{gh, gh^{-1}, g^{-1}h, g^{-1}h^{-1}\}$. Since $G$ is finite, this digraph is strongly connected: there exists at least one path from any vertex to any other vertex (traveling all edges in the correct direction). The shortest such path cannot repeat any vertices (except the starting and ending vertices in case they coincide), and so has length at most $|G|$.

**Second solution:** For $r$ a positive integer, let $S_r$ be the set of $s \in G$ which admit a representation of length at most $r$ (terminology as in the first solution); obviously $S_r \subseteq S_{r+1}$. We will show that $S_r \neq S_{r+1}$ unless $S_r = G$; this will imply by induction on $r$ that $\#S_r \ge \min\{r, |G|\}$ and hence that $S_r = G$ for some $r \le |G|$.

Suppose that $S_r = S_{r+1}$. Then the map $s \mapsto sgh$ defines an injective map $S_r \to S_{r+1} = S_r$, so $S_r$ is closed under right multiplication by $gh$. By the same token, $S_r$ is closed under right multiplication by each of $gh^{-1}, g^{-1}h, g^{-1}h^{-1}$. Since $gh, gh^{-1}, g^{-1}h, g^{-1}h^{-1}$ generate $G$ as in the first solution, it follows that $S_r = G$ as claimed.since $r+1 \leq |G|$, we are done in this case also.

**Remark:** The condition on the order of $g$ is needed to rule out the case where $G$ admits a (necessarily normal) subgroup $H$ of index 2 not containing either $g$ or $h$; in this case, all products of the indicated form belong to $H$. On the other hand, if one assumes that both $g$ and $h$ have odd order, then one can say a bit more: there exists some positive integer $r$ with $1 \leq r \leq |G|$ such that every element of $G$ has a representation of length exactly $r$. (Namely, the set of such elements for a given $r$ strictly increases in size until it is stable under right multiplication by both $gh(g^{-1}h)^{-1} = g^2$ and $gh(gh^{-1})^{-1} = gh^2g^{-1}$, but under the present hypotheses these generate $G$.)

A6 We prove that the smallest such value of $C$ is $5/6$.

**First solution:** (based on a suggestion of Daniel Kane)

We first reduce to the case where $P$ is nonnegative in $[0,1]$ and $P(0) = 0$. To achieve this reduction, suppose that a given value $C$ obeys the inequality for such $P$. For $P$ general, divide the interval $[0,1]$ into subintervals $I_1, \dots, I_k$ at the roots of $P$. Write $\ell(I_i)$ for the length of the interval $I_i$; since each interval is bounded by a root of $P$, we may make a linear change of variable to see that

$$\int_{I_i} |P(x)|\,dx \leq C\ell(I_i) \max_{x \in I_i} |P(x)| \quad (i = 1, \dots, k).$$

Summing over $i$ yields the desired inequality.

Suppose now that $P$ takes nonnegative values on $[0,1]$, $P(0) = 0$, and $\max_{x\in[0,1]} P(x) = 1$. Write $P(x) = ax^3 + bx^2 + cx$ for some $a,b,c \in \mathbb{R}$; then

$$\begin{aligned}
\int_0^1 P(x)\,dx &= \frac{1}{4}a + \frac{1}{3}b + \frac{1}{2}c \\
&= \frac{2}{3}\left(\frac{1}{8}a + \frac{1}{4}b + \frac{1}{2}c\right) + \frac{1}{6}(a+b+c) \\
&= \frac{2}{3}P\left(\frac{1}{2}\right) + \frac{1}{6}P(1) \\
&\leq \frac{2}{3} + \frac{1}{6} = \frac{5}{6}.
\end{aligned}$$

Consequently, the originally claimed inequality holds with $C = 5/6$. To prove that this value is best possible, it suffices to exhibit a polynomial $P$ as above with $\int_0^1 P(x)\,dx = 5/6$; we will verify that

$$P(x) = 4x^3 - 8x^2 + 5x$$

has this property. It is apparent that $\int_0^1 P(x)\,dx = 5/6$. Since $P'(x) = (2x-1)(6x-5)$ and

$$P(0) = 0, P\left(\frac{1}{2}\right) = 1, P\left(\frac{5}{6}\right) = \frac{25}{27}, P(1) = 1,$$

it follows that $P$ increases from 0 at $x = 0$ to 1 at $x = 1/2$, then decreases to a positive value at $x = 5/6$, then increases to 1 at $x = 1$. Hence $P$ has the desired form.

**Remark:** Here is some conceptual motivation for the preceding solution. Let $V$ be the set of polynomials of degree at most 3 vanishing at 0, viewed as a three-dimensional vector space over $\mathbb{R}$. Let $S$ be the subset of $V$ consisting of those polynomials $P(x)$ for which $0 \leq P(x) \leq 1$ for all $x \in [0,1]$; this set is convex and compact. We may then compute the minimal $C$ as the maximum value of $\int_0^1 P(x)\,dx$ over all $P \in S$, provided that the maximum is achieved for some polynomial of degree exactly 3. (Note that any extremal polynomial must satisfy $\max_{x\in[0,1]} P(x) = 1$, as otherwise we could multiply it by some constant $c > 1$ so as to increase $\int_0^1 P(x)\,dx$.)

Let $f : V \to \mathbb{R}$ be the function taking $P(x)$ to $\int_0^1 P(x)\,dx$. This function is linear, so we can characterize its extrema on $S$ easily: there exist exactly two level surfaces for $f$ which are supporting planes for $S$, and the intersections of these two planes with $S$ are the minima and the maxima. It is obvious that the unique minimum is achieved by the zero polynomial, so this accounts for one of the planes.

It thus suffices to exhibit a single polynomial $P(x) \in S$ such that the level plane of $f$ through $P$ is a supporting plane for $S$. The calculation made in the solution amounts to verifying that

$$P(x) = 4x^3 - 8x^2 + 5x$$

has this property, by interpolating between the constraints $P(1/2) \leq 1$ and $P(1) \leq 1$.

This still leaves the matter of correctly guessing the optimal polynomial. If one supposes that it should be extremized both at $x = 1$ and at an interval value of the disc, it is forced to have the form $P(x) = 1 + (x-1)(cx-1)^2$ for some $c > 0$; the interpolation property then pins down $c$ uniquely.

**Second solution:** (by James Merryfield, via AoPS) As in the first solution, we may assume that $P$ is nonnegative on $[0,1]$ and $P(0) = 0$. Since $P$ has degree at most 3, Simpson's rule for approximating $\int_0^1 P(x)\,dx$ is an exact formula:

$$\int_0^1 P(x)\,dx = \frac{1}{6}\left(P(0) + 4P\left(\frac{1}{2}\right) + P(1)\right).$$

This immediately yields the claimed inequality for $C = 5/6$. Again as in the first solution, we obtain an example showing that this value is best possible.

B1 Note that the function $e^x - x$ is strictly increasing for $x > 0$ (because its derivative is $e^x - 1$, which is positive because $e^x$ is strictly increasing), and its value at 0 is 1. By induction on $n$, we see that $x_n > 0$ for all $n$.

By exponentiating the equation defining $x_{n+1}$, we obtain the expression

$$x_n = e^{x_n} - e^{x_{n+1}}.$$

We use this equation repeatedly to acquire increasingly precise information about the sequence $\{x_n\}$.

- Since $x_n > 0$, we have $e^{x_n} > e^{x_{n+1}}$, so $x_n > x_{n+1}$.
- Since the sequence $\{x_n\}$ is decreasing and bounded below by 0, it converges to some limit $L$.
- Taking limits in the equation yields $L = e^L - e^L$, whence $L = 0$.
- Since $L = 0$, the sequence $\{e^{x_n}\}$ converges to 1.

We now have a telescoping sum:

$$\begin{aligned} x_0 + \cdots + x_n &= (e^{x_0} - e^{x_1}) + \cdots + (e^{x_n} - e^{x_{n+1}}) \\ &= e^{x_0} - e^{x_{n+1}} = e - e^{x_{n+1}}. \end{aligned}$$

By taking limits, we see that the sum $x_0 + x_1 + \cdots$ converges to the value $e - 1$.

B2 We prove that the limit exists for $\alpha = \frac{3}{4}$, $\beta = \frac{4}{3}$.

For any given positive integer $n$, the integers which are closer to $n^2$ than to any other perfect square are the ones in the interval $[n^2 - n - 1, n^2 + n]$. The number of squarish numbers in this interval is $1 + \lfloor \sqrt{n-1} \rfloor + \lfloor \sqrt{n} \rfloor$. Roughly speaking, this means that

$$S(N) \sim \int_0^{\sqrt{N}} 2\sqrt{x}\,dx = \frac{4}{3} N^{3/4}.$$

To make this precise, we use the bounds $x - 1 \leq \lfloor x \rfloor \leq x$, and the upper and lower Riemann sum estimates for the integral of $\sqrt{x}$, to derive upper and lower bounds on $S(N)$:

$$\begin{aligned} S(N) &\geq \sum_{n=1}^{\lfloor \sqrt{N} \rfloor - 1} (2\sqrt{n-1} - 1) \\ &\geq \int_0^{\lfloor \sqrt{N} \rfloor - 2} 2\sqrt{x}\,dx - \sqrt{N} \\ &\geq \frac{4}{3}(\sqrt{N} - 3)^{3/2} - \sqrt{N} \end{aligned}$$

$$\begin{aligned} S(N) &\leq \sum_{n=1}^{\lceil \sqrt{N} \rceil} (2\sqrt{n} + 1) \\ &\leq \int_0^{\lceil \sqrt{N} \rceil + 1} 2\sqrt{x}\,dx + \sqrt{N} + 1 \\ &\leq \frac{4}{3}(\sqrt{N} + 2)^{3/2} + \sqrt{N} + 1. \end{aligned}$$

**Remark:** John Rickert points out that when $N = n^4$, one can turn the previous estimates into exact calculations to obtain the formula

$$S(N) = \frac{4}{3}\left(n^3 + \frac{n}{2}\right) = \frac{4}{3} N^{3/4} + \frac{2}{3} N^{1/4}.$$

For general $N$, one can then use the estimates

$$\begin{aligned} \frac{4}{3}(N-1)^{3/4} + \frac{2}{3}(N-1)^{1/4} &\leq S(\lfloor N^{1/4} \rfloor^4) \\ &\leq S(N) \\ &\leq S(\lceil N^{1/4} \rceil^4) \\ &\leq \frac{4}{3}(N+1)^{3/4} + \frac{2}{3}(N+1)^{1/4} \end{aligned}$$

to obtain the desired limit.

B3 Since $S$ is finite, we can choose three points $A, B, C$ in $S$ so as to maximize the area of the triangle $ABC$. Let $A', B', C'$ be the points in the plane such that $A, B, C$ are the midpoints of the segments $B'C', C'A', A'B'$; the triangle $A'B'C'$ is similar to $ABC$ with sides twice as long, so its area is 4 times that of $ABC$ and hence no greater than 4.

We claim that this triangle has the desired effect; that is, every point $P$ of $S$ is contained within the triangle $A'B'C'$. (To be precise, the problem statement requires a triangle of area exactly 4, which need not be the case for $A'B'C'$, but this is trivially resolved by scaling up by a homothety.) To see this, note that since the area of the triangle $PBC$ is no more than that of $ABC$, $P$ must lie in the half-plane bounded by $B'C'$ containing $B$ and $C$. Similarly, $P$ must lie in the half-plane bounded by $C'A'$ containing $C$ and $A$, and the half-plane bounded by $A'B'$ containing $A$ and $B$. These three half-planes intersect precisely in the region bounded by the triangle $A'B'C'$, proving the claim.

B4 The expected value equals

$$\frac{(2n)!}{4^n n!}.$$

**First solution:**

Write the determinant of $A - A^t$ as the sum over permutations $\sigma$ of $\{1, \ldots, 2n\}$ of the product

$$\mathrm{sgn}(\sigma) \prod_{i=1}^{2n} (A - A^t)_{i\sigma(i)} = \mathrm{sgn}(\sigma) \prod_{i=1}^{2n} (A_{i\sigma(i)} - A_{\sigma(i)i});$$

then the expected value of the determinant is the sum over $\sigma$ of the expected value of this product, which we denote by $E_\sigma$.

Note that if we partition $\{1, \ldots, 2n\}$ into orbits for the action of $\sigma$, then partition the factors of the product accordingly, then no entry of $A$ appears in more than one of these factors; consequently, these factors are independent random variables. This means that we can compute $E_\sigma$ as the product of the expected values of the individual factors.

It is obvious that any orbit of size 1 gives rise to the zero product, and hence the expected value of the corresponding factor is zero. For an orbit of size $m \geq 3$, the corresponding factor contains $2m$ distinct matrix entries, so again we may compute the expected value of the factor as the product of the expected values of the individual terms $A_{i\sigma(i)} - A_{\sigma(i)i}$. However, the distribution of this term is symmetric about 0, so its expected value is 0.

We conclude that $E_\sigma = 0$ unless $\sigma$ acts with $n$ orbits of size 2. To compute $E_\sigma$ in this case, assume without loss of generality that the orbits of $\sigma$ are $\{1,2\},\dots,\{2n-1,2n\}$; note that $\mathrm{sgn}(\sigma) = (-1)^n$. Then $E_\sigma$ is the expected value of $\prod_{i=1}^n -(A_{(2i-1)2i} - A_{2i(2i-1)})^2$, which is $(-1)^n$ times the $n$-th power of the expected value of $(A_{12} - A_{21})^2$. Since $A_{12} - A_{21}$ takes the values $-1, 0, 1$ with probabilities $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$, its square takes the values $0, 1$ with probabilities $\frac{1}{2}, \frac{1}{2}$; we conclude that

$$E_\sigma = 2^{-n}.$$

The permutations $\sigma$ of this form correspond to unordered partitions of $\{1,\dots,2n\}$ into $n$ sets of size 2, so there are

$$\frac{(2n)!}{n!(2!)^n}$$

such permutations. Putting this all together yields the claimed result.

**Second solution:** (by Manjul Bhargava) Note that the matrix $A - A^t$ is skew-symmetric:

$$(A - A^t)^t = A^t - A = -(A - A^t).$$

The determinant of a $2n \times 2n$ skew-symmetric matrix $M$ is the square of the *Pfaffian* of $M$, which is a polynomial of degree $n$ in the entries of $M$ defined as follows. Define a *perfect matching* of $\{1,\dots,2n\}$ to be a permutation of $\{1,\dots,2n\}$ that is the product of $n$ disjoint transpositions. Then the Pfaffian of $M$ is given by

$$\sum_\alpha \mathrm{sgn}(\alpha) M_{i_1,j_1} \cdots M_{i_n,j_n} \qquad (1)$$

where the sum is over perfect matchings $\alpha = (i_1, j_1) \cdots (i_n, j_n)$, and $\mathrm{sgn}(\alpha)$ denotes the sign of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & (2n-1) & 2n \\ i_1 & j_1 & i_2 & j_2 & \cdots & i_n & j_n \end{pmatrix}$. The determinant of $M$ is then the square of (1), i.e.,

$$\det(M) = \sum_{\alpha,\beta} \mathrm{sgn}(\alpha)\,\mathrm{sgn}(\beta) M_{i_1,j_1} \cdots M_{i_n,j_n} M_{i'_1,j'_1} \cdots M_{i'_n,j'_n} \qquad (2)$$

where the sum is now over ordered pairs

$$(\alpha = (i_1, j_1) \cdots (i_n, j_n), \beta = (i'_1, j'_1) \cdots (i'_n, j'_n))$$

of perfect matchings.

Taking $M = A - A^t$, so that $M_{ij} = A_{ij} - A_{ji}$, we wish to find the expected value of (2); again, this is the sum of the expected values of each summand in (2). Note that each $M_{ij}$ with $i < j$ is an independent random variable taking the values $-1, 0, 1$ with probabilities $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$, respectively.

Consider first a summand in (2) with $\alpha \neq \beta$. Then some factor $M_{ij}$ occurs with exponent 1; since the distribution of $M_{ij}$ is symmetric about 0, any such summand has expected value 0.

Consider next a summand in (2) with $\alpha = \beta$. This summand is a product of distinct factors of the form $M_{ij}^2$; from the distributions of the $M_{ij}$, we see that the expected value of each of these terms is $1/2^n$.

Since the total number of perfect matchings $\alpha$ is $(2n)!/(2^n n!)$, the expected value of (2) is therefore $(2n)!/(2^n n!) \cdot 1/2^n = (2n)!/(4^n n!)$, as desired.

B5 It is obvious that for any $c > 0$, the function $f(x) = x^c$ has the desired property; we will prove that conversely, any function with the desired property has this form for some $c$.

Define the function $g : (0,\infty) \to (0,\infty)$ given by $g(x) = \log f(e^x)$; this function has the property that if $x, y \in (0,\infty)$ and $2x \leq y \leq 3x$, then $2g(x) \leq g(y) \leq 3g(x)$. It will suffice to show that there exists $c > 0$ such that $g(x) = cx$ for all $x > 0$.

Similarly, define the function $h : \mathbb{R} \to \mathbb{R}$ given by $h(x) = \log g(e^x)$; this function has the property that if $x, y \in \mathbb{R}$ and $x + \log 2 \leq y \leq x + \log 3$, then $h(x) + \log 2 \leq h(y) \leq h(x) + \log 3$. It will suffice to show that there exists $c > 0$ such that $h(x) = x + c$ for all $x \in \mathbb{R}$ (as then $h(x) = e^c x$ for all $x > 0$).

By interchanging the roles of $x$ and $y$, we may restate the condition on $h$ as follows: if $x - \log 3 \leq y \leq x - \log 2$, then $h(x) - \log 3 \leq h(y) \leq h(x) - \log 2$. This gives us the cases $a + b = 0, 1$ of the following statement, which we will establish in full by induction on $a + b$, we deduce the following: for any nonnegative integers $a, b$, for all $x, y \in \mathbb{R}$ such that

$$x + a\log 2 - b\log 3 \leq y \leq x + a\log 3 - b\log 2,$$

we have

$$h(x) + a\log 2 - b\log 3 \leq h(y) \leq h(x) + a\log 3 - b\log 2.$$

To this end, suppose that $a + b > 0$ and that the claim is known for all smaller values of $a + b$. In particular, either $a > 0$ or $b > 0$; the two cases are similar, so we treat only the first one. Define the function

$$j(t) = \frac{(a+b-1)t - b(\log 2 + \log 3)}{a+b},$$

so that

$$\begin{gathered} j(a\log 2 - b\log 3) = a\log 2 - b\log 3, \\ j(a\log 3 - b\log 2) = (a-1)\log 3 - b\log 2, \\ \log 2 \leq t \leq \log 3 \qquad (t \in [a\log 2 - b\log 3, a\log 3 - b\log 2]). \end{gathered}$$

For $t \in [a\log 2 - b\log 3, a\log 3 - b\log 2]$ and $y = x+t$, we then have

$$(a-1)\log 2 - b\log 3 \leq h(x+j(t)) - h(x) \leq (a-1)\log 3 - b\log 2$$
$$\log 2 \leq h(y) - h(x+j(t)) \leq \log 3$$

and thus the desired inequalities.

Now fix two values $x, y \in \mathbb{R}$ with $x \leq y$. Since $\log 2$ and $\log 3$ are linearly independent over $\mathbb{Q}$, the fractional parts of the nonnegative integer multiples of $\log 3/\log 2$ are dense in $[0,1)$. (This result is due to Kronecker; a stronger result of Weyl shows that the fractional parts are uniformly distributed in $[0,1)$.) In particular, for any $\varepsilon > 0$ and any $N > 0$, we can find integers $a, b > N$ such that

$$y - x < a\log 3 - b\log 2 < y - x + \varepsilon.$$

By writing

$$a\log 2 - b\log 3 = \frac{\log 2}{\log 3}(a\log 3 - b\log 2) - b\frac{(\log 3)^2 - (\log 2)^2}{\log 3},$$

we see that this quantity tends to $-\infty$ as $N \to \infty$; in particular, for $N$ sufficiently large we have that $a\log 2 - b\log 3 < y - x$. We thus have $h(y) \leq h(x) + a\log 2 - b\log 3 < y - x + \varepsilon$; since $\varepsilon > 0$ was chosen arbitrarily, we deduce that $h(y) - h(x) \leq y - x$. A similar argument shows that $h(y) - h(x) \geq y - x$; we deduce that $h(y) - h(x) = y - x$, or equivalently $h(y) - y = h(x) - x$. In other words, the function $x \mapsto h(x) - x$ is constant, as desired.

B6 Let $S$ denote the desired sum. We will prove that $S = 1$.

**First solution:** Write

$$\sum_{n=0}^\infty \frac{1}{k2^n+1} = \frac{1}{k+1} + \sum_{n=1}^\infty \frac{1}{k2^n+1};$$

then we may write $S = S_1 + S_2$ where

$$S_1 = \sum_{k=1}^\infty \frac{(-1)^{k-1}}{k(k+1)}$$
$$S_2 = \sum_{k=1}^\infty \frac{(-1)^{k-1}}{k} \sum_{n=1}^\infty \frac{1}{k2^n+1}.$$

The rearrangement is valid because both $S_1$ and $S_2$ converge absolutely in $k$, by comparison to $\sum 1/k^2$.

To compute $S_1$, note that

$$\sum_{k=1}^N \frac{(-1)^{k-1}}{k(k+1)} = \sum_{k=1}^N (-1)^{k-1}\left(\frac{1}{k} - \frac{1}{k+1}\right) = -1 + \frac{(-1)^N}{N+1} + 2\sum_{k=1}^N \frac{(-1)^{k-1}}{k}$$

converges to $2\ln 2 - 1$ as $N \to \infty$, and so $S_1 = 2\ln 2 - 1$.

To compute $S_2$, write $\frac{1}{k2^n+1} = \frac{1}{k2^n} \cdot \frac{1}{1+1/(k2^n)}$ as the geometric series $\sum_{m=0}^\infty \frac{(-1)^m}{k^{m+1}2^{mn+n}}$, whence

$$S_2 = \sum_{k=1}^\infty \sum_{n=1}^\infty \sum_{m=0}^\infty \frac{(-1)^{k+m-1}}{k^{m+2}2^{mn+n}}.$$

(This step requires $n \geq 1$, as otherwise the geometric series would not converge for $k = 0$.) Now note that this triple sum converges absolutely: we have

$$\sum_{m=0}^\infty \frac{1}{k^{m+2}2^{mn+n}} = \frac{1}{k^2 2^n} \cdot \frac{1}{1 - \frac{1}{k2^n}} = \frac{1}{k(k2^n-1)} \leq \frac{1}{k^2 2^{n-1}}$$

and so

$$\sum_{k=1}^\infty \sum_{n=1}^\infty \sum_{m=0}^\infty \frac{1}{k^{m+2}2^{mn+n}} \leq \sum_{k=1}^\infty \sum_{n=1}^\infty \frac{1}{k^2 2^{n-1}} = \sum_{k=1}^\infty \frac{2}{k^2} < \infty.$$

Thus we can rearrange the sum to get

$$S_2 = \sum_{m=0}^\infty (-1)^m \left(\sum_{n=1}^\infty \frac{1}{2^{mn+n}}\right)\left(\sum_{k=1}^\infty \frac{(-1)^{k-1}}{k^{m+2}}\right).$$

The sum in $n$ is the geometric series

$$\frac{1}{2^{m+1}(1 - \frac{1}{2^{m+1}})} = \frac{1}{2^{m+1}-1}.$$

If we write the sum in $k$ as $S_3$, then note that

$$\sum_{k=1}^\infty \frac{1}{k^{m+2}} = S_3 + 2\sum_{k=1}^\infty \frac{1}{(2k)^{m+2}} = S_3 + \frac{1}{2^{m+1}}\sum_{k=1}^\infty \frac{1}{k^{m+2}}$$

(where we can rearrange terms in the first equality because all of the series converge absolutely), and so

$$S_3 = \left(1 - \frac{1}{2^{m+1}}\right)\sum_{k=1}^\infty \frac{1}{k^{m+2}}.$$

It follows that

$$\begin{aligned} S_2 &= \sum_{m=0}^\infty \frac{(-1)^m}{2^{m+1}} \sum_{k=1}^\infty \frac{1}{k^{m+2}} \\ &= \sum_{k=1}^\infty \frac{1}{2k^2} \sum_{m=0}^\infty \left(-\frac{1}{2k}\right)^m \\ &= \sum_{k=1}^\infty \frac{1}{k(2k+1)} \\ &= 2\sum_{k=1}^\infty \left(\frac{1}{2k} - \frac{1}{2k+1}\right) = 2(1 - \ln 2). \end{aligned}$$

Finally, we have $S = S_1 + S_2 = 1$.

**Second solution:** (by Tewodros Amdeberhan) Since $\int_0^1 x^t\,dx = \frac{1}{1+t}$ for any $t \geq 1$, we also have

$$S = \sum_{k=1}^{\infty}\sum_{n=0}^{\infty} \frac{(-1)^{k-1}}{k} \int_0^1 x^{k2^n}\,dx.$$

Again by absolute convergence, we are free to permute the integral and the sums:

$$\begin{aligned} S &= \int_0^1 dx \sum_{n=0}^{\infty}\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} x^{k2^n} \\ &= -\int_0^1 dx \sum_{n=0}^{\infty} \log(1+x^{2^n}). \end{aligned}$$

Due to the uniqueness of binary expansions of nonnegative integers, we have the identity of formal power series

$$\frac{1}{1-x} = \prod_{n=0}^{\infty}(1+x^{2^n});$$

the product converges absolutely for $0 \leq x < 1$. We thus have

$$\begin{aligned} S &= -\int_0^1 \log(1-x)\,dx \\ &= ((1-x)\log(1-x) - (1-x))_0^1 \\ &= 1. \end{aligned}$$

**Third solution:** (by Serin Hong) Again using absolute convergence, we may write

$$S = \sum_{m=2}^{\infty} \frac{1}{m} \sum_k \frac{(-1)^{k-1}}{k}$$

where $k$ runs over all positive integers for which $m = k2^n + 1$ for some $n$. If we write $e$ for the 2-adic valuation of $m-1$ and $j = (m-1)2^{-e}$ for the odd part of $m-1$, then the values of $k$ are $j2^i$ for $i = 0, \dots, e$. The inner sum can thus be evaluated as

$$\frac{1}{j} - \sum_{i=1}^{e} \frac{1}{2^i j} = \frac{1}{2^e j} = \frac{1}{m-1}.$$

We thus have

$$S = \sum_{m=2}^{\infty} \frac{1}{m(m-1)} = \sum_{m=2}^{\infty}\left(\frac{1}{m-1} - \frac{1}{m}\right) = 1.$$

**Fourth solution:** (by Liang Xiao) Let $S_0$ and $S_1$ be the sums $\sum_k \frac{1}{k} \sum_{n=0}^{\infty} \frac{1}{k2^n+1}$ with $k$ running over all odd and all even positive integers, respectively, so that

$$S = S_0 - S_1.$$

In $S_1$, we may write $k = 2\ell$ to obtain

$$\begin{aligned} S_1 &= \sum_{\ell=1}^{\infty} \frac{1}{2\ell} \sum_{n=0}^{\infty} \frac{1}{\ell 2^{n+1} + 1} \\ &= \frac{1}{2}(S_0 + S_1) - \sum_{\ell=1}^{\infty} \frac{1}{2\ell(\ell+1)} \\ &= \frac{1}{2}(S_0 + S_1) - \frac{1}{2} \end{aligned}$$

because the last sum telescopes; this immediately yields $S = 1$.

# The 78th William Lowell Putnam Mathematical Competition
# Saturday, December 2, 2017

A1 Let $S$ be the smallest set of positive integers such that

(a) 2 is in $S$,

(b) $n$ is in $S$ whenever $n^2$ is in $S$, and

(c) $(n+5)^2$ is in $S$ whenever $n$ is in $S$.

Which positive integers are not in $S$?

(The set $S$ is "smallest" in the sense that $S$ is contained in any other such set.)

A2 Let $Q_0(x) = 1$, $Q_1(x) = x$, and

$$Q_n(x) = \frac{(Q_{n-1}(x))^2 - 1}{Q_{n-2}(x)}$$

for all $n \geq 2$. Show that, whenever $n$ is a positive integer, $Q_n(x)$ is equal to a polynomial with integer coefficients.

A3 Let $a$ and $b$ be real numbers with $a < b$, and let $f$ and $g$ be continuous functions from $[a,b]$ to $(0,\infty)$ such that $\int_a^b f(x)\,dx = \int_a^b g(x)\,dx$ but $f \neq g$. For every positive integer $n$, define

$$I_n = \int_a^b \frac{(f(x))^{n+1}}{(g(x))^n}\,dx.$$

Show that $I_1, I_2, I_3, \ldots$ is an increasing sequence with $\lim_{n\to\infty} I_n = \infty$.

A4 A class with $2N$ students took a quiz, on which the possible scores were $0, 1, \ldots, 10$. Each of these scores occurred at least once, and the average score was exactly 7.4. Show that the class can be divided into two groups of $N$ students in such a way that the average score for each group was exactly 7.4.

A5 Each of the integers from 1 to $n$ is written on a separate card, and then the cards are combined into a deck and shuffled. Three players, $A$, $B$, and $C$, take turns in the order $A, B, C, A, \ldots$ choosing one card at random from the deck. (Each card in the deck is equally likely to be chosen.) After a card is chosen, that card and all higher-numbered cards are removed from the deck, and the remaining cards are reshuffled before the next turn. Play continues until one of the three players wins the game by drawing the card numbered 1.

Show that for each of the three players, there are arbitrarily large values of $n$ for which that player has the highest probability among the three players of winning the game.

A6 The 30 edges of a regular icosahedron are distinguished by labeling them $1, 2, \ldots, 30$. How many different ways are there to paint each edge red, white, or blue such that each of the 20 triangular faces of the icosahedron has two edges of the same color and a third edge of a different color? [Note: the top matter on each exam paper included the logo of the Mathematical Association of America, which is itself an icosahedron.]

B1 Let $L_1$ and $L_2$ be distinct lines in the plane. Prove that $L_1$ and $L_2$ intersect if and only if, for every real number $\lambda \neq 0$ and every point $P$ not on $L_1$ or $L_2$, there exist points $A_1$ on $L_1$ and $A_2$ on $L_2$ such that $\overrightarrow{PA_2} = \lambda \overrightarrow{PA_1}$.

B2 Suppose that a positive integer $N$ can be expressed as the sum of $k$ consecutive positive integers

$$N = a + (a+1) + (a+2) + \cdots + (a+k-1)$$

for $k = 2017$ but for no other values of $k > 1$. Considering all positive integers $N$ with this property, what is the smallest positive integer $a$ that occurs in any of these expressions?

B3 Suppose that $f(x) = \sum_{i=0}^{\infty} c_i x^i$ is a power series for which each coefficient $c_i$ is 0 or 1. Show that if $f(2/3) = 3/2$, then $f(1/2)$ must be irrational.

B4 Evaluate the sum

$$\sum_{k=0}^{\infty}\left(3\cdot\frac{\ln(4k+2)}{4k+2} - \frac{\ln(4k+3)}{4k+3} - \frac{\ln(4k+4)}{4k+4} - \frac{\ln(4k+5)}{4k+5}\right)$$
$$= 3\cdot\frac{\ln 2}{2} - \frac{\ln 3}{3} - \frac{\ln 4}{4} - \frac{\ln 5}{5} + 3\cdot\frac{\ln 6}{6} - \frac{\ln 7}{7} - \frac{\ln 8}{8} - \frac{\ln 9}{9} + 3\cdot\frac{\ln 10}{10} - \cdots.$$

(As usual, $\ln x$ denotes the natural logarithm of $x$.)

B5 A line in the plane of a triangle $T$ is called an *equalizer* if it divides $T$ into two regions having equal area and equal perimeter. Find positive integers $a > b > c$, with $a$ as small as possible, such that there exists a triangle with side lengths $a, b, c$ that has exactly two distinct equalizers.

B6 Find the number of ordered 64-tuples $(x_0, x_1, \ldots, x_{63})$ such that $x_0, x_1, \ldots, x_{63}$ are distinct elements of $\{1, 2, \ldots, 2017\}$ and

$$x_0 + x_1 + 2x_2 + 3x_3 + \cdots + 63x_{63}$$

is divisible by 2017.

# Solutions to the 78th William Lowell Putnam Mathematical Competition
## Saturday, December 2, 2017

Kiran Kedlaya and Lenny Ng

A1 We claim that the positive integers not in $S$ are 1 and all multiples of 5. If $S$ consists of all other natural numbers, then $S$ satisfies the given conditions: note that the only perfect squares not in $S$ are 1 and numbers of the form $(5k)^2$ for some positive integer $k$, and it readily follows that both (b) and (c) hold.

Now suppose that $T$ is another set of positive integers satisfying (a), (b), and (c). Note from (b) and (c) that if $n \in T$ then $n+5 \in T$, and so $T$ satisfies the following property:

(d) if $n \in T$, then $n+5k \in T$ for all $k \geq 0$.

The following must then be in $T$, with implications labeled by conditions (b) through (d):

$$2 \stackrel{c}{\Rightarrow} 49 \stackrel{c}{\Rightarrow} 54^2 \stackrel{d}{\Rightarrow} 56^2 \stackrel{b}{\Rightarrow} 56 \stackrel{d}{\Rightarrow} 121 \stackrel{b}{\Rightarrow} 11$$
$$11 \stackrel{d}{\Rightarrow} 16 \stackrel{b}{\Rightarrow} 4 \stackrel{d}{\Rightarrow} 9 \stackrel{b}{\Rightarrow} 3$$
$$16 \stackrel{d}{\Rightarrow} 36 \stackrel{b}{\Rightarrow} 6$$

Since $2,3,4,6 \in T$, by (d) $S \subseteq T$, and so $S$ is smallest.

A2 **First solution.** Define $P_n(x)$ for $P_0(x) = 1$, $P_1(x) = x$, and $P_n(x) = xP_{n-1}(x) - P_{n-2}(x)$. We claim that $P_n(x) = Q_n(x)$ for all $n \geq 0$; since $P_n(x)$ clearly is a polynomial with integer coefficients for all $n$, this will imply the desired result.

Since $\{P_n\}$ and $\{Q_n\}$ are uniquely determined by their respective recurrence relations and the initial conditions $P_0, P_1$ or $Q_0, Q_1$, it suffices to check that $\{P_n\}$ satisfies the same recurrence as $Q$: that is, $(P_{n-1}(x))^2 - P_n(x)P_{n-2}(x) = 1$ for all $n \geq 2$. Here is one proof of this: for $n \geq 1$, define the $2 \times 2$ matrices

$$M_n = \begin{pmatrix} P_{n-1}(x) & P_n(x) \\ P_{n-2}(x) & P_{n-1}(x) \end{pmatrix}, \quad T = \begin{pmatrix} x & -1 \\ 1 & 0 \end{pmatrix}$$

with $P_{-1}(x) = 0$ (this value being consistent with the recurrence). Then $\det(T) = 1$ and $TM_n = M_{n+1}$, so by induction on $n$ we have

$$(P_{n-1}(x))^2 - P_n(x)P_{n-2}(x) = \det(M_n) = \det(M_1) = 1.$$

**Remark:** A similar argument shows that any second-order linear recurrent sequence also satisfies a quadratic second-order recurrence relation. A familiar example is the identity $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$ for $F_n$ the $n$-th Fibonacci number. More examples come from various classes of *orthogonal polynomials*, including the Chebyshev polynomials mentioned below.

**Second solution.** We establish directly that $Q_n(x) = xQ_{n-1}(x) - Q_{n-2}(x)$, which again suffices. From the equation

$$1 = Q_{n-1}(x)^2 - Q_n(x)Q_{n-2}(x) = Q_n(x)^2 - Q_{n+1}(x)Q_{n-1}(x)$$

we deduce that

$$Q_{n-1}(x)(Q_{n-1}(x) + Q_{n+1}(x)) = Q_n(x)(Q_n(x) + Q_{n-2}(x)).$$

Since $\deg(Q_n(x)) = n$ by an obvious induction, the polynomials $Q_n(x)$ are all nonzero. We may thus rewrite the previous equation as

$$\frac{Q_{n+1}(x) + Q_{n-1}(x)}{Q_n(x)} = \frac{Q_n(x) + Q_{n-2}(x)}{Q_{n-1}(x)},$$

meaning that the rational functions $\frac{Q_n(x)+Q_{n-2}(x)}{Q_{n-1}(x)}$ are all equal to a constant value. By taking $n = 2$ and computing from the definition that $Q_2(x) = x^2 - 1$, we find the constant value to be $x$; this yields the desired recurrence.

**Remark:** By induction, one may also obtain the explicit formula

$$Q_n(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n-k}{k} x^{n-2k}.$$

**Remark:** In light of the explicit formula for $Q_n(x)$, Karl Mahlburg suggests the following bijective interpretation of the identity $Q_{n-1}(x)^2 - Q_n(x)Q_{n-2}(x) = 1$. Consider the set $C_n$ of integer compositions of $n$ with all parts 1 or 2; these are ordered tuples $(c_1, \dots, c_k)$ such that $c_1 + \cdots + c_k = n$ and $c_i \in \{1,2\}$ for all $i$. For a given composition $c$, let $o(c)$ and $d(c)$ denote the number of 1's and 2's, respectively. Define the generating function

$$R_n(x) = \sum_{c \in C_n} x^{o(c)};$$

then $R_n(x) = \sum_j \binom{n-j}{j} x^{n-2j}$, so that $Q_n(x) = i^{-n/2} R_n(ix)$. (The polynomials $R_n(x)$ are sometimes called *Fibonacci polynomials*; they satisfy $R_n(1) = F_n$. This interpretation of $F_n$ as the cardinality of $C_n$ first arose in the study of Sanskrit prosody, specifically the analysis of a line of verse as a sequence of long and short syllables, at least 500 years prior to the work of Fibonacci.)

The original identity is equivalent to the identity

$$R_{n+1}(x)R_{n-1}(x) - R_n(x)^2 = (-1)^{n-1}.$$

This follows because if we identify the composition $c$ with a tiling of a $1\times n$ rectangle by $1\times 1$ squares and $1\times 2$ dominoes, it is *almost* a bijection to place two tilings of length $n$ on top of each other, offset by one square, and hinge at the first possible point (which is the first square in either). This only fails when both tilings are all dominoes, which gives the term $(-1)^{n-1}$.

**Remark:** This problem appeared on the 2012 India National Math Olympiad; see `https://artofproblemsolving.com/community/c6h1219629`. Another problem based on the same idea is problem A2 from the 1993 Putnam.

A3 **First solution.** Extend the definition of $I_n$ to $n=0$, so that $I_0=\int_a^b f(x)\,dx>0$. Since $\int_a^b(f(x)-g(x))\,dx=0$, we have

$$\begin{aligned} I_1-I_0 &= \int_a^b \frac{f(x)}{g(x)}(f(x)-g(x))\,dx \\ &= \int_a^b \frac{(f(x)-g(x))^2}{g(x)}\,dx>0, \end{aligned}$$

where the inequality follows from the fact that the integrand is a nonnegative continuous function on $[a,b]$ that is not identically 0. Now for $n\geq 0$, the Cauchy–Schwarz inequality gives

$$\begin{aligned} I_nI_{n+2} &= \left(\int_a^b \frac{(f(x))^{n+1}}{(g(x))^n}\,dx\right)\left(\int_a^b \frac{(f(x))^{n+3}}{(g(x))^{n+2}}\,dx\right) \\ &\geq \left(\int_a^b \frac{(f(x))^{n+2}}{(g(x))^{n+1}}\,dx\right)^2 = I_{n+1}^2. \end{aligned}$$

It follows that the sequence $\{I_{n+1}/I_n\}_{n=0}^\infty$ is nondecreasing. Since $I_1/I_0>1$, this implies that $I_{n+1}>I_n$ for all $n$; also, $I_n/I_0=\prod_{k=0}^{n-1}(I_{k+1}/I_k)\geq (I_1/I_0)^n$, and so $\lim_{n\to\infty}I_n=\infty$ since $I_1/I_0>1$ and $I_0>0$.

**Remark:** Noam Elkies suggests the following variant of the previous solution, which eliminates the need to separately check that $I_1>I_0$. First, the proof that $I_nI_{n+2}\geq I_{n+1}^2$ applies also for $n=-1$ under the convention that $I_{-1}=\int_a^b g(x)\,dx$ (as in the fourth solution below). Second, this equality must be strict for each $n\geq -1$: otherwise, the equality condition in Cauchy–Schwarz would imply that $g(x)=cf(x)$ identically for some $c>0$, and the equality $\int_a^b f(x)\,dx=\int_a^b g(x)\,dx$ would then force $c=1$, contrary to assumption. Consequently, the sequence $I_{n+1}/I_n$ is strictly increasing; since $I_0/I_{-1}=1$, it follows that for $n\geq 0$, we again have $I_{n+1}/I_n\geq I_1/I_0>1$ and so on.

**Second solution.** (from Art of Problem Solving, user `MSTang`) Since $\int_a^b(f(x)-g(x))\,dx=0$, we have

$$\begin{aligned} I_{n+1}-I_n &= \int_a^b\left(\frac{(f(x))^{n+2}}{(g(x))^{n+1}}-\frac{(f(x))^{n+1}}{(g(x))^n}\right)dx \\ &= \int_a^b \frac{(f(x))^{n+1}}{(g(x))^{n+1}}(f(x)-g(x))\,dx \\ &= \int_a^b\left(\frac{(f(x))^{n+1}}{(g(x))^{n+1}}-1\right)(f(x)-g(x))\,dx \\ &= \int_a^b \frac{(f(x)-g(x))^2((f(x))^n+\cdots+g(x)^n)}{(g(x))^{n+1}}\,dx. \end{aligned}$$

The integrand is continuous, nonnegative, and not identically zero; hence $I_{n+1}-I_n>0$.

To prove that $\lim_{n\to\infty}I_n=\infty$, note that we cannot have $f(x)\leq g(x)$ identically, as then the equality $\int_a^b f(x)\,dx=\int_a^b g(x)\,dx$ would imply $f(x)=g(x)$ identically. That is, there exists some $t\in[a,b]$ such that $f(t)>g(t)$. By continuity, there exist a quantity $c>1$ and an interval $J=[t_0,t_1]$ in $[a,b]$ such that $f(x)\geq cg(x)$ for all $x\in J$. We then have

$$I_n\geq \int_{t_0}^{t_1}\frac{(f(x))^{n+1}}{(g(x))^n}\,dx\geq c^n\int_{t_0}^{t_1}f(x)\,dx;$$

since $f(x)>0$ everywhere, we have $\int_{t_0}^{t_1}f(x)\,dx>0$ and hence $I_n$ is bounded below by a quantity which tends to $\infty$.

**Remark:** One can also give a variation of the second half of the solution which shows directly that $I_{n+1}-I_n\geq c^nd$ for some $c>1,d>0$, thus proving both assertions at once.

**Third solution.** (from David Savitt, via Art of Problem Solving) Extend the definition of $I_n$ to all *real* $n$, and note that

$$I_{-1}=\int_a^b g(x)\,dx=\int_a^b f(x)\,dx=I_0.$$

By writing

$$I_n=\int_a^b \exp((n+1)\log f(x)-n\log g(x))\,dx,$$

we see that the integrand is a strictly convex function of $n$, as then is $I_n$. It follows that $I_n$ is strictly increasing and unbounded for $n\geq 1$.

**Fourth solution.** (by David Rusin) Again, extend the definition of $I_n$ to $n=-1$. Now note that for $n\geq 0$ and $x\in[a,b]$, we have

$$(f(x)-g(x))\left(\left(\frac{f(x)}{g(x)}\right)^{n+1}-\left(\frac{f(x)}{g(x)}\right)^n\right)\geq 0$$

because both factors have the same sign (depending on the comparison between $f(x)$ and $g(x)$); moreover, equality only occurs when $f(x)=g(x)$. Since $f$ and $g$ are not identically equal, we deduce that

$$I_{n+1}-I_n>I_n-I_{n-1}$$

and so in particular

$$I_{n+1} - I_n \geq I_1 - I_0 > I_0 - I_{-1} = 0.$$

This proves both claims.

**Remark:** This problem appeared in 2005 on an undergraduate math olympiad in Brazil. See `https://artofproblemsolving.com/community/c7h57686p354392` for discussion.

A4 **First solution.** Let $a_1, \dots, a_{2N}$ be the scores in nondecreasing order, and define the sums $s_i = \sum_{j=i+1}^{i+N} a_j$ for $i = 0, \dots, N$. Then $s_0 \leq \cdots \leq s_N$ and $s_0 + s_N = \sum_{j=1}^{2N} a_j = 7.4(2N)$, so $s_0 \leq 7.4N \leq s_N$. Let $i$ be the largest index for which $s_i \leq 7.4N$; note that we cannot have $i = N$, as otherwise $s_0 = s_N = 7.4N$ and hence $a_1 = \cdots = a_{2N} = 7.4$, contradiction. Then $7.4N - s_i < s_{i+1} - s_i = a_{i+N+1} - a_i$ and so

$$a_i < s_i + a_{i+N+1} - 7.4N \leq a_{i+N+1};$$

since all possible scores occur, this means that we can find $N$ scores with sum $7.4N$ by taking $a_{i+1}, \dots, a_{i+N+1}$ and omitting one occurrence of the value $s_i + a_{i+N+1} - 7.4N$.

**Remark:** David Savitt (via Art of Problem Solving) points out that a similar argument applies provided that there are an even number of students, the total score is even, and the achieved scores form a block of consecutive integers.

**Second solution.** We first claim that for any integer $m$ with $15 \leq m \leq 40$, we can find five distinct elements of the set $\{1, 2, \dots, 10\}$ whose sum is $m$. Indeed, for $0 \leq k \leq 4$ and $1 \leq \ell \leq 6$, we have

$$\left(\sum_{j=1}^{k} j\right) + (k + \ell) + \left(\sum_{j=k+7}^{10} j\right) = 34 - 5k + \ell,$$

and for fixed $k$ this takes all values from $35 - 5k$ to $40 - 5k$ inclusive; then as $k$ ranges from 0 to 4, this takes all values from 15 to 40 inclusive.

Now suppose that the scores are $a_1, \dots, a_{2N}$, where we order the scores so that $a_k = k$ for $k \leq 10$ and the subsequence $a_{11}, a_{12}, \dots, a_{2N}$ is nondecreasing. For $1 \leq k \leq N - 4$, define $S_k = \sum_{j=k+10}^{k+N+4} a_j$. Note that for each $k$, $S_{k+1} - S_k = a_{k+N+5} - a_{k+10}$ and so $0 \leq S_{k+1} - S_k \leq 10$. Thus $S_1, \dots, S_{N-4}$ is a nondecreasing sequence of integers where each term is at most 10 more than the previous one. On the other hand, we have

$$\begin{aligned} S_1 + S_{N-4} &= \sum_{j=11}^{2N} a_j \\ &= (7.4)(2N) - \sum_{j=1}^{10} a_j \\ &= (7.4)(2N) - 55, \end{aligned}$$

whence $S_1 \leq 7.4N - 27.5 \leq S_{N-4}$. It follows that there is some $k$ such that $S_k \in [7.4N - 40, 7.4N - 15]$, since this interval has length 25 and $7.4N - 27.5$ lies inside it.

For this value of $k$, note that both $S_k$ and $7.4N$ are integers (the latter since the sum of all scores in the class is the integer $(7.4)(2N)$ and so $N$ must be divisible by 5). Thus there is an integer $m$ with $15 \leq m \leq 40$ for which $S_k = 7.4N - m$. By our first claim, we can choose five scores from $a_1, \dots, a_{10}$ whose sum is $m$. When we add these to the sum of the $N - 5$ scores $a_{k+10}, \dots, a_{k+N+4}$, we get precisely $7.4N$. We have now found $N$ scores whose sum is $7.4N$ and thus whose average is 7.4.

**Third solution.** It will suffices to show that given any partition of the students into two groups of $N$, if the sums are not equal we can bring them closer together by swapping one pair of students between the two groups. To state this symbolically, let $S$ be the set of students and, for any subset $T$ of $S$, let $\Sigma T$ denote the sum of the scores of the students in $T$; we then show that if $S = A \cup B$ is a partition into two $N$-element sets with $\Sigma A > \Sigma B$, then there exist students $a \in A, B \in B$ such that the sets

$$A' = A \setminus \{a\} \cup \{b\}, \qquad B' = A \setminus \{b\} \cup \{a\}$$

satisfy

$$0 \leq \Sigma A' - \Sigma B' < \Sigma A - \Sigma B.$$

In fact, this argument will apply at the same level of generality as in the remark following the first solution.

To prove the claim, let $a_1, \dots, a_n$ be the scores in $A$ and let $b_1, \dots, b_n$ be the scores in $B$ (in any order). Since $\Sigma A - \Sigma B \equiv \Sigma S \pmod{2}$ and the latter is even, we must have $\Sigma A - \Sigma B \geq 2$. In particular, there must exist indices $i, j \in \{1, \dots, n\}$ such that $a_i > b_j$. Consequently, if we sort the sequence $a_1, \dots, a_n, b_1, \dots, b_n$ into nondecreasing order, it must be the case that some term $b_j$ is followed by some term $a_i$. Moreover, since the achieved scores form a range of consecutive integers, we must in fact have $a_i = b_j + 1$. Consequently, if we take $a = a_i$, $b = b_j$, we then have $\Sigma A' - \Sigma' B = \Sigma A - \Sigma B - 2$, which proves the claim.

A5 **First solution.** Let $a_n, b_n, c_n$ be the probabilities that players $A$, $B$, $C$, respectively, will win the game. We compute these by induction on $n$, starting with the values

$$a_1 = 1, \qquad b_1 = 0, \qquad c_1 = 0.$$

If player $A$ draws card $k$, then the resulting game state is that of a deck of $k - 1$ cards with the players taking turns in the order $B, C, A, B, \dots$. In this state, the probabilities that players $A, B, C$ will win are $c_{k-1}, a_{k-1}, b_{k-1}$ provided that we adopt the convention that

$$a_0 = 0, \qquad b_0 = 0, \qquad c_0 = 1.$$

We thus have

$$a_n = \frac{1}{n}\sum_{k=1}^{n} c_{k-1}, \quad b_n = \frac{1}{n}\sum_{k=1}^{n} a_{k-1}, \quad c_n = \frac{1}{n}\sum_{k=1}^{n} b_{k-1}.$$

Put

$$x_n = a_n - b_n, \quad y_n = b_n - c_n, \quad z_n = c_n - a_n;$$

we then have

$$\begin{aligned} x_{n+1} &= \frac{n}{n+1}x_n + \frac{1}{n+1}z_n, \\ y_{n+1} &= \frac{n}{n+1}y_n + \frac{1}{n+1}x_n, \\ z_{n+1} &= \frac{n}{n+1}z_n + \frac{1}{n+1}y_n. \end{aligned}$$

Note that if $a_{n+1} = b_{n+1} = c_{n+1} = 0$, then

$$x_n = -nz_n = n^2 y_n = -n^3 x_n = n^4 z_n$$

and so $x_n = z_n = 0$, or in other words $a_n = b_n = c_n$. By induction on $n$, we deduce that $a_n, b_n, c_n$ cannot all be equal. That is, the quantities $x_n, y_n, z_n$ add up to zero and at most one of them vanishes; consequently, the quantity $r_n = \sqrt{x_n^2 + y_n^2 + z_n^2}$ is always positive and the quantities

$$x'_n = \frac{x_n}{r_n}, \quad y'_n = \frac{y_n}{r_n}, \quad z'_n = \frac{z_n}{r_n}$$

form the coordinates of a point $P_n$ on a fixed circle $C$ in $\mathbb{R}^3$.

Let $P'_n$ be the point $(z_n, x_n, y_n)$ obtained from $P_n$ by a clockwise rotation of angle $\frac{2\pi}{3}$. The point $P_{n+1}$ then lies on the ray through the origin passing through the point dividing the chord from $P_n$ to $P'_n$ in the ratio $1:n$. The (clockwise) arc from $P_n$ to $P_{n+1}$ therefore has a measure of

$$\arctan \frac{\sqrt{3}}{2n-1} = \frac{\sqrt{3}}{2n-1} + O(n^{-3});$$

these measures form a null sequence whose sum diverges. It follows that any arc of $C$ contains infinitely many of the $P_n$; taking a suitably short arc around the point $(\frac{\sqrt{2}}{2}, 0, -\frac{\sqrt{2}}{2})$, we deduce that for infinitely many $n$, $A$ has the highest winning probability, and similarly for $B$ and $C$.

**Remark:** From the previous analysis, we also deduce that

$$\frac{r_{n+1}}{r_n} = \frac{\sqrt{n^2-n+1}}{n+1} = 1 - \frac{3}{2(n+1)} + O(n^{-2}),$$

from which it follows that $r_n \sim cn^{-3/2}$ for some $c > 0$.

**Second solution.** (by Noam Elkies) In this approach, we instead compute the probability $p_n(m)$ that the game ends after exactly $m$ turns (the winner being determined by the residue of $m$ mod 3). We use the convention that $p_0(0) = 1$, $p_0(m) = 0$ for $m > 0$. Define the generating function $P_n(X) = \sum_{m=0}^{n} p_n(m)x^m$. We will establish that

$$P_n(X) = \frac{X(X+1)\cdots(X+n-1)}{n!}$$

(which may be guessed by computing $p_n(m)$ for small $n$ by hand). There are several ways to do this; for instance, this follows from the recursion

$$P_n(X) = \frac{1}{n}XP_{n-1}(X) + \frac{(n-1)}{n}P_{n-1}(X).$$

(In this recursion, the first term corresponds to conditional probabilities given that the first card drawn is $n$, and the second term corresponds to the remaining cases.)

Let $\omega$ be a primitive cube root of 1. With notation as in the first solution, we have

$$P_n(\omega) = a_n + b_n\omega + c_n\omega;$$

combining this with the explicit formula for $P_n(X)$ and the observation that

$$\arg(w+n) = \arctan\frac{\sqrt{3}}{2n-1}$$

recovers the geometric description of $a_n, b_n, c_n$ given in the first solution (as well as the remark following the first solution).

**Third solution.** For this argument, we use the auxiliary quantities

$$a'_n = a_n - \frac{1}{3}, \quad b'_n = b_n - \frac{1}{3}, \quad c'_n = c_n - \frac{1}{3};$$

these satisfy the relations

$$a'_n = \frac{1}{n}\sum_{k=1}^{n} c'_{k-1}, \quad b'_n = \frac{1}{n}\sum_{k=1}^{n} a'_{k-1}, \quad c'_n = \frac{1}{n}\sum_{k=1}^{n} b'_{k-1}$$

as well as

$$\begin{aligned} a'_{n+1} &= a'_n + \frac{1}{n+1}(c'_n - a'_n) \\ b'_{n+1} &= b'_n + \frac{1}{n+1}(a'_n - b'_n) \\ c'_{n+1} &= c'_n + \frac{1}{n+1}(b'_n - c'_n). \end{aligned}$$

We now show that $\sum_{n=1}^{\infty} a'_n$ cannot diverge to $+\infty$ (and likewise for $\sum_{n=1}^{\infty} b'_n$ and $\sum_{n=1}^{\infty} c'_n$ by similar reasoning). Suppose the contrary; then there exists some $\varepsilon > 0$ and some $n_0 > 0$ such that $\sum_{k=1}^{n} a'_k \geq \varepsilon$ for all $n \geq n_0$. For $n > n_0$, we have $b'_n \geq \varepsilon$; this in turn implies that $\sum_{n=1}^{\infty} b'_n$ diverges to $+\infty$. Continuing around the circle, we deduce that for $n$ sufficiently large, all three of $a'_n, b'_n, c'_n$ are positive; but this contradicts the identity

$a_n' + b_n' + c_n' = 0$. We thus conclude that $\sum_{n=1}^\infty a_n'$ does not diverge to $+\infty$; in particular, $\liminf_{n\to\infty} a_n' \leq 0$.

By the same token, we may see that $\sum_{n=1}^\infty a_n'$ cannot converge to a positive limit $L$ (and likewise for $\sum_{n=1}^\infty b_n'$ and $\sum_{n=1}^\infty c_n'$ by similar reasoning). Namely, this would imply that $b_n' \geq L/2$ for $n$ sufficiently large, contradicting the previous argument.

By similar reasoning, $\sum_{n=1}^\infty a_n'$ cannot diverge to $-\infty$ or converge to a negative limit $L$ (and likewise for $\sum_{n=1}^\infty b_n'$ and $\sum_{n=1}^\infty c_n'$ by similar reasoning).

We next establish that there are infinitely many $n$ for which $a_n' > 0$ (and likewise for $b_n'$ and $c_n'$ by similar reasoning). Suppose to the contrary that for $n$ sufficiently large, we have $a_n' \leq 0$. By the previous arguments, the sum $\sum_{n=1}^\infty a_n'$ cannot diverge to $\infty$ or converge to a nonzero limit; it must therefore converge to 0. In particular, for $n$ sufficiently large, we have $b_n' = \sum_{k=1}^n a_{k-1}' \geq 0$. Iterating the construction, we see that for $n$ sufficiently large, we must have $c_n' \leq 0, a_n' \geq 0$, $b_n' \leq 0$, and $c_n' \geq 0$. As a result, for $n$ sufficiently large we must have $a_n' = b_n' = c_n' = 0$; but we may rule this out as in the original solution.

By similar reasoning, we may deduce that there are infinitely many $n$ for which $a_n' < 0$ (and likewise for $b_n'$ and $c_n'$ by similar reasoning). We now continue using a suggestion of Jon Atkins. Define the values of the sequence $x_n$ according to the relative comparison of $a_n', b_n', c_n'$ (using the fact that these cannot all be equal):

$$\begin{aligned}
x_n = 1: &\quad a_n' \leq b_n' < c_n' \\
x_n = 2: &\quad b_n' \leq c_n' < a_n' \\
x_n = 3: &\quad c_n' \leq a_n' < b_n' \\
x_n = 4: &\quad a_n' < c_n' \leq b_n' \\
x_n = 5: &\quad b_n' < a_n' \leq c_n' \\
x_n = 6: &\quad c_n' < b_n' \leq a_n'.
\end{aligned}$$

We consider these values as *states* and say that there is a *transition* from state $i$ to state $j$, and write $i \Rightarrow j$, if for every $n \geq 2$ with $x_n = i$ there exists $n' > n$ with $x_{n'} = j$. (In all cases when we use this notation, it will in fact be the case that the *first* value of $n' > n$ for which $x_{n'} \neq i$ satisfes $x_{n'} = j$, but this is not logically necessary for our final conclusion.)

Suppose that $x_n = 1$. By the earlier discussion, we must have $a_{n'}' > 0$ for some $n' > n$, and so we cannot have $x_{n'} = 1$ for all $n' > n$. On the other hand, as long as $x_n = 1$, we have

$$\begin{aligned}
c_{n+1}' - b_{n+1}' &= c_n' - b_n' + \frac{1}{n+1}(2b_n' - a_n' - c_n') \\
&= \frac{n-1}{n+1}(c_n' - b_n') + \frac{1}{n+1}(c_n' - a_n') > 0 \\
c_{n+1}' - a_{n+1}' &= c_n' - a_n' + \frac{1}{n+1}(a_n' + b_n' - 2c_n') \\
&= \frac{n-1}{n+1}(c_n' - a_n') + \frac{1}{n+1}(b_n' - a_n') > 0.
\end{aligned}$$

Consequently, for $n'$ the smallest value for which $x_{n'} \neq x_n$, we must have $x_{n'} = 2$. By this and two similar arguments, we deduce that

$$1 \Rightarrow 5, \quad 2 \Rightarrow 6, \quad 3 \Rightarrow 4.$$

Suppose that $x_n = 4$. By the earlier discussion, we must have $a_{n'}' < 0$ for some $n' > n$, and so we cannot have $x_{n'} = 4$ for all $n' > n$. On the other hand, as long as $x_n = 4$, we have

$$\begin{aligned}
b_{n+1}' - a_{n+1}' &= b_n' - a_n' + \frac{1}{n+1}(2a_n' - b_n' - c_n') \\
&= \frac{n-1}{n+1}(b_n' - a_n') + \frac{1}{n+1}(b_n' - c_n') > 0 \\
c_{n+1}' - a_{n+1}' &= c_n' - a_n' + \frac{1}{n+1}(a_n' + b_n' - 2c_n') \\
&= \frac{n-1}{n+1}(c_n' - a_n') + \frac{1}{n+1}(b_n' - a_n') > 0.
\end{aligned}$$

Consequently, for $n'$ the smallest value for which $x_{n'} \neq x_n$, we must have $x_{n'} = 1$. By this and two similar arguments, we deduce that

$$4 \Rightarrow 1, \quad 5 \Rightarrow 2, \quad 6 \Rightarrow 3.$$

Combining, we obtain

$$1 \Rightarrow 5 \Rightarrow 2 \Rightarrow 6 \Rightarrow 3 \Rightarrow 4 \Rightarrow 1$$

and hence the desired result.

A6 The number of such colorings is $2^{20}3^{10} = 61917364224$.

**First solution:** Identify the three colors red, white, and blue with (in some order) the elements of the field $\mathbb{F}_3$ of three elements (i.e., the ring of integers mod 3). The set of colorings may then be identified with the $\mathbb{F}_3$-vector space $\mathbb{F}_3^E$ generated by the set $E$ of edges. Let $F$ be the set of faces, and let $\mathbb{F}_3^F$ be the $\mathbb{F}_3$-vector space on the basis $F$; we may then define a linear transformation $T: \mathbb{F}_3^E \to \mathbb{F}_3^F$ taking a coloring to the vector whose component corresponding to a given face equals the sum of the three edges of that face. The colorings we wish to count are the ones whose images under $T$ consist of vectors with no zero components.

We now show that $T$ is surjective. (There are many possible approaches to this step; for instance, see the following remark.) Let $\Gamma$ be the dual graph of the icosahedron, that is, $\Gamma$ has vertex set $F$ and two elements of $F$ are adjacent in $\Gamma$ if they share an edge in the icosahedron. The graph $\Gamma$ admits a hamiltonian path, that is, there exists an ordering $f_1, \dots, f_{20}$ of the faces such that any two consecutive faces are adjacent in $\Gamma$. For example, such an ordering can be constructed with $f_1, \dots, f_5$ being the five faces sharing a vertex of the icosahedron and $f_{16}, \dots, f_{20}$ being the five faces sharing the antipodal vertex.

For $i = 1, \dots, 19$, let $e_i$ be the common edge of $f_i$ and $f_{i+1}$; these are obviously all distinct. By prescribing components for $e_1,\dots,e_{19}$ in turn and setting the others to zero, we can construct an element of $\mathbb{F}_3^E$ whose image under $T$ matches any given vector of $\mathbb{F}_3^F$ in the components of $f_1,\dots,f_{19}$. The vectors in $\mathbb{F}_3^F$ obtained in this way thus form a 19-dimensional subspace; this subspace may also be described as the vectors for which the components of $f_1,\dots,f_{19}$ have the same sum as the components of $f_2,\dots,f_{20}$.

By performing a mirror reflection, we can construct a second hamiltonian path $g_1,\dots,g_{20}$ with the property that

$$g_1 = f_1, g_2 = f_5, g_3 = f_4, g_4 = f_3, g_5 = f_2.$$

Repeating the previous construction, we obtain a *different* 19-dimensional subspace of $\mathbb{F}_3^F$ which is contained in the image of $T$. This implies that $T$ is surjective, as asserted earlier.

Since $T$ is a surjective homomorphism from a 30-dimensional vector space to a 20-dimensional vector space, it has a 10-dimensional kernel. Each of the $2^{20}$ elements of $\mathbb{F}_3^F$ with no zero components is then the image of exactly $3^{10}$ colorings of the desired form, yielding the result.

**Remark:** There are many ways to check that $T$ is surjective. One of the simplest is the following (from Art of Problem Solving, user `Ravi12346`): form a vector in $\mathbb{F}^E$ with components $2,1,2,1,2$ at the five edges around some vertex and all other components 0. This maps to a vector in $\mathbb{F}^F$ with only a single nonzero component; by symmetry, every standard basis vector of $\mathbb{F}^F$ arises in this way.

**Second solution:** (from Bill Huang, via Art of Problem Solving user `superpi83`) Let $v$ and $w$ be two antipodal vertices of the icosahedron. Let $S_v$ (resp. $S_w$) be the set of five edges incident to $v$ (resp. $w$). Let $T_v$ (resp. $T_w$) be the set of five edges of the pentagon formed by the opposite endpoints of the five edges in $S_v$ (resp. $S_w$). Let $U$ be the set of the ten remaining edges of the icosahedron.

Consider any one of the $3^{10}$ possible colorings of $U$. The edges of $T_v \cup U$ form the boundaries of five faces with no edges in common; thus each edge of $T_v$ can be colored in one of two ways consistent with the given condition, and similarly for $T_w$. That is, there are $3^{10}2^{10}$ possible colorings of $T_v \cup T_w \cup U$ consistent with the given condition.

To complete the count, it suffices to check that there are exactly $2^5$ ways to color $S_v$ consistent with any given coloring of $T_v$. Using the linear-algebraic interpretation from the first solution, this follows by observing that (by the previous remark) the map from $\mathbb{F}_3^{S_v}$ to the $\mathbb{F}_3$-vector space on the faces incident to $v$ is surjective, and hence an isomorphism for dimensional reasons. A direct combinatorial proof is also possible.

B1 Recall that $L_1$ and $L_2$ intersect if and only if they are not parallel. In one direction, suppose that $L_1$ and $L_2$ intersect. Then for any $P$ and $\lambda$, the dilation (homothety) of the plane by a factor of $\lambda$ with center $P$ carries $L_1$ to another line parallel to $L_1$ and hence not parallel to $L_2$. Let $A_2$ be the unique intersection of $L_2$ with the image of $L_1$, and let $A_1$ be the point on $L_1$ whose image under the dilation is $A_2$; then $\overrightarrow{PA_2} = \lambda \overrightarrow{PA_1}$.

In the other direction, suppose that $L_1$ and $L_2$ are parallel. Let $P$ be any point in the region between $L_1$ and $L_2$ and take $\lambda = 1$. Then for any point $A_1$ on $L_1$ and any point $A_2$ on $L_2$, the vectors $\overrightarrow{PA_1}$ and $\overrightarrow{PA_2}$ have components perpendicular to $L_1$ pointing in opposite directions; in particular, the two vectors cannot be equal.

**Reinterpretation:** (by Karl Mahlburg) In terms of vectors, we may find vectors $\vec{v}_1, \vec{v}_2$ and scalars $c_1, c_2$ such that $L_i = \{\vec{x} \in \mathbb{R}^2 : \vec{v}_i \cdot \vec{x} = c_i\}$. The condition in the problem amounts to finding a vector $\vec{w}$ and a scalar $t$ such that $P + \vec{w} \in L_1, P + \lambda w \in L_2$; this comes down to solving the linear system

$$\begin{aligned} \vec{v}_1 \cdot (P + \vec{w}) &= c_1 \\ \vec{v}_2 \cdot (P + \lambda \vec{w}) &= c_2 \end{aligned}$$

which is nondegenerate and solvable for all $\lambda$ if and only if $\vec{v}_1, \vec{v}_2$ are linearly independent.

B2 We prove that the smallest value of $a$ is 16.

Note that the expression for $N$ can be rewritten as $k(2a+k-1)/2$, so that $2N = k(2a+k-1)$. In this expression, $k > 1$ by requirement; $k < 2a+k-1$ because $a > 1$; and obviously $k$ and $2a+k-1$ have opposite parity. Conversely, for any factorization $2N = mn$ with $1 < m < n$ and $m,n$ of opposite parity, we obtain an expression of $N$ in the desired form by taking $k = m$, $a = (n+1-m)/2$.

We now note that 2017 is prime. (On the exam, solvers would have had to verify this by hand. Since $2017 < 45^2$, this can be done by trial division by the primes up to 43.) For $2N = 2017(2a+2016)$ not to have another expression of the specified form, it must be the case that $2a+2016$ has no odd divisor greater than 1; that is, $2a+2016$ must be a power of 2. This first occurs for $2a+2016 = 2048$, yielding the claimed result.

**Reinterpretation:** (by Karl Mahlburg) To avoid $N$ having another representation, for $k = 2,\dots,2016$, we must have

$$N \not\equiv \begin{cases} k/2 & k \equiv 0 \pmod 2 \\ 0 & k \equiv 1 \pmod 2. \end{cases}$$

Consequently, $N \not\equiv 0 \pmod p$ for any odd prime $p < 2017$ and $N \equiv 0 \pmod{1024}$. Since $N$ must be divisible by 2017, this again yields the claimed value of $a$.

B3 Suppose by way of contradiction that $f(1/2)$ is rational. Then $\sum_{i=0}^{\infty} c_i 2^{-i}$ is the binary expansion of a rational number, and hence must be eventually periodic; that is, there exist some integers $m,n$ such that $c_i = c_{m+i}$ for all

$i \geq n$. We may then write

$$f(x) = \sum_{i=0}^{n-1} c_i x^i + \frac{x^n}{1-x^m} \sum_{i=0}^{m-1} c_{n+i} x^i.$$

Evaluating at $x = 2/3$, we may equate $f(2/3) = 3/2$ with

$$\frac{1}{3^{n-1}} \sum_{i=0}^{n-1} c_i 2^i 3^{n-i-1} + \frac{2^n 3^m}{3^{n+m-1}(3^m - 2^m)} \sum_{i=0}^{m-1} c_{n+i} 2^i 3^{m-1-i};$$

since all terms on the right-hand side have odd denominator, the same must be true of the sum, a contradiction.

**Remark:** Greg Marks asks whether the assumption that $f(2/3) = 3/2$ further ensures that $f(1/2)$ is transcendental. We do not know of any existing results that would imply this. However, the following result follows from a theorem of T. Tanaka (Algebraic independence of the values of power series generated by linear recurrences, *Acta Arith.* **74** (1996), 177–190), building upon work of Mahler. Let $\{a_n\}_{n=0}^\infty$ be a linear recurrent sequence of positive integers with characteristic polynomial $P$. Suppose that $P(0), P(1), P(-1) \neq 0$ and that no two distinct roots of $P$ have ratio which is a root of unity. Then for $f(x) = \sum_{n=0}^\infty x^{a_n}$, the values $f(1/2)$ and $f(2/3)$ are algebraically independent over $\mathbb{Q}$. (Note that for $f$ as in the original problem, the condition on ratios of roots of $P$ fails.)

B4 We prove that the sum equals $(\log 2)^2$; as usual, we write $\log x$ for the natural logarithm of $x$ instead of $\ln x$. Note that of the two given expressions of the original sum, the first is absolutely convergent (the summands decay as $\log(x)/x^2$) but the second one is not; we must thus be slightly careful when rearranging terms.

**First solution.** Define $a_k = \frac{\log k}{k} - \frac{\log(k+1)}{k+1}$. The infinite sum $\sum_{k=1}^\infty a_k$ converges to 0 since $\sum_{k=1}^n a_k$ telescopes to $-\frac{\log(n+1)}{n+1}$ and this converges to 0 as $n \to \infty$. Note that $a_k > 0$ for $k \geq 3$ since $\frac{\log x}{x}$ is a decreasing function of $x$ for $x > e$, and so the convergence of $\sum_{k=1}^\infty a_k$ is absolute.

Write $S$ for the desired sum. Then since $3a_{4k+2} + 2a_{4k+3} + a_{4k+4} = (a_{4k+2} + a_{4k+4}) + 2(a_{4k+2} + a_{4k+3})$, we have

$$\begin{aligned} S &= \sum_{k=0}^\infty (3a_{4k+2} + 2a_{4k+3} + a_{4k+4}) \\ &= \sum_{k=1}^\infty a_{2k} + \sum_{k=0}^\infty 2(a_{4k+2} + a_{4k+3}), \end{aligned}$$

where we are allowed to rearrange the terms in the infinite sum since $\sum a_k$ converges absolutely. Now $2(a_{4k+2} + a_{4k+3}) = \frac{\log(4k+2)}{2k+1} - \frac{\log(4k+4)}{2k+2} = a_{2k+1} + (\log 2)(\frac{1}{2k+1} - \frac{1}{2k+2})$, and summing over $k$ gives

$$\begin{aligned} \sum_{k=0}^\infty 2(a_{4k+2} + a_{4k+3}) &= \sum_{k=0}^\infty a_{2k+1} + (\log 2) \sum_{k=1}^\infty \frac{(-1)^{k+1}}{k} \\ &= \sum_{k=0}^\infty a_{2k+1} + (\log 2)^2. \end{aligned}$$

Finally, we have

$$\begin{aligned} S &= \sum_{k=1}^\infty a_{2k} + \sum_{k=0}^\infty a_{2k+1} + (\log 2)^2 \\ &= \sum_{k=1}^\infty a_k + (\log 2)^2 = (\log 2)^2. \end{aligned}$$

**Second solution.** We start with the following observation: for any positive integer $n$,

$$\left.\frac{d}{ds} n^{-s}\right|_{s=1} = -(\log n) n^{-s}.$$

(Throughout, we view $s$ as a *real* parameter, but see the remark below.) For $s > 0$, consider the absolutely convergent series

$$L(s) = \sum_{k=0}^\infty (3(4k+2)^{-s} - (4k+3)^{-s} - (4k+4)^{-s} - (4k+5)^{-s});$$

in the same range we have

$$\begin{aligned} L'(s) = \sum_{k=0}^\infty \biggl( 3\frac{\log(4k+2)}{(4k+2)^s} &- \frac{\log(4k+3)}{(4k+3)^s} \\ + \frac{\log(4k+4)}{(4k+4)^s} &- \frac{\log(4k+5)}{(4k+5)^s} \biggr), \end{aligned}$$

so we may interchange the summation with taking the limit at $s = 1$ to equate the original sum with $-L'(1)$.

To make further progress, we introduce the Riemann zeta function $\zeta(s) = \sum_{n=1}^\infty n^{-s}$, which converges absolutely for $s > 1$. In that region, we may freely rearrange sums to write

$$\begin{aligned} L(s) + \zeta(s) &= 1 + 4(2^{-s} + 6^{-s} + 10^{-s} + \cdots) \\ &= 1 + 2^{2-s}(1 + 3^{-s} + 5^{-s} + \cdots) \\ &= 1 + 2^{2-s}(\zeta(s) - 2^{-s} - 4^{-s} - \cdots) \\ &= 1 + 2^{2-s}\zeta(s) - 2^{2-2s}\zeta(s). \end{aligned}$$

In other words, for $s > 1$, we have

$$L(s) = 1 + \zeta(s)(-1 + 2^{2-s} - 2^{2-2s}).$$

Now recall that $\zeta(s) - \frac{s}{s-1}$ extends to a $C^\infty$ function for $s > 0$, e.g., by applying Abel summation to obtain

$$\begin{aligned} \zeta(s) - \frac{s}{s-1} &= \sum_{n=1} n(n^{-s} - (n+1)^{-s}) - \frac{s}{s-1} \\ &= s \sum_{n=1}^\infty n \int_n^{n+1} x^{-s-1}\, dx - \frac{s}{s-1} \\ &= -s \int_1^\infty (x - \lfloor x \rfloor) x^{-s-1}\, dx. \end{aligned}$$

Also by writing $2^{2-s} = 2\exp((1-s)\log 2$ and $2^{2-2s} = \exp(2(1-s)\log 2)$, we may use the exponential series to compute the Taylor expansion of

$$f(s) = \frac{-1 + 2^{2-s} - 2^{2-2s}}{s-1}$$

at $s=1$; we get

$$f(s) = -(\log 2)^2(s-1)^2 + O((s-1)^3).$$

Consequently, if we rewrite the previous expression for $L(s)$ as

$$L(s) = 1 + (s-1)\zeta(s) \cdot \frac{-1+2^{2-s}-2^{2-2s}}{s-1},$$

then we have an equality of $C^\infty$ functions for $s>1$, and hence (by continuity) an equality of Taylor series about $s=1$. That is,

$$L(s) = 1 - (\log 2)^2(s-1) + O((s-1)^2),$$

which yields the desired result.

**Remark:**

The use of series $\sum_{n=1}^\infty c_n n^{-s}$ as functions of a *real* parameter $s$ dates back to Euler, who observed that the divergence of $\zeta(s)$ as $s \to 1$ gives a proof of the infinitude of primes distinct from Euclid's approach, and Dirichlet, who upgraded this idea to prove his theorem on the distribution of primes across arithmetic progressions. It was Riemann who introduced the idea of viewing these series as functions of a *complex* parameter, thus making it possible to use the tools of complex analysis (e.g., the residue theorem) and leading to the original proof of the prime number theorem by Hadamard and de la Vallée Poussin.

In the language of complex analysis, one may handle the convergence issues in the second solution in a different way: use the preceding calculation to establish the equality

$$L(s) = 1 + \zeta(s)(-1+2^{2-s}-2^{2-2s})$$

for $\mathrm{Real}(s) > 1$, then observe that both sides are holomorphic for $\mathrm{Real}(s) > 0$ and so the equality extends to that larger domain.

B5 The desired integers are $(a,b,c) = (9,8,7)$.

Suppose we have a triangle $T = \triangle ABC$ with $BC = a$, $CA = b$, $AB = c$ and $a > b > c$. Say that a line is an *area equalizer* if it divides $T$ into two regions of equal area. A line intersecting $T$ must intersect two of the three sides of $T$. First consider a line intersecting the segments $AB$ at $X$ and $BC$ at $Y$, and let $BX = x$, $BY = y$. This line is an area equalizer if and only if $xy\sin B = 2\,\mathrm{area}(\triangle XBY) = \mathrm{area}(\triangle ABC) = \frac{1}{2}ac\sin B$, that is, $2xy = ac$. Since $x \leq c$ and $y \leq a$, the area equalizers correspond to values of $x,y$ with $xy = ac/2$ and $x \in [c/2,c]$. Such an area equalizer is also an equalizer if and only if $p/2 = x+y$, where $p = a+b+c$ is the perimeter of $T$. If we write $f(x) = x + ac/(2x)$, then we want to solve $f(x) = p/2$ for $x \in [c/2,c]$. Now note that $f$ is convex, $f(c/2) = a + c/2 > p/2$, and $f(c) = a/2 + c < p/2$; it follows that there is exactly one solution to $f(x) = p/2$ in $[c/2,c]$. Similarly, for equalizers intersecting $T$ on the sides $AB$ and $AC$, we want to solve $g(x) = p/2$ where $g(x) = x + bc/(2x)$ and $x \in [c/2,c]$; since $g$ is convex and $g(c/2) < p/2$, $g(c) < p/2$, there are no such solutions.

It follows that if $T$ has exactly two equalizers, then it must have exactly one equalizer intersecting $T$ on the sides $AC$ and $BC$. Here we want to solve $h(x) = p/2$ where $h(x) = x + ab/(2x)$ and $x \in [a/2,a]$. Now $h$ is convex and $h(a/2) > p/2$, $h(a) > p/2$; thus $h(x) = p/2$ has exactly one solution $x \in [a/2,a]$ if and only if there is $x_0 \in [a/2,a]$ with $h'(x_0) = 0$ and $h(x_0) = p/2$. The first condition implies $x_0 = \sqrt{ab/2}$, and then the second condition gives $8ab = p^2$. Note that $\sqrt{ab/2}$ is in $[a/2,a]$ since $a > b$ and $a < b+c < 2b$.

We conclude that $T$ has two equalizers if and only if $8ab = (a+b+c)^2$. Note that $(a,b,c) = (9,8,7)$ works. We claim that this is the only possibility when $a > b > c$ are integers and $a \leq 9$. Indeed, the only integers $(a,b)$ such that $2 \leq b < a \leq 9$ and $8ab$ is a perfect square are $(a,b) = (4,2)$, $(6,3)$, $(8,4)$, $(9,2)$, and $(9,8)$, and the first four possibilities do not produce triangles since they do not satisfy $a < 2b$. This gives the claimed result.

B6 **First solution.** The desired count is $\frac{2016!}{1953!} - 63! \cdot 2016$, which we compute using the principle of inclusion-exclusion. As in A2, we use the fact that 2017 is prime; this means that we can do linear algebra over the field $\mathbb{F}_{2017}$. In particular, every nonzero homogeneous linear equation in $n$ variables over $\mathbb{F}_{2017}$ has exactly $2017^{n-1}$ solutions.

For $\pi$ a partition of $\{0,\dots,63\}$, let $|\pi|$ denote the number of distinct parts of $\pi$, Let $\pi_0$ denote the partition of $\{0,\dots,63\}$ into 64 singleton parts. Let $\pi_1$ denote the partition of $\{0,\dots,63\}$ into one 64-element part. For $\pi,\sigma$ two partitions of $\{0,\dots,63\}$, write $\pi|\sigma$ if $\pi$ is a refinement of $\sigma$ (that is, every part in $\sigma$ is a union of parts in $\pi$). By induction on $|\pi|$, we may construct a collection of integers $\mu_\pi$, one for each $\pi$, with the properties that

$$\sum_{\pi|\sigma} \mu_\pi = \begin{cases} 1 & \sigma = \pi_0 \\ 0 & \sigma \neq \pi_0 \end{cases}.$$

Define the sequence $c_0,\dots,c_{63}$ by setting $c_0 = 1$ and $c_i = i$ for $i > 1$. Let $N_\pi$ be the number of ordered 64-tuples $(x_0,\dots,x_{63})$ of elements of $\mathbb{F}_{2017}$ such that $x_i = x_j$ whenever $i$ and $j$ belong to the same part and $\sum_{i=0}^{63} c_i x_i$ is divisible by 2017. Then $N_\pi$ equals $2017^{|\pi|-1}$ unless for each part $S$ of $\pi$, the sum $\sum_{i\in S} c_i$ vanishes; in that case, $N_\pi$ instead equals $2017^{|\pi|}$. Since $c_0,\dots,c_{63}$ are positive integers which sum to $1 + \frac{63\cdot 64}{2} = 2017$, the second outcome only occurs for $\pi = \pi_1$. By inclusion-exclusion, the desired count may be written as

$$\sum_\pi \mu_\pi N_\pi = 2016 \cdot \mu_{\pi_1} + \sum_\pi \mu_\pi 2017^{|\pi|-1}.$$

Similarly, the number of ordered 64-tuples with no repeated elements may be written as

$$64!\binom{2017}{64} = \sum_{\pi} \mu_\pi 2017^{|\pi|}.$$

The desired quantity may thus be written as $\frac{2016!}{1953!} + 2016\mu_{\pi_1}$.

It remains to compute $\mu_{\pi_1}$. We adopt an approach suggested by David Savitt: apply inclusion-exclusion to count distinct 64-tuples in an *arbitrary* set $A$. As above, this yields

$$|A|(|A|-1)\cdots(|A|-63) = \sum_{\pi} \mu_\pi |A|^{|\pi|}.$$

Viewing both sides as polynomials in $|A|$ and comparing coefficients in degree 1 yields $\mu_\pi = -63!$ and thus the claimed answer.

**Second solution.** (from Art of Problem Solving, user `ABCDE`) We first prove an auxiliary result.

**Lemma.** *Fix a prime $p$ and define the function $f(k)$ on positive integers by the conditions*

$$f(1,p) = 0$$
$$f(k,p) = \frac{(p-1)!}{(p-k)!} - kf(k-1,p) \qquad (k>1).$$

*Then for any positive integers $a_1,\dots,a_k$ with $a_1+\cdots+a_k < p$, there are exactly $f(p)$ solutions to the equation $a_1x_1+\cdots+a_kx_k = 0$ with $x_1,\dots,x_k \in \mathbb{F}_p$ nonzero and pairwise distinct.*

*Proof.* We check the claim by induction, with the base case $k=1$ being obvious. For the induction step, assume the claim for $k-1$. Let $S$ be the set of $k$-tuples of distinct elements of $\mathbb{F}_p$; it consists of $\frac{p!}{(p-k)!}$ elements. This set is stable under the action of $i \in \mathbb{F}_p$ by translation:

$$(x_1,\dots,x_k) \mapsto (x_1+i,\dots,x_k+i).$$

Since $0 < a_1\cdots+a_k < p$, exactly one element of each orbit gives a solution of $a_1x_1+\cdots+a_kx_k = 0$. Each of these solutions contributes to $f(k)$ except for those in which $x_i = 0$ for some $i$. Since then $x_j \neq 0$ for all $j \neq i$, we may apply the induction hypothesis to see that there are $f(k-1,p)$ solutions that arise this way for a given $i$ (and these do not overlap). This proves the claim. $\square$

To compute $f(k,p)$ explicitly, it is convenient to work with the auxiliary function

$$g(k,p) = \frac{pf(k,p)}{k!};$$

by the lemma, this satisfies $g(1,p) = 0$ and

$$\begin{aligned} g(k,p) &= \binom{p}{k} - g(k-1,p) \\ &= \binom{p-1}{k} + \binom{p-1}{k-1} - g(k-1,p) \qquad (k>1). \end{aligned}$$

By induction on $k$, we deduce that

$$\begin{aligned} g(k,p) - \binom{p-1}{k} &= (-1)^{k-1}\left(g(1,p) - \binom{p-1}{1}\right) \\ &= (-1)^k(p-1) \end{aligned}$$

and hence $g(k,p) = \binom{p-1}{k} + (-1)^k(p-1)$.

We now set $p = 2017$ and count the tuples in question. Define $c_0,\dots,c_{63}$ as in the first solution. Since $c_0+\cdots+c_{63} = p$, the translation action of $\mathbb{F}_p$ preserves the set of tuples; we may thus assume without loss of generality that $x_0 = 0$ and multiply the count by $p$ at the end. That is, the desired answer is

$$\begin{aligned} 2017f(63,2017) &= 63!g(63,2017) \\ &= 63!\left(\binom{2016}{63} - 2016\right) \end{aligned}$$

as claimed.

# The 79th William Lowell Putnam Mathematical Competition
# Saturday, December 1, 2018

A1 Find all ordered pairs $(a,b)$ of positive integers for which

$$\frac{1}{a}+\frac{1}{b}=\frac{3}{2018}.$$

A2 Let $S_1,S_2,\dots,S_{2^n-1}$ be the nonempty subsets of $\{1,2,\dots,n\}$ in some order, and let $M$ be the $(2^n-1)\times(2^n-1)$ matrix whose $(i,j)$ entry is

$$m_{ij}=\begin{cases}0 & \text{if } S_i\cap S_j=\emptyset;\\ 1 & \text{otherwise.}\end{cases}$$

Calculate the determinant of $M$.

A3 Determine the greatest possible value of $\sum_{i=1}^{10}\cos(3x_i)$ for real numbers $x_1,x_2,\dots,x_{10}$ satisfying $\sum_{i=1}^{10}\cos(x_i)=0$.

A4 Let $m$ and $n$ be positive integers with $\gcd(m,n)=1$, and let

$$a_k=\left\lfloor\frac{mk}{n}\right\rfloor-\left\lfloor\frac{m(k-1)}{n}\right\rfloor$$

for $k=1,2,\dots,n$. Suppose that $g$ and $h$ are elements in a group $G$ and that

$$gh^{a_1}gh^{a_2}\cdots gh^{a_n}=e,$$

where $e$ is the identity element. Show that $gh=hg$. (As usual, $\lfloor x\rfloor$ denotes the greatest integer less than or equal to $x$.)

A5 Let $f:\mathbb{R}\to\mathbb{R}$ be an infinitely differentiable function satisfying $f(0)=0$, $f(1)=1$, and $f(x)\geq 0$ for all $x\in\mathbb{R}$. Show that there exist a positive integer $n$ and a real number $x$ such that $f^{(n)}(x)<0$.

A6 Suppose that $A,B,C$, and $D$ are distinct points, no three of which lie on a line, in the Euclidean plane. Show that if the squares of the lengths of the line segments $AB$, $AC$, $AD$, $BC$, $BD$, and $CD$ are rational numbers, then the quotient

$$\frac{\text{area}(\triangle ABC)}{\text{area}(\triangle ABD)}$$

is a rational number.

B1 Let $\mathscr{P}$ be the set of vectors defined by

$$\mathscr{P}=\left\{\begin{pmatrix}a\\b\end{pmatrix}\middle|\,0\leq a\leq 2, 0\leq b\leq 100, \text{ and } a,b\in\mathbb{Z}\right\}.$$

Find all $\mathbf{v}\in\mathscr{P}$ such that the set $\mathscr{P}\setminus\{\mathbf{v}\}$ obtained by omitting vector $\mathbf{v}$ from $\mathscr{P}$ can be partitioned into two sets of equal size and equal sum.

B2 Let $n$ be a positive integer, and let $f_n(z)=n+(n-1)z+(n-2)z^2+\cdots+z^{n-1}$. Prove that $f_n$ has no roots in the closed unit disk $\{z\in\mathbb{C}\colon |z|\leq 1\}$.

B3 Find all positive integers $n<10^{100}$ for which simultaneously $n$ divides $2^n$, $n-1$ divides $2^n-1$, and $n-2$ divides $2^n-2$.

B4 Given a real number $a$, we define a sequence by $x_0=1$, $x_1=x_2=a$, and $x_{n+1}=2x_nx_{n-1}-x_{n-2}$ for $n\geq 2$. Prove that if $x_n=0$ for some $n$, then the sequence is periodic.

B5 Let $f=(f_1,f_2)$ be a function from $\mathbb{R}^2$ to $\mathbb{R}^2$ with continuous partial derivatives $\frac{\partial f_i}{\partial x_j}$ that are positive everywhere. Suppose that

$$\frac{\partial f_1}{\partial x_1}\frac{\partial f_2}{\partial x_2}-\frac{1}{4}\left(\frac{\partial f_1}{\partial x_2}+\frac{\partial f_2}{\partial x_1}\right)^2>0$$

everywhere. Prove that $f$ is one-to-one.

B6 Let $S$ be the set of sequences of length 2018 whose terms are in the set $\{1,2,3,4,5,6,10\}$ and sum to 3860. Prove that the cardinality of $S$ is at most

$$2^{3860}\cdot\left(\frac{2018}{2048}\right)^{2018}.$$

# Solutions to the 79th William Lowell Putnam Mathematical Competition
# Saturday, December 1, 2018

Kiran Kedlaya and Lenny Ng

While preparing these solutions, we learned of the November 27 death of Kent Merryfield, who moderated the Putnam discussions on the Art of Problem Solving Forums and thereby contributed directly and indirectly to these solutions over many years. His presence will be dearly missed.

A1 By clearing denominators and regrouping, we see that the given equation is equivalent to

$$(3a-2018)(3b-2018) = 2018^2.$$

Each of the factors is congruent to 1 (mod 3). There are 6 positive factors of $2018^2 = 2^2 \cdot 1009^2$ that are congruent to 1 (mod 3): 1, $2^2$, 1009, $2^2 \cdot 1009$, $1009^2$, $2^2 \cdot 1009^2$. These lead to the 6 possible pairs: $(a,b) = (673, 1358114)$, $(674, 340033)$, $(1009, 2018)$, $(2018, 1009)$, $(340033, 674)$, and $(1358114, 673)$.

As for negative factors, the ones that are congruent to 1 (mod 3) are $-2, -2\cdot 1009, -2\cdot 1009^2$. However, all of these lead to pairs where $a \leq 0$ or $b \leq 0$.

A2 The answer is 1 if $n=1$ and $-1$ if $n>1$. Write $M_n$ for a $(2^n-1)\times(2^n-1)$ matrix of the given form, and note that $\det M_n$ does not depend on the ordering of the subsets: transposing two subsets has the effect of transposing two rows and then transposing two columns in $M_n$, and this does not change the determinant.

Clearly $\det M_1 = 1$. We claim that for $n>1$, $\det M_n = -(\det M_{n-1})^2$, and the desired answer will follow by induction. Let $S'_1, \dots, S'_{2^{n-1}-1}$ denote the nonempty subsets of $\{1,\dots,n-1\}$ in any order, with resulting matrix $M_{n-1}$. Let $m'_{ij}$ denote the $(i,j)$ entry of $M_{n-1}$. Now order the nonempty subsets $S_1,\dots,S_{2^n-1}$ of $\{1,\dots,n\}$ as follows:

$$S_i = \begin{cases} S'_i & i \leq 2^{n-1}-1 \\ S'_{i-2^{n-1}+1} \cup \{n\} & 2^{n-1} \leq i \leq 2^n-2 \\ \{n\} & i = 2^n-1. \end{cases}$$

(For example, if $S'_1,\dots,S'_{2^{n-1}-1}$ are ordered in lexicographic order as binary strings, then so are $S_1,\dots,S_{2^n-1}$.) Let $M_n$ be the resulting matrix. Then we have:

$$M_n = \left(\begin{array}{c|ccc|c} & & & & 0 \\ M_{n-1} & & M_{n-1} & & \vdots \\ & & & & 0 \\ \hline & 1 & \cdots & 1 & 1 \\ M_{n-1} & \vdots & \ddots & \vdots & \vdots \\ & 1 & \cdots & 1 & 1 \\ \hline 0 \ \cdots \ 0 & 1 & \cdots & 1 & 1 \end{array}\right).$$

In $M_n$, perform the following operations, which do not change the determinant: subtract the final row from rows $2^{n-1}$ through $2^n-2$, and then subtract the final column from columns $2^{n-1}$ through $2^n-2$. The result is the matrix

$$\left(\begin{array}{c|ccc|c} & & & & 0 \\ M_{n-1} & & M_{n-1} & & \vdots \\ & & & & 0 \\ \hline & 0 & \cdots & 0 & 0 \\ M_{n-1} & \vdots & \ddots & \vdots & \vdots \\ & 0 & \cdots & 0 & 0 \\ \hline 0 \ \cdots \ 0 & 0 & \cdots & 0 & 1 \end{array}\right).$$

We can remove the final row and column without changing the determinant. Now swap the first $2^{n-1}-1$ rows with the final $2^{n-1}-1$ rows: this changes the determinant by an overall factor of $(-1)^{(2^{n-1}-1)^2} = -1$. The result is the block-diagonal matrix $\begin{pmatrix} M_{n-1} & 0 \\ M_{n-1} & M_{n-1} \end{pmatrix}$, whose determinant is $(\det M_{n-1})^2$. Thus $\det M_n = -(\det M_{n-1})^2$ as desired.

A3 The maximum value is $480/49$. Since $\cos(3x_i) = 4\cos(x_i)^3 - 3\cos(x_i)$, it is equivalent to maximize $4\sum_{i=1}^{10} y_i^3$ for $y_1,\dots,y_{10} \in [-1,1]$ with $\sum_{i=1}^{10} y_i = 0$; note that this domain is compact, so the maximum value is guaranteed to exist. For convenience, we establish something slightly stronger: we maximize $4\sum_{i=1}^n y_i^3$ for $y_1,\dots,y_n \in [-1,1]$ with $\sum_{i=1}^n y_i = 0$, where $n$ may be any even nonnegative integer up to 10, and show that the maximum is achieved when $n=10$.

We first study the effect of varying $y_i$ and $y_j$ while fixing their sum. If that sum is $s$, then the function $y \mapsto y^3 + (s-y)^3$ has constant second derivative $6s$, so it is either everywhere convex or everywhere concave. Consequently, if $(y_1,\dots,y_n)$ achieves the maximum, then for any two indices $i<j$, at least one of the following must be true:

- one of $y_i, y_j$ is extremal (i.e., equal to 1 or $-1$);
- $y_i = y_j < 0$ (in which case $s<0$ and the local maximum is achieved above);
- $y_i = -y_j$ (in which case $s=0$ above).

In the third case, we may discard $y_i$ and $y_j$ and achieve a case with smaller $n$; we may thus assume that this does not occur. In this case, all of the non-extremal values are equal to some common value $y<0$, and moreover we cannot have both 1 and -1. We cannot omit 1, as otherwise the condition $\sum_{i=1}^n y_i = 0$ cannot be achieved; we must thus have only the terms 1 and $y$, occurring with some positive multiplicities $a$ and $b$ adding up to $n$. Since $a+b=n$ and $a+by=0$, we can solve for $y$ to obtain $y=-a/b$; we then have

$$4\sum_{i=1}^n y_i^3 = a+by^3 = 4a\left(1-\frac{a^2}{b^2}\right).$$

Since $y>-1$, we must have $a<b$. For fixed $a$, the target function increases as $b$ increases, so the optimal case must occur when $a+b=10$. The possible pairs $(a,b)$ at this point are

$$(1,9),(2,8),(3,7),(4,6);$$

computing the target function for these values yields respectively

$$\frac{32}{9},\frac{15}{2},\frac{480}{49},\frac{80}{9},$$

yielding $480/49$ as the maximum value.

**Remark.** Using Lagrange multipliers yields a similar derivation, but with a slight detour required to separate local minima and maxima. For general $n$, the above argument shows that the target function is maximized when $a+b=n$.

A4 **First solution.** We prove the claim by induction on $m+n$. For the base case, suppose that $n=1$; we then have $m=1$ and the given equation becomes $gh=e$. The claim then reduces to the fact that a one-sided inverse in $G$ is also a two-sided inverse. (Because $G$ is a group, $g$ has an inverse $g^{-1}$; since $gh=e$, we have $h=g^{-1}(gh)=g^{-1}e=g^{-1}$, so $hg=e=gh$.)

Suppose now that $n>1$. In case $m>n$, set $\tilde{g}=gh$, $\tilde{h}=h$, and

$$b_k = \left\lfloor \frac{(m-n)k}{n} \right\rfloor - \left\lfloor \frac{(m-n)(k-1)}{n} \right\rfloor \qquad (k=1,\dots,n).$$

then

$$\tilde{g}\tilde{h}^{b_1}\cdots\tilde{g}\tilde{h}^{b_n} = gh^{a_1}\cdots gh^{a_n} = e,$$

so the induction hypothesis implies that $\tilde{g}$ and $\tilde{h}$ commute; this implies that $g$ and $h$ commute.

In case $m<n$, note that $a_k\in\{0,1\}$ for all $k$. Set $\tilde{g}=h^{-1}$, $\tilde{h}=g^{-1}$, and

$$b_l = \left\lfloor \frac{n\ell}{m} \right\rfloor - \left\lfloor \frac{n(\ell-1)}{m} \right\rfloor \qquad (\ell=1,\dots,m);$$

we claim that

$$\tilde{g}\tilde{h}^{b_1}\cdots\tilde{g}\tilde{h}^{b_m} = (gh^{a_1}\cdots gh^{a_n})^{-1} = e,$$

so the induction hypothesis implies that $\tilde{h}$ and $\tilde{g}$ commute; this implies that $g$ and $h$ commute.

To clarify this last equality, consider a lattice walk starting from $(0,0)$, ending at $(n,m)$, staying below the line $y=mx/n$, and keeping as close to this line as possible. If one follows this walk and records the element $g$ for each horizontal step and $h$ for each vertical step, one obtains the word $gh^{a_1}\cdots gh^{a_n}$. Now take this walk, reflect across the line $y=x$, rotate by a half-turn, then translate to put the endpoints at $(0,0)$ and $(m,n)$; this is the analogous walk for the pair $(n,m)$.

**Remark.** By tracing more carefully through the argument, one sees in addition that there exists an element $k$ of $G$ for which $g=k^m, h=k^{-n}$.

**Second solution.** (by Greg Martin) Since $\gcd(m,n)=1$, there exist integers $x,y$ such that $mx+ny=1$; we may further assume that $x\in\{1,\dots,n\}$. We first establish the identity

$$a_{k-x} = \begin{cases} a_k-1 & \text{if } k\equiv 0 \pmod{n} \\ a_k+1 & \text{if } k\equiv 1 \pmod{n} \\ a_k & \text{otherwise.}\end{cases}$$

Namely, by writing $-mx=ny-1$, we see that

$$\begin{aligned} a_{k-x} &= \left\lfloor \frac{m(k-x)}{n} \right\rfloor - \left\lfloor \frac{m(k-x-1)}{n} \right\rfloor \\ &= \left\lfloor \frac{mk+ny-1}{n} \right\rfloor - \left\lfloor \frac{m(k-1)+ny-1}{n} \right\rfloor \\ &= \left\lfloor \frac{mk-1}{n} \right\rfloor - \left\lfloor \frac{m(k-1)-1}{n} \right\rfloor \end{aligned}$$

and so

$$\begin{aligned} a_{k-x}-a_k &= \left(\left\lfloor \frac{mk-1}{n} \right\rfloor - \left\lfloor \frac{mk}{n} \right\rfloor\right) \\ &\quad - \left(\left\lfloor \frac{m(k-1)-1}{n} \right\rfloor - \left\lfloor \frac{m(k-1)}{n} \right\rfloor\right). \end{aligned}$$

The first parenthesized expression equals 1 if $n$ divides $mk$, or equivalently $n$ divides $k$, and 0 otherwise. Similarly, the second parenthesized expression equals 1 if $n$ divides $k-1$ and 0 otherwise. This proves the stated identity.

We now use the given relation $gh^{a_1}\cdots gh^{a_n}=e$ to write

$$\begin{aligned} ghg^{-1}h^{-1} &= gh(h^{a_1}gh^{a_2}\cdots gh^{a_{n-1}}gh^{a_n})h^{-1} \\ &= gh^{a_1+1}gh^{a_2}\cdots gh^{a_{n-1}}gh^{a_n-1} \\ &= gh^{a_{1-x}}\cdots gh^{a_{n-x}} \\ &= (gh^{a_{n+1-x}}\cdots gh^{a_n})(gh^{a_1}\cdots gh^{a_{n-x}}). \end{aligned}$$

The two parenthesized expressions multiply in the opposite order to $gh^{a_1}\cdots gh^{a_n}=e$, so they must be (two-sided) inverses of each other. We deduce that $ghg^{-1}h^{-1}=e$, meaning that $g$ and $h$ commute.

**Third solution.** (by Sucharit Sarkar) Let $T$ denote the torus $\mathbb{R}^2/\mathbb{Z}^2$. The line segments from $(0,0)$ to $(1,0)$

and from $(0,0)$ to $(0,1)$ are closed loops in $T$, and we denote them by $g$ and $h$ respectively. Now let $p$ be the (image of the) point $(\varepsilon,-\varepsilon)$ in $T$ for some $0<\varepsilon \ll 1$. The punctured torus $T\setminus\{p\}$ deformation retracts onto the union of the loops $g$ and $h$, and so $\pi_1(T\setminus\{p\})$, the fundamental group of $T\setminus\{p\}$ based at $(0,0)$, is the free group on two generators, $\langle g,h\rangle$.

Let $\gamma$ and $\tilde\gamma$ denote the following loops based at $(0,0)$ in $T$: $\gamma$ is the image of the line segment from $(0,0)$ to $(n,m)$ under the projection $\mathbb{R}^2\to T$, and $\tilde\gamma$ is the image of the lattice walk from $(0,0)$ to $(n,m)$, staying just below the line $y=mx/n$, that was described in the first solution. There is a straight-line homotopy with fixed endpoints between the two paths in $\mathbb{R}^2$ from $(0,0)$ to $(n,m)$, the line segment and the lattice walk, and this homotopy does not pass through any point of the form $(a+\varepsilon,b-\varepsilon)$ for $a,b\in\mathbb{Z}$ by the construction of the lattice walk. It follows that $\gamma$ and $\tilde\gamma$ are homotopic loops in $T\setminus\{p\}$. Since the class of $\tilde\gamma$ in $\pi_1(T\setminus\{p\})$ is evidently $gh^{a_1}gh^{a_2}\cdots gh^{a_n}$, it follows that the class of $\gamma$ in $\pi_1(T\setminus\{p\})$ is the same.

Now since $\gcd(m,n)=1$, there is an element $\phi\in GL_2(\mathbb{Z})$ sending $(n,m)$ to $(1,0)$, which then sends the line segment from $(0,0)$ to $(n,m)$ to the segment from $(0,0)$ to $(1,0)$. Then $\phi$ induces a homeomorphism of $T$ sending $\gamma$ to $g$, which in turn induces an isomorphism $\phi_*:\pi_1(T\setminus\{p\})\to\pi_1(T\setminus\{\phi^{-1}(p)\})$. Both fundamental groups are equal to $\langle g,h\rangle$, and we conclude that $\phi_*$ sends $gh^{a_1}gh^{a_2}\cdots gh^{a_n}$ to $g$. It follows that $\phi_*$ induces an isomorphism

$$\langle g,h\,|\,gh^{a_1}gh^{a_2}\cdots gh^{a_n}\rangle \to \langle g,h\,|\,g\rangle \cong \langle h\rangle \cong \mathbb{Z}.$$

Since $\mathbb{Z}$ is abelian, $g$ and $h$ must commute in $\langle g,h\,|\,gh^{a_1}gh^{a_2}\cdots gh^{a_n}\rangle$, whence they must also commute in $G$.

A5 **First solution.** Call a function $f\colon\mathbb{R}\to\mathbb{R}$ *ultraconvex* if $f$ is infinitely differentiable and $f^{(n)}(x)\geq 0$ for all $n\geq 0$ and all $x\in\mathbb{R}$, where $f^{(0)}(x)=f(x)$; note that if $f$ is ultraconvex, then so is $f'$. Define the set

$$S=\{f:\mathbb{R}\to\mathbb{R}\,|\,f \text{ ultraconvex and } f(0)=0\}.$$

For $f\in S$, we must have $f(x)=0$ for all $x<0$: if $f(x_0)>0$ for some $x_0<0$, then by the mean value theorem there exists $x\in(0,x_0)$ for which $f'(x)=\frac{f(x_0)}{x_0}<0$. In particular, $f'(0)=0$, so $f'\in S$ also.

We show by induction that for all $n\geq 0$,

$$f(x)\leq \frac{f^{(n)}(1)}{n!}x^n \qquad (f\in S, x\in[0,1]).$$

We induct with base case $n=0$, which holds because any $f\in S$ is nondecreasing. Given the claim for $n=m$, we apply the induction hypothesis to $f'\in S$ to see that

$$f'(t)\leq \frac{f^{(n+1)}(1)}{n!}t^n \qquad (t\in[0,1]),$$

then integrate both sides from 0 to $x$ to conclude.

Now for $f\in S$, we have $0\leq f(1)\leq \frac{f^{(n)}(1)}{n!}$ for all $n\geq 0$. On the other hand, by Taylor's theorem with remainder,

$$f(x)\geq \sum_{k=0}^{n}\frac{f^{(k)}(1)}{k!}(x-1)^k \qquad (x\geq 1).$$

Applying this with $x=2$, we obtain $f(2)\geq \sum_{k=0}^n \frac{f^{(k)}(1)}{k!}$ for all $n$; this implies that $\lim_{n\to\infty}\frac{f^{(n)}(1)}{n!}=0$. Since $f(1)\leq \frac{f^{(n)}(1)}{n!}$, we must have $f(1)=0$.

For $f\in S$, we proved earlier that $f(x)=0$ for all $x\leq 0$, as well as for $x=1$. Since the function $g(x)=f(cx)$ is also ultraconvex for $c>0$, we also have $f(x)=0$ for all $x>0$; hence $f$ is identically zero.

To sum up, if $f\colon\mathbb{R}\to\mathbb{R}$ is infinitely differentiable, $f(0)=0$, and $f(1)=1$, then $f$ cannot be ultraconvex. This implies the desired result.

**Variant.** (by Yakov Berchenko-Kogan) Another way to show that any $f\in S$ is identically zero is to show that for $f\in S$ and $k$ a positive integer,

$$f(x)\leq \frac{x}{k}f'(x) \qquad (x\geq 0).$$

We prove this by induction on $k$. For the base case $k=1$, note that $f''(x)\geq 0$ implies that $f'$ is nondecreasing. For $x\geq 0$, we thus have

$$f(x)=\int_0^x f'(t)\,dt\leq \int_0^x f'(x)\,dt = xf'(x).$$

To pass from $k$ to $k+1$, apply the induction hypothesis to $f'$ and integrate by parts to obtain

$$\begin{aligned} kf(x) &= \int_0^x kf'(t)\,dt \\ &\leq \int_0^x tf''(t)\,dt \\ &= xf'(x)-\int_0^x f'(t)\,dt = xf'(x)-f(x). \end{aligned}$$

**Remark.** Noam Elkies points out that one can refine the argument to show that if $f$ is ultraconvex, then it is analytic (i.e., it is represented by an entire Taylor series about any point, as opposed to a function like $f(x)=e^{-1/x^2}$ whose Taylor series at 0 is identically zero); he attributes the following argument to Peter Shalen. Let $g_n(x)=\sum_{k=0}^n \frac{1}{k!}f^{(k)}(0)x^k$ be the $n$-th order Taylor polynomial of $f$. By Taylor's theorem with remainder (a/k/a Lagrange's theorem), $f(x)-g_n(x)$ is everywhere nonnegative; consequently, for all $x\geq 0$, the Taylor series $\sum_{n=0}^\infty \frac{1}{n!}f^{(n)}(0)x^n$ converges and is bounded above by $f$. But since $f^{(n+1)}(x)$ is nondecreasing, Lagrange's theorem also implies that $f(x)-g_n(x)\leq \frac{1}{(n+1)!}f^{(n+1)}(x)$; for fixed $x\geq 0$, the right side tends to 0 as $n\to\infty$. Hence $f$ is represented by its Taylor series for $x\geq 0$, and so is analytic for $x > 0$; by replacing $f(x)$ with $f(x-c)$, we may conclude that $f$ is everywhere analytic.

**Remark.** We record some properties of the class of ultraconvex functions.

- Any nonnegative constant function is ultraconvex. The exponential function is ultraconvex.
- If $f$ is ultraconvex, then $f'$ is ultraconvex. Conversely, if $f'$ is ultraconvex and $\liminf_{x\to-\infty} f(x) \geq 0$, then $f$ is ultraconvex.
- The class of ultraconvex functions is closed under addition, multiplication, and composition.

**Second solution.** (by Zachary Chase) In this solution, we use *Bernstein's theorem on monotone functions*. To state this result, we say that a function $f:[0,\infty)\to\mathbb{R}$ is *totally monotone* if $f$ is continuous, $f$ is infinitely differentiable on $(0,\infty)$, and $(-1)^n f^{(n)}(x)$ is nonnegative for all positive integers $n$ and all $x > 0$. For such a function, Bernstein's theorem asserts that there is a nonnegative finite Borel measure $\mu$ on $[0,\infty)$ such that

$$f(x) = \int_0^\infty e^{-tx} d\mu(t) \qquad (x \geq 0).$$

For $f$ as in the problem statement, for any $M > 0$, the restriction of $f(M-x)$ to $[0,\infty)$ is totally monotone, so Bernstein's theorem provides a Borel measure $\mu$ for which $f(M-x) = \int_0^\infty e^{-tx} d\mu(t)$ for all $x \geq 0$. Taking $x = M$, we see that $\int_0^\infty e^{-Mt} d\mu(t) = f(0) = 0$; since $\mu$ is a nonnegative measure, it must be identically zero. Hence $f(x)$ is identically zero for $x \leq M$; varying over all $M$, we deduce the desired result.

**Third solution.** (from Art of Problem Solving user `chronondecay`) In this solution, we only consider the behavior of $f$ on $[0,1]$. We first establish the following result. Let $f:(0,1)\to\mathbb{R}$ be a function such that for each positive integer $n$, $f^{(n)}(x)$ is nonnegative on $(0,1)$, tends to 0 as $x\to 0^+$, and tends to some limit as $x\to 1^-$. Then for each nonnegative integer $n$, $f(x)x^{-n}$ is nondecreasing on $(0,1)$.

To prove the claimed result, we proceed by induction on $n$, the case $n=0$ being a consequence of the assumption that $f'(x)$ is nonnegative on $(0,1)$. Given the claim for some $n \geq 0$, note that since $f'$ also satisfies the hypotheses of the problem, $f'(x)x^{-n}$ is also nondecreasing on $(0,1)$. Choose $c \in (0,1)$ and consider the function

$$g(x) = \frac{f'(c)}{c^n} x^n \qquad (x \in [0,1)).$$

For $x \in (0,c)$, $f'(x)x^{-n} \leq f'(c)c^{-n}$, so $f'(x) \leq g(x)$; similarly, for $x \in (c,1)$, $f'(x) \geq g(x)$. It follows that if $f'(c) > 0$, then

$$\frac{\int_c^1 f'(x)\,dx}{\int_0^c f'(x)\,dx} \geq \frac{\int_c^1 g(x)\,dx}{\int_0^c g(x)\,dx} \Rightarrow \frac{\int_0^c f'(x)\,dx}{\int_0^1 f'(x)\,dx} \leq \frac{\int_0^c g(x)\,dx}{\int_0^1 g(x)\,dx}$$

and so $f(c)/f(1) \leq c^{n+1}$. (Here for convenience, we extend $f$ continuously to $[0,1]$.) That is, $f(c)/c^{n+1} \leq f(1)$ for all $c \in (0,1)$. For any $b \in (0,1)$, we may apply the same logic to the function $f(bx)$ to deduce that if $f'(c) > 0$, then $f(bc)/c^{n+1} \leq f(b)$, or equivalently

$$\frac{f(bc)}{(bc)^{n+1}} \leq \frac{f(b)}{b^{n+1}}.$$

This yields the claim unless $f'$ is identically 0 on $(0,1)$, but in that case the claim is obvious anyway.

We now apply the claim to show that for $f$ as in the problem statement, it cannot be the case that $f^{(n)}(x)$ is nonnegative on $(0,1)$ for all $n$. Suppose the contrary; then for any fixed $x \in (0,1)$, we may apply the previous claim with arbitrarily large $n$ to deduce that $f(x) = 0$. By continuity, we also then have $f(1) = 0$, a contradiction.

**Fourth solution.** (by Alexander Karabegov) As in the first solution, we may see that $f^{(n)}(0) = 0$ for all $n$. Consequently, for all $n$ we have

$$f(x) = \frac{1}{(n-1)!}\int_0^x (x-t)^{n-1} f^{(n)}(t)\,dt \qquad (x \in \mathbb{R})$$

and hence

$$\int_0^1 f(x)\,dx = \frac{1}{n!}\int_0^1 (1-t)^n f^{(n)}(t)\,dt.$$

Suppose now that $f$ is infinitely differentiable, $f(1) = 1$, and $f^{(n)}(x) \geq 0$ for all $n$ and all $x \in [0,1]$. Then

$$\begin{aligned}
\int_0^1 f(x)\,dx &= \frac{1}{n}\cdot\frac{1}{(n-1)!}\int_0^1 (1-t)^n f^{(n)}(t)\,dt \\
&\leq \frac{1}{n}\cdot\frac{1}{(n-1)!}\int_0^1 (1-t)^{n-1} f^{(n)}(t)\,dt \\
&= \frac{1}{n} f(1) = \frac{1}{n}.
\end{aligned}$$

Since this holds for all $n$, we have $\int_0^1 f(x)\,dx = 0$, and so $f(x) = 0$ for $x \in [0,1]$; this yields the desired contradiction.

A6 **First solution.** Choose a Cartesian coordinate system with origin at the midpoint of $AB$ and positive $x$-axis containing $A$. By the condition on $AB$, we have $A = (\sqrt{a}, 0)$, $B = (-\sqrt{a}, 0)$ for some positive rational number $a$. Let $(x_1, y_1)$ and $(x_2, y_2)$ be the respective coordinates of $C$ and $D$; by computing the lengths of the segments $AC, BC, AD, BD, CD$, we see that the quantities

$$\begin{gathered}
(x_1 - \sqrt{a})^2 + y_1^2, \quad (x_1 + \sqrt{a})^2 + y_1^2, \\
(x_2 - \sqrt{a})^2 + y_2^2, \quad (x_2 + \sqrt{a})^2 + y_2^2, \\
(x_1 - x_2)^2 + (y_1 - y_2)^2
\end{gathered}$$

are all rational numbers. By adding and subtracting the first two quantities, and similarly for the next two, we see that the quantities

$$x_1^2+y_1^2, \quad x_1\sqrt{a}, \quad x_2^2+y_2^2, \quad x_2\sqrt{a}$$

are rational numbers. Since $a$ is a rational number, so then are

$$\begin{aligned}
x_1^2 &= \frac{(x_1\sqrt{a})^2}{a} \\
x_2^2 &= \frac{(x_2\sqrt{a})^2}{a} \\
x_1x_2 &= \frac{(x_1\sqrt{a})(x_2\sqrt{a})}{a} \\
y_1^2 &= (x_1^2+y_1^2)-x_1^2 \\
y_2^2 &= (x_2^2+y_2^2)-x_2^2.
\end{aligned}$$

Now note that the quantity

$$(x_1-x_2)^2+(y_1-y_2)^2 = x_1^2-2x_1x_2+x_2^2+y_1^2-2y_1y_2+y_2^2$$

is known to be rational, as is every summand on the right except $-2y_1y_2$; thus $y_1y_2$ is also rational. Since $y_1^2$ is also rational, so then is $y_1/y_2 = (y_1y_2)/(y_1^2)$; since

$$\operatorname{area}(\triangle ABC) = \sqrt{a}y_1, \qquad \operatorname{area}(\triangle ABD) = \sqrt{a}y_2,$$

this yields the desired result.

**Second solution.** (by Manjul Bhargava) Let $\mathbf{b},\mathbf{c},\mathbf{d}$ be the vectors $AB, AC, AD$ viewed as column vectors. The desired ratio is given by

$$\begin{aligned}
\frac{\det(\mathbf{b},\mathbf{c})}{\det(\mathbf{b},\mathbf{d})} &= \frac{\det(\mathbf{b},\mathbf{c})^T\det(\mathbf{b},\mathbf{c})}{\det(\mathbf{b},\mathbf{c})^T\det(\mathbf{b},\mathbf{d})} \\
&= \det\begin{pmatrix} \mathbf{b}\cdot\mathbf{b} & \mathbf{b}\cdot\mathbf{c} \\ \mathbf{c}\cdot\mathbf{b} & \mathbf{c}\cdot\mathbf{c} \end{pmatrix} \det\begin{pmatrix} \mathbf{b}\cdot\mathbf{b} & \mathbf{b}\cdot\mathbf{d} \\ \mathbf{c}\cdot\mathbf{b} & \mathbf{c}\cdot\mathbf{d} \end{pmatrix}^{-1}.
\end{aligned}$$

The square of the length of $AB$ is $\mathbf{b}\cdot\mathbf{b}$, so this quantity is rational. The square of the lengths of $AC$ and $BC$ are $\mathbf{c}\cdot\mathbf{c}$ and $(\mathbf{c}-\mathbf{b})\cdot(\mathbf{c}-\mathbf{b}) = \mathbf{b}\cdot\mathbf{b}+\mathbf{c}\cdot\mathbf{c}-2\mathbf{b}\cdot\mathbf{c}$, so $\mathbf{b}\cdot\mathbf{c} = \mathbf{c}\cdot\mathbf{b}$ is rational. Similarly, using $AD$ and $BD$, we deduce that $\mathbf{d}\cdot\mathbf{d}$ and $\mathbf{b}\cdot\mathbf{d}$ is rational; then using $CD$, we deduce that $\mathbf{c}\cdot\mathbf{d}$ is rational.

**Third solution.** (by David Rusin) Recall that Heron's formula (for the area of a triangle in terms of its side length) admits the following three-dimensional analogue due to Piero della Francesca: if $V$ denotes the volume of a tetrahedron with vertices $A,B,C,D \in \mathbb{R}^3$, then

$$288V^2 = \det\begin{pmatrix} 0 & AB^2 & AC^2 & AD^2 & 1 \\ AB^2 & 0 & BC^2 & BD^2 & 1 \\ AC^2 & BC^2 & 0 & CD^2 & 1 \\ AD^2 & BD^2 & CD^2 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

In particular, the determinant vanishes if and only if $A,B,C,D$ are coplanar. From the identity

$$\begin{aligned}
&64(4\operatorname{Area}(\triangle ABC)^2\operatorname{Area}(\triangle ABD)^2-9AB^2V^2) \\
&= (AB^4-AB^2(AC^2+AD^2+BC^2+BD^2-2CD^2) \\
&\qquad +(AC^2-BC^2)(AD^2-BD^2))^2
\end{aligned}$$

we see that $\operatorname{Area}(\triangle ABC)\operatorname{Area}(\triangle ABD)$ is rational; since each of the areas has rational square, we deduce the claim.

**Fourth solution.** (by Greg Martin) Define the signed angles $\alpha = \angle BAC, \beta = \angle BAD, \gamma = \angle CAD$, so that $\alpha+\gamma = \beta$. By the Law of Cosines,

$$\begin{aligned}
2AB\cdot AC\cos\alpha &= AB^2+AC^2-BC^2 \in \mathbb{Q} \\
2AB\cdot AD\cos\beta &= AB^2+AD^2-BD^2 \in \mathbb{Q} \\
2AC\cdot AD\cos\gamma &= AC^2+AD^2-CD^2 \in \mathbb{Q}.
\end{aligned}$$

In particular, $(2AB\cdot AC\cos\alpha)^2 \in \mathbb{Q}$, and so $\cos^2\alpha \in \mathbb{Q}$ and $\sin^2\alpha = 1-\cos^2\alpha \in \mathbb{Q}$, and similarly for the other two angles.

Applying the addition formula to $\cos\beta$, we deduce that

$$2AB\cdot AD\cos\alpha\cos\gamma - 2AB\cdot AD\sin\alpha\sin\gamma \in \mathbb{Q}.$$

The first of these terms equals

$$\frac{(2AB\cdot AC\cos\alpha)(2AB\cdot AC\cos\alpha)}{AC^2} \in \mathbb{Q},$$

so the second term must also be rational. But now

$$\begin{aligned}
\frac{\operatorname{Area}(\triangle ABC)}{\operatorname{Area}(\triangle ACD)} &= \frac{AB\cdot AC\sin\alpha}{AC\cdot AD\sin\gamma} \\
&= \frac{2AB\cdot AD\sin\alpha\sin\gamma}{2AD^2\sin^2\gamma} \in \mathbb{Q}
\end{aligned}$$

as desired.

**Remark.** Derek Smith observes that this result is Proposition 1 of: M. Knopf, J. Milzman, D. Smith, D. Zhu and D. Zirlin, Lattice embeddings of planar point sets, *Discrete and Computational Geometry* **56** (2016), 693–710.

**Remark.** It is worth pointing out that it is indeed possible to choose points $A,B,C,D$ satisfying the conditions of the problem; one can even ensure that the lengths of all four segments are themselves rational. For example, it was originally observed by Euler that one can find an infinite set of points on the unit circle whose pairwise distances are all rational numbers. One way to see this is to apply the linear fractional transformation $f(z) = \frac{z+i}{z-i}$ to the Riemann sphere to carry the real axis (plus $\infty$) to the unit circle, then compute that

$$|f(z_1)-f(z_2)| = \frac{2|z_1-z_2||}{|(z_1-i)(z_2-i)|}.$$

Let $S$ be the set of rational numbers $z$ for which $2(z^2+1)$ is a perfect square; the set $f(S)$ has the desired property provided that it is infinite. That can be checked in various ways; for instance, the equation $2(x^2+1)=(2y)^2$ equates to $x^2-2y^2=-1$ (a modified Brahmagupta-Pell equation), which has infinitely many solutions even over the integers:

$$x+y\sqrt{2}=(1+\sqrt{2})^{2n+1}.$$

B1 The answer is the collection of vectors $(1,b)$ where $0\leq b\leq 100$ and $b$ is even. (For ease of typography, we write tuples instead of column vectors.)

First we show that if $\mathscr{P}\setminus\{\mathbf{v}\}$ can be partitioned into subsets $S_1$ and $S_2$ of equal size and equal sum, then $\mathbf{v}$ must be of the form $(1,b)$ where $b$ is even. For a finite nonempty set $S$ of vectors in $\mathbb{Z}^2$, let $\Sigma(S)$ denote the sum of the vectors in $S$. Since the average $x$- and $y$-coordinates in $\mathscr{P}$ are 1 and 50, respectively, and there are $3\cdot 101$ elements in $\mathscr{P}$, we have

$$\Sigma(P)=303\cdot(1,50)=(303,15150).$$

On the other hand,

$$\Sigma(P)=\mathbf{v}+\Sigma(S_1)+\Sigma(S_2)=\mathbf{v}+2\Sigma(S_1).$$

By parity considerations, the entries of $\mathbf{v}$ must be odd and even, respectively, and thus $\mathbf{v}$ is of the claimed form.

Next suppose $\mathbf{v}=(1,b)$ where $b$ is even. Note that $\mathscr{P}\setminus\{(1,50)\}$ can be partitioned into 151 pairs of (distinct) vectors $(x,y)$ and $(2-x,100-y)$, each summing to $(2,100)$. If $b\neq 50$ then three of these pairs are $\{(1,b),(1,100-b)\},\{(2,b),(0,100-b)\}$, and $\{(2,25+b/2),(0,75-b/2)\}$. Of the remaining 148 pairs, assign half of them to $S_1$ and half to $S_2$, and then complete the partition of $\mathscr{P}\setminus\{\mathbf{v}\}$ by assigning $(0,100-b)$, $(2,25+b/2)$, and $(1,50)$ to $S_1$ and $(1,100-b)$, $(2,b)$, and $(0,75-b/2)$ to $S_2$. (Note that the three vectors assigned to each of $S_1$ and $S_2$ have the same sum $(3,175-b/2)$.) By construction, $S_1$ and $S_2$ have the same number of elements, and $\Sigma(S_1)=\Sigma(S_2)$.

For $b=50$, this construction does not work because $(1,b)=(100-b)$, but a slight variation can be made. In this case, three of the pairs in $\mathscr{P}\setminus\{(1,50)\}$ are $\{(2,50),(0,50)\}$, $\{(1,51),(1,49)\}$, and $\{(0,49),(2,51)\}$. Assign half of the other 148 pairs to $S_1$ and half to $S_2$, and complete the partition of $\mathscr{P}\setminus\{(1,50)\}$ by assigning $(2,50)$, $(1,51)$, and $(0,49)$ to $S_1$ and $(0,50)$, $(1,49)$, and $(2,51)$ to $S_2$.

B2 **First solution.** Note first that $f_n(1)>0$, so 1 is not a root of $f_n$. Next, note that

$$(z-1)f_n(z)=z^n+\cdots+z-n;$$

however, for $|z|\leq 1$, we have $|z^n+\cdots+z|\leq n$ by the triangle inequality; equality can only occur if $z,\dots,z^n$ have norm 1 and the same argument, which only happens for $z=1$. Thus there can be no root of $f_n$ with $|z|\leq 1$.

**Second solution.** (by Karl Mahlburg) Define the polynomial

$$g_n(z)=nz^{n-1}+\cdots+2z+1$$

and note that $z^{n-1}g_n(z^{-1})=f_n(z)$. Since $f_n(0)\neq 0$, to prove the claim it is equivalent to show that $g_n$ has no roots in the region $|z|\geq 1$.

Now note that $g_n(z)=h_n'(z)$ for

$$h_n(z)=z^n+\cdots+z+1,$$

a polynomial with roots $e^{2\pi ij/(n+1)}$ for $j=0,\dots,n$. By the Gauss-Lucas theorem, the roots of $g_n$ lie in the convex hull of the roots of $h_n$, and moreover cannot be vertices of the convex hull because $h_n$ has no repeated roots. This implies the claim.

**Remark.** Yet another approach is to use the *Eneström-Kakeya theorem*: if $P_n(z)=a_0+\cdots+a_nz^n$ is a polynomial with real coefficients satisfying $|a_n|\geq\cdots\geq|a_0|>0$, then the roots of $P_n(z)$ all satisfy $|z|\leq 1$. Namely, applying this to the polynomial $g_n(z/c)$ for $c=n/(n-1)$ shows that the roots of $g_n$ all satisfy $|z|\leq 1/c$.

**Remark.** For a related problem, see problem A5 from the 2014 Putnam competition.

B3 The values of $n$ with this property are $2^{2^\ell}$ for $\ell=1,2,4,8$. First, note that $n$ divides $2^n$ if and only if $n$ is itself a power of 2; we may thus write $n=2^m$ and note that if $n<10^{100}$, then

$$2^m=n<10^{100}<(10^3)^{34}<(2^{10})^{34}=2^{340}.$$

Moreover, the case $m=0$ does not lead to a solution because for $n=1$, $n-1=0$ does not divide $2^n-1=1$; we may thus assume $1\leq m\leq 340$.

Next, note that modulo $n-1=2^m-1$, the powers of 2 cycle with period $m$ (the terms $2^0,\dots,2^{m-1}$ remain the same upon reduction, and then the next term repeats the initial 1); consequently, $n-1$ divides $2^n-1$ if and only if $m$ divides $n$, which happens if and only if $m$ is a power of 2. Write $m=2^\ell$ and note that $2^\ell<340<512$, so $\ell<9$. The case $\ell=0$ does not lead to a solution because for $n=2$, $n-2=0$ does not divide $2^n-2=2$; we may thus assume $1\leq\ell\leq 8$.

Finally, note that $n-2=2^m-2$ divides $2^n-2$ if and only if $2^{m-1}-1$ divides $2^{n-1}-1$. By the same logic as the previous paragraph, this happens if and only if $m-1$ divides $n-1$, that is, if $2^\ell-1$ divides $2^m-1$. This in turn happens if and only if $\ell$ divides $m=2^\ell$, which happens if and only if $\ell$ is a power of 2. The values allowed by the bound $\ell<9$ are $\ell=1,2,4,8$; for these values, $m\leq 2^8=256$ and

$$n=2^m\leq 2^{256}\leq(2^3)^{86}<10^{86}<10^{100},$$

so the solutions listed do satisfy the original inequality.

B4 We first rule out the case $|a| > 1$. In this case, we prove that $|x_{n+1}| \geq |x_n|$ for all $n$, meaning that we cannot have $x_n = 0$. We proceed by induction; the claim is true for $n = 0, 1$ by hypothesis. To prove the claim for $n \geq 2$, write

$$\begin{aligned} |x_{n+1}| &= |2x_n x_{n-1} - x_{n-2}| \\ &\geq 2|x_n||x_{n-1}| - |x_{n-2}| \\ &\geq |x_n|(2|x_{n-1}| - 1) \geq |x_n|, \end{aligned}$$

where the last step follows from $|x_{n-1}| \geq |x_{n-2}| \geq \cdots \geq |x_0| = 1$.

We may thus assume hereafter that $|a| \leq 1$. We can then write $a = \cos b$ for some $b \in [0, \pi]$. Let $\{F_n\}$ be the Fibonacci sequence, defined as usual by $F_1 = F_2 = 1$ and $F_{n+1} = F_n + F_{n-1}$. We show by induction that

$$x_n = \cos(F_n b) \qquad (n \geq 0).$$

Indeed, this is true for $n = 0, 1, 2$; given that it is true for $n \leq m$, then

$$\begin{aligned} 2x_m x_{m-1} &= 2\cos(F_m b)\cos(F_{m-1} b) \\ &= \cos((F_m - F_{m-1})b) + \cos((F_m + F_{m-1})b) \\ &= \cos(F_{m-2} b) + \cos(F_{m+1} b) \end{aligned}$$

and so $x_{m+1} = 2x_m x_{m-1} - x_{m-2} = \cos(F_{m+1} b)$. This completes the induction.

Since $x_n = \cos(F_n b)$, if $x_n = 0$ for some $n$ then $F_n b = \frac{k}{2}\pi$ for some odd integer $k$. In particular, we can write $b = \frac{c}{d}(2\pi)$ where $c = k$ and $d = 4F_n$ are integers.

Let $x_n$ denote the pair $(F_n, F_{n+1})$, where each entry in this pair is viewed as an element of $\mathbb{Z}/d\mathbb{Z}$. Since there are only finitely many possibilities for $x_n$, there must be some $n_2 > n_1$ such that $x_{n_1} = x_{n_2}$. Now $x_n$ uniquely determines both $x_{n+1}$ and $x_{n-1}$, and it follows that the sequence $\{x_n\}$ is periodic: for $\ell = n_2 - n_1$, $x_{n+\ell} = x_n$ for all $n \geq 0$. In particular, $F_{n+\ell} \equiv F_n \pmod{d}$ for all $n$. But then $\frac{F_{n+\ell}c}{d} - \frac{F_n c}{d}$ is an integer, and so

$$\begin{aligned} x_{n+\ell} &= \cos\left(\frac{F_{n+\ell}c}{d}(2\pi)\right) \\ &= \cos\left(\frac{F_n c}{d}(2\pi)\right) = x_n \end{aligned}$$

for all $n$. Thus the sequence $\{x_n\}$ is periodic, as desired.

**Remark.** Karl Mahlburg points out that one can motivate the previous solution by computing the terms

$$x_2 = 2a^2 - 1, x_3 = 4a^3 - 3a, x_4 = 16a^5 - 20a^3 + 5a$$

and recognizing these as the Chebyshev polynomials $T_2, T_3, T_5$. (Note that $T_3$ was used in the solution of problem A3.)

**Remark.** It is not necessary to handle the case $|a| > 1$ separately; the cosine function extends to a surjective analytic function on $\mathbb{C}$ and continues to satisfy the addition formula, so one can write $a = \cos b$ for some $b \in \mathbb{C}$ and then proceed as above.

B5 Let $(a_1, a_2)$ and $(a_1', a_2')$ be distinct points in $\mathbb{R}^2$; we want to show that $f(a_1, a_2) \neq f(a_1', a_2')$. Write $(v_1, v_2) = (a_1', a_2') - (a_1, a_2)$, and let $\gamma(t) = (a_1, a_2) + t(v_1, v_2)$, $t \in [0, 1]$, be the path between $(a_1, a_2)$ and $(a_1', a_2')$. Define a real-valued function $g$ by $g(t) = (v_1, v_2) \cdot f(\gamma(t))$. By the Chain Rule,

$$f'(\gamma(t)) = \begin{pmatrix} \partial f_1/\partial x_1 & \partial f_1/\partial x_2 \\ \partial f_2/\partial x_1 & \partial f_2/\partial x_2 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}.$$

Abbreviate $\partial f_i/\partial x_j$ by $f_{ij}$; then

$$\begin{aligned} g'(t) &= \begin{pmatrix} v_1 & v_2 \end{pmatrix} \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \\ &= f_{11} v_1^2 + (f_{12} + f_{21}) v_1 v_2 + f_{22} v_2^2 \\ &= f_{11}\left(v_1 + \frac{f_{12} + f_{21}}{2f_{11}} v_2\right)^2 + \frac{4f_{11}f_{22} - (f_{12} + f_{21})^2}{4f_{11}} v_2^2 \\ &\geq 0 \end{aligned}$$

since $f_{11}$ and $f_{11}f_{22} - (f_{12} + f_{21})^2/4$ are positive by assumption. Since the only way that equality could hold is if $v_1$ and $v_2$ are both 0, we in fact have $g'(t) > 0$ for all $t$. But if $f(a_1, a_2) = f(a_1', a_2')$, then $g(0) = g(1)$, a contradiction.

**Remark.** A similar argument shows more generally that $f : \mathbb{R}^n \to \mathbb{R}^n$ is injective if at all points in $\mathbb{R}^n$, the Jacobian matrix $Df$ satisfies the following property: the quadratic form associated to the bilinear form with matrix $Df$ (or the symmetrized bilinear form with matrix $(Df + (Df)^T)/2$) is positive definite. In the setting of the problem, the symmetrized matrix is

$$\begin{pmatrix} f_{11} & (f_{12} + f_{21})/2 \\ (f_{12} + f_{21})/2 & f_{22} \end{pmatrix},$$

and this is positive definite if and only if $f_{11}$ and the determinant of the matrix are both positive (Sylvester's criterion). Note that the assumptions that $f_{12}, f_{21} > 0$ are unnecessary for the argument; it is also easy to see that the hypotheses $f_{11}, f_{12} > 0$ are also superfluous. (The assumption $f_{11}f_{22} - (f_{12} + f_{21})^2 > 0$ implies $f_{11}f_{22} > 0$, so both are nonzero and of the same sign; by continuity, this common sign must be constant over all of $\mathbb{R}^2$. If it is negative, then apply the same logic to $(-f_1, -f_2)$.)

B6 (by Manjul Bhargava) Let $a(k, n)$ denote the number of sequences of length $k$ taken from the set $\{1, 2, 3, 4, 5, 6, 10\}$ and having sum $n$. We prove that

$$a(k, n) < 2^n \left(\frac{2018}{2048}\right)^k$$

by double induction on $n + k$ and $n - k$. The claim is clearly true when $n - k \leq 0$ and in particular when $n = k = 1$, the smallest case for $n + k$.

We categorize the sequences counted by $a(k,n)$ by whether they end in $1,2,3,4,5,6,10$; removing the last term of such a sequence yields a sequence counted by $a(k-1,n-1), a(k-1,n-2), a(k-1,n-3), a(k-1,n-4), a(k-1,n-5), a(k-1,n-6), a(k-1,n-10)$, respectively. Therefore,

$$\begin{aligned}
a(k,n) &= a(k-1,n-1)+\cdots \\
&\qquad + a(k-1,n-6)+a(k-1,n-10) \\
&< (2^{n-1}+\cdots+2^{n-6}+2^{n-10})\left(\frac{2018}{2048}\right)^{k-1} \\
&= 2^n\left(\frac{1}{2}+\cdots+\frac{1}{64}+\frac{1}{1024}\right)\left(\frac{2018}{2048}\right)^{k-1} \\
&= 2^n\left(\frac{1009}{1024}\right)\left(\frac{2018}{2048}\right)^{k-1} \\
&= 2^n\left(\frac{2018}{2048}\right)^{k}
\end{aligned}$$

where we used directly the induction hypothesis to obtain the inequality on the second line. The case $k = 2018, n = 3860$ yields the desired result.

**Remark.** K. Soundararajan suggests the following reinterpretation of this argument. The quantity $a(k,n)$ can be interpreted as the coefficient of $x^n$ in $(x+x^2+\cdots+x^6+x^{10})^k$. Since this polynomial has nonnegative coefficients, for any $x$, we have

$$a(k,n)x^n < (x+x^2+\cdots+x^6+x^{10})^k.$$

Substituting $x = \frac{1}{2}$ yields the bound stated above.

On a related note, Alexander Givental suggests that the value $n = 3860$ (which is otherwise irrelevant to the problem) may have been chosen for the following reason: as a function of $x$, the upper bound $x^{-n}(x+x^2+\cdots+x^6+x^{10})^k$ is minimized when

$$\frac{x(1+2x+\cdots+6x^5+x^9)}{x+x^2+\cdots+x^6+x^{10}} = \frac{n}{k}.$$

In order for this to hold for $x = 1/2$, $k = 2018$, one must take $n = 3860$.

**Remark.** For purposes of comparison, the stated bound is about $10^{1149}$, while the trivial upper bound given by counting all sequences of length 2018 of positive integers that sum to 3860 is

$$\binom{3859}{2017} \sim 10^{1158}.$$

The latter can be easily derived by a "stars and bars" argument: visualize each sequence of this form by representing the value $n$ by $n$ stars and inserting a bar between adjacent terms of the sequence. The resulting string of symbols consists of one star at the beginning, 2017 bar-star combinations, and 3860-2018 more stars. Using a computer, it is practical to compute the exact cardinality of $S$ by finding the coefficient of $x^{3860}$ in $(x+x^2+\cdots+x^6+x^{10})^{2018}$. For example, this can be done in `Sage` in a couple of seconds as follows. (The truncation is truncated modulo $x^{4000}$ for efficiency.)

```
sage: P.<x> = PowerSeriesRing(ZZ, 4000)
sage: f = (x + x^2 + x^3 + x^4 + \
....:      x^5 + x^6 + x^10)^2018
sage: m = list(f)[3860]
sage: N(m)
8.04809122940636e1146
```

This computation shows that the upper bound of the problem differs from the true value by a factor of about 150.

# The 80th William Lowell Putnam Mathematical Competition
# Saturday, December 7, 2019

A1 Determine all possible values of the expression

$$A^3+B^3+C^3-3ABC$$

where $A, B$, and $C$ are nonnegative integers.

A2 In the triangle $\triangle ABC$, let $G$ be the centroid, and let $I$ be the center of the inscribed circle. Let $\alpha$ and $\beta$ be the angles at the vertices $A$ and $B$, respectively. Suppose that the segment $IG$ is parallel to $AB$ and that $\beta = 2\tan^{-1}(1/3)$. Find $\alpha$.

A3 Given real numbers $b_0, b_1, \ldots, b_{2019}$ with $b_{2019} \neq 0$, let $z_1, z_2, \ldots, z_{2019}$ be the roots in the complex plane of the polynomial

$$P(z) = \sum_{k=0}^{2019} b_k z^k.$$

Let $\mu = (|z_1| + \cdots + |z_{2019}|)/2019$ be the average of the distances from $z_1, z_2, \ldots, z_{2019}$ to the origin. Determine the largest constant $M$ such that $\mu \geq M$ for all choices of $b_0, b_1, \ldots, b_{2019}$ that satisfy

$$1 \leq b_0 < b_1 < b_2 < \cdots < b_{2019} \leq 2019.$$

A4 Let $f$ be a continuous real-valued function on $\mathbb{R}^3$. Suppose that for every sphere $S$ of radius 1, the integral of $f(x,y,z)$ over the surface of $S$ equals 0. Must $f(x,y,z)$ be identically 0?

A5 Let $p$ be an odd prime number, and let $\mathbb{F}_p$ denote the field of integers modulo $p$. Let $\mathbb{F}_p[x]$ be the ring of polynomials over $\mathbb{F}_p$, and let $q(x) \in \mathbb{F}_p[x]$ be given by

$$q(x) = \sum_{k=1}^{p-1} a_k x^k,$$

where

$$a_k = k^{(p-1)/2} \mod p.$$

Find the greatest nonnegative integer $n$ such that $(x-1)^n$ divides $q(x)$ in $\mathbb{F}_p[x]$.

A6 Let $g$ be a real-valued function that is continuous on the closed interval $[0,1]$ and twice differentiable on the open interval $(0,1)$. Suppose that for some real number $r > 1$,

$$\lim_{x \to 0^+} \frac{g(x)}{x^r} = 0.$$

Prove that either

$$\lim_{x \to 0^+} g'(x) = 0 \qquad \text{or} \qquad \limsup_{x \to 0^+} x^r |g''(x)| = \infty.$$

B1 Denote by $\mathbb{Z}^2$ the set of all points $(x,y)$ in the plane with integer coordinates. For each integer $n \geq 0$, let $P_n$ be the subset of $\mathbb{Z}^2$ consisting of the point $(0,0)$ together with all points $(x,y)$ such that $x^2+y^2 = 2^k$ for some integer $k \leq n$. Determine, as a function of $n$, the number of four-point subsets of $P_n$ whose elements are the vertices of a square.

B2 For all $n \geq 1$, let

$$a_n = \sum_{k=1}^{n-1} \frac{\sin\left(\frac{(2k-1)\pi}{2n}\right)}{\cos^2\left(\frac{(k-1)\pi}{2n}\right)\cos^2\left(\frac{k\pi}{2n}\right)}.$$

Determine

$$\lim_{n \to \infty} \frac{a_n}{n^3}.$$

B3 Let $Q$ be an $n$-by-$n$ real orthogonal matrix, and let $u \in \mathbb{R}^n$ be a unit column vector (that is, $u^T u = 1$). Let $P = I - 2uu^T$, where $I$ is the $n$-by-$n$ identity matrix. Show that if 1 is not an eigenvalue of $Q$, then 1 is an eigenvalue of $PQ$.

B4 Let $\mathscr{F}$ be the set of functions $f(x,y)$ that are twice continuously differentiable for $x \geq 1$, $y \geq 1$ and that satisfy the following two equations (where subscripts denote partial derivatives):

$$xf_x + yf_y = xy\ln(xy),$$
$$x^2 f_{xx} + y^2 f_{yy} = xy.$$

For each $f \in \mathscr{F}$, let

$$m(f) = \min_{s \geq 1}\left(f(s+1,s+1) - f(s+1,s) - f(s,s+1) + f(s,s)\right).$$

Determine $m(f)$, and show that it is independent of the choice of $f$.

B5 Let $F_m$ be the $m$th Fibonacci number, defined by $F_1 = F_2 = 1$ and $F_m = F_{m-1} + F_{m-2}$ for all $m \geq 3$. Let $p(x)$ be the polynomial of degree 1008 such that $p(2n+1) = F_{2n+1}$ for $n = 0, 1, 2, \ldots, 1008$. Find integers $j$ and $k$ such that $p(2019) = F_j - F_k$.

B6 Let $\mathbb{Z}^n$ be the integer lattice in $\mathbb{R}^n$. Two points in $\mathbb{Z}^n$ are called *neighbors* if they differ by exactly 1 in one coordinate and are equal in all other coordinates. For which integers $n \geq 1$ does there exist a set of points $S \subset \mathbb{Z}^n$ satisfying the following two conditions?

(1) If $p$ is in $S$, then none of the neighbors of $p$ is in $S$.

(2) If $p \in \mathbb{Z}^n$ is not in $S$, then exactly one of the neighbors of $p$ is in $S$.

# Solutions to the 80th William Lowell Putnam Mathematical Competition
# Saturday, December 7, 2019

Kiran Kedlaya and Lenny Ng

A1 The answer is all nonnegative integers not congruent to 3 or 6 (mod 9). Let $X$ denote the given expression; we first show that we can make $X$ equal to each of the claimed values. Write $B = A+b$ and $C = A+c$, so that

$$X = (b^2 - bc + c^2)(3A + b + c).$$

By taking $(b,c) = (0,1)$ or $(b,c) = (1,1)$, we obtain respectively $X = 3A+1$ and $X = 3A+2$; consequently, as $A$ varies, we achieve every nonnegative integer not divisible by 3. By taking $(b,c) = (1,2)$, we obtain $X = 9A+9$; consequently, as $A$ varies, we achieve every positive integer divisible by 9. We may also achieve $X = 0$ by taking $(b,c) = (0,0)$.

In the other direction, $X$ is always nonnegative: either apply the arithmetic mean-geometric mean inequality, or write $b^2 - bc + c^2 = (b - c/2)^2 + 3c^2/4$ to see that it is nonnegative. It thus only remains to show that if $X$ is a multiple of 3, then it is a multiple of 9. Note that $3A + b + c \equiv b + c \pmod 3$ and $b^2 - bc + c^2 \equiv (b+c)^2 \pmod 3$; consequently, if $X$ is divisible by 3, then $b+c$ must be divisible by 3, so each factor in $X = (b^2 - bc + c^2)(3A + b + c)$ is divisible by 3. This proves the claim.

**Remark.** The factorization of $X$ used above can be written more symmetrically as

$$X = (A+B+C)(A^2+B^2+C^2-AB-BC-CA).$$

One interpretation of the factorization is that $X$ is the determinant of the circulant matrix

$$\begin{pmatrix} A & B & C \\ C & A & B \\ B & C & A \end{pmatrix}$$

which has the vector $(1,1,1)$ as an eigenvector (on either side) with eigenvalue $A+B+C$. The other eigenvalues are $A + \zeta B + \zeta^2 C$ where $\zeta$ is a primitive cube root of unity; in fact, $X$ is the norm form for the ring $\mathbb{Z}[T]/(T^3-1)$, from which it follows directly that the image of $X$ is closed under multiplication. (This is similar to the fact that the image of $A^2+B^2$, which is the norm form for the ring $\mathbb{Z}[i]$ of Gaussian integers, is closed under multiplication.)

One can also the unique factorization property of the ring $\mathbb{Z}[\zeta]$ of Eisenstein integers as follows. The three factors of $X$ over $\mathbb{Z}[\zeta_3]$ are pairwise congruent modulo $1-\zeta_3$; consequently, if $X$ is divisible by 3, then it is divisible by $(1-\zeta_3)^3 = -3\zeta_3(1-\zeta_3)$ and hence (because it is a rational integer) by $3^2$.

A2 **Solution 1.** Let $M$ and $D$ denote the midpoint of $AB$ and the foot of the altitude from $C$ to $AB$, respectively, and let $r$ be the inradius of $\triangle ABC$. Since $C,G,M$ are collinear with $CM = 3GM$, the distance from $C$ to line $AB$ is 3 times the distance from $G$ to $AB$, and the latter is $r$ since $IG \parallel AB$; hence the altitude $CD$ has length $3r$. By the double angle formula for tangent, $\frac{CD}{DB} = \tan\beta = \frac{3}{4}$, and so $DB = 4r$. Let $E$ be the point where the incircle meets $AB$; then $EB = r/\tan(\frac{\beta}{2}) = 3r$. It follows that $ED = r$, whence the incircle is tangent to the altitude $CD$. This implies that $D = A$, $ABC$ is a right triangle, and $\alpha = \frac{\pi}{2}$.

**Remark.** One can obtain a similar solution by fixing a coordinate system with $B$ at the origin and $A$ on the positive $x$-axis. Since $\tan\frac{\beta}{2} = \frac{1}{3}$, we may assume without loss of generality that $I = (3,1)$. Then $C$ lies on the intersection of the line $y = 3$ (because $CD = 3r$ as above) with the line $y = \frac{3}{4}x$ (because $\tan\beta = \frac{3}{4}$ as above), forcing $C = (4,3)$ and so forth.

**Solution 2.** Let $a,b,c$ be the lengths of $BC,CA,AB$, respectively. Let $r$, $s$, and $K$ denote the inradius, semiperimeter, and area of $\triangle ABC$. By Heron's Formula,

$$r^2 s^2 = K^2 = s(s-a)(s-b)(s-c).$$

If $IG$ is parallel to $AB$, then

$$\frac{1}{2}rc = \text{area}(\triangle ABI) = \text{area}(\triangle ABG) = \frac{1}{3}K = \frac{1}{3}rs$$

and so $c = \frac{a+b}{2}$. Since $s = \frac{3(a+b)}{4}$ and $s - c = \frac{a+b}{4}$, we have $3r^2 = (s-a)(s-b)$. Let $E$ be the point at which the incircle meets $AB$; then $s - b = EB = r/\tan(\frac{\beta}{2})$ and $s - a = EA = r/\tan(\frac{\alpha}{2})$. It follows that $\tan(\frac{\alpha}{2})\tan(\frac{\beta}{2}) = \frac{1}{3}$ and so $\tan(\frac{\alpha}{2}) = 1$. This implies that $\alpha = \frac{\pi}{2}$.

**Remark.** The equality $c = \frac{a+b}{2}$ can also be derived from the vector representations

$$G = \frac{A+B+C}{3}, \qquad I = \frac{aA+bB+cC}{a+b+c}.$$

**Solution 3.** (by Catalin Zara) It is straightforward to check that a right triangle with $AC = 3, AB = 4, BC = 5$ works. For example, in a coordinate system with $A = (0,0), B = (4,0), C = (0,3)$, we have

$$G = \left(\frac{4}{3}, 1\right), \qquad I = (1,1)$$

and for $D = (1,0)$,

$$\tan\frac{\beta}{2} = \frac{ID}{BD} = \frac{1}{3}.$$

It thus suffices to suggest that this example is unique up to similarity.

Let $C'$ be the foot of the angle bisector at $C$. Then

$$\frac{CI}{IC'} = \frac{CA+CB}{AB}$$

and so $IG$ is parallel to $AB$ if and only if $CA+CB = 2AB$. We may assume without loss of generality that $A$ and $B$ are fixed, in which case this condition restricts $C$ to an ellipse with foci at $A$ and $B$. Since the angle $\beta$ is also fixed, up to symmetry $C$ is further restricted to a half-line starting at $B$; this intersects the ellipse in a unique point.

**Remark.** Given that $CA+CB = 2AB$, one can also recover the ratio of side lengths using the law of cosines.

A3 The answer is $M = 2019^{-1/2019}$. For any choices of $b_0,\dots,b_{2019}$ as specified, AM-GM gives

$$\mu \geq |z_1 \cdots z_{2019}|^{1/2019} = |b_0/b_{2019}|^{1/2019} \geq 2019^{-1/2019}.$$

To see that this is best possible, consider $b_0,\dots,b_{2019}$ given by $b_k = 2019^{k/2019}$ for all $k$. Then

$$P(z/2019^{1/2019}) = \sum_{k=0}^{2019} z^k = \frac{z^{2020}-1}{z-1}$$

has all of its roots on the unit circle. It follows that all of the roots of $P(z)$ have modulus $2019^{-1/2019}$, and so $\mu = 2019^{-1/2019}$ in this case.

A4 The answer is no. Let $g : \mathbb{R} \to \mathbb{R}$ be any continuous function with $g(t+2) = g(t)$ for all $t$ and $\int_0^2 g(t)\,dt = 0$ (for instance, $g(t) = \sin(\pi t)$). Define $f(x,y,z) = g(z)$. We claim that for any sphere $S$ of radius 1, $\iint_S f\,dS = 0$.

Indeed, let $S$ be the unit sphere centered at $(x_0,y_0,z_0)$. We can parametrize $S$ by $S(\phi,\theta) = (x_0,y_0,z_0) + (\sin\phi\cos\theta, \sin\phi\sin\theta, \cos\phi)$ for $\phi \in [0,\pi]$ and $\theta \in [0,2\pi]$. Then we have

$$\begin{aligned}
\iint_S f(x,y,z)\,dS &= \int_0^\pi \int_0^{2\pi} f(S(\phi,\theta)) \left\| \frac{\partial S}{\partial \phi} \times \frac{\partial S}{\partial \theta} \right\| d\theta\,d\phi \\
&= \int_0^\pi \int_0^{2\pi} g(z_0 + \cos\phi)\sin\phi\,d\theta\,d\phi \\
&= 2\pi \int_{-1}^1 g(z_0+t)\,dt,
\end{aligned}$$

where we have used the substitution $t = \cos\phi$; but this last integral is 0 for any $z_0$ by construction.

**Remark.** The solution recovers the famous observation of Archimedes that the surface area of a spherical cap is linear in the height of the cap. In place of spherical coordinates, one may also compute $\iint_S f(x,y,z)\,dS$ by computing the integral over a ball of radius $r$, then computing the derivative with respect to $r$ and evaluating at $r=1$.

Noam Elkies points out that a similar result holds in $\mathbb{R}^n$ for any $n$. Also, there exist nonzero continuous functions on $\mathbb{R}^n$ whose integral over any unit ball vanishes; this implies certain negative results about image reconstruction.

A5 The answer is $\frac{p-1}{2}$. Define the operator $D = x\frac{d}{dx}$, where $\frac{d}{dx}$ indicates formal differentiation of polynomials. For $n$ as in the problem statement, we have $q(x) = (x-1)^n r(x)$ for some polynomial $r(x)$ in $\mathbb{F}_p$ not divisible by $x-1$. For $m = 0,\dots,n$, by the product rule we have

$$(D^m q)(x) \equiv n^m x^m (x-1)^{n-m} r(x) \pmod{(x-1)^{n-m+1}}.$$

Since $r(1) \neq 0$ and $n \not\equiv 0 \pmod{p}$ (because $n \leq \deg(q) = p-1$), we may identify $n$ as the smallest nonnegative integer for which $(D^n q)(1) \neq 0$.

Now note that $q = D^{(p-1)/2} s$ for

$$s(x) = 1 + x + \cdots + x^{p-1} = \frac{x^p-1}{x-1} = (x-1)^{p-1}$$

since $(x-1)^p = x^p - 1$ in $\mathbb{F}_p[x]$. By the same logic as above, $(D^n s)(1) = 0$ for $n = 0,\dots,p-2$ but not for $n = p-1$. This implies the claimed result.

**Remark.** One may also finish by checking directly that for any positive integer $m$,

$$\sum_{k=1}^{p-1} k^m \equiv \begin{cases} -1 \pmod{p} & \text{if } (p-1)|m \\ 0 \pmod{p} & \text{otherwise.} \end{cases}$$

If $(p-1)|m$, then $k^m \equiv 1 \pmod{p}$ by the little Fermat theorem, and so the sum is congruent to $p-1 \equiv -1 \pmod{p}$. Otherwise, for any primitive root $\ell$ mod $p$, multiplying the sum by $\ell^m$ permutes the terms modulo $p$ and hence does not change the sum modulo $p$; since $\ell^n \not\equiv 1 \pmod{p}$, this is only possible if the sum is zero modulo $p$.

A6 **Solution 1.** (by Harm Derksen) We assume that $\limsup_{x\to 0^+} x^r |g''(x)| < \infty$ and deduce that $\lim_{x\to 0^+} g'(x) = 0$. Note that

$$\limsup_{x\to 0^+} x^r \sup\{|g''(\xi)| : \xi \in [x/2, x]\} < \infty.$$

Suppose for the moment that there exists a function $h$ on $(0,1)$ which is positive, nondecreasing, and satisfies

$$\lim_{x\to 0^+} \frac{g(x)}{h(x)} = \lim_{x\to 0^+} \frac{h(x)}{x^r} = 0.$$

For some $c > 0$, $h(x) < x^r < x$ for $x \in (0,c)$. By Taylor's theorem with remainder, we can find a function $\xi$ on $(0,c)$ such that $\xi(x) \in [x-h(x), x]$ and

$$g(x-h(x)) = g(x) - g'(x)h(x) + \frac{1}{2} g''(\xi(x)) h(x)^2.$$

We can thus express $g'(x)$ as

$$\frac{g(x)}{h(x)} + \frac{1}{2} x^r g''(\xi(x)) \frac{h(x)}{x^r} - \frac{g(x-h(x))}{h(x-h(x))} \frac{h(x-h(x))}{h(x)}.$$

As $x \to 0^+$, $g(x)/h(x)$, $g(x-h(x))/h(x-h(x))$, and $h(x)/x^r$ tend to 0, while $x^r g''(\xi(x))$ remains bounded (because $\xi(x) \geq x - h(x) \geq x - x^r \geq x/2$ for $x$ small) and $h(x-h(x))/h(x)$ is bounded in $(0,1]$. Hence $\lim_{x\to 0^+} g'(x) = 0$ as desired.

It thus only remains to produce a function $h$ with the desired properties; this amounts to "inserting" a function between $g(x)$ and $x^r$ while taking care to ensure the positive and nondecreasing properties. One of many options is $h(x) = x^r \sqrt{f(x)}$ where

$$f(x) = \sup\{|z^{-r} g(z)| : z \in (0,x)\},$$

so that

$$\frac{h(x)}{x^r} = \sqrt{f(x)}, \qquad \frac{g(x)}{h(x)} = \sqrt{f(x)} x^{-r} g(x).$$

**Solution 2.** We argue by contradiction. Assume that $\limsup_{x\to 0^+} x^r |g''(x)| < \infty$, so that there is an $M$ such that $|g''(x)| < Mx^{-r}$ for all $x$; and that $\lim_{x\to 0^+} g'(x) \neq 0$, so that there is an $\varepsilon_0 > 0$ and a sequence $x_n \to 0$ with $|g'(x_n)| > \varepsilon_0$ for all $n$.

Now let $\varepsilon > 0$ be arbitrary. Since $\lim_{x\to 0^+} g(x) x^{-r} = 0$, there is a $\delta > 0$ for which $|g(x)| < \varepsilon x^r$ for all $x < \delta$. Choose $n$ sufficiently large that $\frac{\varepsilon_0 x_n^r}{2M} < x_n$ and $x_n < \delta/2$; then $x_n + \frac{\varepsilon_0 x_n^r}{2M} < 2x_n < \delta$. In addition, we have $|g'(x)| > \varepsilon_0/2$ for all $x \in [x_n, x_n + \frac{\varepsilon_0 x_n^r}{2M}]$ since $|g'(x_n)| > \varepsilon_0$ and $|g''(x)| < Mx^{-r} \leq Mx_n^{-r}$ in this range. It follows that

$$\begin{aligned}
\frac{\varepsilon_0^2}{2} \frac{x_n^r}{2M} &< |g(x_n + \frac{\varepsilon_0 x_n^r}{2M}) - g(x_n)| \\
&\leq |g(x_n + \frac{\varepsilon_0 x_n^r}{2M})| + |g(x_n)| \\
&< \varepsilon \left( (x_n + \frac{\varepsilon_0 x_n^r}{2M})^r + x_n^r \right) \\
&< \varepsilon (1 + 2^r) x_n^r,
\end{aligned}$$

whence $4M(1+2^r)\varepsilon > \varepsilon_0^2$. Since $\varepsilon > 0$ is arbitrary and $M, r, \varepsilon_0$ are fixed, this gives the desired contradiction.

**Remark.** Harm Derksen points out that the "or" in the problem need not be exclusive. For example, take

$$g(x) = \begin{cases} x^5 \sin(x^{-3}) & x \in (0,1] \\ 0 & x = 0. \end{cases}$$

Then for $x \in (0,1)$,

$$\begin{aligned}
g'(x) &= 5x^4 \sin(x^{-3}) - 3x \cos(x^{-3}) \\
g''(x) &= (20x^3 - 9x^{-3}) \sin(x^{-3}) - 18 \cos(x^{-3}).
\end{aligned}$$

For $r = 2$, $\lim_{x\to 0^+} x^{-r} g(x) = \lim_{x\to 0^+} x^3 \sin(x^{-3}) = 0$, $\lim_{x\to 0^+} g'(x) = 0$ and $x^r g''(x) = (20x^5 - 9x^{-1}) \sin(x^{-3}) - 18x^2 \cos(x^{-3})$ is unbounded as $x \to 0^+$. (Note that $g'(x)$ is not differentiable at $x = 0$.)

B1 The answer is $5n+1$.

We first determine the set $P_n$. Let $Q_n$ be the set of points in $\mathbb{Z}^2$ of the form $(0, \pm 2^k)$ or $(\pm 2^k, 0)$ for some $k \leq n$. Let $R_n$ be the set of points in $\mathbb{Z}^2$ of the form $(\pm 2^k, \pm 2^k)$ for some $k \leq n$ (the two signs being chosen independently). We prove by induction on $n$ that

$$P_n = \{(0,0)\} \cup Q_{\lfloor n/2 \rfloor} \cup R_{\lfloor (n-1)/2 \rfloor}.$$

We take as base cases the straightforward computations

$$\begin{aligned}
P_0 &= \{(0,0), (\pm 1, 0), (0, \pm 1)\} \\
P_1 &= P_0 \cup \{(\pm 1, \pm 1)\}.
\end{aligned}$$

For $n \geq 2$, it is clear that $\{(0,0)\} \cup Q_{\lfloor n/2 \rfloor} \cup R_{\lfloor (n-1)/2 \rfloor} \subseteq P_n$, so it remains to prove the reverse inclusion. For $(x,y) \in P_n$, note that $x^2 + y^2 \equiv 0 \pmod 4$; since every perfect square is congruent to either 0 or 1 modulo 4, $x$ and $y$ must both be even. Consequently, $(x/2, y/2) \in P_{n-2}$, so we may appeal to the induction hypothesis to conclude.

We next identify all of the squares with vertices in $P_n$. In the following discussion, let $(a,b)$ and $(c,d)$ be two opposite vertices of a square, so that the other two vertices are

$$\left( \frac{a-b+c+d}{2}, \frac{a+b-c+d}{2} \right)$$

and

$$\left( \frac{a+b+c-d}{2}, \frac{-a+b+c+d}{2} \right).$$

- Suppose that $(a,b) = (0,0)$. Then $(c,d)$ may be any element of $P_n$ not contained in $P_0$. The number of such squares is $4n$.
- Suppose that $(a,b), (c,d) \in Q_k$ for some $k$. There is one such square with vertices

  $$\{(0, 2^k), (0, 2^{-k}), (2^k, 0), (2^{-k}, 0)\}$$

  for $k = 0, \dots, \lfloor \frac{n}{2} \rfloor$, for a total of $\lfloor \frac{n}{2} \rfloor + 1$. To show that there are no others, by symmetry it suffices to rule out the existence of a square with opposite vertices $(a,0)$ and $(c,0)$ where $a > |c|$. The other two vertices of this square would be $((a+c)/2, (a-c)/2)$ and $((a+c)/2, (-a+c)/2)$. These cannot belong to any $Q_k$, or be equal to $(0,0)$, because $|a+c|, |a-c| \geq a - |c| > 0$ by the triangle inequality. These also cannot belong to any $R_k$ because $(a+|c|)/2 > (a-|c|)/2$. (One can also phrase this argument in geometric terms.)
- Suppose that $(a,b), (c,d) \in R_k$ for some $k$. There is one such square with vertices

  $$\{(2^k, 2^k), (2^k, -2^k), (-2^k, 2^k), (-2^k, -2^k)\}$$

  for $k = 0, \dots, \lfloor \frac{n-1}{2} \rfloor$, for a total of $\lfloor \frac{n+1}{2} \rfloor$. To show that there are no others, we may reduce to the previous case: rotating by an angle of $\frac{\pi}{4}$ and then rescaling by a factor of $\sqrt{2}$ would yield a square with two opposite vertices in some $Q_k$ not centered at $(0,0)$, which we have already ruled out.

– It remains to show that we cannot have $(a,b) \in Q_k$ and $(c,d) \in R_k$ for some $k$. By symmetry, we may reduce to the case where $(a,b) = (0,2^k)$ and $(c,d) = (2^\ell, \pm 2^\ell)$. If $d > 0$, then the third vertex $(2^{k-1}, 2^{k-1}+2^\ell)$ is impossible. If $d < 0$, then the third vertex $(-2^{k-1}, 2^{k-1}-2^\ell)$ is impossible.

Summing up, we obtain

$$4n + \left\lfloor \frac{n}{2} \right\rfloor + 1 + \left\lfloor \frac{n+1}{2} \right\rfloor = 5n+1$$

squares, proving the claim.

**Remark.** Given the computation of $P_n$, we can alternatively show that the number of squares with vertices in $P_n$ is $5n+1$ as follows. Since this is clearly true for $n=1$, it suffices to show that for $n \geq 2$, there are exactly 5 squares with vertices in $P_n$, at least one of which is not in $P_{n-1}$. Note that the convex hull of $P_n$ is a square $S$ whose four vertices are the four points in $P_n \setminus P_{n-1}$. If $v$ is one of these points, then a square with a vertex at $v$ can only lie in $S$ if its two sides containing $v$ are in line with the two sides of $S$ containing $v$. It follows that there are exactly two squares with a vertex at $v$ and all vertices in $P_n$: the square corresponding to $S$ itself, and a square whose vertex diagonally opposite to $v$ is the origin. Taking the union over the four points in $P_n \setminus P_{n-1}$ gives a total of 5 squares, as desired.

B2 The answer is $\frac{8}{\pi^3}$.

**Solution 1.** By the double angle and sum-product identities for cosine, we have

$$\begin{aligned}2\cos^2\left(\frac{(k-1)\pi}{2n}\right) - 2\cos^2\left(\frac{k\pi}{2n}\right) &= \cos\left(\frac{(k-1)\pi}{n}\right) - \cos\left(\frac{k\pi}{n}\right) \\ &= 2\sin\left(\frac{(2k-1)\pi}{2n}\right)\sin\left(\frac{\pi}{2n}\right),\end{aligned}$$

and it follows that the summand in $a_n$ can be written as

$$\frac{1}{\sin\left(\frac{\pi}{2n}\right)}\left(-\frac{1}{\cos^2\left(\frac{(k-1)\pi}{2n}\right)} + \frac{1}{\cos^2\left(\frac{k\pi}{2n}\right)}\right).$$

Thus the sum telescopes and we find that

$$a_n = \frac{1}{\sin\left(\frac{\pi}{2n}\right)}\left(-1 + \frac{1}{\cos^2\left(\frac{(n-1)\pi}{2n}\right)}\right) = -\frac{1}{\sin\left(\frac{\pi}{2n}\right)} + \frac{1}{\sin^3\left(\frac{\pi}{2n}\right)}.$$

Finally, since $\lim_{x\to 0} \frac{\sin x}{x} = 1$, we have $\lim_{n\to\infty}\left(n \sin \frac{\pi}{2n}\right) = \frac{\pi}{2}$, and thus $\lim_{n\to\infty} \frac{a_n}{n^3} = \frac{8}{\pi^3}$.

**Solution 2.** We first substitute $n-k$ for $k$ to obtain

$$a_n = \sum_{k=1}^{n-1} \frac{\sin\left(\frac{(2k+1)\pi}{2n}\right)}{\sin^2\left(\frac{(k+1)\pi}{2n}\right)\sin^2\left(\frac{k\pi}{2n}\right)}.$$

We then use the estimate

$$\frac{\sin x}{x} = 1 + O(x^2) \qquad (x \in [0,\pi])$$

to rewrite the summand as

$$\frac{\left(\frac{(2k-1)\pi}{2n}\right)}{\left(\frac{(k+1)\pi}{2n}\right)^2\left(\frac{k\pi}{2n}\right)^2}\left(1 + O\left(\frac{k^2}{n^2}\right)\right)$$

which simplifies to

$$\frac{8(2k-1)n^3}{k^2(k+1)^2\pi^3} + O\left(\frac{n}{k}\right).$$

Consequently,

$$\begin{aligned}\frac{a_n}{n^3} &= \sum_{k=1}^{n-1}\left(\frac{8(2k-1)}{k^2(k+1)^2\pi^3} + O\left(\frac{1}{kn^2}\right)\right) \\ &= \frac{8}{\pi^3}\sum_{k=1}^{n-1}\frac{(2k-1)}{k^2(k+1)^2} + O\left(\frac{\log n}{n^2}\right).\end{aligned}$$

Finally, note that

$$\sum_{k=1}^{n-1}\frac{(2k-1)}{k^2(k+1)^2} = \sum_{k=1}^{n-1}\left(\frac{1}{k^2} - \frac{1}{(k+1)^2}\right) = 1 - \frac{1}{n^2}$$

converges to 1, and so $\lim_{n\to\infty}\frac{a_n}{n^3} = \frac{8}{\pi^3}$.

B3 **Solution 1.** We first note that $P$ corresponds to the linear transformation on $\mathbb{R}^n$ given by reflection in the hyperplane perpendicular to $u$: $P(u) = -u$, and for any $v$ with $\langle u,v\rangle = 0$, $P(v) = v$. In particular, $P$ is an orthogonal matrix of determinant $-1$.

We next claim that if $Q$ is an $n \times n$ orthogonal matrix that does not have 1 as an eigenvalue, then $\det Q = (-1)^n$. To see this, recall that the roots of the characteristic polynomial $p(t) = \det(tI - Q)$ all lie on the unit circle in $\mathbb{C}$, and all non-real roots occur in conjugate pairs ($p(t)$ has real coefficients, and orthogonality implies that $p(t) = \pm t^n p(t^{-1})$). The product of each conjugate pair of roots is 1; thus $\det Q = (-1)^k$ where $k$ is the multiplicity of $-1$ as a root of $p(t)$. Since 1 is not a root and all other roots appear in conjugate pairs, $k$ and $n$ have the same parity, and so $\det Q = (-1)^n$.

Finally, if neither of the orthogonal matrices $Q$ nor $PQ$ has 1 as an eigenvalue, then $\det Q = \det(PQ) = (-1)^n$, contradicting the fact that $\det P = -1$. The result follows.

**Remark.** It can be shown that any $n \times n$ orthogonal matrix $Q$ can be written as a product of at most $n$ hyperplane reflections (Householder matrices). If equality occurs, then $\det(Q) = (-1)^n$; if equality does not occur, then $Q$ has 1 as an eigenvalue. Consequently, equality fails for one of $Q$ and $PQ$, and that matrix has 1 as an eigenvalue.

Sucharit Sarkar suggests the following topological interpretation: an orthogonal matrix without 1 as an eigenvalue induces a fixed-point-free map from the $(n-1)$-sphere to itself, and the degree of such a map must be $(-1)^n$.

**Solution 2.** This solution uses the (reverse) *Cayley transform*: if $Q$ is an orthogonal matrix not having 1 as an eigenvalue, then

$$A = (I-Q)(I+Q)^{-1}$$

is a skew-symmetric matrix (that is, $A^T = -A$).

Suppose then that $Q$ does not have 1 as an eigenvalue. Let $V$ be the orthogonal complement of $u$ in $\mathbb{R}^n$. On one hand, for $v \in V$,

$$(I-Q)^{-1}(I-QP)v = (I-Q)^{-1}(I-Q)v = v.$$

On the other hand,

$$(I-Q)^{-1}(I-QP)u = (I-Q)^{-1}(I+Q)u = Au$$

and $\langle u, Au\rangle = \langle A^T u, u\rangle = \langle -Au, u\rangle$, so $Au \in V$. Put $w = (1-A)u$; then $(1-QP)w = 0$, so $QP$ has 1 as an eigenvalue, and the same for $PQ$ because $PQ$ and $QP$ have the same characteristic polynomial.

**Remark.** The *Cayley transform* is the following construction: if $A$ is a skew-symmetric matrix, then $I+A$ is invertible and

$$Q = (I-A)(I+A)^{-1}$$

is an orthogonal matrix.

**Remark.** (by Steven Klee) A related argument is to compute $\det(PQ-I)$ using the *matrix determinant lemma*: if $A$ is an invertible $n \times n$ matrix and $v, w$ are $1 \times n$ column vectors, then

$$\det(A + vw^T) = \det(A)(1 + w^T A^{-1} v).$$

This reduces to the case $A = I$, in which case it again comes down to the fact that the product of two square matrices (in this case, obtained from $v$ and $w$ by padding with zeroes) retains the same characteristic polynomial when the factors are reversed.

B4 **Solution 1.** We compute that $m(f) = 2\ln 2 - \frac{1}{2}$. Label the given differential equations by (1) and (2). If we write, e.g., $x\frac{\partial}{\partial x}(1)$ for the result of differentiating (1) by $x$ and multiplying the resulting equation by $x$, then the combination $x\frac{\partial}{\partial x}(1) + y\frac{\partial}{\partial y}(1) - (1) - (2)$ gives the equation $2xyf_{xy} = xy\ln(xy) + xy$, whence $f_{xy} = \frac{1}{2}(\ln(x) + \ln(y) + 1)$.

Now we observe that

$$\begin{aligned} &f(s+1,s+1) - f(s+1,s) - f(s,s+1) + f(s,s) \\ &= \int_s^{s+1}\int_s^{s+1} f_{xy}\,dy\,dx \\ &= \frac{1}{2}\int_s^{s+1}\int_s^{s+1} (\ln(x)+\ln(y)+1)\,dy\,dx \\ &= \frac{1}{2} + \int_s^{s+1} \ln(x)\,dx. \end{aligned}$$

Since $\ln(x)$ is increasing, $\int_s^{s+1}\ln(x)\,dx$ is an increasing function of $s$, and so it is minimized over $s \in [1,\infty)$ when $s = 1$. We conclude that

$$m(f) = \frac{1}{2} + \int_1^2 \ln(x)\,dx = 2\ln 2 - \frac{1}{2}$$

independent of $f$.

**Remark.** The phrasing of the question suggests that solvers were not expected to prove that $\mathscr{F}$ is nonempty, even though this is necessary to make the definition of $m(f)$ logically meaningful. Existence will be explicitly established in the next solution.

**Solution 2.** We first verify that

$$f(x,y) = \frac{1}{2}(xy\ln(xy) - xy)$$

is an element of $\mathscr{F}$, by computing that

$$\begin{aligned} xf_x = yf_y &= \frac{1}{2}xy\ln(xy) \\ x^2 f_{xx} = y^2 f_{yy} &= xy. \end{aligned}$$

(See the following remark for motivation for this guess.)

We next show that the only elements of $\mathscr{F}$ are $f + a\ln(x/y) + b$ where $a, b$ are constants. Suppose that $f+g$ is a second element of $\mathscr{F}$. As in the first solution, we deduce that $g_{xy} = 0$; this implies that $g(x,y) = u(x) + v(y)$ for some twice continuously differentiable functions $u$ and $v$. We also have $xg_x + yg_y = 0$, which now asserts that $xg_x = -yg_y$ is equal to some constant $a$. This yields that $g = a\ln(x/y) + b$ as desired.

We next observe that

$$g(s+1,s+1) - g(s+1,s) - g(s,s+1) + g(s,s) = 0,$$

so $m(f) = m(f+g)$. It thus remains to compute $m(f)$. To do this, we verify that

$$f(s+1,s+1) - f(s+1,s) - f(s,s+1) + f(s,s)$$

is nondecreasing in $s$ by computing its derivative to be $\ln(s+1) - \ln(s)$ (either directly or using the integral representation from the first solution). We thus minimize by taking $s = 1$ as in the first solution.

**Remark.** One way to make a correct guess for $f$ is to notice that the given equations are both symmetric in $x$ and $y$ and posit that $f$ should also be symmetric. Any symmetric function of $x$ and $y$ can be written in terms of the variables $u = x+y$ and $v = xy$, so in principle we could translate the equations into those variables and solve. However, before trying this, we observe that $xy$ appears explicitly in the equations, so it is reasonable to make a first guess of the form $f(x,y) = h(xy)$. For such a choice, we have

$$xf_x + yf_y = 2xyh' = xy\ln(xy)$$

which forces us to set $h(t) = \frac{1}{2}(t\ln(t) - t)$.

B5 **Solution 1.** We prove that $(j,k) = (2019,1010)$ is a valid solution. More generally, let $p(x)$ be the polynomial of degree $N$ such that $p(2n+1) = F_{2n+1}$ for $0 \leq n \leq N$. We will show that $p(2N+3) = F_{2N+3} - F_{N+2}$.

Define a sequence of polynomials $p_0(x),\dots,p_N(x)$ by $p_0(x) = p(x)$ and $p_k(x) = p_{k-1}(x) - p_{k-1}(x+2)$ for $k \geq 1$. Then by induction on $k$, it is the case that $p_k(2n+1) = F_{2n+1+k}$ for $0 \leq n \leq N-k$, and also that $p_k$ has degree (at most) $N-k$ for $k \geq 1$. Thus $p_N(x) = F_{N+1}$ since $p_N(1) = F_{N+1}$ and $p_N$ is constant.

We now claim that for $0 \leq k \leq N$, $p_{N-k}(2k+3) = \sum_{j=0}^k F_{N+1+j}$. We prove this again by induction on $k$: for the induction step, we have

$$\begin{aligned} p_{N-k}(2k+3) &= p_{N-k}(2k+1) + p_{N-k+1}(2k+1) \\ &= F_{N+1+k} + \sum_{j=0}^{k-1} F_{N+1+j}. \end{aligned}$$

Thus we have $p(2N+3) = p_0(2N+3) = \sum_{j=0}^N F_{N+1+j}$.

Now one final induction shows that $\sum_{j=1}^m F_j = F_{m+2} - 1$, and so $p(2N+3) = F_{2N+3} - F_{N+2}$, as claimed. In the case $N = 1008$, we thus have $p(2019) = F_{2019} - F_{1010}$.

**Solution 2.** This solution uses the *Lagrange interpolation formula*: given $x_0,\dots,x_n$ and $y_0,\dots,y_n$, the unique polynomial $P$ of degree at most $n$ satisfying $P(x_i) = y_i$ for $i = 0,\dots,n$ is

$$\sum_{i=0}^n P(x_i) \prod_{j \neq i} \frac{x - x_j}{x_i - x_j} =$$

Write

$$F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^{-n}), \qquad \alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}.$$

For $\gamma \in \mathbb{R}$, let $p_\gamma(x)$ be the unique polynomial of degree at most 1008 satisfying

$$p_1(2n+1) = \gamma^{2n+1}, p_2(2n+1) = \gamma^{2n+1}\ (n = 0,\dots,1008);$$

then $p(x) = \frac{1}{\sqrt{5}}(p_\alpha(x) - p_\beta(x))$.

By Lagrange interpolation,

$$\begin{aligned} p_\gamma(2019) &= \sum_{n=0}^{1008} \gamma^{2n+1} \prod_{0 \leq j \leq 1008, j \neq n} \frac{2019 - (2j+1)}{(2n+1) - (2j+1)} \\ &= \sum_{n=0}^{1008} \gamma^{2n+1} \prod_{0 \leq j \leq 1008, j \neq n} \frac{1009 - j}{n - j} \\ &= \sum_{n=0}^{1008} \gamma^{2n+1} (-1)^{1008-n} \binom{1009}{n} \\ &= -\gamma((\gamma^2 - 1)^{1009} - (\gamma^2)^{1009}). \end{aligned}$$

For $\gamma \in \{\alpha, \beta\}$ we have $\gamma^2 = \gamma + 1$ and so

$$p_\gamma(2019) = \gamma^{2019} - \gamma^{1010}.$$

We thus deduce that $p(x) = F_{2019} - F_{1010}$ as claimed.

**Remark.** Karl Mahlburg suggests the following variant of this. As above, use Lagrange interpolation to write

$$p(2019) = \sum_{j=0}^{1008} \binom{1009}{j} F_j;$$

it will thus suffice to verify (by substiting $j \mapsto 1009 - j$) that

$$\sum_{j=0}^{1009} \binom{1009}{j} F_{j+1} = F_{2019}.$$

This identity has the following combinatorial interpretation. Recall that $F_{n+1}$ counts the number of ways to tile a $1 \times n$ rectangle with $1 \times 1$ squares and $1 \times 2$ dominoes (see below). In any such tiling with $n = 2018$, let $j$ be the number of squares among the first 1009 tiles. These can be ordered in $\binom{1009}{j}$ ways, and the remaining $2018 - j - 2(1009 - j) = j$ squares can be tiled in $F_{j+1}$ ways.

As an aside, this interpretation of $F_{n+1}$ is the oldest known interpretation of the Fibonacci sequence, long predating Fibonacci himself. In ancient Sanskrit, syllables were classified as long or short, and a long syllable was considered to be twice as long as a short syllable; consequently, the number of syllable patterns of total length $n$ equals $F_{n+1}$.

**Remark.** It is not difficult to show that the solution $(j,k) = (2019,2010)$ is unique (in positive integers). First, note that to have $F_j - F_k > 0$, we must have $k < j$. If $j < 2019$, then

$$F_{2019} - F_{1010} = F_{2018} + F_{2017} - F_{1010} > F_j > F_j - F_k.$$

If $j > 2020$, then

$$F_j - F_k \geq F_j - F_{j-1} = F_{j-2} \geq F_{2019} > F_{2019} - F_{1010}.$$

Since $j = 2019$ obviously forces $k = 1010$, the only other possible solution would be with $j = 2020$. But then

$$(F_j - F_k) - (F_{2019} - F_{1010}) = (F_{2018} - F_k) + F_{1010}$$

which is negative for $k = 2019$ (it equals $F_{1010} - F_{2017}$) and positive for $k \leq 2018$.

B6 Such a set exists for every $n$. To construct an example, define the function $f : \mathbb{Z}^n \to \mathbb{Z}/(2n+1)\mathbb{Z}$ by

$$f(x_1,\dots,x_n) = x_1 + 2x_2 + \cdots + nx_n \pmod{2n+1},$$

then let $S$ be the preimage of 0.

To check condition (1), note that if $p \in S$ and $q$ is a neighbor of $p$ differing only in coordinate $i$, then

$$f(q) = f(p) \pm i \equiv \pm i \pmod{2n+1}$$

and so $q \notin S$.

To check condition (2), note that if $p \in \mathbb{Z}^n$ is not in $S$, then there exists a unique choice of $i \in \{1, \dots, n\}$ such that $f(p)$ is congruent to one of $+i$ or $-i$ modulo $2n+1$. The unique neighbor $q$ of $p$ in $S$ is then obtained by either subtracting 1 from, or adding 1 to, the $i$-th coordinate of $p$.

**Remark.** According to Art of Problem Solving (thread c6h366290), this problem was a 1985 IMO submission from Czechoslovakia. For an application to steganography, see: J. Fridrich and P. Lisoněk, Grid colorings in steganography, *IEEE Transactions on Information Theory* **53** (2007), 1547–1549.

# The 81st William Lowell Putnam Mathematical Competition
# Saturday, February 20, 2021

A1 How many positive integers $N$ satisfy all of the following three conditions?

(i) $N$ is divisible by 2020.

(ii) $N$ has at most 2020 decimal digits.

(iii) The decimal digits of $N$ are a string of consecutive ones followed by a string of consecutive zeros.

A2 Let $k$ be a nonnegative integer. Evaluate

$$\sum_{j=0}^{k} 2^{k-j}\binom{k+j}{j}.$$

A3 Let $a_0 = \pi/2$, and let $a_n = \sin(a_{n-1})$ for $n \geq 1$. Determine whether

$$\sum_{n=1}^{\infty} a_n^2$$

converges.

A4 Consider a horizontal strip of $N+2$ squares in which the first and the last square are black and the remaining $N$ squares are all white. Choose a white square uniformly at random, choose one of its two neighbors with equal probability, and color this neighboring square black if it is not already black. Repeat this process until all the remaining white squares have only black neighbors. Let $w(N)$ be the expected number of white squares remaining. Find

$$\lim_{N\to\infty} \frac{w(N)}{N}.$$

A5 Let $a_n$ be the number of sets $S$ of positive integers for which

$$\sum_{k\in S} F_k = n,$$

where the Fibonacci sequence $(F_k)_{k\geq 1}$ satisfies $F_{k+2} = F_{k+1} + F_k$ and begins $F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3$. Find the largest integer $n$ such that $a_n = 2020$.

A6 For a positive integer $N$, let $f_N$[1] be the function defined by

$$f_N(x) = \sum_{n=0}^{N} \frac{N+1/2-n}{(N+1)(2n+1)} \sin((2n+1)x).$$

Determine the smallest constant $M$ such that $f_N(x) \leq M$ for all $N$ and all real $x$.

[1] Corrected from $F_N$ in the source.

B1 For a positive integer $n$, define $d(n)$ to be the sum of the digits of $n$ when written in binary (for example, $d(13) = 1+1+0+1 = 3$). Let

$$S = \sum_{k=1}^{2020} (-1)^{d(k)} k^3.$$

Determine $S$ modulo 2020.

B2 Let $k$ and $n$ be integers with $1 \leq k < n$. Alice and Bob play a game with $k$ pegs in a line of $n$ holes. At the beginning of the game, the pegs occupy the $k$ leftmost holes. A legal move consists of moving a single peg to any vacant hole that is further to the right. The players alternate moves, with Alice playing first. The game ends when the pegs are in the $k$ rightmost holes, so whoever is next to play cannot move and therefore loses. For what values of $n$ and $k$ does Alice have a winning strategy?

B3 Let $x_0 = 1$, and let $\delta$ be some constant satisfying $0 < \delta < 1$. Iteratively, for $n = 0, 1, 2, \ldots$, a point $x_{n+1}$ is chosen uniformly from the interval $[0, x_n]$. Let $Z$ be the smallest value of $n$ for which $x_n < \delta$. Find the expected value of $Z$, as a function of $\delta$.

B4 Let $n$ be a positive integer, and let $V_n$ be the set of integer $(2n+1)$-tuples $\mathbf{v} = (s_0, s_1, \cdots, s_{2n-1}, s_{2n})$ for which $s_0 = s_{2n} = 0$ and $|s_j - s_{j-1}| = 1$ for $j = 1, 2, \cdots, 2n$. Define

$$q(\mathbf{v}) = 1 + \sum_{j=1}^{2n-1} 3^{s_j},$$

and let $M(n)$ be the average of $\frac{1}{q(\mathbf{v})}$ over all $\mathbf{v} \in V_n$. Evaluate $M(2020)$.

B5 For $j \in \{1,2,3,4\}$, let $z_j$ be a complex number with $|z_j| = 1$ and $z_j \neq 1$. Prove that

$$3 - z_1 - z_2 - z_3 - z_4 + z_1 z_2 z_3 z_4 \neq 0.$$

B6 Let $n$ be a positive integer. Prove that

$$\sum_{k=1}^{n} (-1)^{\lfloor k(\sqrt{2}-1)\rfloor} \geq 0.$$

(As usual, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to $x$.)

# Solutions to the 81st William Lowell Putnam Mathematical Competition
# Saturday, February 20, 2021

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A1 The values of $N$ that satisfy (ii) and (iii) are precisely the numbers of the form $N = (10^a - 10^b)/9$ for $0 \leq b < a \leq 2020$; this expression represents the integer with $a$ digits beginning with a string of 1's and ending with $b$ 0's. A value $N$ of this form is divisible by $2020 = 2^2 \cdot 5 \cdot 101$ if and only if $10^b(10^{a-b}-1)$ is divisible by each of $3^2$, $2^2 \cdot 5$, and 101. Divisibility by $3^2$ is a trivial condition since $10 \equiv 1 \pmod 9$. Since $10^{a-b}-1$ is odd, divisibility by $2^2 \cdot 5$ occurs if and only if $b \geq 2$. Finally, since $10^2 \equiv -1 \pmod{101}$, we see that $10^{a-b}$ is congruent to 10, $-1$, $-10$, or $1 \pmod{101}$ depending on whether $a-b$ is congruent to 1, 2, 3, or $0 \pmod 4$; thus $10^{a-b}-1$ is divisible by 101 if and only if $a-b$ is divisible by 4.

It follows that we need to count the number of $(a,b)$ with $2 \leq b < a \leq 2020$ with $4 \,|\, a-b$. For given $b$, there are $\lfloor \frac{2020-b}{4} \rfloor$ possible values of $a$. Thus the answer is

$$\begin{aligned}&504+504+504+503+503+503+503+\cdots+1+1+1+1 \\ &\quad = 4(504+503+\cdots+1)-504 = 504\cdot 1009 = 508536.\end{aligned}$$

A2 The answer is $4^k$.

**First solution.** Let $S_k$ denote the given sum. Then, with the convention that $\binom{n}{-1} = 0$ for any $n \geq 0$, we have for $k \geq 1$,

$$\begin{aligned}S_k &= \sum_{j=0}^k 2^{k-j}\left[\binom{k-1+j}{j} + \binom{k-1+j}{j-1}\right] \\ &= 2\sum_{j=0}^{k-1} 2^{k-1-j}\binom{k-1+j}{j} + \binom{2k-1}{k} + \sum_{j=1}^k 2^{k-j}\binom{k-1+j}{j-1} \\ &= 2S_{k-1} + \binom{2k-1}{k} + \sum_{j=0}^{k-1} 2^{k-j-1}\binom{k+j}{j} \\ &= 2S_{k-1} + S_k/2\end{aligned}$$

and so $S_k = 4S_{k-1}$. Since $S_0 = 1$, it follows that $S_k = 4^k$ for all $k$.

**Second solution.** Consider a sequence of fair coin flips $a_1, a_2, \dots$ and define the random variable $X$ to be the index of the $(k+1)$-st occurrence of heads. Then

$$P[X=n] = \binom{n-1}{k}2^{-n};$$

writing $n = k+j+1$, we may thus rewrite the given sum as

$$2^{2k+1}P[X \leq 2k+1].$$

It now suffices to observe that $P[X \leq 2k+1] = \frac{1}{2}$: we have $X \leq 2k+1$ if and only if there are at least $k+1$ heads among the first $2k+1$ flips, and there are exactly as many outcomes with at most $k$ heads.

**Third solution.** (by Pankaj Sinha) The sum in question in the coefficient of $x^k$ in the formal power series

$$\begin{aligned}\sum_{j=0}^k 2^{k-j}(1+x)^{k+j} &= 2^k(1+x)^k\sum_{j=0}^k 2^{-j}(1+x)^j \\ &= 2^k(1+x)^k\frac{1-(1+x)^{k+1}/2^{k+1}}{1-(1+x)/2} \\ &= \frac{2^{k+1}(1+x)^k - (1+x)^{2k+1}}{1-x} \\ &= (2^{k+1}(1+x)^k - (1+x)^{2k+1})(1+x+\cdots).\end{aligned}$$

This evidently equals

$$\begin{aligned}2^{k+1}\sum_{j=0}^k\binom{k}{j} - \sum_{j=0}^k\binom{2k+1}{j} &= 2^{k+1}(2^k) - \frac{1}{2}2^{2k+1} \\ &= 2^{2k+1} - 2^{2k} = 2^{2k} = 4^k.\end{aligned}$$

**Remark.** This sum belongs to a general class that can be evaluated mechanically using the *WZ method*. See for example the book $A = B$ by Petvoksek–Wilf–Zeilberger.

A3 The series diverges. First note that since $\sin(x) < x$ for all $x > 0$, the sequence $\{a_n\}$ is positive and decreasing, with $a_1 = 1$. Next, we observe that for $x \in [0,1]$, $\sin(x) \geq x - x^3/6$: this follows from Taylor's theorem with remainder, since $\sin(x) = x - x^3/6 + (\sin c)x^4/24$ for some $c$ between 0 and $x$.

We now claim that $a_n \geq 1/\sqrt{n}$ for all $n \geq 1$; it follows that $\sum a_n^2$ diverges since $\sum 1/n$ diverges. To prove the claim, we induct on $n$, with $n = 1$ being trivial. Suppose that $a_n \geq 1/\sqrt{n}$. To prove $\sin(a_n) \geq 1/\sqrt{n+1}$, note that since $\sin(a_n) \geq \sin(1/\sqrt{n})$, it suffices to prove that $x - x^3/6 \geq (n+1)^{-1/2}$ where $x = 1/\sqrt{n}$. Squaring both sides and clearing denominators, we find that this is equivalent to $(n+1)(6n-1)^2 \geq 36n^3$, or $24n^2 - 11n + 1 \geq 0$. But this last inequality is true since $24n^2 - 11n + 1 = (3n-1)(8n-1)$, and the induction is complete.

A4 The answer is $1/e$. We first establish a recurrence for $w(N)$. Number the squares 1 to $N+2$ from left to right. There are $2(N-1)$ equally likely events leading to the first new square being colored black: either we choose one of squares $3, \dots, N+1$ and color the square to its left, or we choose one of squares $2, \dots, N$ and color the square to its right. Thus the probability of square $i$ being the first new square colored black is $\frac{1}{2(N-1)}$ if $i=2$ or $i=N+1$ and $\frac{1}{N-1}$ if $3 \leq i \leq N$. Once we have changed the first square $i$ from white to black, then the strip divides into two separate systems, squares 1 through $i$ and squares $i$ through $N+2$, each with first and last square black and the rest white, and we can view the remaining process as continuing independently for each system. Thus if square $i$ is the first square to change color, the expected number of white squares at the end of the process is $w(i-2)+w(N+1-i)$. It follows that

$$\begin{aligned} w(N) = \frac{1}{2(N-1)}&(w(0)+w(N-1))+ \\ &\frac{1}{N-1}\left(\sum_{i=3}^{N}(w(i-2)+w(N+1-i))\right) \\ &+\frac{1}{2(N-1)}(w(N-1)+w(0)) \end{aligned}$$

and so

$$(N-1)w(N) = 2(w(1)+\cdots+w(N-2))+w(N-1).$$

If we replace $N$ by $N-1$ in this equation and subtract from the original equation, then we obtain the recurrence

$$w(N) = w(N-1)+\frac{w(N-2)}{N-1}.$$

We now claim that $w(N) = (N+1)\sum_{k=0}^{N+1}\frac{(-1)^k}{k!}$ for $N \geq 0$. To prove this, we induct on $N$. The formula holds for $N=0$ and $N=1$ by inspection: $w(0)=0$ and $w(1)=1$. Now suppose that $N \geq 2$ and $w(N-1) = N\sum_{k=0}^{N}\frac{(-1)^k}{k!}$, $w(N-2) = (N-1)\sum_{k=0}^{N-1}\frac{(-1)^k}{k!}$. Then

$$\begin{aligned} w(N) &= w(N-1)+\frac{w(N-2)}{N-1} \\ &= N\sum_{k=0}^{N}\frac{(-1)^k}{k!}+\sum_{k=0}^{N-1}\frac{(-1)^k}{k!} \\ &= (N+1)\sum_{k=0}^{N-1}\frac{(-1)^k}{k!}+\frac{N(-1)^N}{N!} \\ &= (N+1)\sum_{k=0}^{N+1}\frac{(-1)^k}{k!} \end{aligned}$$

and the induction is complete.

Finally, we compute that

$$\begin{aligned} \lim_{N\to\infty}\frac{w(N)}{N} &= \lim_{N\to\infty}\frac{w(N)}{N+1} \\ &= \sum_{k=0}^{\infty}\frac{(-1)^k}{k!} = \frac{1}{e}. \end{aligned}$$

**Remark.** AoPS user pieater314159 suggests the following alternate description of $w(N)$. Consider the numbers $\{1,\dots,N+1\}$ all originally colored white. Choose a permutation $\pi \in S_{N+1}$ uniformly at random. For $i=1,\dots,N+1$ in succession, color $\pi(i)$ black in case $\pi(i+1)$ is currently white (regarding $i+1$ modulo $N+1$). After this, the expected number of white squares remaining is $w(N)$.

**Remark.** Andrew Bernoff reports that this problem was inspired by a similar question of Jordan Ellenberg (disseminated via Twitter), which in turn was inspired by the final question of the 2017 MATHCOUNTS competition. See `http://bit-player.org/2017/counting-your-chickens-before-theyre-pecked` for more discussion.

A5 The answer is $n = F_{4040}-1$. In both solutions, we use freely the identity

$$F_1+F_2+\cdots+F_{m-2} = F_m-1 \qquad (1)$$

which follows by a straightforward induction on $m$. We also use the directly computed values

$$a_1 = a_2 = 2, a_3 = a_4 = 3. \qquad (2)$$

**First solution.** (by George Gilbert)

We extend the definition of $a_n$ by setting $a_0 = 1$.

**Lemma 1.** *For $m > 0$ and $F_m \leq n < F_{m+1}$,*

$$a_n = a_{n-F_m}+a_{F_{m+1}-n-1}. \qquad (3)$$

*Proof.* Consider a set $S$ for which $\sum_{k\in S}F_k = n$. If $m \in S$ then $S\setminus\{m\}$ gives a representation of $n-F_m$, and this construction is reversible because $n-F_m < F_{m-1} \leq F_m$. If $m \notin S$, then $\{1,\dots,m-1\}\setminus S$ gives a representation of $F_{m+1}-n-1$, and this construction is also reversible. This implies the desired equality. □

**Lemma 2.** *For $m \geq 2$,*

$$a_{F_m} = a_{F_{m+1}-1} = \left\lfloor\frac{m+2}{2}\right\rfloor.$$

*Proof.* By (2), this holds for $m = 2,3,4$. We now proceed by induction; for $m \geq 5$, given all preceding cases, we have by Lemma 1 that

$$\begin{aligned} a_{F_m} &= a_0+a_{F_{m-1}-1} = 1+\left\lfloor\frac{m}{2}\right\rfloor = \left\lfloor\frac{m+2}{2}\right\rfloor \\ a_{F_{m+1}-1} &= a_{F_{m-1}-1}+a_0 = a_{F_m}. \end{aligned}$$ □

Using Lemma 2, we see that $a_n = 2020$ for $n = F_{4040}-1$.

**Lemma 3.** *For $F_m \leq n < F_{m+1}$, $a_n \geq a_{F_m}$.*

*Proof.* We again induct on $m$. By Lemma 2, we may assume that

$$1 \leq n-F_m \leq (F_{m+1}-2)-F_m = F_{m-1}-2. \qquad (4)$$

By (2), we may also assume $n \geq 6$, so that $m \geq 5$. We apply Lemma 1, keeping in mind that

$$(n - F_m) + (F_{m+1} - n - 1) = F_{m-1} - 1.$$

If $\max\{n - F_m, F_{m+1} - n - 1\} \geq F_{m-2}$, then one of the summands in (5) is at least $a_{F_{m-2}}$ (by the induction hypothesis) and the other is at least 2 (by (4) and the induction hypothesis), so

$$a_n \geq a_{F_{m-2}} + 2 = \left\lfloor \frac{m+4}{2} \right\rfloor.$$

Otherwise, $\min\{n - F_m, F_{m+1} - n - 1\} \geq F_{m-3}$ and so by the induction hypothesis again,

$$a_n \geq 2a_{F_{m-3}} = 2\left\lfloor \frac{m-1}{2} \right\rfloor \geq 2\frac{m-2}{2} \geq \left\lfloor \frac{m+2}{2} \right\rfloor. \qquad \square$$

Combining Lemma 2 and Lemma 3, we deduce that for $n > F_{4040} - 1$, we have $a_n \geq a_{F_{4040}} = 2021$. This completes the proof.

**Second solution.** We again start with a computation of some special values of $a_n$.

**Lemma 1.** *For all $m \geq 1$,*

$$a_{F_m - 1} = \left\lfloor \frac{m+1}{2} \right\rfloor$$

*Proof.* We proceed by induction on $m$. The result holds for $m = 1$ and $m = 2$ by (2). For $m > 2$, among the sets $S$ counted by $a_{F_m - 1}$, by (1) the only one not containing $m - 1$ is $S = \{1, 2, \ldots, m-2\}$, and there are $a_{F_m - F_{m-1} - 1}$ others. Therefore,

$$\begin{aligned} a_{F_m - 1} &= a_{F_m - F_{m-1} - 1} + 1 \\ &= a_{F_{m-2} - 1} + 1 = \left\lfloor \frac{m-1}{2} \right\rfloor + 1 = \left\lfloor \frac{m+1}{2} \right\rfloor. \qquad \square \end{aligned}$$

Given an arbitrary positive integer $n$, define the set $S_0$ as follows: start with the largest $k_1$ for which $F_{k_1} \leq n$, then add the largest $k_2$ for which $F_{k_1} + F_{k_2} \leq n$, and so on, stopping once $\sum_{k \in S_0} F_k = n$. Then form the bitstring

$$s_n = \cdots e_1 e_0, \qquad e_k = \begin{cases} 1 & k \in S_0 \\ 0 & k \notin S_0; \end{cases}$$

note that no two 1s in this string are consecutive. We can thus divide $s_n$ into segments

$$t_{k_1, \ell_1} \cdots t_{k_r, \ell_r} \qquad (k_i, \ell_i \geq 1)$$

where the bitstring $t_{k,\ell}$ is given by

$$t_{k,\ell} = (10)^k (0)^\ell$$

(that is, $k$ repetitions of 10 followed by $\ell$ repetitions of 0). Note that $\ell_r \geq 1$ because $e_1 = e_0 = 0$.

For $a = 1, \ldots, k$ and $b = 0, \ldots, \lfloor (\ell - 1)/2 \rfloor$, we can replace $t_{k,\ell}$ with the string of the same length

$$(10)^{k-a}(0)(1)^{2a-1}(01)^b 10^{\ell - 2b}$$

to obtain a new bitstring corresponding to a set $S$ with $\sum_{k \in S} F_k = n$. Consequently,

$$a_n \geq \prod_{i=1}^{r} \left(1 + k_i \left\lfloor \frac{\ell_i + 1}{2} \right\rfloor \right). \qquad (5)$$

For integers $k, \ell \geq 1$, we have

$$1 + k\left\lfloor \frac{\ell+1}{2} \right\rfloor \geq k + \left\lfloor \frac{\ell+1}{2} \right\rfloor \geq 2.$$

Combining this with repeated use of the inequality

$$xy \geq x + y \qquad (x, y \geq 2),$$

we deduce that

$$a_n \geq \sum_{i=1}^{r} \left(k_i + \left\lfloor \frac{\ell_i + 1}{2} \right\rfloor \right) \geq \left\lfloor \frac{1 + \sum_{i=1}^{r} (2k_i + \ell_i)}{2} \right\rfloor.$$

In particular, for any even $m \geq 2$, we have $a_n > \frac{m}{2}$ for all $n \geq F_m$. Taking $m = 4040$ yields the desired result.

**Remark.** It can be shown with a bit more work that the set $S_0$ gives the unique representation of $n$ as a sum of distinct Virahanka–Fibonacci numbers, no two consecutive; this is commonly called the *Zeckendorf representation* of $n$, but was first described by Lekkerkerker. Using this property, one can show that the lower bound in (5) is sharp.

A6 The smallest constant $M$ is $\pi/4$.

We start from the expression

$$f_N(x) = \sum_{n=0}^{N} \frac{1}{2} \left( \frac{2}{2n+1} - \frac{1}{N+1} \right) \sin((2n+1)x). \qquad (6)$$

Note that if $\sin(x) > 0$, then

$$\begin{aligned} \sum_{n=0}^{N} \sin((2n+1)x) &= \frac{1}{2i} \sum_{n=0}^{N} (e^{i(2n+1)x} - e^{-i(2n+1)x}) \\ &= \frac{1}{2i} \left( \frac{e^{i(2N+3)x} - e^{ix}}{e^{2ix} - 1} - \frac{e^{-i(2N+3)x} - e^{-ix}}{e^{-2ix} - 1} \right) \\ &= \frac{1}{2i} \left( \frac{e^{i(2N+2)x} - 1}{e^{ix} - e^{-ix}} - \frac{e^{-i(2N+2)x} - 1}{e^{-ix} - e^{ix}} \right) \\ &= \frac{1}{2i} \frac{e^{i(2N+2)x} + e^{-i(2N+2)x} - 2}{e^{ix} - e^{-ix}} \\ &= \frac{2\cos((2N+2)x) - 2}{2i(2i\sin(x))} \\ &= \frac{1 - \cos((2N+2)x)}{2\sin(x)} \geq 0. \end{aligned}$$

We use this to compare the expressions of $f_N(x)$ and $f_{N+1}(x)$ given by (6). For $x \in (0,\pi)$ with $\sin((2N+3)x) \geq 0$, we may omit the summand $n = N+1$ from $f_{N+1}(x)$ to obtain

$$\begin{aligned} &f_{N+1}(x) - f_N(x) \\ &\geq \frac{1}{2}\left(\frac{1}{N+1} - \frac{1}{N+2}\right)\sum_{n=0}^{N} \sin((2n+1)x) \geq 0. \end{aligned}$$

For $x \in (0,\pi)$ with $\sin((2N+3)x) \leq 0$, we may insert the summand $n = N+1$ into $f_{N+1}(x)$ to obtain

$$\begin{aligned} &f_{N+1}(x) - f_N(x) \\ &\geq \frac{1}{2}\left(\frac{1}{N+1} - \frac{1}{N+2}\right)\sum_{n=0}^{N+1} \sin((2n+1)x) \geq 0. \end{aligned}$$

In either case, we deduce that for $x \in (0,\pi)$, the sequence $\{f_N(x)\}_N$ is nondecreasing.

Now rewrite (6) as

$$f_N(x) = \sum_{n=0}^{N} \frac{\sin((2n+1)x)}{2n+1} - \frac{1-\cos((2N+2)x)}{4(N+1)\sin(x)} \qquad (7)$$

and note that the last term tends to 0 as $N \to \infty$. Consequently, $\lim_{N\to\infty} f_N(x)$ equals the sum of the series

$$\sum_{n=0}^{\infty} \frac{1}{2n+1}\sin((2n+1)x),$$

which is the Fourier series for the "square wave" function defined on $(-\pi,\pi]$ by

$$x \mapsto \begin{cases} -\frac{\pi}{4} & x \in (-\pi,0) \\ \frac{\pi}{4} & x \in (0,\pi) \\ 0 & x = 0,\pi \end{cases}$$

and extended periodically. Since this function is continuous on $(0,\pi)$, we deduce that the Fourier series converges to the value of the function; that is,

$$\lim_{N\to\infty} f_N(x) = \frac{\pi}{4} \qquad (x \in (0,\pi)).$$

This is enough to deduce the desired result as follows. Since

$$f_N(x+2\pi) = f_N(x), \qquad f_N(-x) = -f_N(x),$$

it suffices to check the bound $f_N(x) \leq \pi$ for $x \in (-\pi,\pi]$. For $x = 0,\pi$ we have $f_N(x) = 0$ for all $N$. For $x \in (-\pi,0)$, the previous arguments imply that

$$0 \geq f_0(x) \geq f_1(x) \geq \cdots$$

For $x \in (0,\pi)$, the previous arguments imply that

$$0 \leq f_0(x) \leq f_1(x) \leq \cdots \leq \frac{\pi}{4}$$

and the limit is equal to $\pi/4$. We conclude that $f_N(x) \leq M$ holds for $M = \pi/4$ but not for any smaller $M$, as desired.

**Remark.** It is also possible to replace the use of the convergence of the Fourier series with a more direct argument; it is sufficient to do this for $x$ in a dense subset of $(0,\pi)$, such as the rational multiples of $\pi$.

Another alternative (described at `https://how-did-i-get-here.com/2020-putnam-a6/`) is to deduce from (7) and a second geometric series computation (omitted here) that

$$\begin{aligned} f_N'(x) &= \sum_{n=0}^{N} \cos((2n+1)x) - \frac{d}{dx}\left(\frac{1-\cos((2N+2)x)}{4(N+1)\sin(x)}\right) \\ &= \frac{\sin((2N+2)x)}{2\sin(x)} \\ &\quad - \frac{(2N+2)\sin((2N+2)x) - \cos(x)(1-\cos((N+2)x)}{4(N+1)\sin(x)^2} \\ &= \frac{\cos(x)(1-\cos((N+2)x)}{4(N+1)\sin(x)^2}, \end{aligned}$$

which is nonnegative for $x \in (0,\pi/2]$ and nonpositive for $x \in [\pi/2,\pi)$. This implies that $f_N(x)$ always has a global maximum at $x = \pi/2$, so it suffices to check the convergence of the Fourier series for the square wave at that point. This reduces to the Madhava–Gregory–Newton series evaluation

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \arctan(1) = \frac{\pi}{4}.$$

B1 Note that

$$(1-x)(1-x^2)(1-x^4)\cdots(1-x^{1024}) = \sum_{k=0}^{2047} (-1)^{d(k)} x^k$$

and

$$x^{2016}(1-x)(1-x^2)\cdots(1-x^{16}) = \sum_{k=2016}^{2047} (-1)^{d(k)} x^k.$$

Applying $x\frac{d}{dx}$ to both sides of each of these two equations three times, and then setting $x = 1$, shows that

$$\sum_{k=0}^{2047} (-1)^{d(k)} k^3 = \sum_{k=2016}^{2047} (-1)^{d(k)} k^3 = 0,$$

and therefore

$$\sum_{k=1}^{2015} (-1)^{d(k)} k^3 = 0.$$

Hence we may write

$$\begin{aligned}
S &= \sum_{k=2016}^{2020} (-1)^{d(k)} k^3 \\
&= \sum_{k=0}^{4} (-1)^{d(k)} (k+2016)^3 \\
&\equiv (-4)^3 + (-1)(-3)^3 + (-1)(-2)^3 + (1)(-1)^3 \\
&= -64 + 27 + 8 - 1 \\
&\equiv -30 \equiv 1990 \pmod{2020}.
\end{aligned}$$

**Remark.** The function $d(n)$ appears in the OEIS as sequence A000120.

B2 We refer to this two-player game, with $n$ holes and $k$ pegs, as the $(n,k)$-*game*. We will show that Alice has a winning strategy for the $(n,k)$-game if and only if at least one of $n$ and $k$ is odd; otherwise Bob has a winning strategy.

We reduce the first claim to the second as follows. If $n$ and $k$ are both odd, then Alice can move the $k$-th peg to the last hole; this renders the last hole, and the peg in it, totally out of play, thus reducing the $(n,k)$-game to the $(n-1,k-1)$-game, for which Alice now has a winning strategy by the second claim. Similarly, if $n$ is odd but $k$ is even, then Alice may move the first peg to the $(k+1)$-st hole, removing the first hole from play and reducing the $(n,k)$-game to the $(n-1,k)$ game. Finally, if $n$ is even but $k$ is odd, then Alice can move the first peg to the last hole, taking the first and last holes, and the peg in the last hole, out of play, and reducing the $(n,k)$-game to the $(n-2,k-1)$-game.

We now assume $n$ and $k$ are both even and describe a winning strategy for the $(n,k)$-game for Bob. Subdivide the $n$ holes into $n/2$ disjoint pairs of adjacent holes. Call a configuration of $k$ pegs *good* if for each pair of holes, both or neither is occupied by pegs, and note that the starting position is good. Bob can ensure that after each of his moves, he leaves Alice with a good configuration: presented with a good configuration, Alice must move a peg from a pair of occupied holes to a hole in an unoccupied pair; then Bob can move the other peg from the first pair to the remaining hole in the second pair, resulting in another good configuration. In particular, this ensures that Bob always has a move to make. Since the game must terminate, this is a winning strategy for Bob.

B3 Let $f(\delta)$ denote the desired expected value of $Z$ as a function of $\delta$. We prove that $f(\delta) = 1 - \log(\delta)$, where log denotes natural logarithm.

For $c \in [0,1]$, let $g(\delta,c)$ denote the expected value of $Z$ given that $x_1 = c$, and note that $f(\delta) = \int_0^1 g(\delta,c)\,dc$. Clearly $g(\delta,c) = 1$ if $c < \delta$. On the other hand, if $c \geq \delta$, then $g(\delta,c)$ is 1 more than the expected value of $Z$ would be if we used the initial condition $x_0 = c$ rather than $x_0 = 1$. By rescaling the interval $[0,c]$ linearly to $[0,1]$ and noting that this sends $\delta$ to $\delta/c$, we see that this latter expected value is equal to $f(\delta/c)$. That is, for $c \geq \delta$, $g(\delta,c) = 1 + f(\delta/c)$. It follows that we have

$$\begin{aligned}
f(\delta) &= \int_0^1 g(\delta,c)\,dc \\
&= \delta + \int_\delta^1 (1 + f(\delta/c))\,dc = 1 + \int_\delta^1 f(\delta/c)\,dc.
\end{aligned}$$

Now define $h : [1,\infty) \to \mathbb{R}$ by $h(x) = f(1/x)$; then we have

$$h(x) = 1 + \int_{1/x}^1 h(cx)\,dc = 1 + \frac{1}{x}\int_1^x h(c)\,dc.$$

Rewriting this as $xh(x) - x = \int_1^x h(c)\,dc$ and differentiating with respect to $x$ gives $h(x) + xh'(x) - 1 = h(x)$, whence $h'(x) = 1/x$ and so $h(x) = \log(x) + C$ for some constant $C$. Since $h(1) = f(1) = 1$, we conclude that $C = 1$, $h(x) = 1 + \log(x)$, and finally $f(\delta) = 1 - \log(\delta)$. This gives the claimed answer.

B4 The answer is $\frac{1}{4040}$. We will show the following more general fact. Let $a$ be any nonzero number and define $q(\mathbf{v}) = 1 + \sum_{j=1}^{2n-1} a^{s_j}$; then the average of $\frac{1}{q(\mathbf{v})}$ over all $\mathbf{v} \in V_n$ is equal to $\frac{1}{2n}$, independent of $a$.

Let $W_n$ denote the set of $(2n)$-tuples $\mathbf{w} = (w_1, \dots, w_{2n})$ such that $n$ of the $w_i$'s are equal to $+1$ and the other $n$ are equal to $-1$. Define a map $\phi : W_n \to W_n$ by $\phi(w_1, w_2, \dots, w_{2n}) = (w_2, \dots, w_{2n}, w_1)$; that is, $\phi$ moves the first entry to the end. For $\mathbf{w} \in W_n$, define the *orbit* of $\mathbf{w}$ to be the collection of elements of $W_n$ of the form $\phi^k(\mathbf{w})$, $k \geq 1$, where $\phi^k$ denotes the $k$-th iterate of $\phi$, and note that $\phi^{2n}(\mathbf{w}) = \mathbf{w}$. Then $W_n$ is a disjoint union of orbits. For a given $\mathbf{w} \in W_n$, the orbit of $\mathbf{w}$ consists of $\mathbf{w}, \phi(\mathbf{w}), \dots, \phi^{m-1}(\mathbf{w})$, where $m$ is the smallest positive integer with $\phi^m(\mathbf{w}) = \mathbf{w}$; the list $\phi(\mathbf{w}), \dots, \phi^{2n}(\mathbf{w})$ runs through the orbit of $\mathbf{w}$ completely $2n/m$ times, with each element of the orbit appearing the same number of times.

Now define the map $f : W_n \to V_n$ by $f(\mathbf{w}) = \mathbf{v} = (s_0, \dots, s_{2n})$ with $s_j = \sum_{i=1}^{j} w_i$; this is a one-to-one correspondence between $W_n$ and $V_n$, with the inverse map given by $w_j = s_j - s_{j-1}$ for $j = 1, \dots, 2n$. We claim that for any $\mathbf{w} \in W_n$, the average of $\frac{1}{q(\mathbf{v})}$, where $\mathbf{v}$ runs over vectors in the image of the orbit of $\mathbf{w}$ under $f$, is equal to $\frac{1}{2n}$. Since $W_n$ is a disjoint union of orbits, $V_n$ is a disjoint union of the images of these orbits under $f$, and it then follows that the overall average of $\frac{1}{q(\mathbf{v})}$ over $\mathbf{v} \in V_n$ is $\frac{1}{2n}$.

To prove the claim, we compute the average of $\frac{1}{q(f(\phi^k(\mathbf{w})))}$ over $k = 1, \dots, 2n$; since $\phi^k(\mathbf{w})$ for $k = 1, \dots, 2n$ runs over the orbit of $\mathbf{w}$ with each element in the orbit appearing equally, this is equal to the desired average. Now if we adopt the convention that the indices in $w_i$ are considered mod $2n$, so that $w_{2n+i} = w_i$ for all $i$, then the $i$-th entry of $\phi^k(\mathbf{w})$ is $w_{i+k}$; we can then define $s_j = \sum_{i=1}^{j} w_i$ for all $j \geq 1$, and $s_{2n+i} = s_i$ for all $i$ since $\sum_{i=1}^{2n} w_i = 0$. We now have

$$q(f(\phi^k(\mathbf{w}))) = \sum_{j=1}^{2n} a^{\sum_{i=1}^{j} w_{i+k}} = \sum_{j=1}^{2n} a^{s_{j+k}-s_k} = a^{-s_k} \sum_{j=1}^{2n} a^{s_j}.$$

Thus

$$\sum_{k=1}^{2n} \frac{1}{q(f(\phi^k(\mathbf{w})))} = \sum_{k=1}^{2n} \frac{a^{s_k}}{\sum_{j=1}^{2n} a^{s_j}} = 1,$$

and the average of $\frac{1}{q(f(\phi^k(\mathbf{w})))}$ over $k = 1, \dots, 2n$ is $\frac{1}{2n}$, as desired.

B5 **First solution.** (by Mitja Mastnak) It will suffice to show that for any $z_1, z_2, z_3, z_4 \in \mathbb{C}$ of modulus 1 such that $|3 - z_1 - z_2 - z_3 - z_4| = |z_1 z_2 z_3 z_4|$, at least one of $z_1, z_2, z_3$ is equal to 1.

To this end, let $z_1 = e^{\alpha i}, z_2 = e^{\beta i}, z_3 = e^{\gamma i}$ and

$$f(\alpha, \beta, \gamma) = |3 - z_1 - z_2 - z_3|^2 - |1 - z_1 z_2 z_3|^2.$$

A routine calculation shows that

$$\begin{aligned} f(\alpha, \beta, \gamma) = 10 &- 6\cos(\alpha) - 6\cos(\beta) - 6\cos(\gamma) \\ &+ 2\cos(\alpha+\beta+\gamma) + 2\cos(\alpha-\beta) \\ &+ 2\cos(\beta-\gamma) + 2\cos(\gamma-\alpha). \end{aligned}$$

Since the function $f$ is continuously differentiable, and periodic in each variable, $f$ has a maximum and a minimum and it attains these values only at points where $\nabla f = (0,0,0)$. A routine calculation now shows that

$$\begin{aligned} \frac{\partial f}{\partial \alpha} + \frac{\partial f}{\partial \beta} + \frac{\partial f}{\partial \gamma} &= 6(\sin(\alpha) + \sin(\beta) + \sin(\gamma) - \sin(\alpha+\beta+\gamma)) \\ &= 24 \sin\left(\frac{\alpha+\beta}{2}\right) \sin\left(\frac{\beta+\gamma}{2}\right) \sin\left(\frac{\gamma+\alpha}{2}\right). \end{aligned}$$

Hence every critical point of $f$ must satisfy one of $z_1 z_2 = 1$, $z_2 z_3 = 1$, or $z_3 z_1 = 1$. By symmetry, let us assume that $z_1 z_2 = 1$. Then

$$f = |3 - 2\mathrm{Re}(z_1) - z_3|^2 - |1 - z_3|^2;$$

since $3 - 2\mathrm{Re}(z_1) \geq 1$, $f$ is nonnegative and can be zero only if the real part of $z_1$, and hence also $z_1$ itself, is equal to 1.

**Remark.** If $z_1 = 1$, we may then apply the same logic to deduce that one of $z_2, z_3, z_4$ is equal to 1. If $z_1 = z_2 = 1$, we may factor the expression

$$3 - z_1 - z_2 - z_3 - z_4 + z_1 z_2 z_3 z_4$$

as $(1 - z_3)(1 - z_4)$ to deduce that at least three of $z_1, \dots, z_4$ are equal to 1.

**Second solution.** We begin with an "unsmoothing" construction.

**Lemma 1.** *Let $z_1, z_2, z_3$ be three distinct complex numbers with $|z_j| = 1$ and $z_1 + z_2 + z_3 \in [0, +\infty)$. Then there exist another three complex numbers $z_1', z_2', z_3'$, not all distinct, with $|z_j'| = 1$ and*

$$z_1' + z_2' + z_3' \in (z_1 + z_2 + z_3, +\infty), \quad z_1 z_2 z_3 = z_1' z_2' z_3'.$$

*Proof.* Write $z_j = e^{i\theta_j}$ for $j = 1, 2, 3$. We are then trying to maximize the target function

$$\cos\theta_1 + \cos\theta_2 + \cos\theta_3$$

given the constraints

$$\begin{aligned} 0 &= \sin\theta_1 + \sin\theta_2 + \sin\theta_3 \\ * &= \theta_1 + \theta_2 + \theta_3 \end{aligned}$$

Since $z_1, z_2, z_3$ run over a compact region without boundary, the maximum must be achieved at a point where the matrix

$$\begin{pmatrix} \sin\theta_1 & \sin\theta_2 & \sin\theta_3 \\ \cos\theta_1 & \cos\theta_2 & \cos\theta_3 \\ 1 & 1 & 1 \end{pmatrix}$$

is singular. Since the determinant of this matrix computes (up to a sign and a factor of 2) the area of the triangle with vertices $z_1, z_2, z_3$, it cannot vanish unless some two of $z_1, z_2, z_3$ are equal. This proves the claim. □

For $n$ a positive integer, let $H_n$ be the *hypocycloid curve* in $\mathbb{C}$ given by

$$H_n = \{(n-1)z + z^{-n+1} : z \in \mathbb{C}, |z| = 1\}.$$

In geometric terms, $H_n$ is the curve traced out by a marked point on a circle of radius 1 rolling one full circuit along the interior of a circle of radius 1, starting from the point $z = 1$. Note that the interior of $H_n$ is not convex, but it is *star-shaped*: it is closed under multiplication by any number in $[0, 1]$.

**Lemma 2.** *For $n$ a positive integer, let $S_n$ be the set of complex numbers of the form $w_1 + \cdots + w_n$ for some $w_1, \dots, w_n \in \mathbb{C}$ with $|w_j| = 1$ and $w_1 \cdots w_n = 1$. Then for $n \leq 4$, $S_n$ is the closed interior of $H_n$ (i.e., including the boundary).*

*Proof.* By considering $n$-tuples of the form $(z, \dots, z, z^{-n+1})$, we see that $H_n \subseteq S_n$. It thus remains to check that $S_n$ lies in the closed interior of $H_n$. We ignore the easy cases $n = 1$ (where $H_1 = S_1 = \{1\}$) and $n = 2$ (where $H_2 = S_2 = [-2, 2]$) and assume hereafter that $n \geq 3$.

By Lemma 1, for each ray emanating from the the origin, the extreme intersection point of $S_n$ with this ray (which exists because $S_n$ is compact) is achieved by some tuple $(w_1, \dots, w_n)$ with at most two distinct values. For $n = 3$, this immediately implies that this point lies on $H_n$. For $n = 4$, we must also consider tuples consisting of two pairs of equal values; however, these only give rise to points in $[-4, 4]$, which are indeed contained in $H_4$. □

Turning to the original problem, consider $z_1,\dots,z_4 \in \mathbb{C}$ with $|z_j| = 1$ and

$$3 - z_1 - z_2 - z_3 - z_4 + z_1z_2z_3z_4 = 0;$$

we must prove that at least one $z_j$ is equal to 1. Let $z$ be any fourth root of $z_1z_2z_3z_4$, put $w_j = z_j/z$, and put $s = w_1 + \cdots + w_4$. In this notation, we have

$$s = z^3 + 3z^{-1},$$

where $s \in S_4$ and $z^3 + 3z^{-1} \in H_4$. That is, $s$ is a boundary point of $S_4$, so in particular it is the extremal point of $S_4$ on the ray emanating from the origin through $s$. By Lemma 1, this implies that $w_1,\dots,w_4$ take at most two distinct values. As in the proof of Lemma 2, we distinguish two cases.

- If $w_1 = w_2 = w_3$, then

  $$w_1^{-3} + 3w_1 = z^3 + 3z^{-1}.$$

  From the geometric description of $H_n$, we see that this forces $w_1^{-1} = z$ and hence $z_1 = 1$.
- If $w_1 = w_2$ and $w_3 = w_4$, then $s \in [-4,4]$ and hence $s = \pm 4$. This can only be achieved by taking $w_1 = \cdots = w_4 = \pm 1$; since $s = z^3 + 3z^{-1}$ we must also have $z = \pm 1$, yielding $z_1 = \cdots = z_4 = 1$.

**Remark.** With slightly more work, one can show that Lemma 2 remains true for all positive integers $n$. The missing extra step is to check that for $m = 1,\dots,n-1$, the hypocycloid curve

$$\{mz^{n-m} + (n-m)z^{-m} : z \in \mathbb{C}, |z| = 1\}$$

is contained in the filled interior of $H_n$. In fact, this curve only touches $H_n$ at points where they both touch the unit circle (i.e., at $d$-th roots of unity for $d = \gcd(m,n)$); this can be used to formulate a corresponding version of the original problem, which we leave to the reader.

B6 **First solution.** Define the sequence $\{a_k\}_{k=0}^\infty$ by $a_k = \lfloor k(\sqrt{2}-1)\rfloor$. The first few terms of the sequence $\{(-1)^{a_k}\}$ are

$$1,1,1,-1,-1,1,1,1,-1,-1,1,1,1,\dots.$$

Define a new sequence $\{c_i\}_{i=0}^\infty$ given by $3,2,3,2,3,\dots$, whose members alternately are the lengths of the clusters of consecutive 1's and the lengths of the clusters of consecutive $-1$'s in the sequence $\{(-1)^{a_k}\}$. Then for any $i$, $c_0 + \cdots + c_i$ is the number of nonnegative integers $k$ such that $\lfloor k(\sqrt{2}-1)\rfloor$ is strictly less than $i+1$, i.e., such that $k(\sqrt{2}-1) < i+1$. This last condition is equivalent to $k < (i+1)(\sqrt{2}+1)$, and we conclude that

$$\begin{aligned} c_0 + \cdots + c_i &= \lfloor (i+1)(\sqrt{2}+1)\rfloor + 1 \\ &= 2i + 3 + \lfloor (i+1)(\sqrt{2}-1)\rfloor. \end{aligned}$$

Thus for $i > 0$,

$$c_i = 2 + \lfloor (i+1)(\sqrt{2}-1)\rfloor - \lfloor i(\sqrt{2}-1)\rfloor. \tag{8}$$

Now note that $\lfloor (i+1)(\sqrt{2}-1)\rfloor - \lfloor i(\sqrt{2}-1)\rfloor$ is either 1 or 0 depending on whether or not there is an integer $j$ between $i(\sqrt{2}-1)$ and $(i+1)(\sqrt{2}-1)$: this condition is equivalent to $i < j(\sqrt{2}+1) < i+1$. That is, for $i > 0$,

$$c_i = \begin{cases} 3 & \text{if } i = \lfloor j(\sqrt{2}+1)\rfloor \text{ for some integer } j, \\ 2 & \text{otherwise;} \end{cases} \tag{9}$$

by inspection, this also holds for $i = 0$.

Now we are asked to prove that

$$\sum_{k=0}^n (-1)^{a_k} \geq 1 \tag{10}$$

for all $n \geq 1$. We will prove that if (10) holds for all $n \leq N$, then (10) holds for all $n \leq 4N$; since (10) clearly holds for $n = 1$, this will imply the desired result.

Suppose that (10) holds for $n \leq N$. To prove that (10) holds for $n \leq 4N$, it suffices to show that the partial sums

$$\sum_{i=0}^m (-1)^i c_i$$

of the sequence $\{(-1)^{a_k}\}$ are positive for all $m$ such that $c_0 + \cdots + c_{m-1} < 4N+3$, since these partial sums cover all clusters through $a_{4N}$. Now if $c_0 + \cdots + c_{m-1} < 4N+3$, then since each $c_i$ is at least 2, we must have $m < 2N+2$. From (9), we see that if $m$ is odd, then

$$\begin{aligned} \sum_{i=0}^m (-1)^i c_i &= \sum_{i=0}^m (-1)^i (c_i - 2) \\ &= \sum_j (-1)^{\lfloor j(\sqrt{2}+1)\rfloor} = \sum_j (-1)^{a_j} \end{aligned}$$

where the sum in $j$ is over nonnegative integers $j$ with $j(\sqrt{2}+1) < m$, i.e., $j < m(\sqrt{2}-1)$; since $m(\sqrt{2}-1) < m/2 < N+1$, $\sum_j (-1)^{a_j}$ is positive by the induction hypothesis. Similarly, if $m$ is even, then $\sum_{i=0}^m (-1)^i c_i = c_m + \sum_j (-1)^{a_j}$ and this is again positive by the induction hypothesis. This concludes the induction step and the proof.

**Remark.** More generally, using the same proof we can establish the result with $\sqrt{2}-1$ replaced by $\sqrt{n^2+1}-n$ for any positive integer $n$.

**Second solution.** For $n \geq 0$, define the function

$$f(n) = \sum_{k=1}^n (-1)^{\lfloor k(\sqrt{2}-1)\rfloor}$$

with the convention that $f(0) = 0$.

Define the sequence $q_0, q_1, \dots$ by the initial conditions

$$q_0 = 0, q_1 = 1$$

and the recurrence relation

$$q_j = 2q_{j-1} + q_{j-2}.$$

This is OEIS sequence A000129; its first few terms are

$$0, 1, 2, 5, 12, 29, 70, \ldots.$$

Note that $q_j \equiv j \pmod 2$.

We now observe that the fractions $q_{j-1}/q_j$ are the *convergents* of the continued fraction expansion of $\sqrt{2}-1$. This implies the following additional properties of the sequence.

- For all $j \geq 0$,

$$\frac{q_{2j}}{q_{2j+1}} < \sqrt{2}-1 < \frac{q_{2j+1}}{q_{2j+2}}.$$

- There is no fraction $r/s$ with $s < q_j + q_{j+1}$ such that $\frac{r}{s}$ separates $\sqrt{2}-1$ from $q_j/q_{j-1}$. In particular, for $k < q_j + q_{j+1}$,

$$\lfloor k(\sqrt{2}-1) \rfloor = \left\lfloor \frac{kq_{j-1}}{q_j} \right\rfloor$$

except when $j$ is even and $k \in \{q_j, 2q_j\}$, in which case they differ by 1.

We use this to deduce a "self-similarity" property of $f(n)$.

**Lemma 1.** *Let $n, j$ be nonnegative integers with $q_j \leq n < q_j + q_{j+1}$.*

*(a) If $j$ is even, then*

$$f(n) = f(q_j) - f(n - q_j).$$

*(b) If $j$ is odd, then*

$$f(n) = f(n - q_j) + 1.$$

*Proof.* If $j$ is even, then

$$\begin{aligned} f(n) &= f(q_j) + \sum_{k=q_j+1}^{n} (-1)^{\lfloor k(\sqrt{2}-1) \rfloor} \\ &= f(q_j) + \sum_{k=q_j+1}^{n} (-1)^{\lfloor kq_{j-1}/q_j \rfloor} + * \end{aligned}$$

where $*$ equals 2 if $n \geq 2q_j$ (accounting for the term $k = 2q_j$) and 0 otherwise. Continuing,

$$\begin{aligned} f(n) &= f(q_j) + \sum_{1}^{n-q_j} (-1)^{q_{j-1} + \lfloor kq_{j-1}/q_j \rfloor} + * \\ &= f(q_j) - \sum_{1}^{n-q_j} (-1)^{q_{j-1} + \lfloor k(\sqrt{2}-1) \rfloor} \\ &= f(q_j) - f(n - q_j). \end{aligned}$$

If $j$ is odd, then

$$\begin{aligned} f(n) &= f(n - q_j) + \sum_{k=n-q_j+1}^{n} (-1)^{\lfloor k(\sqrt{2}-1) \rfloor} \\ &= f(n - q_j) - 2 + \sum_{k=n-q_j+1}^{n} (-1)^{\lfloor kq_{j-1}/q_j \rfloor}. \end{aligned}$$

Since

$$\lfloor (k + q_j)q_{j-1}/q_j \rfloor \equiv \lfloor kq_{j-1}/q_j \rfloor \pmod 2,$$

we also have

$$f(n) = f(n - q_j) + \sum_{k=1}^{q_j} (-1)^{\lfloor kq_{j-1}/q_j \rfloor}.$$

In this sum, the summand indexed by $q_j$ contributes 1, and the summands indexed by $k$ and $q_j - k$ cancel each other out for $k = 1, \ldots, q_j - 1$. We thus have

$$f(n) = f(n - q_j) + 1$$

as claimed. □

From Lemma 1, we have

$$f(q_{2j}) = f(q_{2j} - 2q_{2j-1}) + 2 = f(q_{2j-2}) + 2.$$

By induction on $j$, $f(q_{2j}) = 2j$ for all $j \geq 0$; by similar logic, we have $f(n) \leq f(q_{2j}) = 2j$ for all $n \leq q_{2j}$. We can now apply Lemma 1 once more to deduce that $f(n) \geq 0$ for all $j$.

**Remark.** As a byproduct of the first solution, we confirm the equality of two sequences that were entered separately in the OEIS but conjectured to be equal: A097509 (indexed from 0) matches the definition of $\{c_i\}$, while A276862 (indexed from 1) matches the characterization of $\{c_{i-1}\}$ given by (8).

**Remark.** We can confirm an additional conjecture from the OEIS by showing that in the notation of the first solution, the sequence $a(n) = c_{n+1}$ indexed from 1 equals A082844: "Start with 3,2 and apply the rule $a(a(1) + a(2) + \cdots + a(n)) = a(n)$, fill in any undefined terms with $a(t) = 2$ if $a(t-1) = 3$ and $a(t) = 3$ if $a(t-1) = 2$." We first verify the recursion. By (10),

$$\begin{aligned} a(1) + \cdots + a(n) &= c_0 + \cdots + c_{n+1} - c_0 - c_1 \\ &= \lfloor (n+2)(\sqrt{2}+1) \rfloor - 4. \end{aligned}$$

From (9), we see that $a(a(1) + \cdots + a(n) + 3) = 3$. Consequently, exactly one of $a(a(1) + \cdots + a(n))$ or $a(a(1) + \cdots + a(n) + 1)$ equals 3, and it is the former if and only if

$$\lfloor (n+2)(\sqrt{2}+1) \rfloor - 3 = \lfloor (n+1)(\sqrt{2}+1) \rfloor,$$

i.e., if and only if $a(n) = c_{n+1} = 3$.

We next check that the definition correctly fills in values not determined by the recursion. If $a(n) = 3$, then $a(a(1)+\cdots+a(n)+1) = 2$ because no two consecutive values can both equal 3; by the same token, $a(n+1) = 2$ and so there are no further values to fill in. If $a(n) = 2$, then $a(a(1)+\cdots+a(n)+1) = 3$ by the previous paragraph; this in turn implies $a(a(1)+\cdots+a(n)+2) = 2$, at which point there are no further values to fill in.

**Remark.** We can confirm an additional conjecture from the OEIS by showing that in the notation of the first solution, the sequence $\{c_i\}$ equals A245219. This depends on some additional lemmas.

**Lemma 2.** *Let k be a positive integer. Then*

$$\left\{i(\sqrt{2}-1)\right\} < \left\{k(\sqrt{2}-1)\right\} \qquad (i = 0,\ldots,k-1)$$

*if and only if $k = q_{2j}$ or $k = q_{2j} + q_{2j-1}$ for some $j > 0$.*

*Proof.* For each $j > 0$, we have

$$\frac{q_{2j-2}}{q_{2j-1}} < \frac{q_{2j}}{q_{2j+1}} = \frac{q_{2j-1}+2q_{2j-2}}{q_{2j}+2q_{2j-1}} < \sqrt{2}-1 < \frac{q_{2j+1}}{q_{2j+2}} < \frac{q_{2j-1}}{q_{2j}}.$$

We also have

$$\frac{q_{2j-2}}{q_{2j-1}} < \frac{q_{2j}}{q_{2j+1}} = \frac{q_{2j-1}+2q_{2j-2}}{q_{2j}+2q_{2j-1}} < \frac{q_{2j-1}+q_{2j-2}}{q_{2j}+q_{2j-1}} < \frac{q_{2j-1}}{q_{2j}}.$$

Moreover, $\frac{q_{2j-1}+q_{2j-2}}{q_{2j}+q_{2j-1}}$ cannot be less than $\sqrt{2}-1$, or else it would be a better approximation to $\sqrt{2}-1$ than the convergent $q_{2j}/q_{2j+1}$ with $q_{2j+1} > q_{2j} + q_{2j-1}$. By the same token, $\frac{q_{2j-1}+q_{2j-2}}{q_{2j}+q_{2j-1}}$ cannot be a better approximation to $\sqrt{2}-1$ than $q_{2j+1}/q_{2j+2}$. We thus have

$$\frac{q_{2j}}{q_{2j+1}} < \sqrt{2}-1 < \frac{q_{2j+1}}{q_{2j+2}} < \frac{q_{2j-1}+q_{2j-2}}{q_{2j}+q_{2j-1}} < \frac{q_{2j-1}}{q_{2j}}.$$

From this, we see that

$$\{q_{2j}(\sqrt{2}-1)\} < \{(q_{2j}+q_{2j-1})(\sqrt{2}-1)\} < \{q_{2j+2}(\sqrt{2}-1)\}.$$

It will now suffice to show that for $q_{2j} < k < q_{2j} + q_{2j-1}$,

$$\{k(\sqrt{2}-1)\} < \{q_{2j}(\sqrt{2}-1)\}$$

while for $q_{2j} + q_{2j-1} < k < q_{2j+2}$,

$$\{k(\sqrt{2}-1)\} < \{(q_{2j}+q_{2j-1})(\sqrt{2}-1)\}.$$

The first of these assertion is an immediate consequence of the "best approximation" property of the convergent $q_{2j-1}/q_{2j}$. As for the second assertion, note that for $k$ in this range, no fraction with denominator $k$ can lie strictly between $\frac{q_{2j}}{q_{2j+1}}$ and $\frac{q_{2j-1}+q_{2j-2}}{q_{2j}+q_{2j-1}}$ because these fractions are consecutive terms in a Farey sequence (that is, their difference has numerator 1 in lowest terms); in particular, such a fraction cannot be a better upper approximation to $\sqrt{2}-1$ than $\frac{q_{2j-1}+q_{2j-2}}{q_{2j}+q_{2j-1}}$. $\square$

**Lemma 3.** *For $j > 0$, the sequence $c_0,\ldots,c_{j-1}$ is palindromic if and only if*

$$j = q_{2i+1} \qquad or \qquad j = q_{2i+1} + q_{2i+2}$$

*for some nonnegative integer i. (That is, j must belong to one of the sequences A001653 or A001541.) In particular, j must be odd.*

*Proof.* Let $j$ be an index for which $\{c_0,\ldots,c_{j-1}\}$ is palindromic. In particular, $c_{j-1} = c_0 = 3$, so from (9), we see that $j-1 = \lfloor k(\sqrt{2}+1)\rfloor$ for some $k$. Given this, the sequence is palindromic if and only if

$$\lfloor i(\sqrt{2}+1)\rfloor + \lfloor (k-i)(\sqrt{2}+1)\rfloor = \lfloor k(\sqrt{2}+1)\rfloor \quad (i = 0,\ldots,k),$$

or equivalently

$$\left\{i(\sqrt{2}-1)\right\} + \left\{(k-i)(\sqrt{2}-1)\right\} = \left\{k(\sqrt{2}-1)\right\} \quad (i = 0,\ldots,k)$$

where the braces denote fractional parts. This holds if and only if

$$\left\{i(\sqrt{2}-1)\right\} < \left\{k(\sqrt{2}-1)\right\} \qquad (i = 0,\ldots,k-1),$$

so we may apply Lemma 2 to identify $k$ and hence $j$. $\square$

**Lemma 4.** *For $j > 0$, if there exists a positive integer k such that*

$$(c_0,\ldots,c_{j-2}) = (c_k,\ldots,c_{k+j-2}) \text{ but } c_{j-1} \neq c_{k+j-1},$$

*then*

$$j = q_{2i+1} \qquad or \qquad j = q_{2i+1} + q_{2i+2}$$

*for some nonnegative integer i. In particular, j is odd and (by Lemma 3) the sequence $(c_0,\ldots,c_{j-1})$ is palindromic.*

*Proof.* Since the sequence $\{c_i\}$ consists of 2s and 3s, we must have $\{c_{j-1}, c_{k+j-1}\} = \{2,3\}$. Since each pair of 3s is separated by either one or two 2s, we must have $c_{j-2} = 2$, $c_{j-3} = 3$. In particular, by (9) there is an integer $i$ for which $j-3 = \lfloor (i-1)(\sqrt{2}+1)\rfloor$; there is also an integer $l$ such that $k = \lfloor l(\sqrt{2}+1)\rfloor$. By hypothesis, we have

$$\lfloor (h+l)(\sqrt{2}+1)\rfloor = \lfloor h(\sqrt{2}+1)\rfloor + \lfloor l(\sqrt{2}+1)\rfloor$$

for $h = 0,\ldots,i-1$ but not for $h = i$. In other words,

$$\left\{(h+l)(\sqrt{2}-1)\right\} = \left\{h(\sqrt{2}-1)\right\} + \left\{l(\sqrt{2}-1)\right\}$$

for $h = 0,\ldots,i-1$ but not for $h = i$. That is, $\{h(\sqrt{2}-1)\}$ belongs to the interval $(0, 1-\{l(\sqrt{2}-1)\})$ for $h = 0,\ldots,i-1$ but not for $h = i$; in particular,

$$\left\{h(\sqrt{2}-1)\right\} < \left\{i(\sqrt{2}-1)\right\} \qquad (h = 0,\ldots,i-1),$$

so we may apply Lemma 2 to identify $i$ and hence $j$. $\square$

The sequence A245219 is defined as the sequence of coefficients of the continued fraction of $\sup\{b_i\}$ where $b_1 = 1$ and for $i > 1$,

$$b_{i+1} = \begin{cases} b_i + 1 & \text{if } i = \lfloor j\sqrt{2} \rfloor \text{ for some integer } j; \\ 1/b_i & \text{otherwise.} \end{cases}$$

It is equivalent to take the supremum over values of $i$ for which $b_{i+1} = 1/b_i$; by Beatty's theorem, this occurs precisely when $i = \lfloor j(2+\sqrt{2}) \rfloor$ for some integer $j$. In this case, $b_i$ has continued fraction

$$[c_{j-1}, \dots, c_0].$$

Let $K$ be the real number with continued fraction $[c_0, c_1, \dots]$; we must show that $K = \sup\{b_i\}$. In one direction, by Lemma 3, there are infinitely many values of $i$ for which $[c_{j-1}, \dots, c_0] = [c_0, \dots, c_{j-1}]$; the corresponding values $b_i$ accumulate at $K$, so $K \le \sup\{b_i\}$.

In the other direction, we show that $K \ge \sup\{b_i\}$ as follows. It is enough to prove that $K \ge b_i$ when $i = \lfloor j(2+\sqrt{2}) \rfloor$ for some integer $j$.

- If $c_0, \dots, c_{j-1}$ is palindromic, then Lemma 3 implies that $j$ is odd; that is, the continued fraction $[c_{j-1}, \dots, c_0]$ has odd length. In this case, replacing the final term $c_0 = c_{j-1}$ by the larger quantity $[c_{j-1}, c_j, \dots]$ increases the value of the continued fraction.
- If $c_0, \dots, c_{j-1}$ is not palindromic, then there is a least integer $k \in \{0, \dots, j-1\}$ such that $c_k \neq c_{j-1-k}$. By Lemma 3, the sequence $c_0, c_1, \dots$ has arbitrarily long palindromic initial segments, so the sequence $(c_{j-1}, \dots, c_{j-1-k})$ also occurs as $c_h, \dots, c_{h+k}$ for some $h > 0$. By Lemma 4, $k$ is even and $c_k = 3 > 2 = c_{j-1-k}$; hence in the continued fraction for $b_i$, replacing the final segment $c_{j-1-k}, \dots, c_0$ by $c_k, c_{k+1}, \dots$ increases the value.

**The 82nd William Lowell Putnam Mathematical Competition**
**Saturday, December 4, 2021**

A1 A grasshopper starts at the origin in the coordinate plane and makes a sequence of hops. Each hop has length 5, and after each hop the grasshopper is at a point whose coordinates are both integers; thus, there are 12 possible locations for the grasshopper after the first hop. What is the smallest number of hops needed for the grasshopper to reach the point $(2021, 2021)$?

A2 For every positive real number $x$, let

$$g(x) = \lim_{r \to 0} ((x+1)^{r+1} - x^{r+1})^{\frac{1}{r}}.$$

Find $\lim_{x \to \infty} \frac{g(x)}{x}$.

A3 Determine all positive integers $N$ for which the sphere

$$x^2 + y^2 + z^2 = N$$

has an inscribed regular tetrahedron whose vertices have integer coordinates.

A4 Let

$$I(R) = \iint_{x^2+y^2 \leq R^2} \left( \frac{1+2x^2}{1+x^4+6x^2y^2+y^4} - \frac{1+y^2}{2+x^4+y^4} \right) dx\,dy.$$

Find

$$\lim_{R \to \infty} I(R),$$

or show that this limit does not exist.

A5 Let $A$ be the set of all integers $n$ such that $1 \leq n \leq 2021$ and $\gcd(n, 2021) = 1$. For every nonnegative integer $j$, let

$$S(j) = \sum_{n \in A} n^j.$$

Determine all values of $j$ such that $S(j)$ is a multiple of 2021.

A6 Let $P(x)$ be a polynomial whose coefficients are all either 0 or 1. Suppose that $P(x)$ can be written as a product of two nonconstant polynomials with integer coefficients. Does it follow that $P(2)$ is a composite integer?

B1 Suppose that the plane is tiled with an infinite checkerboard of unit squares. If another unit square is dropped on the plane at random with position and orientation independent of the checkerboard tiling, what is the probability that it does not cover any of the corners of the squares of the checkerboard?

B2 Determine the maximum value of the sum

$$S = \sum_{n=1}^{\infty} \frac{n}{2^n} (a_1 a_2 \cdots a_n)^{1/n}$$

over all sequences $a_1, a_2, a_3, \cdots$ of nonnegative real numbers satisfying

$$\sum_{k=1}^{\infty} a_k = 1.$$

B3 Let $h(x,y)$ be a real-valued function that is twice continuously differentiable throughout $\mathbb{R}^2$, and define

$$\rho(x,y) = y h_x - x h_y.$$

Prove or disprove: For any positive constants $d$ and $r$ with $d > r$, there is a circle $\mathscr{S}$ of radius $r$ whose center is a distance $d$ away from the origin such that the integral of $\rho$ over the interior of $\mathscr{S}$ is zero.

B4 Let $F_0, F_1, \ldots$ be the sequence of Fibonacci numbers, with $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. For $m > 2$, let $R_m$ be the remainder when the product $\prod_{k=1}^{F_m - 1} k^k$ is divided by $F_m$. Prove that $R_m$ is also a Fibonacci number.

B5 Say that an $n$-by-$n$ matrix $A = (a_{ij})_{1 \leq i,j \leq n}$ with integer entries is *very odd* if, for every nonempty subset $S$ of $\{1, 2, \ldots, n\}$, the $|S|$-by-$|S|$ submatrix $(a_{ij})_{i,j \in S}$ has odd determinant. Prove that if $A$ is very odd, then $A^k$ is very odd for every $k \geq 1$.

B6 Given an ordered list of $3N$ real numbers, we can *trim* it to form a list of $N$ numbers as follows: We divide the list into $N$ groups of 3 consecutive numbers, and within each group, discard the highest and lowest numbers, keeping only the median.

Consider generating a random number $X$ by the following procedure: Start with a list of $3^{2021}$ numbers, drawn independently and uniformly at random between 0 and 1. Then trim this list as defined above, leaving a list of $3^{2020}$ numbers. Then trim again repeatedly until just one number remains; let $X$ be this number. Let $\mu$ be the expected value of $|X - \frac{1}{2}|$. Show that

$$\mu \geq \frac{1}{4} \left( \frac{2}{3} \right)^{2021}.$$

# Solutions to the 82nd William Lowell Putnam Mathematical Competition
# Saturday, December 4, 2021

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A1 The answer is 578.

Each hop corresponds to adding one of the 12 vectors $(0,\pm 5)$, $(\pm 5,0)$, $(\pm 3,\pm 4)$, $(\pm 4,\pm 3)$ to the position of the grasshopper. Since $(2021,2021) = 288(3,4) + 288(4,3) + (0,5) + (5,0)$, the grasshopper can reach $(2021,2021)$ in $288+288+1+1 = 578$ hops.

On the other hand, let $z = x+y$ denote the sum of the $x$ and $y$ coordinates of the grasshopper, so that it starts at $z = 0$ and ends at $z = 4042$. Each hop changes the sum of the $x$ and $y$ coordinates of the grasshopper by at most 7, and $4042 > 577 \times 7$; it follows immediately that the grasshopper must take more than 577 hops to get from $(0,0)$ to $(2021,2021)$.

**Remark.** This solution implicitly uses the distance function

$$d((x_1,y_1),(x_2,y_2)) = |x_1-x_2| + |y_1-y_2|$$

on the plane, variously called the *taxicab metric*, the *Manhattan metric*, or the $L^1$-*norm* (or $\ell_1$-norm).

A2 The limit is $e$.

**First solution.** By l'Hôpital's Rule, we have

$$\begin{aligned}
&\lim_{r\to 0} \frac{\log((x+1)^{r+1}-x^{r+1})}{r} \\
&= \lim_{r\to 0} \frac{d}{dr}\log((x+1)^{r+1}-x^{r+1}) \\
&= \lim_{r\to 0} \frac{(x+1)^{r+1}\log(x+1) - x^{r+1}\log x}{(x+1)^{r+1}-x^{r+1}} \\
&= (x+1)\log(x+1) - x\log x,
\end{aligned}$$

where log denotes natural logarithm. It follows that $g(x) = e^{(x+1)\log(x+1)-x\log x} = \frac{(x+1)^{x+1}}{x^x}$. Thus

$$\lim_{x\to\infty} \frac{g(x)}{x} = \left(\lim_{x\to\infty}\frac{x+1}{x}\right)\cdot\left(\lim_{x\to\infty}\left(1+\frac{1}{x}\right)^x\right) = 1\cdot e = e.$$

**Second solution.** We first write

$$\begin{aligned}
\lim_{x\to\infty}\frac{g(x)}{x} &= \lim_{x\to\infty}\lim_{r\to 0}\frac{((x+1)^{r+1}-x^{r+1})^{1/r}}{x} \\
&= \lim_{x\to\infty}\lim_{r\to 0}\frac{((r+1)x^r + O(x^{r-1}))^{1/r}}{x}.
\end{aligned}$$

We would like to interchange the order of the limits, but this requires some justification. Using Taylor's theorem with remainder, for $x \geq 1$, $r \leq 1$ we can bound the error term $O(x^{r-1})$ in absolute value by $(r+1)rx^{r-1}$. This means that if we continue to rewrite the orginial limit as

$$\lim_{r\to 0}\lim_{x\to\infty}(r+1+O(x^{-1}))^{1/r},$$

the error term $O(x^{-1})$ is bounded in absolute value by $(r+1)r/x$. For $x \geq 1$, $r \leq 1$ this quantity is bounded in absolute value by $(r+1)r$, *independently of* $x$. This allows us to continue by interchanging the order of the limits, obtaining

$$\begin{aligned}
&\lim_{r\to 0}\lim_{x\to\infty}(r+1+O(x^{-1}))^{1/r} \\
&\quad= \lim_{r\to 0}(r+1)^{1/r} \\
&\quad= \lim_{s\to\infty}(1+1/s)^s = e,
\end{aligned}$$

where in the last step we take $s = 1/r$.

A3 The integers $N$ with this property are those of the form $3m^2$ for some positive integer $m$.

In one direction, for $N = 3m^2$, the points

$$(m,m,m),(m,-m,-m),(-m,m,-m),(-m,-m,m)$$

form the vertices of a regular tetrahedron inscribed in the sphere $x^2+y^2+z^2 = N$.

Conversely, suppose that $P_i = (x_i,y_i,z_i)$ for $i = 1,\dots,4$ are the vertices of an inscribed regular tetrahedron. Then the center of this tetrahedron must equal the center of the sphere, namely $(0,0,0)$. Consequently, these four vertices together with $Q_i = (-x_i,-y_i,-z_i)$ for $i = 1,\dots,4$ form the vertices of an inscribed cube in the sphere. The side length of this cube is $(N/3)^{1/2}$, so its volume is $(N/3)^{3/2}$; on the other hand, this volume also equals the determinant of the matrix with row vectors $Q_2-Q_1, Q_3-Q_1, Q_4-Q_1$, which is an integer. Hence $(N/3)^3$ is a perfect square, as then is $N/3$.

A4 The limit exists and equals $\frac{\sqrt{2}}{2}\pi\log 2$.

We first note that we can interchange $x$ and $y$ to obtain

$$I(R) = \iint_{x^2+y^2\leq R^2}\left(\frac{1+2y^2}{1+x^4+6x^2y^2+y^4} - \frac{1+x^2}{2+x^4+y^4}\right)dx\,dy.$$

Averaging the two expressions for $I(R)$ yields

$$I(R) = \iint_{x^2+y^2\leq R^2}(f(x,y)-g(x,y))\,dx\,dy$$

where

$$\begin{aligned}
f(x,y) &= \frac{1+x^2+y^2}{1+x^4+6x^2y^2+y^4} \\
g(x,y) &= \frac{1+x^2/2+y^2/2}{2+x^4+y^4}.
\end{aligned}$$

Now note that

$$f(x,y) = 2g(x+y, x-y).$$

We can thus write

$$I(R) = \iint_{R^2 \leq x^2+y^2 \leq 2R^2} g(x,y)\,dx\,dy.$$

To compute this integral, we switch to polar coordinates:

$$\begin{aligned} I(R) &= \int_R^{R\sqrt{2}} \int_0^{2\pi} g(r\cos\theta, r\sin\theta) r\,dr\,d\theta \\ &= \int_R^{R\sqrt{2}} \int_0^{2\pi} \frac{1+r^2/2}{2+r^4(1-(\sin^2 2\theta)/2)} r\,dr\,d\theta. \end{aligned}$$

We rescale $r$ to remove the factor of $R$ from the limits of integration:

$$I(R) = \int_1^{\sqrt{2}} \int_0^{2\pi} \frac{1+R^2r^2/2}{2+R^4r^4(1-(\sin^2 2\theta)/2)} R^2 r\,dr\,d\theta.$$

Since the integrand is uniformly bounded for $R \gg 0$, we may take the limit over $R$ through the integrals to obtain

$$\begin{aligned} \lim_{R\to\infty} I(R) &= \int_1^{\sqrt{2}} \int_0^{2\pi} \frac{r^2/2}{r^4(1-(\sin^2 2\theta)/2)} r\,dr\,d\theta \\ &= \int_1^{\sqrt{2}} \frac{dr}{r} \int_0^{2\pi} \frac{1}{2-\sin^2 2\theta} d\theta \\ &= \log\sqrt{2} \int_0^{2\pi} \frac{1}{1+\cos^2 2\theta} d\theta \\ &= \frac{1}{2}\log 2 \int_0^{2\pi} \frac{2}{3+\cos 4\theta} d\theta. \end{aligned}$$

It thus remains to evaluate

$$\int_0^{2\pi} \frac{2}{3+\cos 4\theta} d\theta = 2\int_0^{\pi} \frac{2}{3+\cos\theta} d\theta.$$

One option for this is to use the half-angle substitution $t = \tan(\theta/2)$ to get

$$\begin{aligned} \int_{-\infty}^{\infty} \frac{4}{3(1+t^2)+(1-t^2)}\,dt &= \int_{-\infty}^{\infty} \frac{2}{2+t^2}\,dt \\ &= \sqrt{2}\arctan\left(\frac{x}{\sqrt{2}}\right)_{-\infty}^{\infty} \\ &= \sqrt{2}\pi. \end{aligned}$$

Putting this together yields the claimed result.

A5 The values of $j$ in question are those not divisible by either 42 or 46.

We first check that for $p$ prime,

$$\sum_{n=1}^{p-1} n^j \equiv 0 \pmod{p} \Leftrightarrow j \not\equiv 0 \pmod{p-1}.$$

If $j \equiv 0 \pmod{p-1}$, then $n^j \equiv 1 \pmod{p}$ for each $n$, so $\sum_{n=1}^{p-1} n^j \equiv p-1 \pmod{p}$. If $j \not\equiv 0 \pmod{p-1}$, we can pick a primitive root $m$ modulo $p$, observe that $m^j \not\equiv 1 \pmod{p}$, and then note that

$$\sum_{n=1}^{p-1} n^j \equiv \sum_{n=1}^{p-1} (mn)^j = m^j \sum_{n=1}^{p-1} n^j \pmod{p},$$

which is only possible if $\sum_{n=1}^{p-1} n^j \equiv 0 \pmod{p}$.

We now note that the prime factorization of 2021 is $43 \times 47$, so it suffices to determine when $S(j)$ is divisible by each of 43 and 47. We have

$$\begin{aligned} S(j) &\equiv 46 \sum_{n=1}^{42} n^j \pmod{43} \\ S(j) &\equiv 42 \sum_{n=1}^{46} n^j \pmod{47}. \end{aligned}$$

Since 46 and 42 are coprime to 43 and 47, respectively, we have

$$\begin{aligned} S(j) \equiv 0 \pmod{43} &\Leftrightarrow j \not\equiv 0 \pmod{42} \\ S(j) \equiv 0 \pmod{47} &\Leftrightarrow j \not\equiv 0 \pmod{46}. \end{aligned}$$

This yields the claimed result.

A6 Yes, it follows that $P(2)$ is a composite integer. (Note: 1 is neither prime nor composite.)

Write $P(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_i \in \{0,1\}$ and $a_n = 1$. Let $\alpha$ be an arbitrary root of $P$. Since $P(\alpha) = 0$, $\alpha$ cannot be a positive real number. In addition, if $\alpha \neq 0$ then

$$\begin{aligned} |1 + a_{n-1}\alpha^{-1}| &= |a_{n-2}\alpha^{-2} + \cdots + a_0\alpha^{-n}| \\ &\leq |\alpha|^{-2} + \cdots + |\alpha|^{-n}. \end{aligned}$$

If $\alpha \neq 0$ and $\mathrm{Re}(\alpha) \geq 0$, then $\mathrm{Re}(1 + a_{n-1}\alpha^{-1}) \geq 1$ and

$$1 \leq |\alpha|^{-2} + \cdots + |\alpha|^{-n} < \frac{|\alpha|^{-2}}{1-|\alpha|^{-1}};$$

this yields $|\alpha| < (1+\sqrt{5})/2$.

By the same token, if $\alpha \neq 0$ then

$$|1 + a_{n-1}\alpha^{-1} + a_{n-2}\alpha^{-2}| \leq |\alpha|^{-3} + \cdots + |\alpha|^{-n}.$$

We deduce from this that $\mathrm{Re}(\alpha) \leq 3/2$ as follows.

- There is nothing to check if $\mathrm{Re}(\alpha) \leq 0$.
- If the argument of $\alpha$ belongs to $[-\pi/4, \pi/4]$, then $\mathrm{Re}(\alpha^{-1}), \mathrm{Re}(\alpha^{-2}) \geq 0$, so

  $$1 \leq |\alpha|^{-3} + \cdots + |\alpha|^{-n} < \frac{|\alpha|^{-3}}{1-|\alpha|^{-1}}.$$

  Hence $|\alpha|^{-1}$ is greater than the unique positive root of $x^3 + x - 1$, which is greater than $2/3$.

- Otherwise, $\alpha$ has argument in $(-\pi/2, \pi/4) \cup (\pi/4, \pi/2)$, so the bound $|\alpha| < (1+\sqrt{5})/2$ implies that $\mathrm{Re}(\alpha) < (1+\sqrt{5})/(2\sqrt{2}) < 3/2$.

By hypothesis, there exists a factorization $P(x) = Q(x)R(x)$ into two nonconstant integer polynomials, which we may assume are monic. $Q(x+3/2)$ is a product of polynomials, each of the form $x-\alpha$ where $\alpha$ is a real root of $P$ or of the form

$$\left(x+\frac{3}{2}-\alpha\right)\left(x+\frac{3}{2}-\overline{\alpha}\right) = x^2 + 2\mathrm{Re}\left(\frac{3}{2}-\alpha\right)x + \left|\frac{3}{2}-\alpha\right|^2$$

where $\alpha$ is a nonreal root of $P$. It follows that $Q(x+3/2)$ has positive coefficients; comparing its values at $x=1/2$ and $x=-1/2$ yields $Q(2) > Q(1)$. We cannot have $Q(1) \leq 0$, as otherwise the intermediate value theorem would imply that $Q$ has a real root in $[1,\infty)$; hence $Q(1) \geq 1$ and so $Q(2) \geq 2$. Similarly $R(2) \geq 2$, so $P(2) = Q(2)R(2)$ is composite.

**Remark.** A theorem of Brillhart, Filaseta, and Odlyzko from 1981 states that if a prime $p$ is written as $\sum_i a_i b^i$ in any base $b \geq 2$, the polynomial $\sum_i a_i x^i$ is irreducible. (The case $b=10$ is an older result of Cohn.) The solution given above is taken from: Ram Murty, Prime numbers and irreducible polynomials, *Amer. Math. Monthly* **109** (2002), 452–458). The final step is due to Pólya and Szegő.

B1 The probability is $2 - \frac{6}{\pi}$.

Set coordinates so that the original tiling includes the (filled) square $S = \{(x,y) : 0 \leq x, y \leq 1\}$. It is then equivalent to choose the second square by first choosing a point uniformly at random in $S$ to be the center of the square, then choosing an angle of rotation uniformly at random from the interval $[0, \pi/2]$.

For each $\theta \in [0, \pi/2]$, circumscribe a square $S_\theta$ around $S$ with angle of rotation $\theta$ relative to $S$; this square has side length $\sin\theta + \cos\theta$. Inside $S_\theta$, draw the smaller square $S'_\theta$ consisting of points at distance greater than $1/2$ from each side of $S_\theta$; this square has side length $\sin\theta + \cos\theta - 1$.

We now verify that a unit square with angle of rotation $\theta$ fails to cover any corners of $S$ if and only if its center lies in the interior of $S'_\theta$. In one direction, if one of the corners of $S$ is covered, then that corner lies on a side of $S_\theta$ which meets the dropped square, so the center of the dropped square is at distance less than $1/2$ from that side of $S_\theta$. To check the converse, note that there are two ways to dissect the square $S_\theta$ into the square $S'_\theta$ plus four $\sin\theta \times \cos\theta$ rectangles. If $\theta \neq 0, \pi/4$, then one of these dissections has the property that each corner $P$ of $S$ appears as an interior point of a side (not a corner) of one of the rectangles $R$. It will suffice to check that if the center of the dropped square is in $R$, then the dropped square covers $P$; this follows from the fact that $\sin\theta$ and $\cos\theta$ are both at most 1.

It follows that the conditional probability, given that the angle of rotation is chosen to be $\theta$, that the dropped square does not cover any corners of $S$ is $(\sin\theta + \cos\theta - 1)^2$. We then compute the original probability as the integral

$$\begin{aligned}
&\frac{2}{\pi}\int_0^{\pi/2} (\sin\theta + \cos\theta - 1)^2\,d\theta \\
&= \frac{2}{\pi}\int_0^{\pi/2} (2 + \sin 2\theta - 2\sin\theta - 2\cos\theta)\,d\theta \\
&= \frac{2}{\pi}\left(2\theta - \frac{1}{2}\cos 2\theta + 2\cos\theta - 2\sin\theta\right)_0^{\pi/2} \\
&= \frac{2}{\pi}(\pi + 1 - 2 - 2) = 2 - \frac{6}{\pi}.
\end{aligned}$$

**Remark:** Noam Elkies has some pictures illustrating this problem: image 1, image 2.

B2 The answer is $2/3$.

By AM-GM, we have

$$\begin{aligned}
2^{n+1}(a_1 \cdots a_n)^{1/n} &= \left((4a_1)(4^2a_2)\cdots(4^na_n)\right)^{1/n} \\
&\leq \frac{\sum_{k=1}^n (4^k a_k)}{n}.
\end{aligned}$$

Thus

$$\begin{aligned}
2S &\leq \sum_{n=1}^\infty \frac{\sum_{k=1}^n (4^k a_k)}{4^n} \\
&= \sum_{n=1}^\infty \sum_{k=1}^n (4^{k-n}a_k) = \sum_{k=1}^\infty \sum_{n=k}^\infty (4^{k-n}a_k) \\
&= \sum_{k=1}^\infty \frac{4a_k}{3} = \frac{4}{3}
\end{aligned}$$

and $S \leq 2/3$. Equality is achieved when $a_k = \frac{3}{4^k}$ for all $k$, since in this case $4a_1 = 4^2a_2 = \cdots = 4^na_n$ for all $n$.

B3 We prove the given statement.

For any circle $\mathscr{S}$ of radius $r$ whose center is at distance $d$ from the origin, express the integral in polar coordinates $s, \theta$:

$$\iint_{\mathscr{S}} \rho = \int_{s_1}^{s_2} \int_{\theta_1(s)}^{\theta_2(s)} (yh_x - xh_y)(s\sin\theta, s\cos\theta)\, s\,d\theta\,ds.$$

For fixed $s$, the integral over $\theta$ is a line integral of $\mathrm{grad}\,h$, which evaluates to $h(P_2) - h(P_1)$ where $P_1, P_2$ are the endpoints of the endpoints of the arc of the circle of radius $s$ centered at the origin lying within $\mathscr{S}$. If we now fix $r$ and $d$ and integrate $\iint_{\mathscr{S}} \rho$ over all choices of $\mathscr{S}$ (this amounts to a single integral over an angle in the range $[0, 2\pi]$), we may interchange the order of integration to first integrate over $\theta$, then over the choice of $\mathscr{S}$, and at this point we get 0 for every $s$. We conclude that the integral of $\iint_{\mathscr{S}}$ over all choices of $\mathscr{S}$ vanishes; since the given integral varies continuously in $\mathscr{S}$, by the intermediate value theorem there must be some $\mathscr{S}$ where the given integral is 0.

B4 We can check directly that $R_3 = R_4 = 1$ are Virahanka–Fibonacci numbers; henceforth we will assume $m \geq 5$.

Denote the product $\prod_{k=1}^{F_m-1} k^k$ by $A$. Note that if $F_m$ is composite, say $F_m = ab$ for $a,b > 1$ integers, then $A$ is divisible by $a^a b^b$ and thus by $F_m = ab$; it follows that $R_m = 0 = F_0$ when $F_m$ is composite.

Now suppose that $F_m$ is prime. Since $F_{2n} = F_n(F_{n+1} + F_{n-1})$ for all $n$, $F_m$ is composite if $m > 4$ is even; thus we must have that $m$ is odd. Write $p = F_m$, and use $\equiv$ to denote congruence $\pmod p$. Then we have

$$A = \prod_{k=1}^{p-1} (p-k)^{p-k} \equiv \prod_{k=1}^{p-1} (-k)^{p-k} = (-1)^{p(p-1)/2} \prod_{k=1}^{p-1} k^{p-k}$$

and consequently

$$\begin{aligned} A^2 &\equiv (-1)^{p(p-1)/2} \prod_{k=1}^{p-1} (k^k k^{p-k}) \\ &= (-1)^{p(p-1)/2} ((p-1)!)^p \\ &\equiv (-1)^{p(p+1)/2}, \end{aligned}$$

where the final congruence follows from Wilson's Theorem. Now observe that when $m$ is odd, $p = F_m$ must be congruent to either 1 or 2 $\pmod 4$: this follows from inspection of the Virahanka–Fibonacci sequence mod 4, which has period 6: $1,1,2,3,1,0,1,1,\dots$. It follows that $A^2 \equiv (-1)^{p(p+1)/2} = -1$.

On the other hand, by the Kepler–Cassini identity

$$F_n^2 = (-1)^{n+1} + F_{n-1} F_{n+1}$$

with $n = m-1$, we have $F_{m-1}^2 \equiv (-1)^m = -1$. Thus we have $0 \equiv A^2 - F_{m-1}^2 \equiv (A - F_{m-1})(A - F_{m-2})$. Since $p$ is prime, it must be the case that either $A = F_{m-1}$ or $A = F_{m-2}$, and we are done.

**Remark.** The Kepler–Cassini identity first appears in a letter of Kepler from 1608. Noam Elkies has scanned the relevant page of Kepler's collected works (slightly NSFW if your boss can read Latin).

B5 For convenience, throughout we work with matrices over the field of 2 elements. In this language, if there exists a permutation matrix $P$ such that $P^{-1}AP$ is unipotent (i.e., has 1s on the main diagonal and 0s below it), then $A$ is very odd: any principal submatrix of $A$ is conjugate to a principal submatrix of $P^{-1}AP$, which is again unipotent and in particular nonsingular. We will solve the problem by showing that conversely, for any very odd matrix $A$, there exists a permutation matrix $P$ such that $P^{-1}AP$ is unipotent. Since the latter condition is preserved by taking powers, this will prove the desired result.

To begin, we may take $S = \{i\}$ to see that $a_{ii} = 1$. We next form a (loopless) directed graph on the vertex set $\{1,\dots,n\}$ with an edge from $i$ to $j$ whenever $a_{ij} = 1$, and claim that this graph has no cycles. To see this, suppose the contrary, choose a cycle of minimal length $m \geq 2$, and let $i_1,\dots,i_m$ be the vertices in order. The minimality of the cycle implies that

$$a_{i_j i_k} = \begin{cases} 1 & \text{if } k - j \equiv 0 \text{ or } 1 \pmod m \\ 0 & \text{otherwise.} \end{cases}$$

The submatrix corresponding to $S = \{i_1,\dots,i_m\}$ has row sum 0 and hence is singular, a contradiction.

We now proceed by induction on $n$. Since the directed graph has no cycles, there must be some vertex which is not the starting point of any edge (e.g., the endpoint of any path of maximal length). We may conjugate by a permutation matrix so that this vertex becomes 1. We now apply the induction hypothesis to the submatrix corresponding to $S = \{2,\dots,n\}$ to conclude.

**Remark.** A directed graph without cycles, as in our solution, is commonly called a *DAG (directed acyclic graph)*. It is a standard fact that a directed graph is a TAG if and only if there is a linear ordering of its vertices consistent with all edge directions. See for example `https://en.wikipedia.org/wiki/Directed_acyclic_graph`.

**Remark.** An $n \times n$ matrix $A = (a_{ij})$ for which the value of $a_{ij}$ depends only on $i - j \pmod n$ is called a *circulant matrix*. The circulant matrix with first row $(1,1,0,\dots,0)$ is an example of an $n \times n$ matrix whose determinant is even, but whose other principal minors are all odd.

B6 **First solution.** (based on a suggestion of Noam Elkies) Let $f_k(x)$ be the probability distribution of $X_k$, the last number remaining when one repeatedly trims a list of $3^k$ random variables chosen with respect to the uniform distribution on $[0,1]$; note that $f_0(x) = 1$ for $x \in [0,1]$. Let $F_k(x) = \int_0^x f_k(t)\,dt$ be the cumulative distribution function; by symmetry, $F_k(\frac{1}{2}) = \frac{1}{2}$. Let $\mu_k$ be the expected value of $X_k - \frac{1}{2}$; then $\mu_0 = \frac{1}{4}$, so it will suffice to prove that $\mu_k \geq \frac{2}{3}\mu_{k-1}$ for $k > 0$.

By integration by parts and symmetry, we have

$$\mu_k = 2\int_0^{1/2} \left(\frac{1}{2} - x\right) f_k(x)\,dx = 2\int_0^{1/2} F_k(x)\,dx;$$

that is, $\mu_k$ computes twice the area under the curve $y = F_k(x)$ for $0 \leq x \leq \frac{1}{2}$. Since $F_k$ is a monotone function from $[0,\frac{1}{2}]$ with $F_k(0) = 0$ and $F_k(\frac{1}{2}) = \frac{1}{2}$, we may transpose the axes to obtain

$$\mu_k = 2\int_0^{1/2} \left(\frac{1}{2} - F_k^{-1}(y)\right) dy. \tag{1}$$

Since $f_k(x)$ is the probability distribution of the median of three random variables chosen with respect to the distribution $f_{k-1}(x)$,

$$f_k(x) = 6f_{k-1}(x)F_{k-1}(x)(1-F_{k-1}(x)) \tag{2}$$

or equivalently

$$F_k(x) = 3F_{k-1}(x)^2 - 2F_{k-1}(x)^3. \tag{3}$$

By induction, $F_k$ is the $k$-th iterate of $F_1(x) = 3x^2 - 2x^3$, so

$$F_k(x) = F_{k-1}(F_1(x)). \tag{4}$$

Since $f_1(t) = 6t(1-t) \leq \frac{3}{2}$ for $t \in [0, \frac{1}{2}]$,

$$\frac{1}{2} - F_1(x) = \int_x^{1/2} 6t(1-t)\,dt \leq \frac{3}{2}\left(\frac{1}{2} - x\right);$$

for $y \in [0, \frac{1}{2}]$, we may take $x = F_k^{-1}(y)$ to obtain

$$\frac{1}{2} - F_k^{-1}(y) \geq \frac{2}{3}\left(\frac{1}{2} - F_{k-1}^{-1}(y)\right). \tag{5}$$

Using (4) and (5), we obtain

$$\begin{aligned}\mu_k &= 2\int_0^{1/2}\left(\frac{1}{2} - F_k^{-1}(y)\right) dy \\ &\geq \frac{4}{3}\int_0^{1/2}\left(\frac{1}{2} - F_{k-1}^{-1}(y)\right) dy = \frac{2}{3}\mu_{k-1}\end{aligned}$$

as desired.

**Second solution.** Retain notation as in the first solution. Again $F_k(\frac{1}{2}) = \frac{1}{2}$, so (2) implies

$$f_k\left(\frac{1}{2}\right) = 6f_{k-1}\left(\frac{1}{2}\right) \times \frac{1}{2} \times \frac{1}{2}.$$

By induction on $k$, we deduce that $f_k(\frac{1}{2}) = (\frac{3}{2})^k$ and $f_k(x)$ is nondecreasing on $[0, \frac{1}{2}]$. (More precisely, besides (2), the second assertion uses that $F_{k-1}(x)$ increases from 0 to $1/2$ and $y \mapsto y - y^2$ is nondecreasing on $[0, 1/2]$.)

The expected value of $|X_k - \frac{1}{2}|$ equals

$$\begin{aligned}\mu_k &= 2\int_0^{1/2}\left(\frac{1}{2} - x\right) f_k(x)\,dx \\ &= 2\int_0^{1/2} x f_k\left(\frac{1}{2} - x\right) dx.\end{aligned}$$

Define the function

$$g_k(x) = \begin{cases} \left(\frac{3}{2}\right)^k & x \in \left[0, \frac{1}{2}\left(\frac{2}{3}\right)^k\right] \\ 0 & \text{otherwise.}\end{cases}$$

Note that for $x \in [0, 1/2]$ we have

$$\int_0^x (g_k(t) - f_k(1/2 - t))\,dt \geq 0$$

with equality at $x = 0$ or $x = 1/2$. (On the interval $[0, (1/2)(2/3)^k]$ the integrand is nonnegative, so the function increases from 0; on the interval $[(1/2)(2/3)^k, 1/2]$ the integrand is nonpositive, so the function decreases to 0.) Hence by integration by parts,

$$\begin{aligned}&\mu_k - 2\int_0^{1/2} x g_k(x)\,dx \\ &= \int_0^{1/2} 2x\left(f_k\left(\frac{1}{2} - x\right) - g_k(x)\right) dx \\ &= \int_0^{1/2} x^2\left(\int_0^x g_k(t) - \int_0^x f_k\left(\frac{1}{2} - t\right) dt\,dt\right) dx \geq 0.\end{aligned}$$

(This can also be interpreted as an instance of the *rearrangement inequality*.)

We now see that

$$\begin{aligned}\mu_k &\geq 2\int_0^{1/2} x g_k(x)\,dx \\ &\geq 2\left(\frac{3}{2}\right)^k \int_0^{(1/2)(2/3)^k} x\,dx \\ &= 2\left(\frac{3}{2}\right)^k \frac{1}{2}x^2\Big|_0^{(1/2)(2/3)^k} \\ &= 2\left(\frac{3}{2}\right)^k \frac{1}{8}\left(\frac{2}{3}\right)^{2k} = \frac{1}{4}\left(\frac{2}{3}\right)^k\end{aligned}$$

as desired.

**Remark.** For comparison, if we instead take the median of a list of $n$ numbers, the probability distribution is given by

$$P_{2n+1}(x) = \frac{(2n+1)!}{n!n!}x^n(1-x)^n.$$

The expected value of the absolute difference between $1/2$ and the median is

$$2\int_0^{1/2}(1/2 - x)P_{2n+1}(x)dx = 2^{-2n-2}\binom{2n+1}{n}.$$

For $n = 3^{2021}$, using Stirling's approximation this can be estimated as $1.13(0.577)^{2021} < 0.25(0.667)^{2021}$. This shows that the trimming procedure produces a quantity that is on average further away from 1/2 than the median.

# The 83rd William Lowell Putnam Mathematical Competition
## Saturday, December 3, 2022

A1 Determine all ordered pairs of real numbers $(a,b)$ such that the line $y = ax+b$ intersects the curve $y = \ln(1+x^2)$ in exactly one point.

A2 Let $n$ be an integer with $n \geq 2$. Over all real polynomials $p(x)$ of degree $n$, what is the largest possible number of negative coefficients of $p(x)^2$?

A3 Let $p$ be a prime number greater than 5. Let $f(p)$ denote the number of infinite sequences $a_1, a_2, a_3, \dots$ such that $a_n \in \{1,2,\dots,p-1\}$ and $a_n a_{n+2} \equiv 1 + a_{n+1} \pmod{p}$ for all $n \geq 1$. Prove that $f(p)$ is congruent to 0 or 2 $\pmod{5}$.

A4 Suppose that $X_1, X_2, \dots$ are real numbers between 0 and 1 that are chosen independently and uniformly at random. Let $S = \sum_{i=1}^{k} X_i/2^i$, where $k$ is the least positive integer such that $X_k < X_{k+1}$, or $k = \infty$ if there is no such integer. Find the expected value of $S$.

A5 Alice and Bob play a game on a board consisting of one row of 2022 consecutive squares. They take turns placing tiles that cover two adjacent squares, with Alice going first. By rule, a tile must not cover a square that is already covered by another tile. The game ends when no tile can be placed according to this rule. Alice's goal is to maximize the number of uncovered squares when the game ends; Bob's goal is to minimize it. What is the greatest number of uncovered squares that Alice can ensure at the end of the game, no matter how Bob plays?

A6 Let $n$ be a positive integer. Determine, in terms of $n$, the largest integer $m$ with the following property: There exist real numbers $x_1, \dots, x_{2n}$ with $-1 < x_1 < x_2 < \cdots < x_{2n} < 1$ such that the sum of the lengths of the $n$ intervals

$$[x_1^{2k-1}, x_2^{2k-1}], [x_3^{2k-1}, x_4^{2k-1}], \dots, [x_{2n-1}^{2k-1}, x_{2n}^{2k-1}]$$

is equal to 1 for all integers $k$ with $1 \leq k \leq m$.

B1 Suppose that $P(x) = a_1 x + a_2 x^2 + \cdots + a_n x^n$ is a polynomial with integer coefficients, with $a_1$ odd. Suppose that $e^{P(x)} = b_0 + b_1 x + b_2 x^2 + \cdots$ for all $x$. Prove that $b_k$ is nonzero for all $k \geq 0$.

B2 Let $\times$ represent the cross product in $\mathbb{R}^3$. For what positive integers $n$ does there exist a set $S \subset \mathbb{R}^3$ with exactly $n$ elements such that

$$S = \{v \times w : v, w \in S\}?$$

B3 Assign to each positive real number a color, either red or blue. Let $D$ be the set of all distances $d > 0$ such that there are two points of the same color at distance $d$ apart. Recolor the positive reals so that the numbers in $D$ are red and the numbers not in $D$ are blue. If we iterate this recoloring process, will we always end up with all the numbers red after a finite number of steps?

B4 Find all integers $n$ with $n \geq 4$ for which there exists a sequence of distinct real numbers $x_1, \dots, x_n$ such that each of the sets

$$\{x_1, x_2, x_3\}, \{x_2, x_3, x_4\}, \dots,$$
$$\{x_{n-2}, x_{n-1}, x_n\}, \{x_{n-1}, x_n, x_1\}, \text{ and } \{x_n, x_1, x_2\}$$

forms a 3-term arithmetic progression when arranged in increasing order.

B5 For $0 \leq p \leq 1/2$, let $X_1, X_2, \dots$ be independent random variables such that

$$X_i = \begin{cases} 1 & \text{with probability } p, \\ -1 & \text{with probability } p, \\ 0 & \text{with probability } 1-2p, \end{cases}$$

for all $i \geq 1$. Given a positive integer $n$ and integers $b, a_1, \dots, a_n$, let $P(b, a_1, \dots, a_n)$ denote the probability that $a_1 X_1 + \cdots + a_n X_n = b$. For which values of $p$ is it the case that

$$P(0, a_1, \dots, a_n) \geq P(b, a_1, \dots, a_n)$$

for all positive integers $n$ and all integers $b, a_1, \dots, a_n$?

B6 Find all continuous functions $f : \mathbb{R}^+ \to \mathbb{R}^+$ such that

$$f(xf(y)) + f(yf(x)) = 1 + f(x+y)$$

for all $x, y > 0$.

# Solutions to the 83rd William Lowell Putnam Mathematical Competition
## Saturday, December 3, 2022

Manjul Bhargava, Kiran Kedlaya, and Lenny Ng

A1 Write $f(x) = \ln(1+x^2)$. We show that $y = ax+b$ intersects $y = f(x)$ in exactly one point if and only if $(a,b)$ lies in one of the following groups:

- $a = b = 0$
- $|a| \geq 1$, arbitrary $b$
- $0 < |a| < 1$, and $b < \ln(1-r_-)^2 - |a|r_-$ or $b > \ln(1-r_+)^2 - |a|r_+$, where

$$r_\pm = \frac{1 \pm \sqrt{1-a^2}}{a}.$$

Since the graph of $y = f(x)$ is symmetric under reflection in the $y$-axis, it suffices to consider the case $a \geq 0$: $y = ax+b$ and $y = -ax+b$ intersect $y = f(x)$ the same number of times. For $a = 0$, by the symmetry of $y = f(x)$ and the fact that $f(x) > 0$ for all $x \neq 0$ implies that the only line $y = b$ that intersects $y = f(x)$ exactly once is the line $y = 0$.

We next observe that on $[0,\infty)$, $f'(x) = \frac{2x}{1+x^2}$ increases on $[0,1]$ from $f'(0) = 0$ to a maximum at $f'(1) = 1$, and then decreases on $[1,\infty)$ with $\lim_{x\to\infty} f'(x) = 0$. In particular, $f'(x) \leq 1$ for all $x$ (including $x < 0$ since then $f'(x) < 0$) and $f'(x)$ achieves each value in $(0,1)$ exactly twice on $[0,\infty)$.

For $a \geq 1$, we claim that any line $y = ax+b$ intersects $y = f(x)$ exactly once. They must intersect at least once by the intermediate value theorem: for $x \ll 0$, $ax+b < 0 < f(x)$, while for $x \gg 0$, $ax+b > f(x)$ since $\lim_{x\to\infty} \frac{\ln(1+x^2)}{x} = 0$. On the other hand, they cannot intersect more than once: for $a > 1$, this follows from the mean value theorem, since $f'(x) < a$ for all $x$. For $a = 1$, suppose that they intersect at two points $(x_0,y_0)$ and $(x_1,y_1)$. Then

$$1 = \frac{y_1-y_0}{x_1-x_0} = \frac{\int_{x_0}^{x_1} f'(x)\,dx}{x_1-x_0} < 1$$

since $f'(x)$ is continuous and $f'(x) \leq 1$ with equality only at one point.

Finally we consider $0 < a < 1$. The equation $f'(x) = a$ has exactly two solutions, at $x = r_-$ and $x = r_+$ for $r_\pm$ as defined above. If we define $g(x) = f(x) - ax$, then $g'(r_\pm) = 0$; $g'$ is strictly decreasing on $(-\infty, r_-)$, strictly increasing on $(r_-,r_+)$, and strictly decreasing on $(r_+,\infty)$; and $\lim_{x\to-\infty} g(x) = \infty$ while $\lim_{x\to\infty} g(x) = -\infty$. It follows that $g(x) = b$ has exactly one solution for $b < g(r_-)$ or $b > g(r_+)$, exactly three solutions for $g(r_-) < b < g(r_+)$, and exactly two solutions for $b = g(r_\pm)$. That is, $y = ax+b$ intersects $y = f(x)$ in exactly one point if and only if $b < g(r_-)$ or $b > g(r_+)$.

A2 The answer is $2n-2$. Write $p(x) = a_nx^n + \cdots + a_1x + a_0$ and $p(x)^2 = b_{2n}x^{2n} + \cdots + b_1x + b_0$. Note that $b_0 = a_0^2$ and $b_{2n} = a_n^2$. We claim that not all of the remaining $2n-1$ coefficients $b_1,\dots,b_{2n-1}$ can be negative, whence the largest possible number of negative coefficients is $\leq 2n-2$. Indeed, suppose $b_i < 0$ for $1 \leq i \leq 2n-1$. Since $b_1 = 2a_0a_1$, we have $a_0 \neq 0$. Assume $a_0 > 0$ (or else replace $p(x)$ by $-p(x)$). We claim by induction on $i$ that $a_i < 0$ for $1 \leq i \leq n$. For $i = 1$, this follows from $2a_0a_1 = b_1 < 0$. If $a_i < 0$ for $1 \leq i \leq k-1$, then

$$2a_0a_k = b_k - \sum_{i=1}^{k-1} a_ia_{k-i} < b_k < 0$$

and thus $a_k < 0$, completing the induction step. But now $b_{2n-1} = 2a_{n-1}a_n > 0$, contradiction.

It remains to show that there is a polynomial $p(x)$ such that $p(x)^2$ has $2n-2$ negative coefficients. For example, we may take

$$p(x) = n(x^n+1) - 2(x^{n-1} + \cdots + x),$$

so that

$$p(x)^2 = n^2(x^{2n}+x^n+1) - 2n(x^n+1)(x^{n-1}+\cdots+x) + (x^{n-1}+\cdots+x)^2.$$

For $i \in \{1,\dots,n-1,n+1,\dots,n-1\}$, the coefficient of $x^i$ in $p(x)^2$ is at most $-2n$ (coming from the cross term) plus $-2n+2$ (from expanding $(x^{n-1}+\cdots+x)^2$), and hence negative.

A3 **First solution.** We view the sequence $a_1,a_2,\dots$ as lying in $\mathbb{F}_p^\times \subset \mathbb{F}_p$. Then the sequence is determined by the values of $a_1$ and $a_2$, via the recurrence $a_{n+2} = (1+a_{n+1})/a_n$. Using this recurrence, we compute

$$a_3 = \frac{1+a_2}{a_1},\, a_4 = \frac{1+a_1+a_2}{a_1a_2},$$
$$a_5 = \frac{1+a_1}{a_2},\, a_6 = a_1,\, a_7 = a_2$$

and thus the sequence is periodic with period 5. The values for $a_1$ and $a_2$ may thus be any values in $\mathbb{F}_p^\times$ provided that $a_1 \neq p-1$, $a_2 \neq p-1$, and $a_1+a_2 \neq p-1$. The number of choices for $a_1,a_2 \in \{1,\dots,p-2\}$ such that $a_1+a_2 \neq p-1$ is thus $(p-2)^2 - (p-2) = (p-2)(p-3)$.

Since $p$ is not a multiple of 5, $(p-2)(p-3)$ is a product of two consecutive integers $a, a+1$, where $a \not\equiv 2 \pmod 5$. Now $0\cdot 1 \equiv 0$, $1\cdot 2 \equiv 2$, $3\cdot 4 \equiv 2$, and

$4 \cdot 0 \equiv 0 \pmod 5$. Thus the number of possible sequences $a_1, a_2, \dots$ is 0 or 2 (mod 5), as desired.

**Second solution.** Say that a sequence is *admissible* if it satisfies the given conditions. As in the first solution, any admissible sequence is 5-periodic.

Now consider the collection $S$ of possible 5-tuples of numbers mod $p$ given by $(a_1, a_2, a_3, a_4, a_5)$ for admissible sequences $\{a_n\}$. Each of these 5-tuples in $S$ comes from a unique admissible sequence, and there is a 5-periodic action on $S$ given by cyclic permutation: $(a,b,c,d,e) \to (b,c,d,e,a)$. This action divides $S$ into finitely many orbits, and each orbit either consists of 5 distinct tuples (if $a,b,c,d,e$ are not all the same) or 1 tuple $(a,a,a,a,a)$. It follows that the number of admissible sequences is a multiple of 5 plus the number of constant admissible sequences.

Constant admissible sequences correspond to nonzero numbers $a \pmod p$ such that $a^2 \equiv 1 + a \pmod p$. Since the quadratic $x^2 - x - 1$ has discriminant 5, for $p > 5$ it has either 2 roots (if the discriminant is a quadratic residue mod $p$) or 0 roots mod $p$.

A4 The expected value is $2e^{1/2} - 3$.

Extend $S$ to an infinite sum by including zero summands for $i > k$. We may then compute the expected value as the sum of the expected value of the $i$-th summand over all $i$. This summand occurs if and only if $X_1, \dots, X_{i-1} \in [X_i, 1]$ and $X_1, \dots, X_{i-1}$ occur in nonincreasing order. These two events are independent and occur with respective probabilities $(1 - X_i)^{i-1}$ and $\frac{1}{(i-1)!}$; the expectation of this summand is therefore

$$\begin{aligned} &\frac{1}{2^i (i-1)!} \int_0^1 t(1-t)^{i-1}\,dt \\ &\quad = \frac{1}{2^i (i-1)!} \int_0^1 ((1-t)^{i-1} - (1-t)^i)\,dt \\ &\quad = \frac{1}{2^i (i-1)!} \left( \frac{1}{i} - \frac{1}{i+1} \right) = \frac{1}{2^i (i+1)!}. \end{aligned}$$

Summing over $i$, we obtain

$$\sum_{i=1}^{\infty} \frac{1}{2^i (i+1)!} = 2 \sum_{i=2}^{\infty} \frac{1}{2^i i!} = 2 \left( e^{1/2} - 1 - \frac{1}{2} \right).$$

A5 We show that the number in question equals 290. More generally, let $a(n)$ (resp. $b(n)$) be the optimal final score for Alice (resp. Bob) moving first in a position with $n$ consecutive squares. We show that

$$\begin{aligned} a(n) &= \left\lfloor \frac{n}{7} \right\rfloor + a\left( n - 7 \left\lfloor \frac{n}{7} \right\rfloor \right), \\ b(n) &= \left\lfloor \frac{n}{7} \right\rfloor + b\left( n - 7 \left\lfloor \frac{n}{7} \right\rfloor \right), \end{aligned}$$

and that the values for $n \leq 6$ are as follows:

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $a(n)$ | 0 | 1 | 0 | 1 | 2 | 1 | 2 |
| $b(n)$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 |

Since $2022 \equiv 6 \pmod 7$, this will yield $a(2022) = 2 + \lfloor \frac{2022}{7} \rfloor = 290$.

We proceed by induction, starting with the base cases $n \leq 6$. Since the number of odd intervals never decreases, we have $a(n), b(n) \geq n - 2\lfloor \frac{n}{2} \rfloor$; by looking at the possible final positions, we see that equality holds for $n = 0,1,2,3,5$. For $n = 4,6$, Alice moving first can split the original interval into two odd intervals, guaranteeing at least two odd intervals in the final position; whereas Bob can move to leave behind one or two intervals of length 2, guaranteeing no odd intervals in the final position.

We now proceed to the induction step. Suppose that $n \geq 7$ and the claim is known for all $m < n$. In particular, this means that $a(m) \geq b(m)$; consequently, it does not change the analysis to allow a player to pass their turn after the first move, as both players will still have an optimal strategy which involves never passing.

It will suffice to check that

$$a(n) = a(n-7) + 1, \qquad b(n) = b(n-7) + 1.$$

Moving first, Alice can leave behind two intervals of length 1 and $n-3$. This shows that

$$a(n) \geq 1 + b(n-3) = a(n-7) + 1.$$

On the other hand, if Alice leaves behind intervals of length $i$ and $n-2-i$, Bob can choose to play in either one of these intervals and then follow Alice's lead thereafter (exercising the pass option if Alice makes the last legal move in one of the intervals). This shows that

$$\begin{aligned} a(n) &\leq \max\{\min\{a(i) + b(n-2-i), \\ &\qquad b(i) + a(n-2-i)\} : i = 0,1,\dots,n-2\} \\ &= a(n-7) + 1. \end{aligned}$$

Moving first, Bob can leave behind two intervals of lengths 2 and $n-4$. This shows that

$$b(n) \leq a(n-4) = b(n-7) + 1.$$

On the other hand, if Bob leaves behind intervals of length $i$ and $n-2-i$, Alice can choose to play in either one of these intervals and then follow Bob's lead thereafter (again passing as needed). This shows that

$$\begin{aligned} b(n) &\geq \min\{\max\{a(i) + b(n-2-i), \\ &\qquad b(i) + a(n-2-i)\} : i = 0,1,\dots,n-2\} \\ &= b(n-7) + 1. \end{aligned}$$

This completes the induction.

A6 **First solution.** The largest such $m$ is $n$. To show that $m \geq n$, we take

$$x_j = \cos \frac{(2n+1-j)\pi}{2n+1} \qquad (j = 1, \dots, 2n).$$

It is apparent that $-1 < x_1 < \cdots < x_{2n} < 1$. The sum of the lengths of the intervals can be interpreted as

$$\begin{aligned}
&-\sum_{j=1}^{2n}((-1)^{2n+1-j}x_j)^{2k-1} \\
&= -\sum_{j=1}^{2n}\left(\cos(2n+1-j)\left(\pi+\frac{\pi}{2n+1}\right)\right)^{2k-1} \\
&= -\sum_{j=1}^{2n}\left(\cos\frac{2\pi(n+1)j}{2n+1}\right)^{2k-1}.
\end{aligned}$$

For $\zeta = e^{2\pi i(n+1)/(2n+1)}$, this becomes

$$\begin{aligned}
&= -\sum_{j=1}^{2n}\left(\frac{\zeta^j+\zeta^{-j}}{2}\right)^{2k-1} \\
&= -\frac{1}{2^{2k-1}}\sum_{j=1}^{2n}\sum_{l=0}^{2k-1}\binom{2k-1}{l}\zeta^{j(2k-1-2l)} \\
&= -\frac{1}{2^{2k-1}}\sum_{l=0}^{2k-1}\binom{2k-1}{l}\sum_{j=1}^{2n}\zeta^{j(2k-1-2l)} \\
&= -\frac{1}{2^{2k-1}}\sum_{l=0}^{2k-1}\binom{2k-1}{l}(-1) = 1,
\end{aligned}$$

using the fact that $\zeta^{2k-1-2l}$ is a *nontrivial* root of unity of order dividing $2n+1$.

To show that $m \leq n$, we use the following lemma. We say that a multiset $\{x_1,\dots,x_m\}$ of complex numbers is *inverse-free* if there are no two indices $1 \leq i \leq j \leq m$ such that $x_i + x_j = 0$; this implies in particular that 0 does not occur.

**Lemma.** *Let $\{x_1,\dots,x_m\},\{y_1,\dots,y_n\}$ be two inverse-free multisets of complex numbers such that*

$$\sum_{i=1}^{m}x_i^{2k-1} = \sum_{i=1}^{n}y_i^{2k-1} \qquad (k=1,\dots,\max\{m,n\}).$$

*Then these two multisets are equal.*

*Proof.* We may assume without loss of generality that $m \leq n$. Form the rational functions

$$f(z) = \sum_{i=1}^{m}\frac{x_iz}{1-x_i^2z^2}, \quad g(z) = \sum_{i=1}^{n}\frac{y_iz}{1-y_i^2z^2};$$

both $f(z)$ and $g(z)$ have total pole order at most $2n$. Meanwhile, by expanding in power series around $z=0$, we see that $f(z)-g(z)$ is divisible by $z^{2n+1}$. Consequently, the two series are equal.

However, we can uniquely recover the multiset $\{x_1,\dots,x_m\}$ from $f(z)$: $f$ has poles at $\{1/x_1^2,\dots,1/x_m^2\}$ and the residue of the pole at $z=1/x_i^2$ uniquely determines both $x_i$ (i.e., its sign) and its multiplicity. Similarly, we may recover $\{y_1,\dots,y_n\}$ from $g(z)$, so the two multisets must coincide. □

Now suppose by way of contradiction that we have an example showing that $m \geq n+1$. We then have

$$1^{2k-1} + \sum_{i=1}^{n}x_{2i-1}^{2k-1} = \sum_{i=1}^{n}x_{2i}^{2k-1} \qquad (k=1,\dots,n+1).$$

By the lemma, this means that the multisets $\{1,x_1,x_3,\dots,x_{2n-1}\}$ and $\{x_2,x_4,\dots,x_{2n}\}$ become equal after removing pairs of inverses until this becomes impossible. However, of the resulting two multisets, the first contains 1 and the second does not, yielding the desired contradiction.

**Remark.** One can also prove the lemma using the invertibility of the Vandermonde matrix

$$(x_i^j)_{i=0,\dots,n;j=0,\dots,n}$$

for $x_0,\dots,x_n$ pairwise distinct (this matrix has determinant $\prod_{0\leq i<j\leq n}(x_i-x_j) \neq 0$). For a similar argument, see Proposition 22 of: M. Bhargava, Galois groups of random integer polynomials and van der Waerden's conjecture, arXiv:2111.06507.

**Remark.** The solution for $m=n$ given above is not unique (see below). However, it does become unique if we add the assumption that $x_i = -x_{2n+1-i}$ for $i = 1,\dots,2n$ (i.e., the set of intervals is symmetric around 0).

**Second solution.** (by Evan Dummit) Define the polynomial

$$p(x) = (x-x_1)(x+x_2)\cdots(x-x_{2n-1})(x+x_{2n})(x+1);$$

by hypothesis, $p(x)$ has $2n+1$ distinct real roots in the interval $[-1,1)$. Let $s_k$ denote the $k$-th power sum of $p(x)$; then for any given $m$, the desired condition is that $s_{2k-1}=0$ for $k=1,\dots,m$. Let $e_k$ denote the $k$-th elementary symmetric function of the roots of $p(x)$; that is,

$$p(x) = x^{2n+1} + \sum_{i=k}^{2n+1}(-1)^k e_k x^{2n+1-k}.$$

By the Girard–Newton identities,

$$(2k-1)e_{2k-1} = s_1e_{2k-2} - s_2e_{2k-2} + \cdots - s_{2k}e_1;$$

hence the desired condition implies that $e_{2k-1}=0$ for $k=1,\dots,m$.

If we had a solution with $m=n+1$, then the vanishing of $e_1,\dots,e_{2k+1}$ would imply that $p(x)$ is an odd polynomial (that is, $p(x)=-p(x)$ for all $x$), which in turn would imply that $x=1$ is also a root of $p$. Since we have already identified $2n+1$ other roots of $p$, this yields a contradiction.

By the same token, a solution with $m=n$ corresponds to a polynomial $p(x)$ of the form $xq(x^2)+a$ for some polynomial $q(x)$ of degree $n$ and some real number $a$ (necessarily equal to $q(1)$). It will thus suffice to choose $q(x)$

so that the resulting polynomial $p(x)$ has roots consisting of $-1$ plus $2n$ distinct values in $(-1,1)$. To do this, start with any polynomial $r(x)$ of degree $n$ with $n$ distinct positive roots (e.g., $r(x) = (x-1)\cdots(x-n)$). The polynomial $xr(x^2)$ then has $2n+1$ distinct real roots; consequently, for $\varepsilon > 0$ sufficiently small, $xr(x^2)+\varepsilon$ also has $2n+1$ distinct real roots. Let $-\alpha$ be the smallest of these roots (so that $\alpha > 0$); we then take $q(x) = r(x\sqrt{\alpha})$ to achieve the desired result.

**Remark.** Brian Lawrence points out that one can also produce solutions for $m = n$ by starting with the degenerate solution

$$-a_{n-1},\dots,-a_1,0,a_1,\dots,a_{n-1},1$$

(where $0 < a_1 < \cdots < a_{n-1} < 1$ but no other conditions are imposed) and deforming it using the implicit function theorem. More precisely, there exists a differentiable parametric solution $x_1(t),\dots,x_{2n}(t)$ with $x_i(t) = x_{2n-i}(t)$ for $i = 1,\dots,n-1$ specializing to the previous solution at $t = 0$, such that $x_i'(0) \neq 0$ for $i = n,\dots,2n$; this is because the Jacobian matrix

$$J = ((2k-1)x_i(0)^{2k-2})_{i=n,\dots,2n;k=1,\dots,n}$$

(interpreting $0^0$ as 1) has the property that every maximal minor is nonzero (these being scaled Vandermonde matrices). In particular we may normalize so that $x_{2n}'(0) < 0$, and then evaluating at a small positive value of $t$ gives the desired example.

In the proof that $m = n+1$ cannot occur, one can similarly use the implicit function theorem (with some care) to reduce to the case where $\{|x_1|,\dots,|x_{2n}|\}$ has cardinality $n+1$. This can be extended to a complete solution, but the details are rather involved.

B1 We prove that $b_k k!$ is an odd integer for all $k \geq 0$.

**First solution.** Since $e^{P(x)} = \sum_{n=0}^\infty \frac{(P(x))^n}{n!}$, the number $k!\,b_k$ is the coefficient of $x^k$ in

$$(P(x))^k + \sum_{n=0}^{k-1} \frac{k!}{n!}(P(x))^n.$$

In particular, $b_0 = 1$ and $b_1 = a_1$ are both odd.

Now suppose $k \geq 2$; we want to show that $b_k$ is odd. The coefficient of $x^k$ in $(P(x))^k$ is $a_1^k$. It suffices to show that the coefficient of $x^k$ in $\frac{k!}{n!}(P(x))^n$ is an even integer for any $n < k$. For $k$ even or $n \leq k-2$, this follows immediately from the fact that $\frac{k!}{n!}$ is an even integer. For $k$ odd and $n = k-1$, we have

$$\begin{aligned}\frac{k!}{(k-1)!}(P(x))^{k-1} &= k(a_1x + a_2x^2 + \cdots)^{k-1} \\ &= k(a_1^{k-1}x^{k-1} + (k-1)a_1^{k-2}a_2x^k + \cdots)\end{aligned}$$

and the coefficient of $x^k$ is $k(k-1)a_1^{k-2}a_2$, which is again an even integer.

**Second solution.** Let $G$ be the set of power series of the form $\sum_{n=0}^\infty c_n \frac{x_n}{n!}$ with $c_0 = 1, c_n \in \mathbb{Z}$; then $G$ forms a group under formal series multiplication because

$$\left(\sum_{n=0}^\infty c_n \frac{x^n}{n!}\right)\left(\sum_{n=0}^\infty d_n \frac{x^n}{n!}\right) = \sum_{n=0}^\infty e_n \frac{x^n}{n!}$$

with

$$e_n = \sum_{m=0}^n \binom{n}{m} c_m d_{n-m}.$$

By the same calculation, the subset $H$ of series with $c_n \in 2\mathbb{Z}$ for all $n \geq 1$ is a subgroup of $G$.

We have $e^{2x} \in H$ because $\frac{2^n}{n!} \in 2\mathbb{Z}$ for all $n \geq 1$: the exponent of 2 in the prime factorization of $n!$ is

$$\sum_{i=1}^\infty \left\lfloor \frac{n}{2^i} \right\rfloor < \sum_{i=1}^\infty \frac{n}{2^i} = n.$$

For any integer $k \geq 2$, we have $e^{x^k} \in H$ because $\frac{(nk)!}{n!} \in 2\mathbb{Z}$ for all $n \geq 1$: this is clear if $k = 2, n = 1$, and in all other cases the ratio is divisible by $(n+1)(n+2)$.

We deduce that $e^{P(x)-x} \in H$. By writing $e^{P(x)}$ as $e^x = \sum_{n=0}^\infty \frac{x^n}{n!}$ times an element of $H$, we deduce that $k!b_k$ is odd for all $k \geq 0$.

**Third solution.** (by David Feldman) We interpret $e^{P(x)}$ using the exponential formula for generating functions. For each $j$, choose a set $S_j$ consisting of $|a_j|$ colors. Then $b_k$ is a weighted count over set partitions of $\{1,\dots,k\}$, with each part of size $j$ assigned a color in $S_j$, and the weight being $(-1)^i$ where $i$ is the number of parts of any size $j$ for which $a_j < 0$.

Since we are only looking for the parity of $b_k$, we may dispense with the signs; that is, we may assume $a_j \geq 0$ for all $j$ and forget about the weights.

Choose an involution on each $S_j$ with at most one fixed point; this induces an involution on the partitions, so to find the parity of $b_k$ we may instead count fixed points of the involution. That is, we may assume that $a_j \in \{0,1\}$.

Let $T_k$ be the set of set partitions in question with the all-singletons partition removed; it now suffices to exhibit a fixed-point-free involution of $T_k$. To wit, for each partition in $T_k$, there is a smallest index $i \in \{1,\dots,k-1\}$ for which $i$ and $i+1$ are not both singletons; we define an involution by swapping the positions of $i$ and $i+1$.

B2 The possible values of $n$ are 1 and 7.

Clearly the set $S = \{0\}$ works. Suppose that $S \neq \{0\}$ is a finite set satisfying the given condition; in particular, $S$ does not consist of a collection of collinear vectors, since otherwise $\{v \times w : v, w \in S\} = \{0\}$. We claim that $S$ cannot contain any nonzero vector $v$ with $\|v\| \neq 1$. Suppose otherwise, and let $w \in S$ be a vector not collinear with $v$. Then $S$ must contain the nonzero vector $u_1 = v \times w$, as well as the sequence of vectors $u_n$ defined inductively by $u_n = v \times u_{n-1}$. Since each $u_n$ is orthogonal to $v$ by construction, we have $\|u_n\| = \|v\|\|u_{n-1}\|$ and so $\|u_n\| = \|v\|^{n-1}\|u_1\|$. The sequence $\|u_n\|$ consists of all distinct numbers and thus $S$ is infinite, a contradiction. This proves the claim, and so every nonzero vector in $S$ is a unit vector.

Next note that any pair of vectors $v, w \in S$ must either be collinear or orthogonal: by the claim, $v, w$ are both unit vectors, and if $v, w$ are not collinear then $v \times w \in S$ must be a unit vector, whence $v \perp w$. Now choose any pair of non-collinear vectors $v_1, v_2 \in S$, and write $v_3 = v_1 \times v_2$. Then $\{v_1, v_2, v_3\}$ is an orthonormal basis of $\mathbb{R}^3$, and it follows that all of these vectors are in $S$: 0, $v_1$, $v_2$, $v_3$, $-v_1 = v_3 \times v_2$, $-v_2 = v_1 \times v_3$, and $-v_3 = v_2 \times v_1$. On the other hand, $S$ cannot contain any vector besides these seven, since any other vector $w$ in $S$ would have to be simultaneously orthogonal to all of $v_1, v_2, v_3$.

Thus any set $S \neq \{0\}$ satisfying the given condition must be of the form $\{0, \pm v_1, \pm v_2, \pm v_3\}$ where $\{v_1, v_2, v_3\}$ is an orthonormal basis of $\mathbb{R}^3$. It is clear that any set of this form does satisfy the given condition. We conclude that the answer is $n = 1$ or $n = 7$.

B3 The answer is yes. Let $R_0, B_0 \subset \mathbb{R}^+$ be the set of red and blue numbers at the start of the process, and let $R_n, B_n$ be the set of red and blue numbers after $n$ steps. We claim that $R_2 = \mathbb{R}^+$.

We first note that if $y \in B_1$, then $y/2 \in R_1$. Namely, the numbers $y$ and $2y$ must be of opposite colors in the original coloring, and then $3y/2$ must be of the same color as one of $y$ or $2y$.

Now suppose by way of contradiction that $x \in B_2$. Then of the four numbers $x, 2x, 3x, 4x$, every other number must be in $R_1$ and the other two must be in $B_1$. By the previous observation, $2x$ and $4x$ cannot both be in $B_1$; it follows that $2x, 4x \in R_1$ and $x, 3x \in B_1$. By the previous observation again, $x/2$ and $3x/2$ must both be in $R_1$, but then $x = 3x/2 - x/2$ is in $R_2$, contradiction. We conclude that $R_2 = \mathbb{R}^+$, as desired.

B4 The values of $n$ in question are the multiples of 3 starting with 9. Note that we interpret "distinct" in the problem statement to mean "pairwise distinct" (i.e., no two equal). See the remark below.

We first show that such a sequence can only occur when $n$ is divisible by 3. If $d_1$ and $d_2$ are the common differences of the arithmetic progressions $\{x_m, x_{m+1}, x_{m+2}\}$ and $\{x_{m+1}, x_{m+2}, x_{m+3}\}$ for some $m$, then $d_2 \in \{d_1, 2d_1, d_1/2\}$. By scaling we may assume that the smallest common difference that occurs is 1; in this case, all of the common differences are integers. By shifting, we may assume that the $x_i$ are themselves all integers. We now observe that any three consecutive terms in the sequence have pairwise distinct residues modulo 3, forcing $n$ to be divisible by 3.

We then observe that for any $m \geq 2$, we obtain a sequence of the desired form of length $3m+3 = (2m-1)+1+(m+1)+2$ by concatenating the arithmetic progressions

$$\begin{gathered}(1, 3, \dots, 4m-3, 4m-1),\\ 4m-2, (4m, 4m-4, \dots, 4, 0), 2.\end{gathered}$$

We see that no terms are repeated by noting that the first parenthesized sequence consists of odd numbers; the second sequence consists of multiples of 4; and the remaining numbers 2 and $4m-2$ are distinct (because $m \geq 2$) but both congruent to 2 mod 4.

It remains to show that no such sequence occurs with $n = 6$. We may assume without loss of generality that the smallest common difference among the arithmetic progressions is 1 and occurs for $\{x_1, x_2, x_3\}$; by rescaling, shifting, and reversing the sequence as needed, we may assume that $x_1 = 0$ and $(x_2, x_3) \in \{(1,2), (2,1)\}$. We then have $x_4 = 3$ and

$$(x_5, x_6) \in \{(4,5), (-1,-5), (-1,7), (5,4), (5,7)\}.$$

In none of these cases does $\{x_5, x_6, 0\}$ form an arithmetic progression.

**Remark.** If one interprets "distinct" in the problem statement to mean "not all equal", then the problem becomes simpler: the same argument as above shows that $n$ must be a multiple of 3, in which case a suitable repetition of the sequence $-1, 0, 1$ works.

B5 **First solution.** The answer is $p \leq 1/4$. We first show that $p > 1/4$ does not satisfy the desired condition. For $p > 1/3$, $P(0,1) = 1 - 2p < p = P(1,1)$. For $p = 1/3$, it is easily calculated (or follows from the next calculation) that $P(0,1,2) = 1/9 < 2/9 = P(1,1,2)$. Now suppose $1/4 < p < 1/3$, and consider $(b, a_1, a_2, a_3, \dots, a_n) = (1, 1, 2, 4, \dots, 2^{n-1})$. The only solution to

$$X_1 + 2X_2 + \cdots + 2^{n-1}X_n = 0$$

with $X_j \in \{0, \pm 1\}$ is $X_1 = \cdots = X_n = 0$; thus $P(0, 1, 2, \dots, 2^{2n-1}) = (1-2p)^n$. On the other hand, the solutions to

$$X_1 + 2X_2 + \cdots + 2^{n-1}X_n = 1$$

with $X_j \in \{0, \pm 1\}$ are

$$\begin{gathered}(X_1, X_2, \dots, X_n) = (1, 0, \dots, 0), (-1, 1, 0, \dots, 0),\\ (-1, -1, 1, 0, \dots, 0), \dots, (-1, -1, \dots, -1, 1),\end{gathered}$$

and so

$$\begin{aligned}&P(1, 1, 2, \dots, 2^{n-1})\\ &= p(1-2p)^{n-1} + p^2(1-2p)^{n-2} + \cdots + p^n\\ &= p\frac{(1-2p)^n - p^n}{1-3p}.\end{aligned}$$

It follows that the inequality $P(0,1,2,\dots,2^{n-1}) \geq P(1,1,2,\dots,2^{n-1})$ is equivalent to

$$p^{n+1} \geq (4p-1)(1-2p)^n,$$

but this is false for sufficiently large $n$ since $4p-1>0$ and $p<1-2p$.

Now suppose $p \leq 1/4$; we want to show that for arbitrary $a_1,\dots,a_n$ and $b \neq 0$, $P(0,a_1,\dots,a_n) \geq P(b,a_1,\dots,a_n)$. Define the polynomial

$$f(x) = px + px^{-1} + 1 - 2p,$$

and observe that $P(b,a_1,\dots,a_n)$ is the coefficient of $x^b$ in $f(x^{a_1})f(x^{a_2})\cdots f(x^{a_n})$. We can write

$$f(x^{a_1})f(x^{a_2})\cdots f(x^{a_n}) = g(x)g(x^{-1})$$

for some real polynomial $g$: indeed, if we define $\alpha = \frac{1-2p+\sqrt{1-4p}}{2p} > 0$, then $f(x) = \frac{p}{\alpha}(x+\alpha)(x^{-1}+\alpha)$, and so we can use

$$g(x) = \left(\frac{p}{\alpha}\right)^{n/2}(x^{a_1}+\alpha)\cdots(x^{a_n}+\alpha).$$

It now suffices to show that in $g(x)g(x^{-1})$, the coefficient of $x^0$ is at least as large as the coefficient of $x^b$ for any $b \neq 0$. Since $g(x)g(x^{-1})$ is symmetric upon inverting $x$, we may assume that $b>0$. If we write $g(x) = c_0x^0 + \cdots + c_mx^m$, then the coefficients of $x^0$ and $x^b$ in $g(x)g(x^{-1})$ are $c_0^2 + c_1^2 + \cdots + c_m^2$ and $c_0c_b + c_1c_{b+1} + \cdots + c_{m-b}c_m$, respectively. But

$$\begin{aligned}
&2(c_0c_b + c_1c_{b+1} + \cdots + c_{m-b}c_m) \\
&\leq (c_0^2+c_b^2) + (c_1^2+c_{b+1}^2) + \cdots + (c_{m-b}^2+c_m^2) \\
&\leq 2(c_0^2+\cdots+c_m^2),
\end{aligned}$$

and the result follows.

**Second solution.** (by Yuval Peres) We check that $p \leq 1/4$ is necessary as in the first solution. To check that it is sufficient, we introduce the following concept: for $X$ a random variable taking finitely many integer values, define the *characteristic function*

$$\varphi_X(\theta) = \sum_{\ell \in \mathbb{Z}} P(X=\ell)e^{i\ell\theta}$$

(i.e., the expected value of $e^{iX\theta}$, or the Fourier transform of the probability measure corresponding to $X$). We use two evident properties of these functions:

- If $X$ and $Y$ are independent, then $\varphi_{X+Y}(\theta) = \varphi_X(\theta) + \varphi_Y(\theta)$.
- For any $b \in \mathbb{Z}$,

  $$P(X=b) = \frac{1}{2}\int_0^{2\pi} e^{-ib\theta}\varphi_X(\theta)\,d\theta.$$

  In particular, if $\varphi_X(\theta) \geq 0$ for all $\theta$, then $P(X=b) \leq P(X=0)$.

For $p \leq 1/4$, we have

$$\varphi_{X_k}(\theta) = (1-2p) + 2p\cos(\theta) \geq 0.$$

Hence for $a_1,\dots,a_n \in \mathbb{Z}$, the random variable $S = a_1X_1 + \cdots + a_nX_n$ satisfies

$$\varphi_S(\theta) = \prod_{k=1}^n \varphi_{a_kX_k}(\theta) = \prod_{k=1}^n \varphi_{X_k}(a_k\theta) \geq 0.$$

We may thus conclude that $P(S=b) \leq P(S=0)$ for any $b \in \mathbb{Z}$, as desired.

B6 The only such functions are the functions $f(x) = \frac{1}{1+cx}$ for some $c \geq 0$ (the case $c=0$ giving the constant function $f(x)=1$). Note that we interpret $\mathbb{R}^+$ in the problem statement to mean the set of positive real numbers, excluding 0.

For convenience, we reproduce here the given equation:

$$f(xf(y)) + f(yf(x)) = 1 + f(x+y) \tag{1}$$

We first prove that

$$\lim_{x\to 0^+} f(x) = 1. \tag{2}$$

Set

$$L_- = \liminf_{x\to 0^+} f(x), \quad L_+ = \limsup_{x\to 0^+} f(x).$$

For any fixed $y$, we have by (1)

$$\begin{aligned}
L_+ &= \limsup_{x\to 0^+} f(xf(y)) \\
&\leq \limsup_{x\to 0^+}(1+f(x+y)) = 1+f(y) < \infty.
\end{aligned}$$

Consequently, $xf(x) \to 0$ as $x \to 0^+$. By (2) with $y=x$,

$$\begin{aligned}
2L_+ &= \limsup_{x\to 0^+} 2f(xf(x)) \\
&= \limsup_{x\to 0^+}(1+f(2x)) = 1+L_+ \\
2L_- &= \liminf_{x\to 0^+} 2f(xf(x)) \\
&= \liminf_{x\to 0^+}(1+f(2x)) = 1+L_-
\end{aligned}$$

and so $L_- = L_+ = 1$, confirming (2).

We next confirm that

$$f(x) \geq 1 \text{ for all } x>0 \Longrightarrow f(x)=1 \text{ for all } x>0. \tag{3}$$

Suppose that $f(x) \geq 1$ for all $x>0$. For $0<c\leq\infty$, put $S_c = \sup\{f(x) : 0<x\leq c\}$; for $c<\infty$, (2) implies that $S_c<\infty$. If there exists $y>0$ with $f(y)>1$, then from (1) we have $f(x+y) - f(xf(y)) = f(yf(x)) - 1 \geq 0$; hence

$$S_c = S_{(c-y)f(y)} \qquad \left(c \geq c_0 = \frac{yf(y)}{f(y)-1}\right)$$

and (since $(c-y)f(y)-c_0 = f(y)(c-c_0)$) iterating this construction shows that $S_\infty = S_c$ for any $c > c_0$. In any case, we deduce that

$$f(x) \geq 1 \text{ for all } x > 0 \Longrightarrow S_\infty < \infty. \tag{4}$$

Still assuming that $f(x) \geq 1$ for all $x > 0$, note that from (1) with $x = y$,

$$f(xf(x)) = \frac{1}{2}(1 + f(2x)).$$

Since $xf(x) \to 0$ as $x \to 0^+$ by (2) and $xf(x) \to \infty$ as $x \to \infty$, $xf(x)$ takes all positive real values by the intermediate value theorem. We deduce that $2S_\infty \leq 1 + S_\infty$ and hence $S_\infty = 1$; this proves (3).

We may thus assume hereafter that $f(x) < 1$ for some $x > 0$. We next check that

$$\lim_{x\to\infty} f(x) = 0. \tag{5}$$

Put $I = \inf\{f(x) : x > 0\} < 1$, choose $\varepsilon \in (0, (1-I)/2)$, and choose $y > 0$ such that $f(y) < I + \varepsilon$. We then must have $xf(x) \neq y$ for all $x$, or else

$$1 + I \leq 1 + f(2x) = 2f(y) < 2I + 2\varepsilon,$$

contradiction. Since $xf(x) \to 0$ as $x \to 0^+$ by (2), we have $\sup\{xf(x) : x > 0\} < \infty$ by the intermediate value theorem, yielding (5).

By (2) plus (5), $f^{-1}(1/2)$ is nonempty and compact. We can now simplify by noting that if $f(x)$ satisfies the original equation, then so does $f(cx)$ for any $c > 0$; we may thus assume that the least element of $f^{-1}(1/2)$ is 1, in which case we must show that $f(x) = \frac{1}{1+x}$.

We next show that

$$\lim_{x\to\infty} xf(x) = 1. \tag{6}$$

For all $x > 0$, by (1) with $y = x$,

$$f(xf(x)) = \frac{1}{2}(1 + f(2x)) > \frac{1}{2} = f(1), \tag{7}$$

so in particular $xf(x) \neq 1$. As in the proof of (5), this implies that $xf(x) < 1$ for all $x > 0$. However, by (5) and (7) we have $f(xf(x)) \to \frac{1}{2}$ as $x \to \infty$, yielding (6).

By substituting $y \mapsto xy$ in (1),

$$f(xf(xy)) + f(xyf(x)) = 1 + f(x + xy).$$

Taking the limit as $x \to \infty$ and applying (6) yields

$$f(1/y) + f(y) = 1. \tag{8}$$

Combining (1) with (8) yields

$$f(xf(y)) = f(x+y) + f\left(\frac{1}{yf(x)}\right).$$

Multiply both sides by $xf(y)$, then take the limit as $x \to \infty$ to obtain

$$\begin{aligned} 1 &= \lim_{x\to\infty} xf(y)f(x+y) + \lim_{x\to\infty} xf(y)f\left(\frac{1}{yf(x)}\right) \\ &= f(y) + \lim_{x\to\infty} xf(y)yf(x) \\ &= f(y) + yf(y) \end{aligned}$$

and solving for $f(y)$ now yields $f(y) = \frac{1}{1+y}$, as desired.

**Remark.** Some variants of the above approach are possible. For example, once we have (5), we can establish that $f$ is monotone decreasing as follows. We first check that

$$f(x) < 1 \text{ for all } x > 0. \tag{9}$$

Suppose by way of contradiction that $f(x) = 1$ for some $x$. By (1),

$$f(2x) + 1 = 2f(xf(x)) = 2f(x) = 2$$

and so $f(2x) = 1$. It follows that $f^{-1}(1)$ is infinite, contradicting (5).

We next check that

$$x < y \Longrightarrow f(x) > f(y). \tag{10}$$

For $x < y$, by substituting $x \mapsto y - x$ in (1) we obtain

$$\begin{aligned} 1 + f(y) &= f(xf(y-x)) + f((y-x)f(x)) \\ &< 1 + f((y-x)f(x)), \end{aligned}$$

whence $f((y-x)f(x)) > f(y)$. Because $(y-x)f(x) \to 0$ as $x \to y^-$ and $(y-x)f(x) \to y$ as $x \to 0^+$, $(y-x)f(x)$ takes all values in $(0, y)$ as $x$ varies over $(0, y)$; this proves (10).