TEORÍA DE NÚMEROS

Metodología Problem Solving

Segunda parte: Aritmética modular y aplicaciones

Gerard Romo Garrido

Toomates Coolección vol. 6

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.
Estos libros se comparten bajo una licencia "**Creative Commons 4.0 (Atribution Non Commercial)**": Se permite, se promueve y se fomenta cualquier uso, reproducción y edición de todos estos materiales siempre que sea sin ánimo de lucro y se cite su procedencia. 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**

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 Calculus & Precalculus

Libros de texto (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

PAU españolas:
Cataluña TEC Cataluña CCSS Valencia Galicia País Vasco Baleares

PAU internacionales:
Portugal Italia Francia Rumanía Hungría Pearson Edexcel International A Level
Pearson Edexcel IGCSE Cambridge International A Level Cambridge IGCSE
AQA GCSE International Baccalaureate (IB)

Evaluación diagnóstica y pruebas de acceso:
ACM6EP ACM4 CFGS PAP

Competiciones matemáticas:
Canguro: España Cataluña Francia USA Reino Unido Austria
USA: Mathcounts AMC8 10 12 AIME USAJMO USAMO TSTST TST ELMO Putnam
España: OME OMEFL OMEC OMEA OMEM CDP
Europa: OMI Arquimede HMMT BMO Balkan MO JBMO
Internacional: IMO IGO SMT INMO CMO HMMT EGMO
AHSME: Book 1 Book 2 Book 3 Book 4 Book 5 Book 6 Book 7 Book 8 Book 9

Otros materiales:
Pizzazz!: Book A Book B Book C Book D Book E Pre-Algebra Algebra , REOIM

¡Genera tus propias versiones de este documento! Siempre que es posible se ofrecen las versiones editables "MS Word" de todos los materiales para facilitar su edición. Descarga en los siguientes enlaces la versión "**.doc**" de este documento:
http://www.toomates.net/biblioteca/Aritmetica01.doc → http://www.toomates.net/biblioteca/Aritmetica14.doc
http://www.toomates.net/biblioteca/AritmeticaS01.doc → http://www.toomates.net/biblioteca/AritmeticaS13.doc

¡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** completo en **http://www.toomates.net**
Descarga toda la biblioteca Toomates en un solo archivo **Aquí** MEGA
Visita mi **Canal de Youtube**: **https://www.youtube.com/c/GerardRomo**
Visita mi **blog: https://toomatesbloc.blogspot.com/**

Versión de este documento: **04/03/2025**

Índice.

Este libro es la continuación de http://www.toomates.net/biblioteca/Aritmetica.pdf

10 Ecuaciones diofánticas. → Archivo doc

10.1 Ecuaciones diofánticas lineales.
10.2 Ternas pitagóricas.
10.3 La ecuación diofántica $x^2 - y^2 = k$.
10.4 El método de la contradicción modular.
10.5 La técnica del descenso infinito de Fermat.
10.6 Resolución de ecuaciones diofánticas mediante factorización.
10.7 Resolución de ecuaciones diofánticas aplicando desigualdades.
10.8 Cuadrados perfectos. Potencias perfectas.
10.9 Ecuaciones de Frobenius. Problema de las monedas.
10.10 Simon's Favorite Factoring Trick (SFFT).
10.11 Ecuaciones diofánticas en competiciones olímpicas.

11 El problema de la primalidad. Encriptación RSA. → Archivo doc

11.1 El test de primalidad de Fermat.
11.2 Aplicación a la criptografía: El método RSA.

12 Números primos de Fermat y de Mersenne. → Archivo doc

12.1 Números primos de Fermat.
12.2 Números primos de Mersenne.

13 Número y suma de los divisores de un entero. → Archivo doc

13.1 Número de divisores de un entero.
13.2 Suma de los divisores de un entero.
13.3 Números perfectos.

14 Encriptación mediante Curvas Elípticas. Encriptación bitcoin. → Archivo doc

14.1 Curvas elípticas sobre cuerpos en general.
14.2 Curvas elípticas sobre cuerpos finitos.
14.3 Protocolo de intercambio de claves Diffie-Hellmann en Curvas Elipticas (ECDH).

Soluciones. → Archivo doc → Archivo doc

5 Aritmética modular básica.

Para ver aplicaciones de la aritmética modular para simplificar problemas de combinatoria, ver, por ejemplo los problemas #1.6.37 y #1.6.40 de
http://www.toomates.net/biblioteca/Combinatoria.pdf

El lenguaje de las congruencias nos permite abordar con éxito problemas aparentemente muy difíciles. Las congruencias es un lenguaje, una técnica, y por tanto solo se aprende practicando, jugando con ellas durante mucho tiempo.

Estamos acostumbrados a trabajar con conjuntos numéricos infinitos.

Por ejemplo, los números naturales:

$$N=\{0,1,2,3,4,...\}$$

Los números enteros:

$$Z=\{...,-4,-3,-2,-1,0,1,2,3,4,...\}$$

Los números racionales:

$$Q=\left\{...,-4,-3,-2,-1,0,1,2,3,4,...,\frac{1}{2},\frac{3}{2},\frac{7}{3},\frac{-11}{5},...\right\}$$

Todos estos conjuntos tienen una cantidad infinita de elementos.

Pero también es perfectamente válido disponer de conjuntos finitos de elementos y hacer operaciones en ellos. En los siguientes apartados vamos a ver unos ejemplos introductorios.

5.1 Primer ejemplo: Las horas del día.

El día tiene 24 horas:

$$D=\{0,1,2,3,4,5,6,7,8,...,22,23\}$$

La hora 24 sería medianoche, es decir, la hora 0. Así pues, podemos decir que la hora 24 y la hora 0 son la misma hora, es el mismo elemento de D. Escribiremos

$$24\equiv 0$$

Para indicar que la hora 24 y la hora 0 son equivalentes.

De la misma forma, podemos decir que la hora 25 es la hora 1, la hora 26 es la hora 2, la hora 27 es la hora 3...

$$25\equiv 1,\ 26\equiv 2,\ 27\equiv 3$$

Utilizaremos el símbolo $\equiv$, que se parece mucho al símbolo $=$, para expresar la idea de que no son iguales, pero son equivalentes: En la práctica, es como si fueran iguales.

Como calcular el equivalente modular.

¿Qué hora sería la hora 67 ? Han pasado dos días completos y quedan 17 horas del tercero:

$$67 = 24 \times 2 + 17$$

Luego $67 \equiv 17$

Lo que estamos haciendo es realizar la división entera entre 24 y tomar el resíduo:

67	24
17	2

¿Qué hora será la hora 349? Realizamos la división entera y tomamos el resíduo:

349	24
13	14

Escribimos $349 \equiv 14$

5.1.1 Ejercicio.

Determina los correspondientes equivalentes modulares en el conjunto D de las horas del día:

a) 7 b) 23 c) 29 d) 168 e) 773

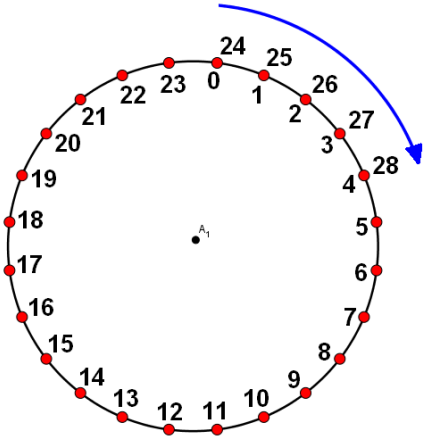
5.1.2 Ejercicio.

Determina los correspondientes equivalentes modulares en el conjunto D de las horas del día:

a) 15 b) 21 c) 30 d) 200 e) 1441

Representación circular.

Puede ser interesante representar las horas en forma circular:



El número de vueltas completas (el cociente de la división) no cuenta para nada, y nos quedamos con el residuo.

Como sumar con aritmética modular.

Si son las 17 horas (las cinco de la tarde) y quiero ver una película de 3 horas, ¿A qué hora acabará la película? Muy fácil, basta hacer una simple suma:

$$17+3\equiv 20$$

Acabará a las 20 horas (las ocho de la tarde).

¿Pero si son las 22 horas, las diez de la noche?

$$22+3=25$$

Nadie dice "Acabará a las 25", todo el mundo dice "acabará a la una (de la madrugada)", ¡y estamos tan acostumbrados que lo hacemos mentalmente!

Primero realizamos la suma y después calculamos el resíduo:

25	24
1	1

Escribiremos $22+3\equiv 1$

5.1.3 Ejercicio.

Calcula (en el conjunto D de horas del día)

a) $5+4$ b) $8+15$ c) $15+9$ d) $20+18$

5.1.4 Ejercicio.

Calcula (en el conjunto D de horas del día)

a) $3+2$ b) $18+15$ c) $25+12$ d) $22+17$

Como hacer operaciones en aritmética modular.

Lo mismo que hemos hecho con las sumas lo podemos hacer con las restas, multiplicaciones y potencias: Basta con realizar la operación usual en Z y quedarnos con el residuo modular. Por ejemplo, en el conjunto

$$D=\{0,1,2,3,4,5,6,7,8,...,22,23\}$$

Podemos restar. Por ejemplo: $32-5\equiv 3$

Primero hemos hecho la resta "normal": $32-5=27$ y luego calculamos el equivalente modular del resultado:

27	24
3	1

Podemos multiplicar. Por ejemplo: $9\times 4=36\equiv 12$

Primero hemos hecho la multiplicación "normal": $9\times 4=36$ y luego calculamos el equivalente modular del resultado:

36	24
12	1

Podemos dividir. Por ejemplo: $144\div 2\equiv 0$

Primero hemos hecho la división "normal": $144\div 2=72$ y luego calculamos el equivalente modular del resultado:

72	24
0	3

Podemos hacer potencias. Por ejemplo: $6^2\equiv 12$

Primero hemos hecho la potencia "normal": $6^2=36$ y luego calculamos el equivalente modular del resultado:

36	24
12	1

5.1.5 Ejercicio.

Realiza las siguientes operaciones (en el conjunto D de horas del día)

a) $30-5$ b) 5×7 c) $42\div 3$ d) 5^2

e) $100-1$ f) 6×4 g) $720\div 9$ h) 4^3

5.1.6 Ejercicio.

Realiza las siguientes operaciones (en el conjunto D de horas del día)

a) $70-20$ b) 6×5 c) $81\div 3$ d) 10^2 e) 2^5

5.1.7

Hoy es jueves. ¿Qué día de la semana será de aquí a 2023 días?

(A) Martes (B) Miércoles (C) Jueves (D) Viernes (E) Sábado

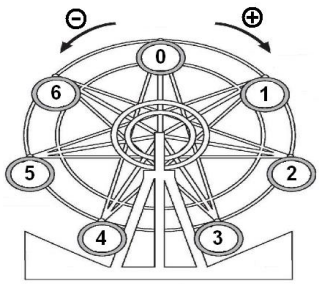
5.2 Segundo ejemplo: El conjunto Z_7.

Definición de Z_7.

Definimos "Zeta siete" como el conjunto de los números del 0 al 6:

$$Z_7 = \{0,1,2,3,4,5,6\}$$

Visualmente podemos considerar este conjunto como una noria de siete compartimentos, en la que sumar quiere decir "girar hacia la derecha" y restar quiere decir "girar hacia la izquierda":



Está claro que en Z_7 sumar o restar 7 es no hacer nada: Damos una vuelta completa y nos quedamos donde estábamos, Escribiremos, por ejemplo:

$$3+7 \equiv 3 \pmod 7 \qquad 5-7 \equiv 5 \pmod 7$$

En Z_7 los múltiples de 7 son todos equivalentes a cero:

$$7 \equiv 0 \pmod 7,\ 14 \equiv 0 \pmod 7,\ 21 \equiv 0 \pmod 7 \ ...$$

También los negativos:

$$-7 \equiv 0 \pmod 7,\ -14 \equiv 0 \pmod 7,\ -21 \equiv 0 \pmod 7 \ ...$$

Esto lo vemos claro con números pequeños. Para números grandes debemos utilizar el método del residuo:

$3421 \equiv 5 \pmod 7$ porque al hacer la división entera 3421 entre 7 obtenemos un residuo igual a 5:

$$\begin{array}{r|l} 3421 & 7 \\ \hline 5 & 488 \end{array}$$

Tablas de la suma y la multiplicación en Z_7.

Ahora podemos hacer la tabla de la suma "módulo 7":

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Observa detenidamente esta tabla. Por ejemplo: Fila "4" columna "5":

$$4+5=9\equiv 2 \pmod 7$$

Observamos las propiedades tradicionales de la suma: Es una operación conmutativa, el cero no hace nada (por eso se llama "elemento neutro") ...

También podemos hacer la tabla de la multiplicación "módulo 7":

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Observa detenidamente como se ha construido esta tabla. Por ejemplo: Fila "3", columna "6":

$$3\cdot 6=18\equiv 4 \pmod 7$$

Y en esta tabla observamos las propiedades tradicionales de la multiplicación: Es una operación conmutativa, el uno no hace nada (es el elemento neutro), cualquier número multiplicado por cero da cero...

5.2.1 Ejercicio.

Completa la tabla de la suma de $Z_5=\{0,1,2,3,4\}$

5.2.2 Ejercicio.

Completa la tabla de la multiplicación de $Z_5=\{0,1,2,3,4\}$.

5.3 Los conjuntos Z_n.

5.3.1 Definición. Congruencias.

Diremos que $a \equiv b \pmod{n}$, y diremos que "**a es congruente con b módulo n**" cuando sucede alguna de estas condiciones equivalentes:

a) $n \mid (a-b)$

b) $a = kn + b$ para cierto entero k.

c) a y b dejan el mismo residuo cuando son divididos entre n.

Por ejemplo: $24 \equiv 3 \pmod{7}$, pues $24 = 3 \cdot 7 + 3$, $34 \equiv 4 \pmod{5}$, pues $34 = 6 \cdot 5 + 4$

En particular: $a \equiv 0 \pmod{n} \Leftrightarrow n \mid a$

5.3.2 Ejemplo.

Determina x tal que $5x \equiv 6 \pmod{8}$.

Solución.

Vamos probando, uno por uno:

$5 \cdot 1 = 5 = 0 \cdot 8 + 5 \equiv 5 \pmod{8}$ $\quad$ $5 \cdot 2 = 10 = 1 \cdot 8 + 2 \equiv 2 \pmod{8}$

$5 \cdot 3 = 15 = 1 \cdot 8 + 7 \equiv 7 \pmod{8}$ $\quad$ $5 \cdot 4 = 20 = 2 \cdot 8 + 4 \equiv 4 \pmod{8}$

$5 \cdot 5 = 25 = 3 \cdot 8 + 1 \equiv 1 \pmod{8}$

$5 \cdot 6 = 30 = 3 \cdot 8 + 6 \equiv 6 \pmod{8} \rightarrow$ La solución es $x \equiv 6 \pmod{8}$

$5 \cdot 7 = 35 = 4 \cdot 8 + 3 \equiv 3 \pmod{8}$

5.3.3 Proposición. Propiedades básicas de las congruencias.

Sea $n > 0$ fijo, y a, b, c, d enteros arbitrarios. Entonces se cumple:

a) $a \equiv a \pmod{n}$ (**Propiedad reflexiva**).

b) Si $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ (**Propiedad simétrica**).

c) Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$ (**Propiedad transitiva**).

d) Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$ y $ac \equiv bd \pmod{n}$.

e) Si $a \equiv b \pmod{n} \Rightarrow ka \equiv kb \pmod{n}$ para cualquier entero k

f) Si $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$ para cualquier entero positivo k.

5.3.4 Ejemplo.

¿ Es $24^{14} - 15^{14}$ divisible entre 9?

Solución.

$24 \equiv 15 \pmod{9} \Rightarrow 24^{14} \equiv 15^{14} \pmod{9} \Leftrightarrow 24^{14} - 15^{14} \equiv 0 \pmod{9} \Leftrightarrow 9 \mid 24^{14} - 15^{14}$, luego sí es divisible.

5.3.5 Observación. Qué funciona y qué no funciona con congruencias.

Las propiedades anteriores nos permiten trabajar con congruencias prácticamente igual a como trabajamos con números, pero no todo lo que hacíamos con números funciona ahora con congruencias:

a) Cancelación de términos:
No funciona en general la cancelación de términos (el "tachar" de toda la vida).
Por ejemplo: $2 \cdot 4 \equiv 2 \cdot 1 \pmod 6$, pero $4 \not\equiv 1 \pmod 6$

$21^7 \equiv 21 \pmod 7$, pero $21^6 \not\equiv 1 \pmod 7$

Aunque existe una **Regla de cancelación**:

Si $(c,n) = 1$, entonces $ca \equiv cb \pmod n \Rightarrow a \equiv b \pmod n$

b) **Principio del producto nulo**:
No existe tampoco el principio del producto nulo en general. Por ejemplo:
$4 \cdot 3 \equiv 0 \pmod{12}$, pero $4 \not\equiv 0 \pmod{12}$ y $3 \not\equiv 0 \pmod{12}$

Pero sí se verifica cuando el módulo es un número primo:

Si p es primo, $a \cdot b \equiv 0 \pmod p \Rightarrow a \equiv 0 \pmod p \; o \; b \equiv 0 \pmod p$

5.3.6 Proposición. Modificaciones en el módulo.

a) Si $(a,m) = d \geq 1$, entonces $ax \equiv ay \pmod m \Rightarrow ax \equiv ay \left(\bmod \frac{m}{d} \right)$.

b) Si $a \equiv b \pmod n$ y $d \mid n \Rightarrow a \equiv b \pmod d$

c) $a \equiv b \pmod n$ y $a \equiv b \pmod m \Leftrightarrow a \equiv b \left(\bmod [n,m] \right)$.

d) Si $(n_1, n_2, \ldots, n_k) = 1$, $a \equiv b \pmod{n_i}$ $i = 1, \ldots, k \Leftrightarrow a \equiv b \pmod{n_1 n_2 \ldots n_k}$

Demostración.

a) $ax \equiv ay \pmod m \Rightarrow m \mid (ax - ay) = m \mid a(x-y) \Rightarrow \frac{m}{d} \mid \frac{a}{d}(x-y)$

b) $a \equiv b \pmod{nm} \Rightarrow nm \mid (a-b) \Rightarrow n \mid (a-b) \Rightarrow a \equiv b \pmod n$

c) $\left.\begin{array}{l} a \equiv b \pmod n \Leftrightarrow n \mid (a-b) \\ a \equiv b \pmod m \Leftrightarrow m \mid (a-b) \end{array}\right\} \Leftrightarrow [n,m] \mid (a-b) \Leftrightarrow a \equiv b \left(\bmod [n,m] \right)$

(ver 5.6b)

d) Es un caso particular de c.

Trabajar con congruencias es una técnica muy potente para resolver problemas de Teoría de Números, como se puede ver en los siguientes ejemplos:

5.3.7 Problema resuelto.

Demostrar que 41 divide $2^{20}-1$

Solución. En primer lugar vemos que $2^5 = 32 = -9 \pmod{41}$

Luego $2^{20} = \left(2^5\right)^4 = (-9)^4 \pmod{41} = (-9)^2(-9)^2 \pmod{41} = 81 \cdot 81 \pmod{41}$

Pero, por otro lado, $81 \pmod{41} = -1 \pmod{41}$

Luego $81 \cdot 81 \pmod{41} = (-1)(-1) \pmod{41} = 1 \pmod{41}$

Finalmente, $2^{20} - 1 \equiv 1 - 1 \pmod{41} = 0 \pmod{41} \Rightarrow 41 \mid 2^{20} - 1$, tal y como queríamos ver.

5.3.8 Problema resuelto.

Determina el residuo al dividir $1!+2!+3!+4!+\ldots+99!+100!$ entre 12.

Solución. Observamos que $4! = 24 \equiv 0 \pmod{12}$, luego, para todo $k \geq 4$,

$$k! = 4! \cdot 5 \cdot 6 \ldots \cdot k \equiv 0 \cdot 5 \cdot 6 \ldots \cdot k \equiv 0 \pmod{12}$$

luego

$$1!+2!+3!+4!+\ldots+99!+100! \equiv 1!+2!+3!+4!+0+\ldots+0+0 \equiv 1!+2!+3!+4! \pmod{12}$$

Y nuestro problema se reduce a encontrar el residuo al dividir $1!+2!+3!+4! = 33$ entre 12, que es 9.

5.4 Aplicación a la criptografía: El cifrado César.

Descripción del cifrado César.

El primer uso documentado de una cifra monoalfabética por sustitución con propósitos militares aparece en el documento "La guerra de las Galias" de Julio César.

En dicho libro, Julio César describe cómo envía un mensaje cifrado a Cicerón, que se encontraba sitiado y a punto de rendirse, aplicando una sustitución simple a las letras del texto en claro de forma que el mensaje fuera ininteligible para el enemigo.

Aunque en aquella ocasión César sustituyó las letras romanas por letras griegas, es común asociarle a su sistema de cifra un desplazamiento de 3 espacios a la derecha en el alfabeto, tal y como lo describe Suetonio en su libro "Vidas de los Césares" en la entrada LVI sobre Cayo Julio César.

Consistía en escribir el mensaje con un alfabeto que estaba formado por las letras del alfabeto latino normal desplazadas tres posiciones a la derecha. Con nuestro alfabeto el sistema quedaría así:

Alfabeto en claro: A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z
Alfabeto cifrado: D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A B C

Por ejemplo, si se quiere enviar el mensaje ATACARALAMANECER, lo que se escribirá realmente es DWDFDUDÑDODPHFHU

El receptor del mensaje conocía la clave secreta de éste (es decir, que estaba escrito con un alfabeto desplazado tres posiciones a la derecha), y podía descifrarlo fácilmente haciendo el desplazamiento inverso con cada letra del mensaje. Pero para el resto de la gente que pudiese accidentalmente llegar a ver el mensaje, el texto carecía de ningún sentido.

Es un cifrado muy débil y poco seguro, pero en la época de Julio César no era de conocimiento general la idea de ocultar el significado de un texto mediante cifrado. De hecho, que un mensaje estuviese por escrito ya era un modo de asegurar la confidencialidad frente a la mayoría de la población analfabeta de la época.

Como dato curioso, más de 1500 años después, un cifrado similar al de César fue utilizado por la reina María Estuardo de Escocia, para conspirar junto con los españoles contra su prima Isabel I (en realidad, fue incitada a conspirar por agentes al servicio de Isabel I; una trampa bien urdida.) Los mensajes cifrados de María fueron fácilmente descifrados mediante sencillos análisis estadísticos por los agentes de Isabel I, y así pues quedó al descubierto la conspiración de la reina escocesa. Junto con la pérdida del

secreto de la comunicación, María perdió la cabeza en su ejecución el 8 de febrero de 1587. Después de esto el cifrado César quedó definitivamente descartado como método de cifrado seguro para los gobernantes del mundo. Desde entonces a hoy, los cifrados usados por los estados para preservar sus secretos han mejorado considerablemente.

El cifrado César desde un punto de vista matemático.

Lo que a nosotros nos interesa del cifrado César es que es un claro ejemplo de utilización de la aritmética modular para garantizar la confidencialidad de la información mediante el cifrado o encriptación. Matemáticamente, las veintisiete letras del alfabeto castellano las podemos interpretar como el conjunto de números naturales del 0 al 26:

$$A=0,\ B=1,\ C=2,\ D=3,\ ...,\ Z=27$$

Y por tanto podemos suponer que trabajamos en el conjunto

$$Z_{27}=\{0,1,2,3,4,5,6,7,8,...,\ 26,27\}$$

El cifrado será la función

$$\begin{aligned} &f: Z_{27} \to Z_{27} \\ &x \mapsto x+3 \pmod{27} \end{aligned}$$

Y el descifrado será su función inversa:

$$\begin{aligned} &g: Z_{27} \to Z_{27} \\ &x \mapsto x-3 \pmod{27} \end{aligned}$$

Observamos que en vez de utilizar el 3 podemos utilizar cualquier otro número k, que sería la clave de encriptación: Un valor que sólo conocerían el emisor y el receptor del mensaje, y sin el cual (supuestamente) nadie podría descifrar el mensaje. Así pues, podemos decir que el método César es un método de encriptación de **clave privada**.

Cifrado:

$$\begin{aligned} &f: Z_{27} \to Z_{27} \\ &x \mapsto x+k \pmod{27} \end{aligned}$$

Descifrado:

$$\begin{aligned} &g: Z_{27} \to Z_{27} \\ &x \mapsto x-k \pmod{27} \end{aligned}$$

Criptoanálisis de los Métodos de Cifrado Monoalfabéticos.

El cifrado monoalfabético constituye la familia de métodos criptográficos más simple de criptoanalizar, puesto que las propiedades estadísticas del texto claro se conservan en el criptograma. Supongamos que, por ejemplo, la letra que más aparece en Castellano es la E. Parece lógico que la letra más frecuente en el texto codificado sea aquella que corresponde con la E. Emparejando las frecuencias relativas de aparición de cada símbolo en el mensaje cifrado con el histograma de frecuencias del idioma en el que se supone está el texto claro, podremos averiguar fácilmente la clave.

Distribución de frecuencias de letras en español para un texto literario:

E - 16,78%	R - 4,94%	Y - 1,54%	J - 0,30%	A - 11,96%
U - 4,80%	Q - 1,53%	Ñ - 0,29%	O - 8,69%	I - 4,15%
B - 0,92%	Z - 0,15%	L - 8,37%	T - 3,31%	H - 0,89%
X - 0,06%	S - 7,88%	C - 2,92%	G - 0,73%	K - 0,00%
N - 7,01%	P - 2,77%	F - 0,52%	W - 0,00%	D - 6,87%
M - 2,12%	V - 0,39%			

Ejercicio 1.

Cifrad con el sistema de clave privada de César y clave secreta k = 5 el mensaje m = VOYALCINE (si al buscar el cifrado de un carácter se llega al final del alfabeto, se sigue la cuenta por el principio del alfabeto). ¿Qué nos han contestado si el mensaje recibido es c = DTRTATD?

Ejercicio 2.

Se ha utilizado cifrado César con clave privada k = 6 para transmitir un nombre en secreto. Se ha recibido BÑIZUX. ¿Cuál es el nombre secreto?

Ejemplo.

Un ejemplo literario y cinematográfico muy conocido es el del nombre HAL del ordenador que aparece en la novela 2001 de Arthur C. Clarke y en la correspondiente película dirigida por Stanley Kubrick, "2001 una odisea en el espacio". No es nada complicado obtener el nombre de una famosa empresa si sabemos que el nombre del maléfico ordenador (HAL) es el cifrado con clave k = 26 del nombre de la empresa.

Cifrado César con Python.

```
#
# Generador de puntos de la curva secp256k1 módulo p por Brute-Force
#
p=257
Total=0
for x in range (0,p):
    for y in range (0,p):
        v=y**2-x**3-7
        if v%p==0:
            print(x,",",y)
            Total=Total+1
print("Total de puntos:",Total)
```

El siguiente programa es un ejemplo de un programa Python que encripta de textos mediante el método César:

```
#
# Encriptador metodo Cesar
#
Clave=3
Frase1="ELATAQUESERAESTANOCHE"
Frase2=""
for c in Frase1:
    n=ord(c)-65
    m=(n+Clave)%26
    Letra=chr(m+65)
    Frase2=Frase2+Letra
print("Frase sin encriptar: ",Frase1)
print("Frase encriptada: ",Frase2)
```

Salida:

Frase sin encriptar: ELATAQUESERAESTANOCHE
Frase encriptada: HODWDTXHVHUDHVWDQRFKH

El programa es un bucle que toma uno a uno cada carácter de Frase1 y lo deposita en la variable c.

`for c in Frase1:`

Para convertir el carácter c en su correspondiente valor numérico se utiliza la función ord(c), que devuelve el código UNICODE del carácter que recibe como parámetro. El problema está en que los códigos UNICODE de las letras mayúsculas empiezan en 65:

$$A \rightarrow 65 , B \rightarrow 66 , C \rightarrow 67 \ldots$$

Por lo que debemos restar 65 para así empezar desde cero:

$$A \rightarrow 65\text{-}65=0 , B \rightarrow 66\text{-}65=1 , C \rightarrow 67\text{-}65=2 \ldots$$

n=ord(c)-65

Ahora ya podemos realizar la encriptación, sumando a n el valor de la Clave y determinando su equivalente módulo 26. Dejando el resultado en la variable m.

```
m=(n+Clave)%26
```

Por último, convertimos el valor numérico m en su correspondiente letra, mediante la función chr(n), que devuelve el carácter UNICODE correspondiente al valor numérico que recibe como parámetro. De nuevo, debemos tener en cuenta que los caracteres UNICODE de las letras mayúsculas empiezan en 65, por lo que debemos sumar 65 al valor de m. Dejamos la letra obtenida en la variable Letra.

```
Letra=chr(m+65)
```

Ya solo queda añadir Letra a la cadena de salida Frase2. Utilizamos para ello el comando +, que en principio realiza la suma de dos números, pero que en el contexto de dos cadenas de caracteres lo que hace es juntar las dos cadenas de caracteres.

```
Frase2=Frase2+Letra
```

Por último, se visualizan las dos frases: La frase de entrada sin encriptar y la frase de salida encriptada.

```
print("Frase sin encriptar: ",Frase1)
print("Frase encriptada: ",Frase2)
```

El correspondiente programa desencriptador es prácticamente idéntico al anterior:

```
#
# Desencriptador Metodo Cesar
#
Clave=3
Frase1="HODWDTXHVHUDHVWDQRFKH"
Frase2=""
for c in Frase1:
    n=ord(c)-65
    m=(n-Clave)%26
    Letra=chr(m+65)
    Frase2=Frase2+Letra
print("Frase encriptada: ",Frase1)
print("Frase desencriptada: ",Frase2)
```

Salida:

Frase encriptada: HODWDTXHVHUDHVWDQRFKH
Frase desencriptada: ELATAQUESERAESTANOCHE

El único cambio significativo está en la línea 9, en donde en vez de sumar la Clave, la restamos.

Mejora al programa anterior. El comando if

En el programa anterior hemos supuesto que los caracteres de la frase de entrada son siempre letras mayúsculas.

Supongamos que queremos poder recibir cualquier carácter, y encriptar solo las letras mayúsculas.

El comando if permite realizar una acción solo si se cumple una determinada condición, y suele venir acompañado del comando else, que indica la acción a realizar en caso contrario.

En nuestro caso, tomamos la letra c y la encriptamos si es una letra mayúscula (A, B, C,…, Z) y la dejamos tal cual en caso contrario:

```
#
# Encriptador Metodo Cesar (ver. 2)
#
Clave=3
Frase1="ATACAR A LAS 4:00 DE ESTA NOCHE"
Frase2=""
for c in Frase1:
        if c.isupper():
            n=ord(c)-65
            m=(n+Clave)%26
            Letra=chr(m+65)
        else:
            Letra=c
        Frase2=Frase2+Letra
print("Frase sin encriptar: ",Frase1)
print("Frase encriptada: ",Frase2)
```

Salida:

```
Frase sin encriptar:  ATACAR A LAS 4:00 DE ESTA NOCHE
Frase encriptada:  DWDFDU D ODV 4:00 GH HVWD QRFKH
```

5.5 Aplicación a la criptografía: El cifrado Hill.

Introducción.

El método César es un método de cifrado por **sustitución monoalfabética**. Este tipo de cifrados se basa en sustituir cada letra del texto original por otra del alfabeto.
Estos métodos representan un gran agujero en su seguridad al poderse determinar con gran facilidad la frecuencia de repetición de cada una de las letras que posteriormente se confronta con las estándar de aparición en el castellano, con lo que con un texto suficientemente largo el mensaje y la clave quedan totalmente al descubierto.

Para evitar los ataques mendiante análisis de frecuencias cifraremos no cada letra individualmente, sino en grupos de dos o más, son los llamados cifrados por **sustitución polialfabética**, como por ejemplo el método Hill que describiremos en este apartado. Este sistema fue inventado por Lester S. Hill en 1929, mediante transformaciones matriciales.

El tamaño de los grupos elegidos para hacer las sustituciones depende del grado de seguridad que deseemos. Aquí realizaremos la presentación del método con matrices 2×2 por su simplicidad, eligiendo una matriz 4×4 la respuesta es casi plana para la frecuencia de cada letra. Es decir, en un texto cifrado por este método todas las letras tienen prácticamente la misma probabilidad de aparecer, con lo cual un estudio de sus frecuencias será totalmente inútil, puesto que todas darán casi el mismo resultado.

Nota importate: Se supone en el lector conocimientos básicos de álgebra lineal, en especial las operaciones con matrices y el concepto de matriz inversa (ver dossier GL)

En IR:

$$\text{A es invertible} \Leftrightarrow \det A \neq 0\text{, en cuyo caso} \quad A^{-1} = \frac{1}{\det A}\left(Adj\ A\right)^T$$

En Z_n:

$$\text{A es invertible} \Leftrightarrow \det A \text{ es invertible módulo n} \Leftrightarrow (\det A, n) = 1$$

$$\text{en cuyo caso} \quad A^{-1} = \left(\det A\right)^{-1}\left(Adj\ A\right)^T$$

Descripción del método.

Dividiremos el texto en grupos de dos letras, que pasaremos a sus equivalentes numèricos Z_{26} como hemos hecho en el apartado anterior. Para cifrar solo necesitamos una matriz que utilizaremos como clave, y descifrar utilizaremos su matriz inversa.

Por ejemplo, tomamos la matriz $A=\begin{pmatrix}35 & -12\\ 3 & -9\end{pmatrix}$ y su inversa $A^{-1}=\begin{pmatrix}-135 & 180\\ -45 & 525\end{pmatrix}$

Las transformamos a módulo 26:

$$A\equiv\begin{pmatrix}9 & 14\\ 3 & 17\end{pmatrix} \text{ y su inversa } A^{-1}\equiv\begin{pmatrix}21 & 24\\ 7 & 5\end{pmatrix}$$

Ahora tomaremos un mensaje en claro: ELCOCHELLEVADOSANTENAS y lo dividiremos en grupos de dos letras.

Primer bloque: "EL"

1. Determinamos sus correspondientes valores numéricos en Z_{26}:

$$E\to 4$$
$$L\to 11$$

Obteniendo así el siguiente vector columna:

$$u=\begin{pmatrix}4\\ 11\end{pmatrix}$$

2. Le aplicamos la transformación lineal de la matriz A, es decir, multiplicamos la matriz clave por el vector u:

$$v=Au=\begin{pmatrix}35 & -12\\ 3 & -9\end{pmatrix}\begin{pmatrix}4\\ 11\end{pmatrix}=\begin{pmatrix}190\\ 199\end{pmatrix}\equiv\begin{pmatrix}8\\ 17\end{pmatrix}\pmod{26}$$

3. Obtenemos las letras asociadas a los valores numéricos:

$$8\to I$$
$$17\to R$$

Ya hemos obtenido las dos primeras letras de nuestra frase encriptada: "IR"

La operación se repite con todos los grupos de letras sucesivamente, obteniendo el siguiente texto en clave: "IRGKMVIRZXHLPNGCTYKZSU"

El método de desenciptación es el mismo, solo que ahora utilizaremos la matriz inversa

$$A^{-1} \equiv \begin{pmatrix} 21 & 24 \\ 7 & 5 \end{pmatrix}$$

Primer bloque: "IR"
1. Determinamos sus correspondientes valores numéricos en Z_{26}:

$$I \to 8$$
$$R \to 17$$

Obteniendo así el siguiente vector columna:

$$v = \begin{pmatrix} 8 \\ 17 \end{pmatrix}$$

2. Le aplicamos la transformación lineal de la matriz A^{-1}:

$$u = A^{-1}v = \begin{pmatrix} 21 & 24 \\ 7 & 5 \end{pmatrix}\begin{pmatrix} 8 \\ 17 \end{pmatrix} = \begin{pmatrix} 576 \\ 141 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 11 \end{pmatrix} \pmod{26}$$

3. Obtenemos las letras asociadas a los valores numéricos:

$$4 \to E$$
$$11 \to L$$

Ya hemos obtenido las dos primeras letras de nuestra frase desencriptada: "EL". Esta operación se realiza con todos los grupos de dos letras recibidos en clave hasta que se forme el mensaje en claro ELCOCHELLEVADOSANTENAS, que coincide con el mensaje original, tal y como era de esperar.

Este método, como hemos dicho, se puede aplicar con qualquier tamaño de matriz cuadarada, y cuanto mayor sea éste, mejor será la seguridad, aunque aumentará también la complicación matemática.

Fuente:Revista Microhobby nº 165.

Codificación Python.

```
#
# Encriptador/Desencriptador metodo Hill
#
Frase1="ELCOCHELLEVADOSANTENAS"
Frase2=""
a11=9
a12=14
a21=3
a22=17
if len(Frase1)%2==1:
    Frase1=Frase1+"X"
c=0
while(c<=len(Frase1)-2):
    l1=Frase1[c:c+1]
    l2=Frase1[c+1:c+2]
    u1=ord(l1)-65
    u2=ord(l2)-65
    v1=(a11*u1+a12*u2)%26
    v2=(a21*u1+a22*u2)%26
    Letra1=chr(v1+65)
    Letra2=chr(v2+65)
    Frase2=Frase2+Letra1
    Frase2=Frase2+Letra2
    c=c+2
print("Frase entrada: ",Frase1)
print("Frase salida: ",Frase2)
```

SALIDA

Frase entrada: ELCOCHELLEVADOSANTENAS
Frase salida: IRGKMVIRZXHLPNGCTYKZSU

Comentarios:
Línia 10:Puesto que trabaja por parejas de letras, sería problemático si la cadena de entrada tuviera una longitud impar. Resolvemos este problema añadiendo en dicho caso una letra final.

El resto de programa no tiene mayor dificultad: Es un bucle que recorre la frase (línea 13) tomando parejas de letras, convirtiendo estas letras en sus respectivos equivalentes numéricos, multiplicando por la matriz y generando las respectivas letras.

El programa desencriptador es el mismo programa, en el que únicamente hemos cambiado las matriz por su inversa:

```
#
# Encriptador/Desencriptador metodo Hill
#
Frase1="IRGKMVIRZXHLPNGCTYKZSU"
Frase2=""
a11=21
a12=24
a21=7
a22=5
if len(Frase1)%2==1:
    Frase1=Frase1+"X"
c=0
while(c<=len(Frase1)-2):
    l1=Frase1[c:c+1]
    l2=Frase1[c+1:c+2]
    u1=ord(l1)-65
    u2=ord(l2)-65
    v1=(a11*u1+a12*u2)%26
    v2=(a21*u1+a22*u2)%26
    Letra1=chr(v1+65)
    Letra2=chr(v2+65)
    Frase2=Frase2+Letra1
    Frase2=Frase2+Letra2
    c=c+2
print("Frase entrada: ",Frase1)
print("Frase salida: ",Frase2)
```

SALIDA:

Frase entrada: IRGKMVIRZXHLPNGCTYKZSU
Frase salida: ELCOCHELLEVADOSANTENAS

5.6 Problemas.

5.6.1 MF

Si $n!$ denota el producto de todos los números del 1 al n, ¿Cuál es el residuo de

$$1!+2!+3!+...+n!$$

al dividirlo entre 9?

5.6.2 MF

Encuentra un ejemplo que demuestre que $a^2 \equiv b^2 \pmod{n}$ no implica $a \equiv b \pmod{n}$.

5.6.3 F

Determina los residuos cuando 2^{50} y 41^{65} son divididos entre 7.

5.6.4 F

Utilizando la teoría de congruencias, demuestra que $89 \mid 2^{44}-1$ y $97 \mid 2^{48}-1$.

5.6.5 F

Determina el último dígito de $9^{1003}-7^{902}+3^{801}$.

5.6.6 MF

Demuestra que para todo $n \in IN$, el número $a_n = 11^{n+2}+12^{2n+1}$ es divisible entre 133.

5.6.7 MF

La cifra de las unidades de 2137^{753} es:

(A) 1 (B) 3 (C) 5 (D) 7 (E) 9

AHSME 1961 #28

5.6.8 F

El dígito de las unidades de $3^{1001}7^{1002}13^{1003}$ es:

(A) 1 (B) 3 (C) 5 (D) 7 (E) 9

AHSME 1983 #14

5.6.9 F

Demuestra que $18^6 \equiv 1 \pmod{7^k}$ para $k = 1,2,3$.

5.6.10 MF

Demuestra que si n es impar, entonces $n^2 \equiv 1 \pmod{8}$

5.6.11 F

Determina el número de enteros n, $1 \le n \le 25$, tales que n^2+3n+2 es divisible entre 6.

5.6.12 F

Demuestra que $2^n + 6 \cdot 9^n$ siempre es divisible entre 7, para todo entero positivo n.

5.6.13 M

Sea $a_n = 6^n + 8^n$. Determina el residuo cuando a_{83} se divide entre 49.

AIME 1983 #6

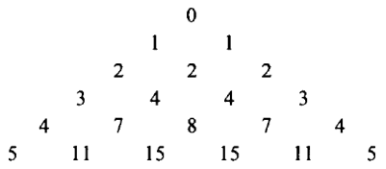
5.6.14 F

Determina el residuo al dividir $9 \times 99 \times 999 \times \ldots \times \underbrace{99\ldots9}_{999 nueves}$ entre 1000.

AIME I 2010 #2

5.6.15 F

Consideremos el esquema triangular de números $0, 1, 2, 3\ldots$ a lo largo de los lados y con números interiores obtenidos sumando los dos números superiores de la fila anterior. Las filas 1 a 6 se muestran en el siguiente esquema:



Sea $f(n)$ la suma de los números de la fila n. ¿Cuál es el residuo cuando dividimos $f(100)$ entre 100?

AHSME 1995 #27

5.6.16 M

Sea $k = 2008^2 + 2^{2008}$. ¿Cuál es el dígito de las unidades de $k^2 + 2^k$?

(A) 0 (B) 2 (C) 4 (D) 6 (E) 8

AMC 12A 2008 #15, AMC 10A 2008 #24

5.6.17 F

Determina el menor entero positivo n tal que n y $107n$ tienen las dos últimas cifras iguales.

HMMT 2008 #2

5.6.18 M

Demuestra que si x, y, z son enteros cumpliendo $x^2 + y^2 = 3z^2$, entonces $x = y = z = 0$.

5.6.19 F

Determina los enteros n tales que $n+2$ divide $(n+18)^2$.

PUMaC 2007/NT #B2

5.6.20 MF

Demuestra que para todo natural n, el número $2^n + 1$ no es divisible entre 7.

IMO 1967 #1 (apartado b)

5.6.21 MF

Determina el último dígito de $\left(\left(\left(7^7\right)^7\right)^7 \ldots\right)^7$ en donde aparece 1001 veces el número 7.

5.6.22 F

Dados cuatro números enteros diferentes a, b, c, d, demuestra que

$$(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$$

es divisible entre 12

5.6.23 F

Tomamos todos los enteros del 19 al 92 y los escribimos consecutivamente para formar el número

$$N = 192021 \cdots 909192$$

Sea 3^k la mayor potencia de 3 que es factor de N. Determina k.

AHSME 1992 #17

5.6.24 F

El día 300 del año N cae en martes. El día 200 del año $N+1$ cae también en martes. Determina en qué día de la semana cae el día 100 del año $N-1$.

AMC 12 2000 #18

5.6.25 M

Determina todos los números naturales $1 \le n \le 25$ tales que $n^2 + 3n + 2$ es divisible entre 6.

5.6.26 F

Sean $\underline{74A52B1}$ y $\underline{326AB4C}$ dos números de 7 dígitos, ambos múltiples de 3. Determina la suma de todos los posibles valores de C.

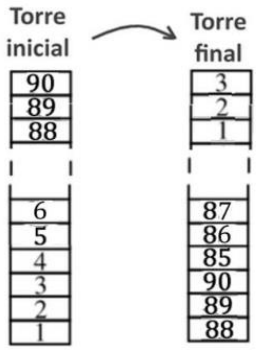
AMC 8 2014 #21

5.6.27 D

Demuestra el criterio de divisibilidad del 9 y del 11 aplicando el lenguaje y técnicas de la aritmética modular.

5.6.28 F

Sobre una mesa hay una torre hecha de bloques numerados del 1 al 90, ordenados en orden creciente de abajo arriba. Roberto los va cogiendo de tres en tres, comenzando por los tres de arriba y los va apilando, ordenadamente, y así construye otra torre, como se puede ver en la siguiente figura:



Cuando los haya acabado de colocar todos, ¿Cuántos bloques habrá entre el 39 y el 40?

(A) 0 (B) 1 (C) 2 (D) 3 (E) 4

Cangur B1 2023 #16, Canguro N5 2023 #16

5.6.29 F

Presentamos las filas 1, 2, 3, 4 y 5 de una tabla de enteros:

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 3 & & 1 & & \\ & 1 & & 5 & & 5 & & 1 & \\ 1 & & 7 & & 11 & & 7 & & 1 \end{array}$$

En la que cada fila se forma poniendo 1 en los extremos y en las posiciones intermedias sumando los dos números inmediatamente superiores de la fila anterior y añadiendo 1. Determina la cifra de las unidades de la suma de los 2023 números de la fila 2023.

(A) 1 (B) 3 (C) 5 (D) 7 (E) 9

AMC 12A 2023 #20

5.6.30 F

Determina el máximo común divisor de los números

$$A_n = 2^{3n} + 3^{6n+2} + 5^{6n+2}$$

Para todo $n = 0,1,...,1999$.

JBMO 2001

5.6.31 MF

Sea n un número natural. Probar que si la última cifra de 7^n es 3, la penúltima es 4.

OMEFL 2018 #5

5.6.32 MF

Demuestra que $2222^{5555}+5555^{2222}$ es múltiplo de 7.

OMEFL #4

5.6.33 M

Determina el número de valores distintos de la expresión

$$\frac{n^2-2}{n^2-n+2}$$

Donde $n\in\{1,2,3,...,100\}$

OME 2017 #1

5.6.34 D

Probar que hay infinitos números primos cuyo resto al dividirlos entre 3 es 2.

OMEFL 2017 #5

5.6.35 M

Determinar razonadamente si el número

$$\lambda_n=\sqrt{3n^2+2n+2}$$

es irracional para todo entero no negativo n.

OME 2012 #1

5.6.36 M

Los números naturales 22, 23, y 24 tienen la siguiente propiedad: los exponentes de los factores primos de su descomposición son todos impares:

$$22=2^1\cdot 11^1,\ 23=23^1,\ 24=2^3\cdot 3^1$$

¿Cuál es el mayor número de naturales consecutivos que pueden tener esa propiedad? Razónese la contestación.

OMEFL 2006 #5

5.6.37 MD

Demuestra que para cada entero n existe un entero de n dígitos, todos impares, divisible por 5^n.

USAMO 2003 #1

5.6.38 D

Demostrar que para cualquier par de enteros positivos k y n, existen k enteros positivos $m_1,m_2,...,m_k$ (no necesariamente distintos) tales que

$$1+\frac{2^k-1}{n}=\left(1+\frac{1}{m_1}\right)\left(1+\frac{1}{m_2}\right)...\left(1+\frac{1}{m_k}\right)$$

IMO 2013 #1

5.6.39 D

Sea n un entero positivo y sean $a_1,...,a_k$ $(k\geq 2)$ enteros distintos del conjunto {1, ...,n}, tales que n divide a $a_i\left(a_{i+1}-1\right)$, para $i=1,...,k-1$. Demostrar que n no divide a $a_k\left(a_1-1\right)$.

IMO 2009 #1

5.6.40 D

Determinar un número de cinco cifras tal que su cuadrado termine en las mismas cinco cifras colocadas en el mismo orden.

OME 1984 #2

5.6.41 M

Determinar todos los números de cuatro cifras $n=\overline{abcd}$ tales que al insertar un dígito 0 en cualquier posición se obtiene un múltiplo de 7.

OMEFL Aragón 2021#3

5.6.42 F

a) Demuestra que $2n-1$ y $2n+1$ son coprimos.

b) Demuestra que, si n es un número par, entonces n^2-1 y $3n+1$ son primos entre sí.

5.6.43 F

Demuestra que $2^{2001}+3^{2001}$ es divisible entre 7.

5.6.44 F

Determina el mayor entero positivo n para el que n^3+100 es divisible entre $n+10$.

AIME 1986

5.6.45 MD

Determina todos los enteros $n>1$ para los cuales si p es un divisor primo de n^6-1, también será un divisor de $\left(n^3-1\right)\left(n^2-1\right)$.

Baltic Mathematics Competition 2002

5.6.46 F

Consideremos los siguientes 100 conjuntos de 10 elementos:

{1, 2, 3, ... , 10},
{11, 21, 31, ... , 20},
...
{991, 991, 991, ... , 1000}.

¿Cuántos de estos conjuntos contienen exactamente dos múltiplos de 7?

(A) 40 (B) 42 (C) 43 (D) 49 (E) 50

AMC 12B 2022 #6, AMC 10B #8

5.6.47 M

Los enteros positivos x e y son tales que $3x+4y$ y $4x+3y$ son cuadrados perfectos. Demuestra que x e y son múltiplos de 7.

OMEFL Castilla y León 2023 #4

5.6.48 M

Encontrar todos los enteros positivos $a,b,c \geq 1$ que satisfacen

$$2^a + 7^b = c^2 + 4$$

OMEFL Aragón 2023 #6

5.6.49 D

Demuestra que, para cada entero positivo n, existe un número entero de n dígitos divisible entre 5^n cuyas cifras son todas impares.

USAMO 2003 #1

5.7 Inversos multiplicativos modulares.

Concepto de inverso multiplicativo. Primeros ejemplos.

Las operaciones de sumar, restar y multiplicar no son problemáticas en aritmética modular: Basta realizar la operación correspondiente en los naturales y después determinar el equivalente modular del resultado. Pero con la división las cosas se complicarán, y mucho. Necesitamos definir y estudiar los llamados inversos multiplicativos.

En el conjunto Q de números racionales, dado cualquier número diferente de cero, por ejemplo 3, podemos determinar la fracción $\frac{1}{3}$, que cumplirá la condición: $3 \cdot \frac{1}{3} = 1$

Así pues, diremos que $\frac{1}{3}$ es el inverso multiplicativo de 3. De la misma forma, $\frac{7}{5}$ es el inverso multiplicativo de $\frac{5}{7}$, por poner otro ejemplo.

En general, dado un número $n \neq 0$, definimos su **inverso multiplicativo** n^{-1} como el número tal que

$$n \cdot n^{-1} = 1$$

Diremos que un número es **invertible** cuando exista su inverso multiplicativo. Está claro que el 0 nunca es invertible.

Notación: Para referirnos al inverso multiplicativo de *k* nunca utilizaremos la notación como fracción $\frac{1}{k}$, siempre utilizaremos la notación exponencial: k^{-1}.

Ejemplo.

Observemos la tabla de multiplicar de Z_5:

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

El inverso multiplicativo de 2 es 3, porque $2 \cdot 3 = 6 \equiv 1 \pmod 5$, y escribiremos

$$2^{-1} = 3 \pmod 5$$

El inverso multiplicativo de 4 es el propio 4, porque $4 \cdot 4 = 16 \equiv 1 \pmod 5$, y escribiremos

$$4^{-1} = 4 \pmod 5$$

5.7.1

Observa atentamente la tabla de multiplicar de Z_7:

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Determina los inversos multiplicativos de 1, 2, 3, 4, 5 y 6. Utiliza la notación exponencial para denotarlos.

Sobre la (no) existencia de inversos multiplicativos.

Observa ahora la tabla de multiplicar de Z_8:

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Observamos que el 2 no tiene inverso multiplicativo: No existe ningún número que multiplicado por 2 dé 1. Diremos que el 2 no es invertible en Z_8.

Tampoco tienen inversos multiplicativos el 4 ni el 6. Así pues, **no siempre existen inversos multiplicativos modulares**.

Más ejemplos.

El inverso de 3 módulo 4 es 3 porque $3 \cdot 3 = 9 \equiv 1 \pmod 4$.

El inverso de 3 módulo 5 es 2 porque $3 \cdot 2 = 6 \equiv 1 \pmod 5$.

5.7.2

Determina totos los elementos invertibles de Z_6 y sus correspondientes inversos.

Teorema. Existencia y unicidad de inversos modulares.

Sean a,b enteros, se cumple $(a,b)=1$ si y solo si existe un entero x tal que $ax\equiv 1 \pmod b$, y este valor es único módulo b.

Demostración. Aplicando el TDB, si $(a,b)=1$ existirán x,y tales que $ax+by=1$, y por tanto $ax\equiv 1 \pmod b$.
Veamos la unicidad: Supongamos que existen dos valores x,x' tales que $ax\equiv 1 \pmod b$ y $ax'\equiv 1 \pmod b$. Entonces

$$x'\equiv 1x'\equiv axx'\equiv ax'x\equiv 1x\equiv x \pmod b$$

Recíprocamente, supongamos que $ax\equiv 1 \pmod b$, es decir, $ax-1=yb$ para cierto entero y, y por tanto $ax-yb=1\Leftrightarrow ax+(-y)b=1$.
Aplicando el TDB se deduce que $(a,b)=1$.

La congruencia lineal $ax\equiv 1 \pmod n$ tiene solución si y solo si $(a,n)\mid 1$, es decir, cuando $(a,n)=1$, así pues, existirá el inverso multiplicativo de a si y solo si $(a,n)=1$, y será único modulo n.

Definición. Cuerpo.

Diremos que Z_n es un **cuerpo** cuando todos los elementos de Z_n excepto el cero tengan su correspondiente inverso multiplicativo.
Así pues, si n es primo, siempre se cumplirá $(a,n)=1$, y por tanto Z_n será un cuerpo.

Ejercicio resuelto.

Determina el inverso de 9 módulo 82.

Solución: Observamos que $9\cdot 9=81\equiv -1 \pmod{82}$, luego $9\cdot(-9)=-81\equiv 1 \pmod{82}$.
El inverso de 9 módulo 82 es $-9\equiv 82-9=73 \pmod{82}$.

Ejercicio resuelto.

Determina todas las parejas de inversos módulo 20.

Solución: Sabemos que serán todos los números coprimos con 20, es decir:

$$\{1,3,7,9,11,13,17,19\}$$

Ahora solo nos queda agruparlos por parejas (o consigo mismo)
El 1 es inverso de sí mismo, pues $1\cdot 1=1\equiv 1 \pmod{20}\Rightarrow 1^{-1}\equiv 1 \pmod{20}$
Vemos que $3\cdot 7=21\equiv 1 \pmod{20}\Rightarrow 3^{-1}\equiv 7 \pmod{20}$, $7^{-1}\equiv 3 \pmod{20}$
Vemos que $17\cdot 13=221\equiv 1 \pmod{20}\Rightarrow 17^{-1}\equiv 13 \pmod{20}$, $13^{-1}\equiv 17 \pmod{20}$
El 11 es inverso de sí mismo, pues $11\cdot 11=121\equiv 1 \pmod{20}\Rightarrow 11^{-1}\equiv 11 \pmod{20}$
El 9 es inverso de sí mismo, pues $9\cdot 9=81\equiv 1 \pmod{20}\Rightarrow 9^{-1}\equiv 9 \pmod{20}$
Finalmente, el 19 también es inverso de sí mismo, pues

$$19\cdot 19=381\equiv 1 \pmod{20}\Rightarrow 19^{-1}\equiv 19 \pmod{20}$$

Otra manera de verlo es observar que $19\equiv -1 \pmod{20}\Rightarrow 19^2\equiv (-1)^2=1 \pmod{20}$

Determinación de inversos multiplicativos mediante el ADE.

Dado un elemento $a \in Z_n$, $a \not\equiv 0$, cumpliendo $(a,n)=1$, sabemos que será invertible, y el ADE nos ofrece la combinación lineal

$$xa+bn=1$$

Luego $xa+bn=1 \Rightarrow xa \equiv 1 \pmod{n} \Rightarrow a = x^{-1} \pmod{n}$

Ejemplo resuelto.

Determina $34^{-1} \pmod{143}$

Solución. Sabemos que, puesto que $(34,143)=1$, existirán enteros x, y tales que $34x+143y=1$, y por tanto $34x=1-143y \Rightarrow 34x \equiv 1 \pmod{143}$.

El Algoritmo de Euclides (4.17) nos permite determinar esta combinación lineal:

$143=34\cdot 4+7 \Rightarrow (143,34)=(34\cdot 4+7,34)=(7,34)$

$34=4\cdot 7+6 \Rightarrow (7,34)=(7,4\cdot 7+6)=(7,6)=1$, luego:

$1=7-6=7-(34-4\cdot 7)=7-34+4\cdot 7=-34+5\cdot 7=-34+5\cdot(143-34\cdot 4)=$

$=-34+5\cdot 143-34\cdot 4\cdot 5=5\cdot 143-21\cdot 34$

Y por tanto $34^{-1} \equiv -21 \equiv 122 \pmod{143}$

Ejemplo resuelto.

Determina el inverso de 11 en Z_{20}.

Solución.

$$20=1\cdot 11+9 \rightarrow 11=1\cdot 9+2 \rightarrow 9=4\cdot 2+1 \rightarrow 2=2\cdot 1$$

Por lo tanto $mcd(11,20)=1$

Ahora sustituimos de abajo hacia arriba los restos:

$$1=9-4\cdot \underline{2}=9-4(11-9)=9-4\cdot 11+4\cdot 9=5\cdot \underline{9}-4\cdot 11=$$
$$=5\cdot(20-11)-4\cdot 11=5\cdot 20-9\cdot 11$$

Luego

$1=5\cdot 20-9\cdot 11 \equiv -9\cdot 11 \pmod{20} \Rightarrow 11^{-1}=-9 \equiv -9+20 \equiv 11 \pmod{20}$

5.7.3

Determinar el inverso de 117 módulo 244.

Problema resuelto.

Demostrar que las seis últimas cifras de 7^{9999} son 857143.

Solución. Las claves de este problema son demostrar que

$$7 \cdot 7^{9999} = 7^{10000} \equiv 1 \left(\text{mod } 10^6\right)$$

y observar que

$$857143 = \frac{6000001}{7} = \frac{6 \cdot 10^6}{7} \Rightarrow 7 \cdot 857143 \equiv 1 \left(\text{mod } 10^6\right)$$

Demostrar que $7^{10000} \equiv 1 \left(\text{mod } 10^6\right)$ se puede hacer "por fuerza bruta", o mediante el Binomio de Newton: $7^4 = 2401 = 24 \cdot 10^2 + 1$, luego

$$7^{10000} = \left(7^4\right)^{2500} = \left(24 \cdot 10^2 + 1\right)^{2500} =$$

$$= 1 + \binom{2500}{1} 24 \cdot 10^2 + \binom{2500}{2} \left(24 \cdot 10^2\right)^2 + \binom{2500}{3} \left(24 \cdot 10^2\right)^3 + \ldots$$

$$= 1 + 2500 \cdot 24 \cdot 10^2 + 1250 \cdot 2499 \left(24 \cdot 10^2\right)^2 + \binom{2500}{3} 24^3 \cdot 10^6 + \ldots$$

$$= 1 + 3 \cdot 2^7 \cdot 5^6 + 2^7 \cdot 3^3 \cdot 5^4 \cdot 7^2 \cdot 17 \cdot 10^4 + \ldots$$

$$= 1 + 3 \cdot 2 \cdot 10^6 + 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 17 \cdot 10^6 + \ldots$$

$$= 1 + \left(3 \cdot 2 + 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 17 + \ldots\right) \cdot 10^6 \Rightarrow 7^{10000} \equiv 1 \left(\text{mod } 10^6\right)$$

Por otro lado, observamos que $857143 = \frac{6000001}{7} = \frac{6 \cdot 10^6}{7}$

Con lo cual:

$$7^{10000} \equiv 1 \left(\text{mod } 10^6\right) \Rightarrow 7^{10000} = k \cdot 10^6 + 1 = k \cdot 10^6 - 6 \cdot 10^6 + 6 \cdot 10^6 + 1 =$$

$$= (k + 6) \cdot 10^6 + 6 \cdot 10^6 + 1$$

$(k + 6) \cdot 10^6 = 7^{10000} - \left(6 \cdot 10^6 + 1\right)$ ambos múltiples de 7, luego $k + 6$ será también múltiplo de 7, es decir: $7^{10000} = 7k' \cdot 10^6 + 6 \cdot 10^6 + 1$

Y por tanto, finalmente:

$$7^{9999} = \frac{7^{10000}}{7} = \frac{7k' \cdot 10^6 + 6 \cdot 10^6 + 1}{7} = k' \cdot 10^6 + 857143$$

tal y como queríamos ver.

Fuente: Jerónimo Vega Guillén en Facebook.

Observamos que

$$\left.\begin{array}{l} 7 \cdot 7^{9999} \equiv 1 \left(\text{mod } 10^6\right) \\ 7 \cdot 857143 \equiv 1 \left(\text{mod } 10^6\right) \end{array}\right\} \Rightarrow 7^{9999} \equiv 857143 \left(\text{mod } 10^6\right)$$

Es consecuencia del teorema anterior, puesto que $\left(7, 10^6\right) = 1$

Corolario. Lema de Gauss.

Si a,b,c son enteros tales que $a \mid bc$ y $(a,b)=1$, entonces $a \mid c$.

Demostración. $(a,b)=1$, luego existirá un x tal que $bx \equiv 1 \pmod{a}$. Pero por otro lado, $a \mid bc \Rightarrow 0 \equiv bc \equiv xbc \equiv cbx \equiv c1 \equiv c \pmod{a} \Rightarrow a \mid c$.

Corolario.

a) $(a,b_1)=(a,b_2)=...=(a,b_n)=1 \Rightarrow \left(a, b_1 \cdot b_2 \cdot ... \cdot b_n\right)=1$

b) En particular, $(a,b)=1 \Rightarrow \left(a,b^k\right)=1$ para todo $k \geq 1$.

Demostración. a) $(a,b_1)=(a,b_2)=...=(a,b_n)=1$, luego existirán $x_1,...,x_n$ tales que $x_i b_i \equiv 1 \pmod{a}$. Multiplicando tenemos que $(x_1 x_2 ... x_n)(b_1 b_2 ... b_n) \equiv 1 \cdot 1 \cdot ... \cdot 1 \equiv 1 \pmod{a}$, y por tanto $\left(a, b_1 \cdot b_2 \cdot ... \cdot b_n\right)=1$ por el recíproco del Teorema del inverso modular.

b) Basta tomar en el apartado anterior $b_1 = b_2 = ... = b_k = b$

Corolario.

$a^n \mid b^n \Rightarrow a \mid b$

Demostración. Si $a=0$ o $b=0$ está claro que $a \mid b$. Supongamos que $a,b \neq 0$.

Sea $d=(a,b) \Rightarrow a=du$, $b=dv$ con $(u,v)=1$.

Luego $a^n \mid b^n \Rightarrow (du)^n \mid (dv)^n \Rightarrow d^n u^n \mid d^n v^n \Rightarrow u^n \mid v^n \Rightarrow u \mid v^n$

Por el corolario anterior, $(u,v)=1 \Rightarrow (u,v^n)=1$, y por tanto $u=\pm 1$, y en consecuencia $a=\pm d$, y por lo tanto divide a $b=dv$.

Corolario.

Si $a \mid c$ y $b \mid c$ con $(a,b)=1$, entonces $ab \mid c$

Demostración. $a \mid c \Rightarrow c=ad$ para cierto d.

$\left.\begin{array}{l} b \mid ad \\ (a,b)=1 \end{array}\right\} \Rightarrow b \mid d$ por el Lema de Gauss, y por tanto $ab \mid ad=c$, como queríamos ver.

Teorema.

Sean a,b enteros positivos coprimos, tales que su producto es una potencia de grado n, es decir, $ab=c^n$ para cierto entero positivo c. Entonces a y b también son ambos potencias de grado n.

Demostración. Sea $d=(a,c)$, y escribimos $a=du$ y $c=dv$ para ciertos u,v coprimos.

$$\left.\begin{array}{l} a=du \\ ab=c^n \end{array}\right\} \Rightarrow dub=(dv)^n=d^n v^n \Rightarrow ub=d^{n-1}v^n \quad (*)$$

De la igualdad anterior se desprende que $u \mid d^{n-1}v^n$, pero por hipótesis,

$(u,v)=1 \Rightarrow (u,v^n)=1$, y por tanto $u \mid d^{n-1}$. Así pues, $v^n = \dfrac{u}{d^{n-1}} b$, es decir, $b \mid v^n$.

Pero de la igualdad (*) también se deduce que $v^n \mid ub$, y puesto que $(u, v^n) = 1$, llegamos a $v^n \mid b$, y finalmente:

$$\left.\begin{array}{l} b \mid v^n \\ v^n \mid b \end{array}\right\} \Rightarrow b = v^n$$

Sustituyendo en (*) se deduce $u = d^{n-1} \Rightarrow a = d^n$, con lo que se concluye la demostración.

Problema resuelto.

Demuestra que el producto de tres números consecutivos nunca puede ser una potencia perfecta.

Solución. Supongamos que $(n-1)n(n+1) = a^k$, para ciertos enteros $a, k > 1$.

Entonces podemos escribir $n(n^2-1) = a^k$. Puesto que $(n, n^2-1) = 1$ podemos aplicar el teorema anterior: $n = b^k$, $n^2 - 1 = c^k$ para ciertos enteros $b, c > 1$.

$n^2 - 1 = c^k \Rightarrow 1 = n^2 - c^k = \left(b^k\right)^2 - c^k = \left(b^2\right)^k - c^k = \left(b^2 - c\right)\left(b^{2(k-1)} + \ldots + c^{k-1}\right)$

Lo cual es imposible pues $b^2 - c \geq 1$ y $b^{2(k-1)} + \ldots + c^{k-1} \geq k > 1$.

Determinación de inversos multiplicativos mediante exponenciación modular.

En 13.1 introduciremos El Pequeño Teorema de Fermat (PTF):

si p es primo y $p \nmid a$, entonces $a^{p-1} \equiv 1 \pmod{p}$

Luego

$$a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^{-1} = a^{p-2} \pmod{p}$$

Y para determinar a^{p-2} podemos aprovechar la exponenciación modular "pow", implementada en Python a partir de su versión 3.8:

```
pow(a,p-2,p)
```

Cancelación modular.

Trabajando en la aritmética convencional con enteros, sabemos que siempre podemos *tachar* factores:

$$a \cdot b = a \cdot c \Rightarrow b = c$$

Pero no ocurre lo mismo en aritmética modular. Por ejemplo:

$$10 \cdot 5 \equiv 10 \cdot 11 \pmod{12} \text{ pero } 5 \not\equiv 11 \pmod{12}$$

Aquí no podemos *tachar* (cancelar) el factor 10 repetido.

Lema. Cancelación de términos en aritmética modular.

Si $(a, n) = 1$, entonces $ar \equiv as \pmod{n} \Rightarrow r \equiv s \pmod{n}$.

Demostración.

Si $(a,n)=1$ entonces existirá un elemento b tal que $ab \equiv 1 \pmod{n}$, y por tanto:

$ar \equiv as \pmod{n} \Rightarrow b(ar) \equiv b(as) = \pmod{n}$

Ahora, aplicando las propiedades asociativa y conmutativa de la multiplicación modular, por un lado, $b(as) = (ab)s \equiv 1s = s \pmod{n}$, y por otro $b(ar) = (ba)r = (ab)r \equiv 1r = r \pmod{n}$, con lo que llegamos a $r \equiv s \pmod{n}$.

División modular.

La división de dos números $a \div b$, con $b \neq 0$ no se considera propiamente una operación, como la suma o el producto, sino que se interpreta como una forma rápida de escribir el producto de a por el inverso de b:

$$a \div b = a \cdot b^{-1}$$

Ejemplo.

Supongamos que queremos calcular $3 \div 2 \pmod{7}$

Observamos la tabla de la multiplicación en Z_7:

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

El inverso multiplicativo de 2 es 4, luego

$3 \div 2 = 3 \cdot 2^{-1} \equiv 3 \cdot 4 = 12 \equiv 5 \pmod{7}$

Teorema. Definición y caracterización de los divisores de cero.

Dado un elemento x de Z_n, diremos que es un **divisor de cero** cuando exista un elemento $y \not\equiv 0$ de Z_n tal que $x \cdot y \equiv 0$. Todo elemento x de Z_n es un divisor de cero si y solo si $(x,n) > 1$, es decir, cuando no sea invertible.

Demostración.

Supongamos que $d = (x,n) > 1$. Luego $x\frac{n}{d} = \frac{x}{d}n \Rightarrow x \cdot \frac{n}{d} \equiv 0 \pmod{n}$

Y se cumple $\frac{n}{d} \not\equiv 0$ pues $d > 1 \Rightarrow \frac{n}{d} < n$ y por lo tanto $\frac{n}{d}$ no puede ser un múltiplo de n.

Ejemplo.

En Z_{15} las clases invertibles son 1, 2, 4, 6, 7, 8, 11, 13 y 14 y las clases divisores de cero son las restantes: 3, 5, 6, 9, 10 y 12.
Por ejemplo: $10 \cdot 3 \equiv 0 \pmod{15}$.

Inverso multiplicativo con Python.

Podemos utilizar la función egcd(a,b) definida anteriormente para construir la función **`modinv(a,m):`**

```
def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, y, x = egcd(b % a, a)
        return (g, x - (b // a) * y, y)

def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
        raise Exception('No existe inverso modular')
    else:
        return x % m
```

División modular en Python.

```
def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, y, x = egcd(b % a, a)
        return (g, x - (b // a) * y, y)

def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
        raise Exception('No existe inverso modular')
    else:
        return x % m

def moddiv(a,b,m):
       invb=modinv(b, m)
       return (a*invb) % m

print(moddiv(3,2,7))
```

6 Congruencias lineales y sistemas de congruencias lineales.

Llamaremos congruencias a las ecuaciones que se plantean en términos modulares. Como es habitual, diremos que una congruencia es lineal cuando sus incógnitas estén elevadas únicamente a la primera potencia.

6.1 Congruencias lineales.

6.1.1

Resuelve las siguientes congruencias lineales:

a) $x-4\equiv 0\pmod 5$ b) $x-1\equiv 1\pmod 5$ c) $x+3\equiv 1\pmod 5$ d) $x+12\equiv 3\pmod 5$

Congruencia lineal.

Toda congruencia lineal se puede reducir a una congruencia de la forma $a\,x\equiv b\pmod n$

Diremos que el entero x_0 satisface la congruencia lineal $a\,x\equiv b\pmod n$ cuando

$$a\,x_0\equiv b\pmod n$$

O equivalentemente: $a\,x_0\equiv b\pmod n \Leftrightarrow a\,x_0=ny_0+b\Leftrightarrow a\,x_0-n\,y_0=b$

Es decir, buscamos soluciones (x_0,y_0) de la ecuación lineal diofántica

$$a\,x_0-n\,y_0=b$$

Ejercicio resuelto.

Suponiendo que $5x\equiv 6\pmod 8$, determina x.

Solución: $5x\equiv 6\pmod 8\Leftrightarrow x\equiv 5^{-1}6\pmod 8$

Determinamos $5^{-1}\pmod 8$ por el método del EGCD.

$8=5+3\,,\,5=3+2\,,\,3=2+1$

Luego

$1=3-2=3-(5-3)=3-5+3=2\cdot 3-5=2(8-5)-5=2\cdot 8-2\cdot 5-5=$

$=2\cdot 8-3\cdot 5$

$1=2\cdot 8-3\cdot 5\Rightarrow 1\equiv 3\cdot 5\pmod 8\Rightarrow 5^{-1}=-3\pmod 8$

$x\equiv 5^{-1}6=(-3)\cdot 6=-18\equiv -2\equiv 6\pmod 8$

6.1.2

Resuelve las siguientes congruencias lineales:

a) $3x\equiv 1\pmod 5$ b) $3x\equiv 2\pmod 5$ c) $2x\equiv 3\pmod 5$ d) $12x\equiv 4\pmod 5$

e) $2x-4\equiv 2\pmod 5$

6.1.3 Teorema. Existencia de soluciones de una congruencia lineal.

La congruencia lineal $ax \equiv b \pmod{n}$ tiene solución si y solo si $d \mid b$, donde $d = (a,n)$, en cuyo caso existen d soluciones diferentes en Z_n, todas ellas de la forma

$$x_o\ ,\ x_1 = x_0 + \frac{n}{d}\ ,\ x_2 = x_0 + \frac{n}{d}\cdot 2\ ,\ x_3 = x_0 + \frac{n}{d}\cdot 3\ ,\ \ldots\ ,\ x_{d-1} = x_0 + \frac{n}{d}\cdot (d-1)$$

Donde x_0 es una solución particular de la ecuación.

Ejemplo.

Resuelve la congruencia $18x \equiv 30 \pmod{42}$

Solución. $d = (18,42) = 6$, y $6 \mid 30$, luego la ecuación anterior tiene seis soluciones. Por tanteo, vemos que $18 \cdot 4 = 72 = 42 \cdot 1 + 30 \Rightarrow 4$ es una solución de la ecuación. Luego las soluciones serán:

$x_0 = 4$

$x_1 = 4 + (42/6)\cdot 1 = 4 + 7 = 11$, efectivamente: $18 \cdot 11 = 198 = 4 \cdot 42 + 30$

$x_2 = 4 + (46/6)\cdot 2 = 4 + 14 = 18$, efectivamente: $18 \cdot 18 = 324 = 7 \cdot 42 + 30$

$x_3 = 4 + (46/6)\cdot 3 = 4 + 21 = 25$, efectivamente: $18 \cdot 25 = 450 = 10 \cdot 42 + 30$

$x_4 = 4 + (46/6)\cdot 4 = 4 + 28 = 32$, efectivamente: $18 \cdot 32 = 576 = 13 \cdot 42 + 30$

$x_5 = 4 + (46/6)\cdot 5 = 4 + 35 = 39$, efectivamente: $18 \cdot 39 = 630 = 16 \cdot 42 + 30$

Las soluciones son: $\{4,11,18,25,32,39\}$

6.1.4 [F]

Resuelve la congruencia $9x \equiv 21 \pmod{30}$

6.1.5 [F]

Resuelve la congruencia lineal $3x \equiv 7 \pmod{10}$

Propiedad. Simplificación de congruencias lineales.

$$ka \equiv kb \pmod{kn} \Rightarrow a \equiv b \pmod{n}$$

Problema resuelto.

Resuelve la congruencia

$$39x \equiv 52 \pmod{130}$$

Solución. Esta congruencia tiene solución pues $d = (39,130) = 13$ y $13 \mid 39$.

Simplificamos la congruencia dividiendo por 13:

$39x \equiv 52 \pmod{130} \Leftrightarrow 3x \equiv 4 \pmod{10}$

El inverso multiplicativo módulo 10 de 3 es 7, luego

$$3x \equiv 4 \pmod{10} \Rightarrow 7 \cdot 3x \equiv 7 \cdot 4 = 28 \equiv 8 \pmod{10} \Rightarrow x \equiv 8 \pmod{10}$$

Luego las soluciones de $39x \equiv 52 \pmod{130}$ son todos los conjuntos de la forma

$$8 + 130k = \{..., -122, 8, 138, 268, ...\}$$
$$18 + 130k = \{..., -112, 18, 438, 278, ...\}$$
$$...$$
$$128 + 130k = \{..., -132, -2, 128, 268, ...\}$$

Problema resuelto.

Resuelve la congruencia

$$140x \equiv 56 \pmod{252}$$

Solución. Esta congruencia tiene solución pues $d = (140,252) = 28$ y $28 \mid 56$.

Vemos que se puede simplificar pues todos los números involucrados son múltiples de 28:

$$140x \equiv 56 \pmod{252} \Leftrightarrow 5x \equiv 2 \pmod{9}$$

Para resolver esta última congruencia vemos que el inverso de 5 módulo 9 es 2:

$$5 \cdot 2 = 10 \equiv 1 \pmod{9}$$

Luego

$$5x \equiv 2 \pmod{9} \Leftrightarrow x \equiv 5^{-1} \cdot 2 \equiv 2 \cdot 2 \equiv 4 \pmod{9}$$

Las 28 soluciones módulo 252 son, por tanto:

$$4, 4+9, 4+18, 4+27, 4+36, ...$$

6.2 Sistemas de congruencias lineales (resolución directa).

Queremos resolver un sistema de congruencias lineales:

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \dots \\ a_r x \equiv b_r \pmod{m_r} \end{cases}$$

En donde vamos a suponer que los módulos m_i son todos coprimos entre ellos.

6.2.1 Problema solucionado paso a paso en vídeo

El residuo de la división de 2021 entre 6, entre 7, entre 8 y entre 9 es 5 en los cuatro casos. ¿Cuántos enteros positivos menores de 2021 hay que tengan esta propiedad?

(A) 1 (B) 3 (C) 2 (D) 4 (E) Cap

Cangur B1 2021 #15, Kangaroo Junior 2021 #14

Solución: https://youtu.be/6kF0qgD2AM4?t=83

6.2.2 Problema solucionado paso a paso en vídeo

El número N tiene dos dígitos. Cuando N se divide entre 9, el residuo es 1. Cuando N se divide entre 10, el residuo es 3. Determina el residuo cuando N se divide entre 11.

(A) 0 (B) 2 (C) 4 (D) 5 (E) 7

AMC 8 2016 #5

Solución: https://youtu.be/6kF0qgD2AM4?t=416

6.2.3 Problema solucionado paso a paso en vídeo

Determina la cantidad de enteros positivos de tres dígitos con la siguiente propiedad: Cuando se divide entre 6, da residuo 2, cuando se divide entre 9, da residuo 5, y cuando se divide entre 11 da residuo 7 .

(A) 1 (B) 2 (C) 3 (D) 4 (E) 5

AMC 8 2018 #21

Solución: https://youtu.be/6kF0qgD2AM4?t=598

6.2.4 Ejemplo.

Resuelve el sistema

$$\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 0 \pmod 5 \end{cases}$$

Solución. De la primera congruencia deducimos que x será un múltiple de 2, y de la segunda que x será un múltiplo de 5, luego x será un múltiplo de 10:

$$x \equiv 0 \pmod{10}$$

Visualmente:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
	X		X		X		X		X		X		X		X		X		X		X		X		X		X		X		X		X		X		X		X
				X					X					X					X						X					X					X					X

6.2.5 Ejemplo.

Resuelve el sistema

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 0 \pmod 7 \end{cases}$$

Solución. De la segunda congruencia deducimos que x debe ser un múltiplo de 7:

7, 14, 21, 28, 35, 42, 49, 56, 63, 70...

De la primera congruencia deducimos que x debe ser de la forma $3a+1$. Los valores de la lista anterior que cumplen esta propiedad son:

7, 28, 49, 70...

Vemos que estos números son todos de la forma $x = 21b + 7$, y que $21 = (3, 7)$. Así pues, parece ser que las soluciones son:

$$x \equiv 7 \pmod{21}.$$

Demostraremos ahora que, efectivamente, $x \equiv 7 \pmod{21}$ son soluciones del sistema.

$x = 21b + 7 = 3 \cdot 7x + 2 \cdot 3 + 1 \equiv 1 \pmod 3$, y por lo tanto satisface la primera congruencia del sistema.

$x = 21b + 7 = 3 \cdot 7x + 1 \cdot 7 \equiv 0 \pmod 7$, y por lo tanto también satisface la segunda congruencia del sistema.

Visualmente:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
X			X			X			X			X			X			X			X			X			X			X			X			X			X			X
						X							X							X							X								X						

6.2.6 Ejemplo.

Resuelve el sistema

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 7 \end{cases}$$

Solución.

$$\begin{cases} x \equiv 3 \pmod 4 \Rightarrow x = 4a + 3 \\ x \equiv 2 \pmod 7 \Rightarrow x = 7b + 2 \end{cases} \Rightarrow 4a + 3 = 7b + 2 \Rightarrow 4a + 1 = 7b \Rightarrow 4a + 1 \equiv 0 \pmod 7$$

$4a+1\equiv 0\pmod 7\Rightarrow 4a\equiv -1\pmod 7\Rightarrow 4a\equiv 6\pmod 7$

Esta última congruencia la podemos resolver con los métodos del apartado anterior: El inverso multiplicativo de 4 módulo 7 es 2, luego:

$a\equiv 2\cdot 6=12\equiv 5\pmod 7\Rightarrow a=7c+5$

Sustituyendo más arriba tenemos:

$x=4a+3=4(7c+5)+3=28c+20+3=28c+23\Leftrightarrow x\equiv 23\pmod{28}$

Visualmente:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
		X				X				X				X				X				X				X				X				X				X	
	X							X							X							X							X								X			

6.2.7 Ejemplo.

Resuelve el sistema $\begin{cases} x\equiv 3\ (\text{mod } 4)\\ x\equiv 1\ (\text{mod } 5)\\ x\equiv 2\ (\text{mod } 3)\end{cases}$

Solución.

(Más adelante, mediante el Teorema chino del residuo, se verá que la solución existe y es única mod 60, pues $(4,5)=(5,3)=(4,3)$)

$x\equiv 3\ (\text{mod } 4)\Leftrightarrow x=4a+3\Rightarrow$

$x\equiv 1\ (\text{mod } 5)\Rightarrow 4a+3\equiv 1\ (\text{mod } 5)\Rightarrow 4a\equiv -2\ (\text{mod } 5)=-2+5\ (\text{mod } 5)=3\ (\text{mod } 5)$

$4a\equiv 3\ (\text{mod } 5)\Rightarrow 4\cdot 4a\equiv 4\cdot 3\ (\text{mod } 5)\Rightarrow 16a\equiv 12\ (\text{mod } 5)\Rightarrow a\equiv 2\ (\text{mod } 5)\Rightarrow$

$a=5b+2\Rightarrow x=4a+3=4(5b+2)+3=20b+11$

Luego:

$x\equiv 2\ (\text{mod } 3)\Rightarrow 20b+11\equiv 2\ (\text{mod } 3)\Rightarrow 20b\equiv -9\ (\text{mod } 3)=0\ (\text{mod } 3)$

$\Rightarrow b=0\ (\text{mod } 3)\Rightarrow b=3c$

Finalmente:

$x=20b+11=20\cdot 3c+11=11+60c\ (\text{mod } 60)$. En efecto:

$11=4\cdot 2+3,\ 11=5\cdot 2+1,\ 11=3\cdot 3+2$

Visualmente:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
		X				X				X				X				X				X				X				X				X				X	
X					X					X					X					X						X				X					X				
	X			X			X			X			X			X			X			X			X			X			X				X			X		

6.2.8 Ejemplo resuelto.

Resuelve el sistema

$$\begin{cases} x\equiv 3\pmod 5\\ x\equiv 4\pmod{11}\end{cases}$$

Solución.

$$\left.\begin{array}{l} x\equiv 3\pmod 5\Leftrightarrow x=5k+3\\ x\equiv 4\pmod{11}\Leftrightarrow x=11q+4\end{array}\right\}\Rightarrow 5k+3=11q+4\Rightarrow 5k-11q=1$$

Mediante el EGCD o probando vemos que $5(-2)-11(-1)=1$, luego

$$\left.\begin{array}{l} x=5(-2)+3=-7\\ x=11(-1)+4=-7\end{array}\right\}\Rightarrow x\equiv -7\equiv 48\pmod{55}$$

6.3 Sistemas de congruencias lineales con módulos coprimos.

6.3.1 Teorema. Teorema chino del residuo. (Primera versión, con coeficientes = 1)

Sean $m_1, m_2, ..., m_r$ enteros positivos tales que $(m_i, m_j) = 1$ si $i \neq j$. Entonces el sistema de congruencias lineales

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ ... \\ x \equiv b_r \pmod{m_r} \end{cases}$$

Tiene una única solución x módulo el entero $m_1 \cdot m_2 \cdot ... \cdot m_r$.

y se obtiene siguiendo los siguientes pasos:

Paso 1: Sea $N = m_1 \cdot m_2 \cdot ... \cdot m_r$,

Paso 2: Sean $N_1 = N / m_1$, $N_2 = N / m_2$, ..., $N_r = N / m_r$.

Paso 3: Resolver las congruencias lineales:

$N_1 y_1 \equiv 1 \pmod{m_1}$, $N_2 y_2 \equiv 1 \pmod{m_2}$, ..., $N_r y_r \equiv 1 \pmod{m_r}$

Paso 4: $x \equiv N_1 y_1 b_1 + N_2 y_2 b_2 + ... + N_r y_r b_r \pmod{N}$ es la única solución del sistema.

Demostración.

Sea $N = m_1 \cdot m_2 \cdot ... \cdot m_r$, y sean $N_1 = N / m_1$, $N_2 = N / m_2$, ..., $N_r = N / m_r$.

Es decir, $N_k = m_1 \cdot m_2 \cdot .... \cdot m_{k-1} \cdot m_{k+1} \cdot ... \cdot m_r$, y puesto que $(m_i, m_j) = 1$ si $i \neq j$, está claro que $(N_k, m_k) = 1$, y por tanto, aplicando el Teorema 8.2.1, cada N_k tendrá un inverso multiplicativo módulo m_k, al que llamaremos y_k.

Sea el entero $x \equiv N_1 y_1 b_1 + N_2 y_2 b_2 + ... + N_r y_r b_r$, y vamos a demostrar que este entero satisface las condiciones del enunciado.

Puesto que $N_k = m_1 \cdot m_2 \cdot .... \cdot m_{k-1} \cdot m_{k+1} \cdot ... \cdot m_r$, está claro que $N_i \equiv 0 \pmod{m_j}$ si $i \neq j$, y por tanto $x \equiv N_k y_k b_k = b_k \pmod{m_k}$, para todo k, es decir, este número satisface todas las congruencias del enunciado.

Veamos que esta solución es única módulo N.

Supongamos que existe otra solución y módulo N. Para cualquier valor de k, $1 \leq k \leq r$,

$$\left.\begin{array}{l} x \equiv y \pmod{N} \Leftrightarrow N \mid x - y \Leftrightarrow m_1 \cdot m_2 \cdot ... \cdot m_r \mid x - y \\ m_k \mid N \end{array}\right\} \Rightarrow m_k \mid x - y \Rightarrow x \equiv y \pmod{m_k}$$

Y por tanto $y \equiv x \equiv b_k \pmod{m_k}$, es decir, y también satisface el sistema de congruencias.

Veamos ahora que todas las soluciones posibles son de esta forma. Supongamos que dos enteros x e y son soluciones del sistema de congruencias, entonces, para todo k, $1 \leq k \leq r$,

$$y \equiv x \equiv b_k \pmod{m_k} \Rightarrow x - y \equiv 0 \pmod{m_k} \Rightarrow m_k \mid x - y$$

Y, puesto que los m_k son coprimos dos a dos, tendremos que

$$N = m_1 \cdot m_2 \cdot ... \cdot m_r \mid x - y \Rightarrow x \equiv y \pmod{N}$$

6.3.2 Ejemplo. El problema de Sun-Tsu.

El Teorema chino del residuo debe su nombre en honor al siguiente problema del siglo I DC: Determina un número cuyos residuos son 2, 3 y 2 al dividirlo entre 3, 5 y 7, respectivamente.

Nota: Este mismo problema aparece en las *Introductio Arithmeticae* del matemático griego **Nicómano de Gerasa**, alrededor del 100 DC.

Solución. Se trata de resolver el sistema de congruencias lineales

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Paso 1: $N = 3 \cdot 5 \cdot 7 = 105$

Paso 2: $N_1 = \dfrac{105}{3} = 35$, $N_2 = \dfrac{105}{5} = 21$, $N_3 = \dfrac{105}{7} = 15$

Paso 3: Las congruencias lineales $35y_1 \equiv 1 \pmod 3$, $21y_2 \equiv 1 \pmod 5$ y $15y_3 \equiv 1 \pmod 7$ tienen soluciones $y_1 = 2$, $y_2 = 1$ y $y_3 = 1$.

Paso 4: $x = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233$ será solución del sistema módulo 105, y $233 \equiv 23 \pmod{105}$

Y por tanto 23 es la única solución del sistema (módulo 105).

En efecto: $23 = 7 \cdot 3 + 2$, $23 = 4 \cdot 5 + 3$, $23 = 3 \cdot 7 + 2$

6.3.3 Ejemplo resuelto.

Resolver el sistema de congruencias

$$\begin{cases} x \equiv 2 \pmod 4 \\ x \equiv 7 \pmod 9 \end{cases}$$

Solución.

Claramente $(4,9) = 1$ y por tanto el sistema tiene solución.

Paso 1: $N = 4 \cdot 9 = 36$

Paso 2: $N_1 = \dfrac{36}{4} = 9$, $N_2 = \dfrac{36}{9} = 4$.

Paso 3: Resolvemos las ecuaciones $9y_1 \equiv 1 \pmod 4$ y $4y_2 \equiv 1 \pmod 9$

Puesto que $9 \cdot 1 = 2 \cdot 4 + 1$, y $4 \cdot 7 = 28 = 3 \cdot 9 + 1$, tenemos que $y_1 = 1$, $y_2 = 7$ son soluciones.

Paso 4: La solución es $x = 9 \cdot 1 \cdot 2 + 4 \cdot 7 \cdot 7 = 214 \pmod{36}$, es decir, 34.

Efectivamente, $34 = 4 \cdot 8 + 2$, y $34 = 9 \cdot 3 + 7$,

6.3.4 [F] Problema solucionado paso a paso en vídeo.

Determina el número de parejas ordenadas (x,y) de enteros positivos, con $y<x\leq 100$ tales que

$$\frac{x}{y}\ ,\ \frac{x+1}{y+1}$$

sean enteros.

AIME 1995 #8

Solución: https://youtu.be/0ZsmuF4WPb8

6.3.5 Teorema. Teorema chino del residuo (Versión general).

Sean $m_1,m_2,...,m_r$ enteros positivos tales que $(m_i,m_j)=1$ si $i\neq j$.

Sean $b_1,b_2,...,b_r$ enteros arbitrarios y $a_1,a_2,...,a_r$ enteros tales que $(a_k,m_k)=1$ para todo $1\leq k\leq r$.

Entonces el sistema de congruencias lineales

$$\begin{cases} a_1 x\equiv b_1 \pmod{m_1} \\ a_2 x\equiv b_2 \pmod{m_2} \\ ... \\ a_r x\equiv b_r \pmod{m_r} \end{cases}$$

Tiene una única solución x módulo el entero $m_1\cdot m_2\cdot ...\cdot m_r$.

En efecto, puesto que $(a_k,m_k)=1$, existirán los inversos multiplicativos de a_k, y podemos reescribir el sistema como

$$\begin{cases} x\equiv a_1^{-1}b_1 \pmod{m_1} \\ x\equiv a_2^{-1}b_2 \pmod{m_2} \\ ... \\ x\equiv a_r^{-1}b_r \pmod{m_r} \end{cases}$$

Y aplicar el Teorema Chino del residuo en su versión del Teorema 6.3.1.

6.4 Sistemas de congruencias lineales con módulos no coprimos.

Se pueden resolver algunos sistemas de congruencias cuando sus módulos no son coprimos, pero no siempre, como veremos en el siguiente ejemplo.

6.4.1 Ejemplo.

Resolver el sistema de congruencias

$$\begin{cases} x \equiv 1 \,(\text{mod } 10) \\ x \equiv 4 \,(\text{mod } 12) \end{cases}$$

Solución.

$$\begin{cases} x \equiv 1 \,(\text{mod } 10) \Leftrightarrow x = 10a + 1 \\ x \equiv 4 \,(\text{mod } 12) \Leftrightarrow x = 12b + 4 \end{cases} \Rightarrow 10a + 1 = 12b + 4 \Leftrightarrow 10a = 12b + 3$$

Esta última igualdad nos lleva a contradicción, pues el valor de la derecha es impar y el valor de la izquierda es par. Así pues, el sistema no tiene solución.

Visualmente:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
X										X										X										X									
			X												X												X											X

6.4.2 Teorema. Teorema chino del residuo con módulos no coprimos y dos congruencias.

El sistema

$$\begin{cases} x \equiv a_1 \,(\text{mod } m_1) \\ x \equiv a_2 \,(\text{mod } m_2) \end{cases}$$

Tiene solución si y solo si $a_1 \equiv a_2 \bmod (m_1, m_2)$, en cuyo caso existe una única solución $\bmod [a_1, a_2]$.

Observamos que el Teorema chino del residuo sería un caso particular de este teorema cuando $(m_1, m_2) = 1$, pues entonces garantizamos que el sistema tenga solución, y $[a_1, a_2] = m_1 m_2$.

6.4.3 Ejemplo.

Resolver el sistema

$$\begin{cases} x \equiv 5 \pmod{12} \\ x \equiv 11 \pmod{18} \end{cases}$$

Solución.

Puesto que $(12,18) = 6$, y $6 \mid (11-5)$, existirá una única solución. La vamos a obtener con el método interactivo.

$$x \equiv 5 \pmod{12} \Rightarrow x = 12a + 5$$
$$x \equiv 11 \pmod{18} \Rightarrow 12a + 5 \equiv 11 \pmod{18} \Rightarrow 12a \equiv 11 - 5 \pmod{18} \Rightarrow 12a \equiv 6 \pmod{18}$$

Esta última congruencia se puede simplificar: 6 divide a 12 y a 6, y además $mcd(6,18) = 6$, luego podemos simplificarla:

$$12a \equiv 6 \pmod{18} \Rightarrow 2a \equiv 1 \pmod{3} \Rightarrow a = 2 \pmod{3} \Rightarrow a = 3k + 2$$
$$x = 12a + 5 = 12(3k + 2) + 5 = 36k + 29 \pmod{36}$$

Donde hemos tenido en cuenta que $[12,18] = 36$

Efectivamente, $29 = 12 \cdot 2 + 5$, y $29 = 18 \cdot 1 + 11$

Visualmente:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
				X												X												X											
										X																		X											

6.4.4 [M]

Diremos que un entero positivo n es *extra-distinct* si sus residuos cuando lo dividimos entre 2, 3, 4, 5 y 6 son distintos. Determina el número de enteros positivos *extra-distinct* menores que 1000.

AIME I 2023 #7

6.4.5 Teorema (versión general de 6.4.2)

Sean $m_1, m_2, ..., m_r$ enteros positivos. Entonces el sistema de congruencias lineales

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \ldots \\ x \equiv b_r \pmod{m_r} \end{cases}$$

Tiene solución si y solo si $b_i \equiv b_j \bmod(m_i, m_j)$ para todo $i \neq j$, en cuyo caso la solución será única $[m_1, m_2, ..., m_r]$.

6.5 Congruencias lineales mediante sistemas de congruencias lineales.

El Teorema chino del residuo se puede usar para convertir una congruencia lineal cuyo módulo es un número compuesto grande en un sistema de varias congruencias con módulos más pequeños, con los que resultará más sencillo operar.

Nos basaremos en el siguiente resultado:

$$a\,x \equiv b \pmod{n\,m} \Leftrightarrow \begin{cases} a\,x \equiv b \pmod{n} \\ a\,x \equiv b \pmod{m} \end{cases}$$

En efecto: $a\,x \equiv b \pmod{n\,m} \Rightarrow a\,x = k\,nm + b = (km)n + b \Rightarrow a\,x \equiv b \pmod{n}$

Existe un recíproco: $a\,x \equiv b \pmod{n}$ *y* $a\,x \equiv b \pmod{m} \Rightarrow a\,x \equiv b \pmod{[n,m]}$

6.5.1 Ejemplo.

Resolver la congruencia lineal $17x \equiv 9 \pmod{276}$.

Solución. Puesto que $276 = 4 \cdot 3 \cdot 23$, la ecuación anterior es equivalente a resolver el sistema de congruencias

$$\begin{cases} 17x \equiv 9 \pmod{3} \\ 17x \equiv 9 \pmod{4} \\ 17x \equiv 9 \pmod{23} \end{cases} \quad \text{o equivalentemente:} \quad \begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{4} \\ 17x \equiv 9 \pmod{23} \end{cases}$$

$x \equiv 0 \pmod{3}$ equivale a decir que $x = 3a$, luego sustituyendo en la segunda ecuación y multiplicando por 3 ambos lados:

$3a \equiv 1 \pmod{4} \Rightarrow 9a \equiv 3 \pmod{4} \Rightarrow a \equiv 3 \pmod{4} \Rightarrow a = 4b + 3 \Rightarrow x = 3a = 12b + 9$

Sustituyendo en la tercera ecuación:

$17x \equiv 9 \pmod{23} \Leftrightarrow 17(12b + 9) \equiv 9 \pmod{23} \Leftrightarrow 204b + 153 \equiv 9 \pmod{23}$

$\Rightarrow 204b \equiv -144 \pmod{23} \Rightarrow 20b \equiv 17 \pmod{23} \Rightarrow -3b \equiv -6 \pmod{23}$

$\Rightarrow 3b \equiv 6 \pmod{23} \Rightarrow b \equiv 2 \pmod{23} \Rightarrow b = 23k + 2$

$\Rightarrow x = 12(23k + 2) + 9 = 276k + 24 + 9 = 276k + 33 \Rightarrow x = 33 \pmod{276}$

Efectivamente, $17 \cdot 33 = 561 = 2 \cdot 276 + 9$.

6.6 Congruencias y sistemas de congruencias lineales con varias variables.

6.6.1 Ejemplo resuelto.

Determina todas las soluciones de $3x-7y\equiv 11 \pmod{13}$

Solución.

$3x-7y\equiv 11 \pmod{13} \Leftrightarrow 3x\equiv 7y+11 \pmod{13}$

En primer lugar, observamos que, fijado un $7y+11$, la congruencia tiene solución en x y es única, puesto que $(3,13)=1$ y $1\mid 7y+11$ para cualquier valor de y (ver Teorema 6.1.3).

Vamos a determinar las soluciones en función del valor de y:

$$y=0 \Rightarrow 3x\equiv 11 \pmod{13} \Leftrightarrow x\equiv 3^{-1}\cdot 11\equiv -4\cdot 11=-44\equiv -5\equiv 8 \pmod{13}$$

En donde hemos utilizado que $3^{-1}\equiv -4 \pmod{13}$, puesto que $13=3\cdot 4+1$.

$$y=1 \Rightarrow 3x\equiv 7\cdot 1+11=18 \pmod{13} \Leftrightarrow x\equiv 3^{-1}\cdot 18\equiv -4\cdot 18\equiv 6 \pmod{13}$$

Y de la misma manera vamos obteniendo el resto de soluciones posibles:

$y\equiv 2 \Rightarrow x\equiv 4 \pmod{13}$, $y\equiv 3 \Rightarrow x\equiv 2 \pmod{13}$

$y\equiv 4 \Rightarrow x\equiv 0 \pmod{13}$, $y\equiv 5 \Rightarrow x\equiv 11 \pmod{13}$

$y\equiv 6 \Rightarrow x\equiv 9 \pmod{13}$, $y\equiv 7 \Rightarrow x\equiv 7 \pmod{13}$

$y\equiv 8 \Rightarrow x\equiv 5 \pmod{13}$, $y\equiv 9 \Rightarrow x\equiv 3 \pmod{13}$

$y\equiv 10 \Rightarrow x\equiv 1 \pmod{13}$, $y\equiv 11 \Rightarrow x\equiv 12 \pmod{13}$

$y\equiv 12 \Rightarrow x\equiv 10 \pmod{13}$

6.6.2

Sea N el mayor entero de cuatro dígitos con la propiedad de que si cualquiera de sus dígitos se reemplaza por un 1, el resultado es divisible entre 7 . Sean Q y R el cociente y residuo, respectivamente, de N dividido entre 1000. Determina Q+R.

AIME II 2024#7

7 Congruencias con potencias.

7.1 Congruencias cuadráticas con módulos primos.

7.1.1 Definición. Congruencias cuadráticas módulo n.

Una congruencia cuadrática es una congruencia de la forma

$$x^2 \equiv a \pmod{n}$$

donde $(a, n) = 1$. Si la congruencia tiene solución, diremos que a es un residuo cuadrático módulo n.

En general, llamaremos congruencia cuadrática a la congruencia

$$Ax^2 + Bx + C \equiv 0 \pmod{n}\text{, con } (A, n) = 1$$

Este primer apartado lo dedicaremos a estudiar las congruencias cuadráticas cuando el módulo es un número primo. El método general para resolver estas congruencias es completar cuadrados, tal y como veremos en los siguientes ejemplos resueltos.

7.1.2 Ejemplo resuelto.

Resuelve la congruencia cuadrática $x^2 + 6x + 5 \equiv 0 \pmod{17}$

En primer lugar completamos el cuadrado, y necesitamos sumar $3^2 = 9$.

$$x^2 + 6x + 5 \equiv 0 \pmod{17} \Leftrightarrow$$
$$x^2 + 2 \cdot 3x + 3^2 + 5 \equiv 3^2 \pmod{17} \Leftrightarrow$$
$$(x+3)^2 + 5 \equiv 9 \pmod{17} \Leftrightarrow$$
$$(x+3)^2 \equiv 4 \pmod{17}$$

Tenemos que resolver la congruencia $u^2 \equiv 4 \pmod{17}$, por tanteo:

$$u^2 \equiv 4 \pmod{17} \Leftrightarrow \begin{cases} u \equiv 2 \pmod{17} & (a) \\ u \equiv -2 \equiv 15 \pmod{17} & (b) \end{cases}$$

(a) $x + 3 \equiv 2 \pmod{17} \Leftrightarrow x \equiv 2 - 3 \equiv -1 \equiv 16 \pmod{17}$

(b) $x + 3 \equiv -2 \pmod{17} \Leftrightarrow x \equiv -2 - 3 \equiv -5 \equiv 12 \pmod{17}$

7.1.3 Ejemplo resuelto.

Resuelve la congruencia cuadrática $x^2+3x+11\equiv 0\pmod{13}$

Completamos cuadrados:

$x^2+3x+11\equiv 0\pmod{13}\Leftrightarrow$

$4x^2+12x+44\equiv 0\pmod{13}\Leftrightarrow$

$(2x)^2+2\cdot 6x+44\equiv 0\pmod{13}\Leftrightarrow$

$(2x)^2+2\cdot 3\cdot 2x+3^2+44\equiv 3^2\pmod{13}\Leftrightarrow$

$(2x+3)^2+44\equiv 3^2\pmod{13}\Leftrightarrow$

$$(2x+3)^2\equiv -35\equiv 4\pmod{13}\Leftrightarrow\begin{cases}2x+3\equiv 2\pmod{13} & (a)\\ 2x+3\equiv -2\pmod{13} & (b)\end{cases}$$

(a) $2x+3\equiv 2\pmod{13}\Leftrightarrow 2x\equiv -1\pmod{13}\Leftrightarrow x\equiv 6\pmod{13}$

(b) $2x+3\equiv -2\pmod{13}\Leftrightarrow 2x\equiv -5\pmod{13}\Leftrightarrow x\equiv 4\pmod{13}$

7.1.4 Ejemplo resuelto.

Resuelve la congruencia cuadrática $2x^2+7x+4\equiv 0\pmod{19}$

Utilizando que $7\equiv -12\pmod{19}$:

$2x^2+7x+4\equiv 0\pmod{19}\Leftrightarrow$

$2x^2-12x+4\equiv 0\pmod{19}\Leftrightarrow$

$4x^2-24x+8\equiv 0\pmod{19}\Leftrightarrow$

$(2x)^2-2\cdot 2x\cdot 6+6^2-6^2+8\equiv 0\pmod{19}\Leftrightarrow$

$(2x-6)^2-6^2+8\equiv 0\pmod{19}\Leftrightarrow$

$(2x-6)^2-6^2+8\equiv 0\pmod{19}\Leftrightarrow$

$(2x-6)^2-28\equiv 0\pmod{19}\Leftrightarrow$

$$(2x-6)^2\equiv 28\equiv 9\pmod{19}\Leftrightarrow\begin{cases}2x-6\equiv 3\pmod{19} & (a)\\ 2x-6\equiv -3\pmod{19} & (b)\end{cases}$$

(a) $2x-6\equiv 3\pmod{19}\Leftrightarrow 2x\equiv 9\pmod{19}\Leftrightarrow x\equiv 14\pmod{19}$

(b) $2x-6\equiv -3\pmod{19}\Leftrightarrow 2x\equiv 3\pmod{19}\Leftrightarrow x\equiv 11\pmod{19}$

7.1.5 Ejercicio resuelto.

Resolver la congruencia

$$x^2+3x-5\equiv 0\pmod 7$$

Solución.

Siguiendo los pasos anteriores llegamos a la congruencia equivalente

$$(2x+3)^2\equiv 1\pmod 7$$

Y vemos que 1 es un residuo cuadrático módulo 7. En efecto: $1^2\equiv 1\pmod 7$ y $6^2\equiv 36\equiv 1\pmod 7$. Luego nuestro problema se reduce a resolver las siguientes congruencias lineales:

$$2x+3\equiv 1\pmod 7 \text{ y } 2x+3\equiv 6\pmod 7$$

$$2x+3\equiv 1\pmod 7\Leftrightarrow 2x\equiv -2\pmod 7\Leftrightarrow x\equiv -1\equiv 6\pmod 7$$
$$2x+3\equiv 6\pmod 7\Leftrightarrow 2x\equiv 3\pmod 7\Leftrightarrow x\equiv 2^{-1}\cdot 3\pmod 7\Leftrightarrow$$
$$x\equiv 4\cdot 3\pmod 7\Leftrightarrow x\equiv 12\pmod 7\Leftrightarrow x\equiv 5\pmod 7$$

En donde hemos utilizado que $2\cdot 4=8\equiv 1\pmod 7\Rightarrow 2^{-1}=4\pmod 7$

Fuente: "Michael Penn Math" https://youtu.be/oPZbKUwBh4s

7.1.6 Ejercicio resuelto.

Resuelve $5x^2-6x+2\equiv 0\pmod{13}$

Solución.

Siguiendo la transformación anterior, esta congruencia es equivalente a

$(10x-6)^2\equiv 9\pmod{13}\Leftrightarrow y^2\equiv 9\pmod{13}$, tomando $y=10x-6$.

Vemos que 9 es un residuo cuadrático módulo 13, en efecto:

$$y^2\equiv 9\pmod{13}\Leftrightarrow \begin{cases} y\equiv 3\pmod{13}\\ y\equiv 13-3=10\pmod{13}\end{cases}$$

Ahora deshacemos el cambio de variable:

a) $y\equiv 3\pmod{13}\Leftrightarrow 10x-6\equiv 3\pmod{13}\Leftrightarrow 10x\equiv 9\pmod{13}\Leftrightarrow (1)$

Calculamos el inverso multiplicativo de 10 módulo 13 mediante el ADE (ver Apartado 7.3):

$$\left.\begin{aligned}13=10\cdot 1+3\rightarrow 3=13-10\\ 10=3\cdot 3+1\rightarrow 1=10-3\cdot 3\end{aligned}\right\}\Rightarrow 1=10-3\cdot 3=10-3(13-10)=$$
$$=10-3\cdot 13+3\cdot 10=4\cdot 10-3\cdot 13\Rightarrow 10^{-1}=4\pmod{13}$$

Y por tanto:

$(1)\Leftrightarrow x\equiv 4\cdot 9=36\equiv 10\pmod{13}$

b)

$$y\equiv 10\pmod{13}\Leftrightarrow 10x-6\equiv 10\pmod{13}\Leftrightarrow 10x=16\equiv 3\pmod{13}\Leftrightarrow$$
$$\Leftrightarrow x=4\cdot 3=12\pmod{13}$$

Así pues, las soluciones son $x\equiv 10,12\pmod{13}$

7.1.7 [D] Problema solucionado paso a paso en vídeo

Sea un número primo positivo dado. Demostrar que existe un entero α tal que $\alpha(\alpha-1)+3$ es divisible por p si y sólo si existe un entero β tal que $\beta(\beta-1)+25$ es divisible por p.

OME 2016 #2

Solución: https://youtu.be/5adoPGcR2hk

7.2 Congruencias cuadráticas con módulos compuestos.

7.2.1 Ejemplo resuelto.

Resuelve la congruencia $x^2 \equiv 26 \pmod{55}$

Solución.
Observamos que $55 = 5 \cdot 11$.
Resolvemos las congruencias $x^2 \equiv 26 \pmod{5}$ y $x^2 \equiv 26 \pmod{11}$ por tanteo:

$$x^2 \equiv 26 \pmod{5} \Leftrightarrow x^2 \equiv 1 \pmod{5} \Leftrightarrow \begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 4 \pmod{5} \end{cases}$$

$$x^2 \equiv 26 \pmod{11} \Leftrightarrow x^2 \equiv 4 \pmod{11} \Leftrightarrow \begin{cases} x \equiv 2 \pmod{11} \\ x \equiv 9 \pmod{11} \end{cases}$$

Así pues, tomando todas las parejas de soluciones posibles, tenemos cuatro sistemas de congruencias lineales, que resolveremos directamente, sin usar el TCR:

a)

$$\left.\begin{cases} x \equiv 1 \pmod{5} \Rightarrow x = 5a + 1 \\ x \equiv 2 \pmod{11} \Rightarrow x = 11b + 2 \end{cases}\right\} \Rightarrow 11b + 2 = 5a + 1 \Rightarrow 11b + 1 = 5a \Rightarrow 5a \equiv 1 \pmod{11}$$

$$5a \equiv 1 \pmod{11} \Rightarrow a \equiv 9 \pmod{11} \Rightarrow a = 11c + 9 \Rightarrow$$

$$x = 5a + 1 = 5(11c + 9) + 1 = 55c + 45 + 1 = 55c + 46 \Rightarrow x \equiv 46 \pmod{55}$$

b)

$$\left.\begin{cases} x \equiv 1 \pmod{5} \Rightarrow x = 5a + 1 \\ x \equiv 9 \pmod{11} \Rightarrow x = 11b + 9 \end{cases}\right\} \Rightarrow 11b + 9 = 5a + 1 \Rightarrow 11b + 8 = 5a \Rightarrow 5a \equiv 8 \pmod{11}$$

$$5a \equiv 8 \pmod{11} \Rightarrow a \equiv 6 \pmod{11} \Rightarrow a = 11c + 6 \Rightarrow$$

$$x = 5a + 1 = 5(11c + 6) + 1 = 55c + 30 + 1 = 55c + 31 \Rightarrow x \equiv 31 \pmod{55}$$

c)

$$\left.\begin{cases} x \equiv 4 \pmod{5} \Rightarrow x = 5a + 4 \\ x \equiv 2 \pmod{11} \Rightarrow x = 11b + 2 \end{cases}\right\} \Rightarrow 11b + 2 = 5a + 4 \Rightarrow 11b - 2 = 5a \Rightarrow 5a \equiv -2 \pmod{11}$$

$$5a \equiv -2 \equiv 9 \pmod{11} \Rightarrow a \equiv 4 \pmod{11} \Rightarrow a = 11c + 4 \Rightarrow$$

$$x = 5a + 4 = 5(11c + 4) + 4 = 55c + 20 + 4 = 55c + 24 \Rightarrow x \equiv 24 \pmod{55}$$

d)

$$\left.\begin{cases} x \equiv 4 \pmod{5} \Rightarrow x = 5a + 4 \\ x \equiv 9 \pmod{11} \Rightarrow x = 11b + 9 \end{cases}\right\} \Rightarrow 11b + 9 = 5a + 4 \Rightarrow 11b + 5 = 5a \Rightarrow 5a \equiv 5 \pmod{11}$$

$$5a \equiv 5 \pmod{11} \Rightarrow a \equiv 1 \pmod{11} \Rightarrow a = 11c + 1 \Rightarrow$$

$$x = 5a + 4 = 5(11c + 1) + 4 = 55c + 5 + 4 = 55c + 9 \Rightarrow x \equiv 9 \pmod{55}$$

Así pues, esta congruencia tiene cuatro soluciones: $x \equiv 9, 24, 31, 46 \pmod{55}$

7.2.2 Ejemplo resuelto.

Resuelve la congruencia $x^2 \equiv 1 \pmod{144}$

Solución.

Puesto que $144 = 16 \cdot 9$, y $(16,9) = 1$, podemos descomponer la ecuación anterior en el sistema no lineal

$$\begin{cases} x^2 = 1 \pmod{16} \\ x^2 = 1 \pmod{9} \end{cases}$$

$x^2 = 1 \pmod{16}$ tiene 4 soluciones: $x \equiv \pm 1$ o $\pm 7 \pmod{16}$

$x^2 = 1 \pmod{9}$ tiene 2 soluciones: $x \equiv \pm 1 \pmod{9}$

Luego tenemos ocho alternativas:

i) $x \equiv 1 \pmod{16}$ y $x \equiv 1 \pmod{9}$

ii) $x \equiv 1 \pmod{16}$ y $x \equiv -1 \pmod{9}$

iii) $x \equiv -1 \pmod{16}$ y $x \equiv 1 \pmod{9}$

iv) $x \equiv -1 \pmod{16}$ y $x \equiv -1 \pmod{9}$

v) $x \equiv 7 \pmod{16}$ y $x \equiv 1 \pmod{9}$

vi) $x \equiv 7 \pmod{16}$ y $x \equiv -1 \pmod{9}$

vii) $x \equiv -7 \pmod{16}$ y $x \equiv 1 \pmod{9}$

viii) $x \equiv -7 \pmod{16}$ y $x \equiv -1 \pmod{9}$

Podemos ir resolviendo cada caso mediante el TCR.

Independientemente del caso, $(16,9) = 1$, luego todos los ocho sistemas tienen solución.

Además: $N_1 = 9$, $N_2 = 16$, $9y_1 = 1 \pmod{16} \Rightarrow y_1 = 9$, $16y_2 = 1 \pmod{9} \Rightarrow y_2 = 4$

i) $x = 9 \cdot 9 \cdot 1 + 16 \cdot 4 \cdot 1 = 145 \pmod{144} = 1 \pmod{144}$

ii) $x = 9 \cdot 9 \cdot 1 + 16 \cdot 4 \cdot (-1) = 17 \pmod{144}$

iii) $x = 9 \cdot 9 \cdot (-1) + 16 \cdot 4 \cdot 1 = -17 \pmod{144}$

iv) $x = 9 \cdot 9 \cdot (-1) + 16 \cdot 4 \cdot (-1) = -145 \pmod{144} = -1 \pmod{144}$

v) $x = 9 \cdot 9 \cdot 7 + 16 \cdot 4 \cdot 1 = 631 \pmod{144} = 55 \pmod{144}$

vi) $x = 9 \cdot 9 \cdot 7 + 16 \cdot 4 \cdot (-1) = 503 \pmod{144} = 71 \pmod{144}$

vii) $x = 9 \cdot 9 \cdot (-7) + 16 \cdot 4 \cdot 1 = -503 \pmod{144} = 73 \pmod{144} = -71 \pmod{144}$

viii) $x = 9 \cdot 9 \cdot (-7) + 16 \cdot 4 \cdot (-1) = -631 \pmod{144} = -55 \pmod{144}$

7.2.3 [F]

Calcula los tres últimos dígitos de $2005^{11} + 2005^{12} + ... + 2005^{2006}$

Senior Hanoi Open MO 2006

7.2.4 [F]

Demostrar que si x es un número impar no divisible entre tres, entonces $x^2 \equiv 1 \bmod 24$.

7.2.5 Ejemplo resuelto.

Resuelva la congruencia $x^2 \equiv 4 \pmod{77}$

Solución:

$$x^2 \equiv 4 \pmod{77} \Leftrightarrow \begin{cases} x^2 \equiv 4 \pmod{7} \Leftrightarrow x \equiv \pm 2 \pmod{7} \\ x^2 \equiv 4 \pmod{11} \Leftrightarrow x \equiv \pm 2 \pmod{11} \end{cases}$$

Luego tenemos cuatro casos:

a) $x \equiv 2 \pmod{7}$, $x \equiv 2 \pmod{11}$
b) $x \equiv -2 \pmod{7}$, $x \equiv 2 \pmod{11}$
c) $x \equiv 2 \pmod{7}$, $x \equiv -2 \pmod{11}$
d) $x \equiv -2 \pmod{7}$, $x \equiv -2 \pmod{11}$

Vamos a resolver estos casos mediante el TCR:

a)

$N = 77$

$N_1 = 11 \to 11y_1 \equiv 1 \pmod{7} \Rightarrow y_1 = 2$

$N_2 = 7 \to 7y_2 \equiv 1 \pmod{11} \Rightarrow y_2 = 8$

$x = 11 \cdot 2 \cdot 2 + 7 \cdot 8 \cdot 2 = 156 = 77 \cdot 2 + 2 \equiv 2 \pmod{77}$

Y por tanto la primera solución es $x = 2 \pmod{77}$

Para ahorrarnos trabajo, podemos deducir el resto de los casos directamente de la última igualdad:

b) $x = 11 \cdot 2 \cdot (-2) + 7 \cdot 8 \cdot 2 = 68 \pmod{77}$
c) $x = 11 \cdot 2 \cdot 2 + 7 \cdot 8 \cdot (-2) = -68 \equiv -68 + 77 = 9 \pmod{77}$
d) $x = 11 \cdot 2 \cdot (-2) + 7 \cdot 8 \cdot (-2) = -156 \equiv -156 + 77 \cdot 3 = 75 \pmod{77}$

Así pues, las soluciones son $x = 2, 9, 68, 75 \pmod{77}$

Fuente: "PROFMAT MA14 12.2" en Youtube.

7.2.6 Ejemplo resuelto.

Resuelve la congruencia $x^2 + x + 1 \equiv 0 \pmod{49}$

Solución.

Puesto que $49 = 7^2$, en primer lugar resolveremos la congruencia $x^2 + x + 1 \equiv 0 \pmod{7}$.

$$x^2 + x + 1 \equiv 0 \pmod{7} \Leftrightarrow$$
$$x^2 + x - 6 \equiv 0 \pmod{7} \Leftrightarrow$$
$$(x+3)(x-2) \equiv 0 \pmod{7} \Leftrightarrow \begin{cases} x+3 \equiv 0 \pmod{7} \Leftrightarrow x \equiv -3 \equiv 4 \pmod{7} & (a) \\ x-2 \equiv 0 \pmod{7} \Leftrightarrow x \equiv 2 \pmod{7} & (b) \end{cases}$$

(b) $x \equiv 2 \pmod{7} \Leftrightarrow x = 7k + 2$. Ahora substituimos en la congruencia inicial:

$$x^2 + x + 1 \equiv 0 \pmod{49} \Leftrightarrow$$
$$(7k+2)^2 + 7k + 2 + 1 \equiv 0 \pmod{49} \Leftrightarrow$$
$$49k^2 + 35k + 7 \equiv 0 \pmod{49} \Leftrightarrow$$
$$35k + 7 \equiv 0 \pmod{49}$$

En donde hemos aplicado que $49 \equiv 0 \pmod{49}$.

$$35k + 7 \equiv 0 \pmod{49} \Leftrightarrow$$
$$7(5k+1) \equiv 0 \pmod{49} \Leftrightarrow$$
$$5k + 1 \equiv 0 \pmod{7} \Leftrightarrow$$
$$5k \equiv -1 \equiv 6 \pmod{7} \Leftrightarrow$$
$$k \equiv 4 \pmod{7} \Leftrightarrow k = 7u + 4$$

Luego $x = 7k + 2 = 7(7u+4) + 2 = 49u + 28 + 2 = 49u + 30 \Leftrightarrow x \equiv 30 \pmod{49}$.

(a) $x \equiv 4 \pmod{7} \Leftrightarrow x = 7k + 4$. Ahora substituimos en la congruencia inicial:

$$x^2 + x + 1 \equiv 0 \pmod{49} \Leftrightarrow$$
$$(7k+4)^2 + 7k + 4 + 1 \equiv 0 \pmod{49} \Leftrightarrow$$
$$49k^2 + 63k + 21 \equiv 0 \pmod{49} \Leftrightarrow$$
$$14k + 21 \equiv 0 \pmod{49}$$

En donde hemos aplicado que $49 \equiv 0 \pmod{49}$ y $63 \equiv 14 \pmod{49}$.

$$14k + 21 \equiv 0 \pmod{49} \Leftrightarrow$$
$$7(2k+3) \equiv 0 \pmod{49} \Leftrightarrow$$
$$2k + 3 \equiv 0 \pmod{7} \Leftrightarrow$$
$$2k \equiv -3 \equiv 4 \pmod{7} \Leftrightarrow$$
$$k \equiv 2 \pmod{7} \Leftrightarrow k = 7v + 2$$

Luego $x = 7k + 4 = 7(7v+2) + 4 = 49v + 18 \Leftrightarrow x \equiv 18 \pmod{49}$.

Así pues, hay dos soluciones para la congruencia del enunciado: $x \equiv 18, 30 \pmod{49}$.

7.2.7 [F]

Determina el menor entero positivo m tal que $m^2+7m+89$ sea un múltiplo de 77.

Mandelbrot 2009

7.3 Congruencias con potencias y polinomios.

Proposición. Congruencias con potencias.

Las propiedades estudiadas en el Tema 4 tienen unas aplicaciones muy importantes en el estudio de las congruencias:

Dados dos enteros positivos d, k, con $d \mid k$, entonces:

a) $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$

b) $a^d \equiv b^d \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$

c) $a^d \equiv -b^d \pmod{n}$ y k/d es impar, $\Rightarrow a^k \equiv -b^k \pmod{n}$

Demostración. a) Basta aplicar $a-b \mid a^k - b^k$ para todo k.

b) Basta aplicar $d \mid k \Rightarrow a^d - b^d \mid a^k - b^k$.

c) $a^d \equiv -b^d \pmod{n} \Leftrightarrow a^d + b^d \equiv 0 \pmod{n} \Leftrightarrow n \mid a^d + b^d$ (*)

Pero si k/d es impar tenemos $a^d + b^d \mid a^k + b^k$, luego

$(*) \Rightarrow n \mid a^k + b^k \Leftrightarrow a^k + b^k \equiv 0 \pmod{n} \Leftrightarrow a^k \equiv -b^k \pmod{n}$

Problema resuelto.

Aprovechando que $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$, demostrar que $641 \mid 2^{32} + 1$.

$641 = 2^4 + 5^4 \Rightarrow 2^4 + 5^4 \equiv 0 \pmod{641} \Rightarrow 5^4 \equiv -2^4 \pmod{641}$

$\Rightarrow 5^4 2^{28} \equiv -2^4 2^{28} \pmod{641} \Rightarrow 5^4 2^{28} \equiv -2^{32} \pmod{641}$

$\Rightarrow \left(5 \cdot 2^7\right)^4 \equiv -2^{32} \pmod{641} \Rightarrow (641-1)^4 \equiv -2^{32} \pmod{641}$

$\Rightarrow (-1)^4 \equiv -2^{32} \pmod{641} \Rightarrow 1 \equiv -2^{32} \pmod{641} \Rightarrow 2^{32} + 1 \equiv 0 \pmod{641}$

$\Rightarrow 641 \mid 2^{32} + 1$

Teorema.

Dado un polinomio con coeficientes enteros $p(x) = c_m x^m + c_{m-1} x + \ldots + c_1 x + c_0$, entonces:

$$a \equiv b \pmod{n} \Rightarrow p(a) \equiv p(b) \pmod{n}$$

Demostración. $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n} \Rightarrow c_k a^k \equiv c_k b^k \pmod{n} \Rightarrow$

$$p(a) = \sum_{k=0}^{m} c_k a^k \equiv p(b) = \sum_{k=0}^{m} c_k b^k \pmod{n}$$

7.3.1 [F]

Dado cualquier número positivo n, y sea S la suma de sus cifras, demuestra:

a) $n - S$ es divisible entre 9.

b) n es divisible entre 9 si y solo si S es divisible entre 9.

En este problema justificamos el "**criterio de divisibilidad del nueve**": Un número es divisible entre nueve si y solo si las suma de sus cifras es divisible entre 9.

7.3.2 [F]

Demuestra el "criterio de divisibilidad del once": Un número es divisible entre 11 si y solo si la suma alternada de sus cifras es múltiplo de 11.

Proposición.

Dado un polinomio con coeficientes enteros $p(x) = c_m x^m + c_{m-1}x + \ldots + c_1 x + c_0$, diremos que a es una solución de la congruencia $p(x) \equiv 0 \pmod{n}$ si $p(a) \equiv 0 \pmod{n}$.
Si a es una solución de la congruencia $p(x) \equiv 0 \pmod{n}$ y $b \equiv a \pmod{n}$ entonces b también es una solución de la congruencia $p(x) \equiv 0 \pmod{n}$.

Demostración. $a \equiv b \pmod{n} \Rightarrow 0 \equiv p(a) \equiv p(b) \pmod{n} \Rightarrow 0 \equiv p(b) \pmod{n}$

7.4 El Teorema de Wilson.

7.4.1 Lema.

Si p es un número primo, $x^2 \equiv 1 \pmod{p} \Leftrightarrow x \equiv \pm 1 \pmod{p}$.

Demostración. $x \equiv \pm 1 \pmod{p} \Rightarrow x^2 \equiv 1 \pmod{p}$ por las propiedades básicas de la aritmética modular.
Veamos el recíproco. Supongamos que $x^2 \equiv 1 \pmod{p} \Leftrightarrow p \mid x^2 - 1 = (x-1)(x+1)$.
Luego, por ser p un número primo, se cumple $p \mid x-1 \Rightarrow x \equiv 1 \pmod{p}$ o se cumple $p \mid x+1 \Rightarrow x \equiv -1 \pmod{p}$, tal y como queríamos ver.

7.4.2 Teorema. Teorema de Wilson.

Si p es un número primo, $(p-1)! \equiv -1 \pmod{p}$

Demostración. Los casos $p = 2$ y $p = 3$ se pueden demostrar directamente.
Supongamos que $p > 2$.
Vemos que todo número $a \in \{2, 3, 4, \ldots, p-2\}$ tiene inverso $a^{-1} \pmod{p}$, y que se cumple $a \not\equiv a^{-1} \pmod{p}$, porque en ese caso tendríamos, aplicando el lema anterior,

$$a^2 \equiv a \cdot a^{-1} \equiv 1 \pmod{p} \Rightarrow a \equiv \pm 1 \pmod{p}$$

llegando a contradicción.
Así pues, podemos agrupar los elementos de $\{2, 3, 4, \ldots, p-2\}$ por parejas, siendo el producto de cada pareja congruente con 1, en lenguaje modular:

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \pmod{p}$$

Luego, finalmente, $(p-1)! = 1 \cdot 2 \cdot 3 \ldots \cdot (p-2)(p-1) = 1 \cdot 1 \cdot (p-1) \equiv p-1 \equiv -1 \pmod{p}$
tal y como queríamos ver.

Observación: El recíproco también es cierto: Si $(n-1)! \equiv -1 \pmod{n}$, entonces n es primo, lo que da un nuevo método para determinar si un número es primo o no, aunque no es nada práctico, pues $(n-1)!$ es enorme.

7.4.3 [F]

Determina el residuo al dividir 14! entre 17.

7.4.4 [F]

Determina el residuo al dividir 2016!–2015! entre 2017.

7.4.5 [F]

Sea a un entero tal que $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{23} = \frac{a}{23!}$

Determina el residuo que obtenemos al dividir a entre 13.

7.4.6 [D]

Dado un primo impar p, demuestra que

$$1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

7.4.7 [M] **Problema solucionado paso a paso en vídeo**

Diremos que un entero $x \in \{1,\ldots,102\}$ es *square-ish* si existe un entero n tal que $x \equiv n^2 + n \pmod{103}$. Calcula el producto de todos los enteros *square-ish* módulo 103.

SMT 2023 Discrete #6

Solución: https://youtu.be/cKKtd6vbT8E

7.5 Residuos cuadráticos. Ley de reciprocidad.

Definición. Residuo cuadrático modular.

Sea p un número primo. Diremos que un entero a no divisible entre p es un residuo cuadrático módulo p cuando sea un cuadrado perfecto módulo p.

Por ejemplo, en $\mathbb{Z}_5$: $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 4$, $4^2 \equiv 1$.

Luego 1 y 4 son residuos cuadráticos en $\mathbb{Z}_5$, mientras que 2 y 3 no lo son.

Residuos cuadráticos y representación simétrica.

Si en vez de utilizar la representación estándar:

$$\mathbb{Z}_p = \{ 0, 1, 2, \dots , p-2, p-1 \}$$

utilizamos la llamada representación simétrica

$$\mathbb{Z}_p = \{ -(p-1)/2, \dots,-2, -1, 0, 1, 2, \dots , (p-1)/2 \}$$

entonces veremos más claro como son los residuos cuadráticos. Por ejemplo, en $\mathbb{Z}_7$:

n	-3	-2	-1	0	1	2	3
n^2	2	-3	1	0	1	-3	2

Hay tres residuos cuadráticos: 1, 2 y -3.

Listado de los residuos cuadráticos asociados a los primeros números primos:

3→ 1
5 → 1,-1
7 → 1,2,-3
11 → 1,3,4,5,-2
13 → 1,3,4,-4,-3,-1
17 → 1,2,4,8,-8,-4,-2,-1
19 → 1,4,5,6,7,9,-8,-3,-2
23 → 1,2,3,4,6,8,9,-11,-10,-7,-5
29 → 1,4,5,6,7,9,13,-13,-9,-7,-6,-5,-4,-1
31 → 1,2,4,5,7,8,9,10,14,-15,-13,-12,-11,-6,-3
37 → 1,3,4,7,9,10,11,12,16,-16,-12,-11,-10,-9,-7,-4,-3,-1
41 → 1,2,4,5,8,9,10,16,18,20,-20,-18,-16,-10,-9,-8,-5,-4,-2,-1
43 → 1,4,6,9,10,11,13,14,15,16,17,21,-20,-19,-18,-12,-8,-7,-5,-3,-2
47 → 1,2,3,4,6,7,8,9,12,14,16,17,18,21,-23,-22,-20,-19,-15,-13,-11,-10,-5
53 → 1,4,6,7,9,10,11,13,15,16,17,24,25,-25,-24,-17,-16,-15,-13,-11,-10,-9,-7,-6,-4,-1
59 → 1,3,4,5,7,9,12,15,16,17,19,20,21,22,25,26,27,28,29,-24,-23,-18,-14,-13,-11,-10,-8,-6,-2
61 → 1,3,4,5,9,12,13,14,15,16,19,20,22,25,27,-27,-25,-22,-20,-19,-16,-15,-14,-13,-12,-9,-5,-4,-3,-1
67 → 1,4,6,9,10,14,15,16,17,19,21,22,23,24,25,26,29,33,-32,-31,-30,-28,-27,-20,-18,-13,-12,-11,-8,-7,-5,-3,-2
71 → 1,2,3,4,5,6,8,9,10,12,15,16,18,19,20,24,25,27,29,30,32,-35,-34,-33,-31,-28,-26,-23,-22,-21,-17,-14,-13,-11,-7
73 → 1,2,3,4,6,8,9,12,16,18,19,23,24,25,27,32,35,36,-36,-35,-32,-27,-25,-24,-23,-19,-18,-16,-12,-9,-8,-6,-4,-3,-2,-1
79 → 1,2,4,5,8,9,10,11,13,16,18,19,20,21,22,23,25,26,31,32,36,38,-39,-37,-35,-34,-33,-30,-29,-28,-27,-24,-17,-15,-14,-12,-7,-6,-3
83 → 1,3,4,7,9,10,11,12,16,17,21,23,25,26,27,28,29,30,31,33,36,37,38,40,41,-39,-35,-34,-32,-24,-22,-20,-19,-18,-15,-14,-13,-8,-6, -5,-2
89 → 1,2,4,5,8,9,10,11,16,17,18,20,21,22,25,32,34,36,39,40,42,44,-44,-42,-40,-39,-36,-34,-32,-25,-22,-21,-20,-18,-17,-16,-11,-10, -9,-8,-5,-4,-2,-1

Teorema.

Si p es un número primo impar (es decir, excluímos $p=2$), en $\mathbb{Z}_p$ se cumple:

a) n es el cuadrado de a si y solo si es el cuadrado de $-a$.

b) En hay exactamente $\frac{p-1}{2}$ residuos cuadráticos y $\frac{p-1}{2}$ valores que no lo son.

Demostración.

a)

$$\left.\begin{array}{l} x^2 \equiv a \pmod{p} \\ y^2 \equiv a \pmod{p} \end{array}\right\} \Rightarrow p \mid x^2 - y^2 = (x-y)(x+y) \Rightarrow \begin{cases} p \mid x-y \Rightarrow x \equiv y \pmod{p} \\ o \\ p \mid x+y \Rightarrow x \equiv -y \pmod{p} \end{cases}$$

Definición. Símbolo de Legendre.

Sea p un número primo impar y sea a un entero. Definimos

$$\left(\frac{a}{q}\right) = \begin{cases} 0 & \text{si } (a,p) > 1 \\ +1 & \text{si a es un residuo cuadrático módulo p} \\ -1 & \text{si a no es un residuo cuadrático módulo p} \end{cases}$$

Siguiendo el ejemplo anterior,

$$\left(\frac{1}{5}\right)=1,\ \left(\frac{2}{5}\right)=-1,\ \left(\frac{3}{5}\right)=-1,\ \left(\frac{4}{5}\right)=1,\ \left(\frac{5}{5}\right)=0$$

Ley de reciprocidad cuadrática de Gauss.

Sean p y q dos números primos impares. Se cumple

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

La ley de reciprocidad cuadrática establece una sorprendente relación entre $\left(\frac{p}{q}\right)$ y $\left(\frac{q}{p}\right)$. Esta ley fue conjeturada, basándose en evidencia numérica, por Euler en 1783 y Lagrange en 1785. Legendre le dio la forma actual a esta ley, pero no pudo dar una prueba completa. La primera prueba rigurosa fue dada por Gauss en a la edad de 18 años. Hasta el 2004 se conocían 190 pruebas diferentes. Gauss llamó a este teorema "Aureum Theorema". Su importancia en la teoría de números no tienen discusión. Al respecto, Hecke afirmó al respecto: "La teoría de números moderna comenzó con el descubrimiento de la Ley de Reciprocidad Cuadrática".

Ejemplo 1.

Queremos determinar cuando 5 es un cuadrado perfecto en $\mathbb{Z}_p$. Observemos la siguiente tabla:

p	$\left(\frac{5}{p}\right)$	$p \bmod 5$
7	-1	2

11	1	1
13	-1	3
17	-1	2
19	1	4
23	-1	3
29	1	4
31	1	1
37	-1	2
41	1	1
43	-1	3
47	-1	2

Observamos que, para determinar si 5 es o no un cuadrado perfecto en $\mathbb{Z}_p$ basta comprobar si $p \bmod 5$ es 1 o 4, es decir, cuando $p \bmod 5$ sea un cuadrado perfecto.

Ejemplo 2.

Determina si 69 es o no un cuadrado perfecto módulo 389.

Aplicando la Ley de reciprocidad cuadrática de Gauss, y teniendo en cuenta que es una función multiplicativa:

$$\left(\frac{69}{389}\right)=\left(\frac{3\cdot 23}{389}\right)=\left(\frac{3}{389}\right)\cdot\left(\frac{23}{389}\right)$$

Por un lado,

$$\left(\frac{3}{389}\right)=(-1)^{(3-1)/2\cdot(389-1)/2}\left(\frac{389}{3}\right)=1\cdot(-1)=-1$$

en donde hemos aplicado:

$$(-1)^{(3-1)/2\cdot(389-1)/2}=(-1)^{388/2}=(-1)^{388/2}=(-1)^{194}=1$$

$389\equiv 2\pmod 3$ no es ningún cuadrado perfecto.

y por otro lado,

$$\left(\frac{23}{389}\right)=(-1)^{(23-1)/2\cdot(389-1)/2}\left(\frac{389}{23}\right)=$$

en donde hemos aplicado:

$$(-1)^{(23-1)/2\cdot(389-1)/2}=(-1)^{11\cdot 194}=-1$$

$389\equiv 21\pmod{23}$ no es ningún cuadrado perfecto.

luego

$$\left(\frac{69}{389}\right)=\left(\frac{3\cdot 23}{389}\right)=\left(\frac{3}{389}\right)\cdot\left(\frac{23}{389}\right)=(-1)(-1)=1$$

y por tanto sí es un cuadrado perfecto.

Observación.

Para saber si $21\pmod{23}$ es o no un cuadrado perfecto se podría haber aplicado de nuevo la Ley de reciprocidad cuadrática de Gauss:

$$\left(\frac{21}{23}\right)=\left(\frac{-2}{389}\right)=\left(\frac{-1}{23}\right)\cdot\left(\frac{2}{23}\right)=(-1)\cdot 1=-1$$

en donde hemos utilizado:

$$\left(\frac{-1}{23}\right)=-1$$

$$\left(\frac{2}{23}\right)=1 \text{ porque } 5^2=25\equiv 2\pmod{23}$$

Criterio de Euler.

$$\left(\frac{a}{p}\right)=1\Leftrightarrow a^{(p-1)/2}\equiv 1\pmod{p}$$

Corolario.

La ecuación $x^2\equiv a\pmod{p}$ no tiene solución si y solo si $a^{(p-1)/2}\equiv -1\pmod{p}$, o dicho de otra manera, $\left(\frac{a}{p}\right)\equiv a^{(p-1)/2}\equiv 1\pmod{p}$.

Ejemplo 1.

Supongamos que $p=11$.

Por un lado, tenemos
$0^2\equiv 0$, $1^2\equiv 1$, $2^2\equiv 4$, $3^2\equiv 9$, $4^2\equiv 5$, $5^2\equiv 3$, $6^2\equiv 3$, $7^2\equiv 5$, $8^2\equiv 9$, $9^2\equiv 4$, $10^2\equiv 1$

Así pues, los cuadrados perfectos en $\mathbb{Z}_{11}$ son 0, 1, 3, 4, 5, 9.

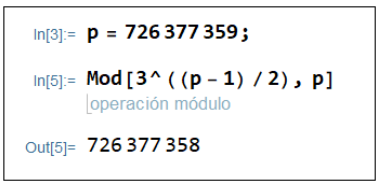
Por otro lado, tenemos $a^{(p-1)/2}=a^{(11-1)/2}=a^5$, y las potencias $a^5\pmod 5$ son
$0^5\equiv 0$, $1^5\equiv 1$, $2^5\equiv$ -1 , $3^5\equiv 1$, $4^5\equiv 1$, $5^5\equiv 1$, $6^5\equiv$ -1, $7^5\equiv$ -1 , $8^5\equiv$ -1 , $9^5\equiv 1$, $10^5\equiv$ -1

Y verificamos que se cumple el Criterio de Euler: $\left(\frac{a}{11}\right)=1\Leftrightarrow a^{(11-1)/2}\equiv 1\pmod{11}$

Ejemplo 2.

¿ 3 es un cuadrado perfecto en $\mathbb{Z}_p$, con p=726377359 ?

Mediante el Criterio de Euler, y usando Mathematica:



Luego $3^{(p-1)/2}\equiv -1\pmod{p}$, y por tanto 3 no es un cuadrado perfecto en este cuerpo.

Mediante la ley de reciprocidad cuadrática de Gauss:

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$$

Aquí hemos aplicado que

$$\frac{p-1}{2}\cdot\frac{q-1}{2} = \frac{p-1}{2}\cdot\frac{3-1}{2} = \frac{726377359\ -1}{2} = \frac{726377358}{2} = 363188679 \quad \text{es impar}$$

y por tanto

$$(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} = 1$$

Para calcular $\left(\frac{p}{3}\right)$ vemos que $p \equiv 1 \pmod 3$ y 1 sí es un cuadrado perfecto en $\mathbb{Z}_3$, es decir,

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = 1$$

Y por tanto 3 sí es un cuadrado perfecto en $\mathbb{Z}_p$.

Observamos que el segundo método, mediante la ley de reciprocidad cuadrática de Gauss, es mucho más efectivo, pues nos ha evitado calcular una potencia modular.

7.6 Residuos cúbicos.

7.6.1 MD

Determina todas las ternas de enteros (a,b,c) tales que el número

$$N=\frac{(a-b)(b-c)(c-a)}{2}+2$$

sea una potencia de 2016.

(Una potencia de 2016 es cualquier entero de la forma 2016^n, donde n es un entero no negativo).

JBMO 2016 #3

7.7 Raíces primitivas. Índices modulares.

Definición. Raíz primitiva.

Diremos que una unidad a de Z_n es una raíz primitiva módulo n si $ord_n(a)=\phi(n)$. Equivalentemente, cuando

$$\langle a\rangle=\{a,a^2,a_3,...,a^{\phi(n)}\}=Z_n^{\times}$$

O de otra forma, si para cualquier entero x coprimo con n, siempre existe un entero j tal que $x=a^j \pmod n$.

Lema.

Sea m un entero positivo y sea x un entero coprimo con m. Para todo par j,k de enteros positivos, se cumple:

$$x^j\equiv x^k \pmod m \Leftrightarrow j\equiv k \pmod d \text{ , donde } d=ord_m(x)$$

Ejercicio resuelto.

Determina $ord_{257}(5)$, y comprueba que 5 es una raíz primitiva módulo 257.

Solución. Puesto que 257 es primo, $\phi(257)=256=2^8$. Así pues, $ord_{257}(5)\mid 2^8$, es decir, será una potencia de 2. Vamos calculándolas una por una:
$5^2=25,\ 5^4=5^2\cdot 5^2=625\equiv 111,\ 5^8=5^4\cdot 5^4=111\cdot 111\equiv 242,\ 5^{16}\equiv 225,\ 5^{32}\equiv 253,$
$5^{64}\equiv 16,\ 5^{128}\equiv 256,\ 5^{256}\equiv 1.$
Así pues, $ord_{257}(5)=256=\phi(257)$, y por tanto es una raíz primitiva módulo 257.

Ejercicio resuelto.

Resuelve la congruencia $x^3\equiv 5 \pmod{17}$, sabiendo que 3 es una raíz primitiva módulo 17.

Solución. Por ser 3 una raíz modular módulo 17, todo elemento de Z_{17} se podrá escribir como $x=3^a$ para cierto a que vamos a determinar.

$$x^3\equiv 5 \pmod{17}\Leftrightarrow (3^a)^3\equiv 5 \pmod{17}\Leftrightarrow 3^{3a}\equiv 5 \pmod{17}$$

Ahora escribimos 5 en forma de potencia de 3:

$$3^1\equiv 3 \pmod{17},\ 3^2\equiv 9 \pmod{17},\ 3^3\equiv 10 \pmod{17},\ 3^4\equiv 13 \pmod{17},$$
$$3^5\equiv 5 \pmod{17}$$

Y por tanto nuestra congruencia queda planteada de manera que podemos aplicar el lema anterior:

$$3^{3a}\equiv 3^5 \pmod{17}\Leftrightarrow 3a\equiv 5 \pmod{\phi(17)}\Leftrightarrow 3a\equiv 5 \pmod{16}$$

Probando con posibles candidatos vemos que

$$3\cdot 11=33\equiv 1 \pmod{17}\Rightarrow 11=3^{-1} \pmod{17}$$

Y por tanto

$$3a \equiv 5 \pmod{16} \Leftrightarrow a \equiv 3^{-1} \cdot 5 \equiv 11 \cdot 5 = 55 \equiv 7 \pmod{16} \Leftrightarrow a = 16b + 7$$

En particular, tomando $b = 0 \Rightarrow a = 7 \Rightarrow x = 3^7 \pmod{17}$

Siguiendo con los cálculos de arriba:

$$3^6 \equiv 15 \pmod{17},\ 3^7 \equiv 11 \pmod{17}$$

Así pues, $x = 11 \pmod{17}$.

Fuente: Michael Penn en YouTube.

Ejercicio resuelto.

Resuelve la congruencia $5^x \equiv 17 \pmod{19}$, sabiendo que 2 es una raíz primitiva módulo 19.

Solución.

Generando la tabla $2^k \pmod{19}$ vemos que $17 \equiv 2^{10} \pmod{19}$ y $5 \equiv 2^{16} \pmod{19}$, por tanto

$$5^x \equiv 17 \pmod{19} \Leftrightarrow \left(2^{16}\right)^x \equiv 2^{10} \pmod{19} \Leftrightarrow 2^{16x} \equiv 2^{10} \pmod{19}$$

$$\Leftrightarrow 16x \equiv 10 \pmod{\phi(19)} \Leftrightarrow 16x \equiv 10 \pmod{18} \Leftrightarrow 16x \equiv 10 \pmod{18} \Leftrightarrow$$

$$8x \equiv 5 \pmod{9}$$

Por tanteo vemos que $8 \cdot 8 = 64 \equiv 1 \pmod{9} \Rightarrow 8^{-1} \equiv 8 \pmod{9}$ y por tanto

$$8x \equiv 5 \pmod{9} \Leftrightarrow x \equiv 8^{-1} \cdot 5 \equiv 8 \cdot 5 \equiv 40 \equiv 4 \pmod{9} \Leftrightarrow x = 9k + 4$$

Tomando $k = 0 \Rightarrow x = 4$, y tomando $k = 1 \Rightarrow x = 13$, es decir, aparecen dos soluciones módulo 19.

Fuente: Michael Penn en YouTube.

Ejercicio resuelto.

Resuelve la siguiente congruencia:

$$17^x \equiv 10 \pmod{27}$$

Solución.

En primer lugar, vemos que, puesto que $27 = 3^3$, existirá una raíz primitiva módulo 27. De hecho, se demuestra que 2 es una raíz primitiva módulo 27.

Para aplicar el lema anterior, debemos escribir 17 y 10 como potencias de la misma base.

$2^1 \equiv 2 \pmod{27}$	$2^2 \equiv 4 \pmod{27}$	$2^3 \equiv 8 \pmod{27}$
$2^4 \equiv 16 \pmod{27}$	$2^5 \equiv 32 \equiv 5 \pmod{27}$	$2^6 \equiv 10 \pmod{27}$
$2^7 \equiv 20 \pmod{27}$	$2^8 \equiv 13 \pmod{27}$	$2^9 \equiv 26 \equiv -1 \pmod{27}$
$2^{10} \equiv -2 \equiv 25 \pmod{27}$	$2^{11} \equiv -4 \equiv 23 \pmod{27}$	$2^{12} \equiv -8 \equiv 19 \pmod{27}$
$2^{13} \equiv 11 \pmod{27}$	$2^{14} \equiv 22 \pmod{27}$	$2^{15} \equiv 44 \equiv 17 \pmod{27}$

Luego $17^x \equiv 10 \pmod{27} \Leftrightarrow \left(2^{15}\right)^x \equiv 2^6 \pmod{27} \Leftrightarrow 2^{15x} \equiv 2^6 \pmod{27}$

Y ahora aplicamos el lema anterior:

$$2^{15x} \equiv 2^6 \pmod{27} \Leftrightarrow 15x \equiv 6 \pmod{18}\ ,\ \text{pues}\ \phi(27) = \phi\left(3^3\right) = 18$$

Con lo que hemos reducido una congruencia exponencial a una congruencia lineal. $15x \equiv 6 \pmod{18} \Leftrightarrow 5x \equiv 2 \pmod{6}$ dividiendo entre tres toda la congruencia.

Esta última congruencia la podemos resolver viendo que $5^{-1} \equiv 5 \pmod{6}$ y por tanto

$$5x \equiv 2 \pmod{6} \Leftrightarrow x \equiv 5^{-1} \cdot 2 \equiv 5 \cdot 2 \equiv 10 \equiv 4 \pmod{6}$$

Puesto que nosotros buscamos soluciones módulo 16, el conjunto total de soluciones será

$$\{4, 4+6, 4+12\} \pmod{18} = \{4, 10, 16\} \pmod{18}$$

Ejercicio resuelto.

Resuelve la siguiente congruencia:

$$9^x \equiv 10 \pmod{13}$$

Solución.

En primer lugar, vemos que 2 es una raíz primitiva módulo 13.

Para poder aplicar el lema anterior, debemos escribir 9 y 10 como potencias de 2:

$2^1 \equiv 2 \pmod{13}$ $\quad 2^2 \equiv 4 \pmod{13}$ $\quad 2^3 \equiv 8 \pmod{13}$

$2^4 \equiv 16 \equiv 3 \pmod{13}$ $\quad 2^5 \equiv 6 \pmod{13}$ $\quad 2^6 \equiv 12 \equiv -1 \pmod{13}$

$2^7 \equiv -2 \equiv 11 \pmod{13}$ $\quad 2^8 \equiv -4 \equiv 9 \pmod{13}$ $\quad 2^9 \equiv 18 \equiv 5 \pmod{13}$

$2^{10} \equiv 10 \pmod{13}$

Luego $9^x \equiv 10 \pmod{13} \Leftrightarrow \left(2^8\right)^x \equiv 2^{10} \pmod{13} \Leftrightarrow 2^{8x} \equiv 2^{10} \pmod{13}$

y aplicando el lema anterior:

$$2^{8x} \equiv 2^{10} \pmod{13} \Leftrightarrow 8x \equiv 10 \pmod{12}, \text{ pues } \phi(13) = 12$$

Pero vemos que esta congruencia lineal no tiene solución $(8,12) = 4$ y $4 \nmid 10$.

Así pues, la congruencia del enunciado no tiene solución.

Ejercicio resuelto.

Resuelve la siguiente congruencia:

$$11^x \equiv 17 \pmod{18}$$

Solución.

Sabemos que 5 es una raíz primitiva módulo 18.

Para poder aplicar el lema anterior, debemos escribir 11 y 17 como potencias de 5:

$5^1 \equiv 5 \pmod{18}$ $\quad 5^2 \equiv 25 \equiv 7 \pmod{18}$ $\quad 5^3 \equiv 35 \equiv -1 \equiv 17 \pmod{18}$

$5^4 \equiv -5 \equiv 13 \pmod{18}$ $\quad 5^5 \equiv -25 \equiv 11 \pmod{18}$

Luego

$$11^x \equiv 17 \pmod{18} \Leftrightarrow \left(5^5\right)^x \equiv 5^3 \pmod{18} \Leftrightarrow 5^{5x} \equiv 5^3 \pmod{18}$$

y aplicando el lema anterior:

$$5^{5x} \equiv 5^3 \pmod{18} \Leftrightarrow 5x \equiv 3 \pmod{6}, \text{ pues } \phi(18) = 6$$

Para resolver esta congruencia lineal aprovechamos que 5 y 6 son coprimos, luego 5 tendrá inverso módulo 6, en efecto, es el propio 5, luego

$$5x \equiv 3 \pmod 6 \Leftrightarrow x \equiv 5^{-1} \cdot 3 \equiv 5 \cdot 3 \equiv 15 \equiv 3 \pmod 6$$

7.7.1 F

Determina el menor entero $n \geq 2021$ para el cual $30n^3 + 143n^2 + 117n - 56$ sea divisible entre 13.

SMT 2021 Number Theory #2

Determinación de raíces primitivas. Teorema.

Supongamos que a es una raíz primitiva módulo n.

a) $ord_n(a^k) = \dfrac{\phi(n)}{(k, \phi(n))}$

b) Si $d \mid \phi(n)$, entonces existen $\phi(d)$ elementos de $Z_n^{\times}$ de orden d, y a^k tiene orden d si y solo si $(k, \phi(n)) = \dfrac{\phi(n)}{d}$

Corolario.

Si Z_n tiene una raíz primitiva a, entonces tiene $\phi(\phi(n))$ raíces primitivas: a^k es una raíz primitiva si y solo si $(k, \phi(n)) = 1$.

Ejercicio resuelto.

Determina las raíces primitivas módulo 17 sabiendo que 3 es raíz primitiva módulo 17.

Solución.

Por el corolario anterior, sabemos que existen $\phi(\phi(17)) = \phi(16) = \phi(2^4) = 8$ raíces primitivas. Serán todas aquellas que se puedan escribir como 3^k con $(k, 16) = 1$, es decir,

$k = 1,3,5,7,9,11,13,15$, que dan lugar a los valores

$3^1 \equiv 3,\ 3^3 \equiv 10,\ 3^5 \equiv 5,\ 3^7 \equiv 11,\ 3^9 \equiv 14,\ 3^{11} \equiv 7,\ 3^{13} \equiv 12,\ 3^{15} \equiv 6$.

Ejercicio resuelto.

Determina las $\phi(\phi(29)) = \phi(28) = 12$ raíces primitivas módulo 29, sabiendo que 2 es una raíz primitiva módulo 29.

Solución.

Aplicando el corolario anterior, las raíces primitivas de Z_{29} serán todos los elementos de la forma 2^k, con $(k, 28) = 1$, es decir, $k = 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27$.

Para estos índices k tenemos los valores $2, 8, 3, 19, 18, 14, 27, 21, 26, 10, 11, 15$, que serán las 12 raíces primitivas buscadas.

El siguiente teorema es una generalización del teorema anterior.

Teorema. Teorema de Gauss.

Existen raíces primitivas módulo $n>1$ si y solo si $n=2,4,p^{\alpha},2p^{\alpha}$ donde p es un primo impar y α es un entero positivo.

Definición. Índice modular.

Sea b una raíz primitiva módulo n. Si $(a,n)=1$, entonces el más pequeño entero positivo k tal que $a\equiv b^{k}\pmod{n}$ se denota por $ind_{b}(a)$ y se llama índice de a respecto a la base b módulo n.

Al índice se le suele llamar también **logaritmo discreto**, pues sus propiedades y sus aplicaciones son similares a las del logaritmo.

Ejercicio resuelto.

a) Demuestra, mediante cálculos directos, que 3 es una raíz primitiva módulo 17, y construye la tabla de índices de base 3 módulo 17.

b) Aplicando la tabla de índices anterior, resuelve la congruencia $7x\equiv 5\pmod{17}$.

c) Aplicando la tabla de índices anterior, resuelve la congruencia $x^{7}\equiv 5\pmod{17}$.

d) Aplicando la tabla de índices anterior, resuelve la congruencia $x^{8}\equiv 8\pmod{17}$.

Solución.

En Z_{17} tenemos: $3^{1}\equiv 3,\ 3^{2}\equiv 9,\ 3^{3}=27\equiv 10,\ 3^{4}\equiv 30\equiv 13,\ 3^{5}\equiv 5,\ 3^{6}\equiv 15,\ 3^{7}\equiv 11,$ $3^{8}\equiv 16,\ 3^{9}\equiv 14,\ 3^{10}\equiv 8,\ 3^{11}\equiv 7,\ 3^{12}\equiv 4,\ 3^{13}\equiv 12,\ 3^{14}\equiv 2,\ 3^{15}\equiv 6,\ 3^{16}\equiv 1.$

Así pues, 3 tiene orden 16 módulo 17, y por tanto es una raíz primitiva módulo 17.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$ind_{3}a$	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

b)

$$7x\equiv 5\pmod{17}\Rightarrow$$
$$ind_{3}(7x)\equiv ind_{3}(5)\pmod{16}\Rightarrow$$
$$ind_{3}(7)+ind_{3}(x)\equiv ind_{3}(5)\pmod{16}\Rightarrow$$
$$ind_{3}(x)\equiv ind_{3}(5)-ind_{3}(7)\pmod{16}$$

Determinamos los índices de la derecha en la tabla del apartado (a):

$$ind_{3}(7)+ind_{3}(x)\equiv ind_{3}(5)\pmod{16}\Rightarrow$$
$$ind_{3}(x)\equiv 5-11=-6\equiv 10\pmod{16}\Rightarrow$$
$$x\equiv 8\pmod{17}$$

c)

$$x^{7}\equiv 5\pmod{17}\Rightarrow ind_{3}(x^{7})\equiv ind_{3}(5)\pmod{16}\Rightarrow$$
$$7ind_{3}(x)\equiv ind_{3}(5)\pmod{16}\Rightarrow 7ind_{3}(x)\equiv 5\pmod{16}\Rightarrow$$
$$ind_{3}(x)\equiv 7^{-1}\cdot 5\pmod{16}\Rightarrow ind_{3}(x)\equiv 7\cdot 5=35\equiv 3\pmod{16}\Rightarrow$$
$$x\equiv 10\pmod{17}$$

d)

$$x^8 \equiv 8 \pmod{17} \Rightarrow$$
$$ind_3(x^8) \equiv ind_3(8) \pmod{16} \Rightarrow$$
$$8 \cdot ind_3(x) \equiv 10 \pmod{16}$$

Pero esta última congruencia no tiene solución, puesto que $(8,16)=8$, y $8 \nmid 10$.

8 Exponenciación modular. El problema del logaritmo discreto.

8.1 Exponenciación modular.

Definimos la exponenciación modular de la forma convencional:

$$a^0 = 1$$
$$a^1 = a$$
$$a^n = \underbrace{a \cdot \ldots \cdot a}_{n \text{ veces}}$$

Ejemplo.

Determina el último dígito de 7^{100}

Solución:

Debemos determinar $7^{100} \pmod{10}$

Primera versión:

Vamos calculando potencias sucesivas:

$7^1 \equiv 7 \pmod{10}$

$7^2 = 49 \equiv 9 \pmod{10}$

$7^3 \equiv 9 \cdot 7 = 63 \equiv 3 \pmod{10}$

$7^4 \equiv 3 \cdot 7 = 21 \equiv 1 \pmod{10}$

Luego $7^4 \equiv 1 \pmod{10} \Rightarrow 7^{100} = 7^{4 \cdot 25} = \left(7^4\right)^{25} \equiv 1^{25} = 1 \pmod{10}$

Segunda versión:

$7^2 = 49 \equiv -1 \pmod{10} \Rightarrow 7^{100} = 7^{2 \cdot 50} = \left(7^2\right)^{50} \equiv (-1)^{50} = 1 \pmod{10}$

8.2 Exponenciación modular optimizada (EMO).

Supongamos que queremos calcular 5^{37}, realizando el mínimo número de operaciones posible.

En primer lugar, escribimos 37 en base 2:

$$37 = 100101_{(2} \Rightarrow 37 = 1\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0$$

Luego

$$5^{37} = 5^{1\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0} =$$
$$= 5^{1\cdot 2^5} \cdot 5^{0\cdot 2^4} \cdot 5^{0\cdot 2^3} \cdot 5^{1\cdot 2^2} \cdot 5^{0\cdot 2^1} \cdot 5^{1\cdot 2^0} =$$
$$= \left(5^{2^5}\right)^1 \cdot \left(5^{2^4}\right)^0 \cdot \left(5^{2^3}\right)^0 \cdot \left(5^{2^2}\right)^1 \cdot \left(5^{2^1}\right)^0 \cdot \left(5^{2^0}\right)^1 =$$
$$= \left(5^{2^5}\right)^1 \cdot \left(5^{2^4}\right)^0 \cdot \left(5^{2^3}\right)^0 \cdot \left(5^{2^2}\right)^1 \cdot \left(5^{2^1}\right)^0 \cdot \left(5^{2^0}\right)^1$$

Y ahora observamos que las sucesivas potencias $5^{(2^k)}$ se pueden calcular recursivamente:

$$5^{(2^0)} = 5^1 = 5 \rightarrow 5^{(2^1)} = 5^2 \rightarrow 5^{(2^2)} = 5^{2\cdot 2} = \left(5^2\right)^2 \rightarrow 5^{(2^3)} = 5^{2^2\cdot 2} = \left(5^{(2^2)}\right)^2 \rightarrow$$
$$\rightarrow 5^{(2^4)} = 5^{2^3\cdot 2} = \left(5^{(2^3)}\right)^2 \rightarrow \ldots \rightarrow 5^{(2^k)} = 5^{2^{k-1}\cdot 2} = \left(5^{(2^{k-1})}\right)^2$$

Así pues, hemos reducido el cálculo de 5^{37} a realizar 5 cuadrados y 2 multiplicaciones.

Este mismo método se puede generalizar para cualquier base y cualquier exponente, obteniendo un método para calcular potencias x^n que requiere un esfuerzo de cálculo del orden $O(\log n)$.
Además, este método es fácilmente codificable:

```
# Iterative Function to calculate
# (x^y)%p in O(log y)
def power(x, y, p) :
        res = 1  # Initialize result
        # Update x if it is more
        # than or equal to p
        x = x % p

        if (x == 0) :
                return 0
        while (y > 0) :
                # If y is odd, multiply
                # x with result
                if ((y & 1) == 1) :
                        res = (res * x) % p
                # y must be even now
                y = y >> 1      # y = y/2
                x = (x * x) % p

        return res
# Driver Code
x = 2; y = 3; p = 10
print("Power is ", power(x, y, p))
# This code is contributed by Nikita Tiwari.
```

Ejemplo 1.

Calcular $3^{11} \pmod{500}$.

Solución.

$11 = 1011_{(2} = 2^3 + 2^1 + 1$

$3^{2^0} = 3^1 = 3 \pmod{500}$

$3^{2^1} = 3^2 = 9 \pmod{500}$

$3^{2^2} = \left(3^2\right)^2 = 81 \pmod{500}$

$3^{2^3} = \left(3^{2^2}\right)^2 = 81^2 = 6561 \equiv 61 \pmod{500}$

Finalmente, $3^{11} = 3^{2^3} \cdot 3^{2^1} \cdot 3^{2^0} = 61 \cdot 9 \cdot 3 = 1647 \equiv 147 \pmod{500}$

Ejemplo 2.

Calcula $3^{94} \pmod{17}$

$94 = 1011110_{(2} \Rightarrow$

$\Rightarrow 94 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6 = 2^1 + 2^2 + 2^3 + 2^4 + 2^6$

$3^{94} = 3^{2^1+2^2+2^3+2^4+2^6} = 3^{\left(2^1\right)} \cdot 3^{\left(2^2\right)} \cdot 3^{\left(2^3\right)} \cdot 3^{\left(2^4\right)} \cdot 3^{\left(2^6\right)}$

$3^2 \equiv 9 \pmod{17}$

$3^{\left(2^2\right)} \equiv 9^2 = 81 \equiv 13 \equiv -4 \pmod{17}$

$3^{\left(2^3\right)} \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}$

$3^{\left(2^4\right)} \equiv (-1)^2 = 1 \pmod{17}$

$3^{\left(2^5\right)} \equiv 1^2 = 1 \pmod{17}$

$3^{\left(2^6\right)} \equiv 1^2 = 1 \pmod{17}$

Luego, finalmente: $3^{94} \equiv 9 \cdot (-4) \cdot (-1) \cdot 1 \cdot 1 \equiv 36 \equiv 2 \pmod{17}$

Ejemplo 3.

Calcula $3^{1000} \pmod{26}$

$1000 = 1111101000_{(2} \Rightarrow 1000 = 2^3 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9 = 8 + 32 + 64 + 128 + 256 + 512$

$3^{1000} = 3^{8+32+64+128+256+512} = 3^8 \cdot 3^{32} \cdot 3^{64} \cdot 3^{128} \cdot 3^{256} \cdot 3^{512} = (*)$

$3^1 \equiv 3 \pmod{26}$

$3^2 \equiv 9 \pmod{26}$

$3^4 \equiv 9^2 = 81 \equiv 3 \pmod{26}$

Vemos que entramos en un bucle:

$3^8 \equiv 3^2 \equiv 9 \pmod{26}$, $3^{16} \equiv 3 \pmod{26}$, $3^{32} \equiv 9 \pmod{26}$, $3^{64} \equiv 3 \pmod{26}$

$3^{128} \equiv 9 \pmod{26}$, $3^{256} \equiv 3 \pmod{26}$, $3^{512} \equiv 9 \pmod{26}$

Por tanto: $(*) = 9 \cdot 9 \cdot 3 \cdot 9 \cdot 3 \cdot 9 = 3 \cdot 3 \cdot 3 \cdot 3 = 9 \cdot 9 = 3 \pmod{26}$

8.2.1

Calcular $3^{172} \pmod{191}$.

Observación.

A partir de la versión 3.8, Python incorpora el comando

```
pow(a,n,m)
```

para determinar $a^n \pmod{m}$ de forma optimizada para aritmética modular, aplicando las técnicas del apartado anterior.

8.3 El problema del logaritmo discreto (PLD).

Acabamos de ver que, dados dos números a, n, calcular $b = a^n$ es un problema que se resuelve realizando una cantidad relativamente pequeña de operaciones, porque no necesitamos realizar toda la cadena de $n-1$ operaciones

$$a \to a^2 = a \cdot a \to a^3 = a^2 \cdot a \to a^4 = a^3 \cdot a \to \ldots \to a^n = a^{n-1} \cdot a$$

Sin embargo, el problema inverso, es decir, dados dos números a, b, encontrar (suponiendo que existe) el valor de n tal que $b = a^n$, al que llamaremos "logaritmo discreto de b en la base a", es terriblemente difícil, pues, al no poder aplicar el truco explicado en el apartado anterior, debemos ir probando, uno por uno, los sucesivos valores

$$a \to a^2 = a \cdot a \to a^3 = a^2 \cdot a \to a^4 = a^3 \cdot a \to \ldots \to a^n = a^{n-1} \cdot a \to \ldots$$

hasta encontrar (si es que existe), el valor b.

Esto, cuando trabajamos con números muy grandes, es un problema que se considera actualmente irresoluble, y es el fundamento de la "Criptografía basada en el Logaritmo Discreto".

8.4 Aplicación a la Criptografía: El sistema Diffie-Hellman (DH).

En el año 1976, Whitfield Diffie y Martin Hellman propusieron el primer protocolo de intercambio de clave basado en la exponenciación en cuerpos finitos y el PLD.

Supongamos que dos personas, Alicia y Benito, quieren acordar una clave secreta común.

Alicia	Espacio público	Bob
En primer lugar pactan un cuerpo finito IF_q y un elemento generador g del mismo. (IF_q, g) son la clave pública. →	**¡Todo lo que pase por aquí será visto por el Enemigo!**	Bob recibe (IF_q, g)
Alicia elige un entero $2 \le a \le q-2$		Bob elige un entero $2 \le b \le q-2$
Alicia envía g^a →		Bob recibe g^a
Alicia recibe g^b ←		Bob envía g^b
Alicia calcula $g^{ab} = (g^b)^a$	El Enemigo puede ver g^a y g^b, pero con ellos no es capaz de deducir g^{ab}.	Bob calcula $g^{ab} = (g^a)^b$

Está claro que si el "Enemigo" hubiera solucionado el PLD, de g^a y g^b hubiera deducido a y b y con ellos hubiera calculado g^{ab}, haciéndose con la clave secreta. Este método nos lleva a plantear el siguiente problema específico, llamado Problema de Diffie-Hellman (PDH):

Dados g^a y g^b y un elemento $s \in IF_q$, deducir si $s = g^{ab}$.

A pesar de que no se ha demostrado que PDH y PLD son equivalentes en el caso general, existen resultados que prueban la equivalencia de ambos problemas bajo ciertas condiciones.

8.5 Aplicación a la Criptografía: El Criptosistema de ElGamal.

Uno de los métodos criptográficos basados en Logaritmo discreto es "ElGamal", propuesto por Taher ElGamal en 1985.

Emisor: Alicia	Espacio público	Receptor: Bob
Emisor y receptor pactan un cuerpo finito IF_q y un elemento generador g del mismo. (IF_q, g) son la clave pública. →	**¡Todo lo que pase por aquí será visto por el Enemigo!** El Enemigo puede ver la clave pública, pero no le servirá de nada (por eso se llama pública)	→ Bob recibe (IF_q, g) Bob elige un entero a tal que $2 \le a \le q-2$ y calcula g^a. El entero a es su clave privada. Envía a Alicia el valor g^a, que es su clave pública.
Alicia recibe g^a ←		
Supongamos que Alicia quiere enviar el mensaje secreto m. Elige un entero k con $2 \le k \le q-2$. Calcula $g^{ak} = (g^a)^k$. Envía $(g^k, m g^{ak})$ →		El receptor recibe $(g^k, m g^{ak})$, y con estos datos es fácil deducir m: Calcula $g^{ak} = (g^k)^a$ y entonces: $m = m g^{ak} / g^{ak}$

Observación 1.

La fórmula que utiliza Bob: $m = m g^{ak} / g^{ak}$, se puede reemplazar por el siguiente método, que evita calcular el inverso modular de g^{ak}:

1. Calcula $(g^k)^{q-1-a}$.
2. Determina $(g^k)^{q-1-a} m g^{ak} = m g^{k(q-1)-ka+ak} = m(g^{q-1})^k = m$

Observación 2.

Es importante reseñar que el valor de k debe cambiar en cada envío. De lo contrario, el Enemigo podría deducir la clave pública.

Ejemplo.

Supongamos que Alicia y Benito quieren intercambiar mensajes utilizando el criptosistema de ElGamal.

Pactan trabajar en el cuerpo IF_{157} con generador $g = 5$.

Bob escoge su clave privada $a = 25$ y envía a Alica su clave pública $g^a = 34$.

Supongamos que Alicia quiere enviar el mensaje $m = 19$ a Bob.

Entonces elige un entero $k = 89$ y envía a Bob el par $\left(5^{89}, 19 \cdot 5^{25 \cdot 89}\right) = \left(131, 45\right)$.

Para obtener el mensaje, Bob calcula $5^{25 \cdot 89} \equiv 85 \pmod{157}$ y calcula

$m = 45/85 \equiv 19 \pmod{157}$

Alternativamente, Bob también podría recuperar el mensaje a partir de $5^{89(157-1-25)} \equiv 133 \pmod{157}$ y por tanto $m = 133 \cdot 45 \equiv 19 \pmod{157}$.

8.6 Problemas.

8.6.1 [D]

Determina la suma de todos los enteros positivos n tales que, cuando $1^3+2^3+3^3+...+n^3$ se divide entre $n+5$, el residuo es 17.

AIME II 2020#10

8.6.2 [D]

Determina el número de enteros $n \le 600$ cuyos valores pueden ser determinados unívocamente si nos dan los valores de $\left\lfloor \frac{n}{4} \right\rfloor$, $\left\lfloor \frac{n}{5} \right\rfloor$ y $\left\lfloor \frac{n}{6} \right\rfloor$, donde $\lfloor x \rfloor$ denota el menor entero menor o igual que el número real x.

AIME II 2022#8

8.6.3 [F]

Determina el máximo común divisor de los números $A_n = 2^{3n} + 3^{6n+2} + 5^{6n+2}$ para todo $n = 0,1,...,1999$.

JBMO 2001

8.6.4 [D] **Problema solucionado paso a paso en vídeo.**

Determina, de entre los siguientes números, número primo menor que 10.

(A) $2^{606}-1$ (B) $2^{606}+1$ (C) $2^{607}-1$ (D) $2^{607}+1$ (E) $2^{607}+3^{607}$

AMC 12B 2022 #15, AMC 10B 2022 #17

Solución: https://youtu.be/rideZfPgmeQ

8.6.5 [D]

Determina el menor entero positivo n para el cual 2^n+5^n-n sea un múltiplo de 1000.

AIME II 2021#13

9 El pequeño Teorema de Fermat. El Teorema de Euler.

9.1 El Pequeño Teorema de Fermat (PTF).

Lema. "Freshman's Dream" ("El sueño de todo bachiller").

Para todo p primo y a,b enteros se cumple:

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

Demostración.

Basta desarrollar $(a+b)^p$ aplicando el Teorema del Binomio. Sus términos son de la forma

$$\binom{p}{k} a^k b^{p-k} \text{ con } \binom{p}{k} = \frac{p!}{k!(p-k)!} \qquad 0 \le k \le p$$

Los términos "internos" $0 < k < p$ contienen el factor primo p que no se cancela, puesto que no aparece como factor en el denominador, luego todos se cancelan al hacer módulo p. Es decir, todos los coeficientes son divisibles entre p excepto el primero y el último.

Teorema. Pequeño Teorema de Fermat (PTF).

Si p es primo,

a) $a^p \equiv a \pmod{p}$ para cualquier entero a.

b) Si $p \nmid a$, entonces $a^{p-1} \equiv 1 \pmod{p}$

Nota: El recíproco no es cierto: $a^{n-1} \equiv 1 \pmod{n}$ para cierto entero $a \not\Rightarrow$ n primo. Esto se estudiará detenidamente en una observación más adelante.

Demostración. a) Aunque en el próximo tema veremos que este teorema es un caso particular de aplicación de la función Phi de Euler, vamos a presentar aquí una demostración directa.

Caso 1: Si $a = 0$. $a = 0 \Rightarrow a^p = 0 = a$ y está claro que entonces $a^p \equiv a \pmod{p}$.

Caso 2: Si $a > 0$. Vamos a demostrarlo por inducción en a:

Si $a = 1$, $a^p = 1^p = 1$ y está claro que entonces $a^p \equiv a \pmod{p}$.

Supongamos cierto $a^p \equiv a \pmod{p}$, queremos ver que entonces es cierto para $a+1$.

Aplicando el lema anterior y la hipótesis de inducción:

$$(a+1)^p \equiv a^p + 1 \pmod{p} \equiv a + 1 \pmod{p}$$

tal y como queríamos ver.

Caso 3: Si $a < 0$. Si $p = 2$, entonces

$$a^2 = (-a)^2 \equiv -a \pmod{2} \Rightarrow 2 \mid a^2 + a \Rightarrow 2 \mid a^2 + a - 2a = a^2 - a \Rightarrow a^2 \equiv a \pmod{2}$$

Si $p \neq 2$, entonces p es impar, y por tanto: $a^p = -(-a)^p \equiv -(-a) \pmod{p} = a \pmod{p}$

En donde hemos aplicado el "Caso 1" pues $-a$ es positivo.

b) Aplicando el apartado anterior, $a^p \equiv a \pmod{p} \Leftrightarrow p \mid a^p - a = a\left(a^{p-1} - 1\right)$.

Aplicando el Lema de Euclides, puesto que, por hipótesis, $p \nmid a$, deducimos que $p \mid a^{p-1} - 1$, o equivalentemente, $a^{p-1} - 1 \equiv 0 \pmod{p} \Leftrightarrow a^{p-1} \equiv 1 \pmod{p}$

Nota histórica.

El 18 de octubre de 1640, Fermat escribió una carta a Bernhard Frenicle de Bessy (1605-1675), un funcionario de la Casa de la Moneda francesa, excelente alumno en teoría de los números. En su carta, Fermat comunica el resultado siguiente: Si p es primo y p no divide a entonces $p|a^{p-1} - 1$. Fermat no presentó una prueba de este resultado, pero una nota adjunta prometía enviar una demostración, siempre que no resultara demasiado extensa. Sin embargo, la primera prueba conocida la dio Euler un siglo después. Este resultado es conocido como el "pequeño" teorema de Fermat para diferenciarlo del "último teorema de Fermat" (1637): La ecuación $x^n + y^n = z^n$ no tiene soluciones enteras positivas si $n > 2$ (demostrado por A.Wiles en 1995.)

Fuente: Introducción a la Teoría de Números (Walter Mora F.)

El PTF se puede aplicar al cálculo de congruencias con potencias de números, como en los siguientes ejemplos:

Ejemplo resuelto.

Demostrar que $5^{38} \equiv 4 \pmod{11}$.

Solución.

Aplicamos el PTF para garantizar que $5^{10} = 1 \pmod{11}$, luego:

$5^{38} = 5^{3\cdot 10+8} = \left(5^{10}\right)^3 5^8 \equiv 1^3 5^8 \pmod{11} \equiv 5^8 \pmod{11} = (*)$

Por otro lado $5^2 = 25 \equiv 3 \pmod{11}$, y por tanto:

$(*) \equiv \left(5^2\right)^4 \pmod{11} \equiv 3^4 \pmod{11} \equiv 81 \pmod{11} \equiv 4 \pmod{11}$

Donde hemos aplicado que $81 = 7 \cdot 11 + 4$

Ejemplo resuelto.

Calcular $7^{121} \pmod{13}$.

Solución.

Puesto que $13 \nmid 7$ podemos aplicar el PTF para garantizar que $7^{12} \equiv 1 \pmod{13}$.

Puesto que $121 = 12 \cdot 10 + 1$ $7^{121} = 7^{12\cdot 10+1} = \left(7^{12}\right)^{10} \cdot 7 \equiv 1^{10} \cdot 7 = 7 \pmod{13}$

Ejemplo resuelto. Aplicación del PTF a la determinación del orden.

Determina los posibles periodos de las secuencias $x, x^2, x^3, \ldots \pmod{13}$ para los diferentes valores de x. Encuentra valores de x para los que se cumplen dichos periodos (el concepto de orden de un entero será desarrollado en el apartado 9.3).

Aplicando el PTF, sabemos que $x^{12} \equiv 1 \pmod{13}$, luego las longitudes de los ciclos serán un factor de 12, porque después de 12 iteraciones siempre se llegará al mismo valor. Así pues, las longitudes de los ciclos pueden ser: 1, 2, 3, 4, 6 y 12.

Elemento con ciclo de longitud 1: $x = 1 \to (1)$

Elemento con ciclo de longitud 12: $x = 2 \to (1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7)$

Puesto que $x = 2$ tiene asociado un ciclo de longitud máxima, podemos ir tomando potencias de 2 para obtener los otros ciclos:

Elemento con ciclo de longitud 2: $x = 2^{12/2} = 2^6 = 64 \equiv 12 \rightarrow (1, 12)$

Elemento con ciclo de longitud 3: $x = 2^{12/3} = 2^4 = 16 \equiv 3 \rightarrow (1, 3, 9)$

Elemento con ciclo de longitud 4: $x = 2^{12/4} = 2^3 = 8 \rightarrow (1, 8, 12, 5)$

Elemento con ciclo de longitud 6: $x = 2^{12/6} = 2^2 = 4 \rightarrow (1, 4, 3, 12, 9, 10)$

Proposición. Descomposición de módulos.

Si p y q son primos diferentes tales que $a^p \equiv a \pmod{q}$ y $a^q \equiv a \pmod{p}$, entonces:

$$a^{pq} \equiv a \pmod{pq}$$

$(a^q)^p \equiv a^q \pmod{p}$ por el Corolario al PTF, y $a^q \equiv a \pmod{p}$ por hipótesis, luego:

Luego $a^{pq} = (a^q)^p \equiv a^q \pmod{p} \equiv a \pmod{p}$, es decir: $p \mid a^{pq} - a$

Con un razonamiento similar llegamos a $q \mid a^{pq} - a$, y por tanto:

$pq \mid a^{pq} - a$, o equivalentemente: $a^{pq} - a \equiv 0 \pmod{pq}$

Ejemplo resuelto.

Demostrar que $2^{340} \equiv 1 \pmod{341}$.

Solución.

Aquí $341 = 11 \cdot 31$, y por otra parte, $2^{10} = 1024 = 31 \cdot 33 + 1$, luego $2^{10} \equiv 1 \bmod(31)$, y por tanto:

$2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1 = 2 \pmod{31}$

Por otro lado, $2^{10} = 1024 = 11 \cdot 93 + 1 \Rightarrow 2^{10} \equiv 1 \pmod{11}$, y por tanto:

$2^{31} = 2(2^{10})^3 \equiv 2(2^{10})^3 \equiv 2 \cdot 1^3 = 2 \pmod{11}$

Y aplicando la proposición anterior: $2^{341} = 2^{11 \cdot 31} \equiv 2 \pmod{341}$, y cancelando un factor 2 llegamos al resultado deseado: $2^{340} \equiv 1 \pmod{341}$

Observación. Los números pseudoprimos y el recíproco del PTF.

El PTF dice que n primo $\Rightarrow$ $2^n \equiv 2 \pmod{n}$, y acabamos de ver que $2^{341} \equiv 2 \pmod{341}$ y sin embargo $341 = 11 \cdot 31$ no es primo, es decir un contraejemplo para el recíproco del PTF.

Este dato es curioso porque $n = 341$ es el primer compuesto tal que $2^n \equiv 2 \pmod{n}$, es decir, sirve como contraejemplo del recíproco del PTF, es decir:

$$n \text{ primo} \Leftrightarrow 2^n \equiv 2 \pmod{n} \text{ para } 2 \le n \le 340$$

Esta es la razón por la que los matemáticos chinos antiguos creyeron, equivocadamente, que $2^n \equiv 2 \pmod{n}$ caracterizaba los números primos.

Los números n tales que $2^n \equiv 2 \pmod{n}$, es decir $n \mid 2^n - 2$ se denominan **pseudoprimos**. Hay infinitos pseudoprimos y los más pequeños son 341, 561, 645 y 1105.

Ejemplo. Como calcular congruencias cuando el módulo no es primo.

Calcular $2018^{2018} \pmod{26}$.

Solución:

Puesto que 26 no es primo, no podemos aplicar directamente el PTF. Puesto que $26 = 2 \cdot 13$, vamos a calcular por separado $2018^{2018} \pmod 2$ y $2018^{2018} \pmod{13}$, y después aplicaremos el Teorema Chino del Residuo para determinar el resultado del enunciado.

Está claro que $2018 \equiv 0 \pmod 2$ y por tanto $2018^{2018} \equiv 0^{2018} = 0 \pmod 2$.

$2018 = 13 \cdot 155 + 3$, luego $13 \nmid 2018$, y por tanto podemos aplicar el PTF:

$2018^{12} \equiv 1 \pmod{13}$.

Por otro lado, $2018 = 12 \cdot 168 + 2$, luego:

$$2018^{2018} = 2018^{12 \cdot 168 + 2} = \left(2018^{12}\right)^{168} 2018^2 \equiv (1)^{168} 2018^2 = 2018^2 \pmod{13}$$

$$2018 = 13 \cdot 155 + 3 \Rightarrow 2018 \equiv 3 \pmod{13} \Rightarrow 2018^2 \equiv 3^2 = 9 \pmod{13}$$

De todo lo anterior tenemos:

$$\begin{cases} 2018^{2018} \equiv 0 \pmod 2 \\ 2018^{2018} \equiv 9 \pmod{13} \end{cases}$$

Y aplicamos el Teorema Chino del Residuo:

$N = 2 \cdot 13 = 26$

$N_1 = 13$

$N_2 = 2$

No hace falta resolver la congruencia $13y_1 \equiv 1 \pmod 2$ pues $b_1 = 0$.

Resolvemos la congruencia $2y_2 \equiv 1 \pmod{13} \Rightarrow y_2 = 7$,

Luego $2018^{2018} = 13 \cdot y_1 \cdot 0 + 2 \cdot 7 \cdot 9 = 126 \pmod{26} = 22 \pmod{26}$

Observación.

Para calcular potencias elevadas con módulos no primos disponemos de dos técnicas: La exponenciación modular optimizada (EMO) (ver 12.2) y el método que acabamos de ver: descomponer el módulo y aplicar el Teorema Chino del Residuo. Es importante dominar estas dos técnicas, pues son la clave para resolver muchísimos problemas de Aritmética. Se propone resolver el siguiente problema mediante las dos técnicas anteriores:

9.1.1 F

Determina los dos últimos dígitos de 1032^{1032}.

HMMT 2009

Y en el siguiente interesante problema podemos observar como aplicar el **Binomio de Newton** para calcular potencias elevadas:

9.1.2 D

Calcula las tres últimas cifras de $2003^{2002^{2001}}$.

CMO 2003 #2

Ejemplo resuelto. Aplicación del PTF a la resolución de congruencias.

Determina una solución de la congruencia $x^{103} \equiv 4 \pmod{11}$

Solución. Puesto que, aplicando el PTF, $x^{10} \equiv 1 \pmod{11}$

$x^{103} = x^{10 \cdot 10+3} = \left(x^{10}\right)^3 x^3 \equiv x^3 \pmod{11}$

Luego hemos reducido nuestro problema a resolver la congruencia $x^3 \equiv x \pmod{11}$

Probando valores $x=1$, $x=2$, $x=3$,... llegamos a $5^3 \equiv 4 \pmod{11}$, y por tanto:

$x \equiv 5 \pmod{11}$

Ejemplo resuelto.

Determina una solución de la congruencia $x^{86} \equiv 6 \pmod{29}$.

Solución.

Aplicando el PTF, sabemos que $x^{28} \equiv 1 \pmod{29}$ para todo x.

Luego $x^{86} = x^{3 \cdot 28+2} = \left(x^{28}\right)^3 x^2 \equiv x^2 \pmod{29}$, luego hemos reducido nuestro problema a resolver la congruencia $x^2 \equiv 6 \pmod{29}$.

Vamos probando valores $x=1$, $x=2$, $x=3$,... hasta llegar a

$x=8 \rightarrow x=64=29 \cdot 2+6 \equiv 6 \pmod{29}$

Luego una solución es $x \equiv 8 \pmod{29}$

Nota: Existe otra solución: $x=21 \rightarrow x^2=441=29 \cdot 15+6 \equiv 6 \pmod{29}$

Para encontrar estas soluciones se puede hacer el siguiente planteamiento:

$6 \equiv 64 \pmod{29}$, y por tanto, la ecuación $x^2 \equiv 6 \pmod{29}$ es equivalente a

$x^2 \equiv 64 \pmod{29}$,

y ahora:

$$x^2 \equiv 64 \pmod{29} \Leftrightarrow x^2-64 \equiv 0 \pmod{29} \Leftrightarrow (x-8)(x+8) \equiv 0 \pmod{29} \Rightarrow \begin{cases} x=8 \\ x=-8 \end{cases}$$

y finalmente: $-8 \equiv 21 \pmod{29}$

9.1.3 F

Aplicando el PTF, determina:

a) $3^{31} \pmod{7}$ b) $2^{35} \pmod{7}$ c) $128^{129} \pmod{17}$

9.1.4 F

Dividimos el número 2^{1000} entre 13. ¿Cuál es el residuo?

AHSME 1972 #31

9.1.5 F

Utilizando el PTF, demuestra que 17 divide a $11^{104}+1$

9.1.6 F

Demuestra que si $(a,35)=1$, entonces $a^{12} \equiv 1 \pmod{35}$

9.1.7 F

Sea $a_1 = 4$, $a_n = 4^{a_{n-1}}$, $n > 1$. Determina el residuo cuando a_{100} se divide entre 7.

9.1.8 F

Demuestra que, si $(a,42) = 1$, entonces $168 = 3 \cdot 7 \cdot 8 \mid a^6 - 1$.

9.1.9 F

Determina $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \pmod 7$

9.1.10 D

En los años 60, tres matemáticos americanos demostraron que una de las conjeturas de Euler era falsa al encontrar un entero positivo n tal que

$$133^5 + 110^5 + 84^5 + 27^5 = n^5$$

Determina n.

AIME 1989 #9

Nota: Se presentan dos soluciones, pero ninguna de las dos es completa: Son argumentos que justifican que un cierto n es el mejor candidato posible.

9.1.11 F

Determina los números primos p para los cuales $29^p + 1$ es múltiplo de p.

9.1.12 D

Determine todos los enteros positivos coprimos con todos los términos de la siguiente sucesión:

$$a_n = 2^n + 3^n + 6^n - 1\ ,\ n \geq 1$$

IMO 2005 #4

9.1.13 MF

Resuelve la congruencia $x^{103} \equiv 4 \pmod{11}$

9.1.14 F

Aplicando el PTF, demuestra que $385 \mid n^{60} - 1$ si $5, 7, 11 \nmid n$.

9.1.15 F

Determina el número de números primos p para los cuales $29^p + 1$ es un múltiplo de p.

Brilliant.org

9.1.16 F

Sea $p \geq 7$ un número primo. Demuestra que el número $\underbrace{11\ldots1}_{p-1}$ es divisible entre p.

9.1.17 D

Sea K el número de secuencias $A_1, A_2, ..., A_n$ en donde n es un entero positivo menor o igual a 10, cada A_i es un subconjunto de $\{1,2,3,...,10\}$ y cada A_{i-1} es un subconjunto de A_i para cada i entre 2 y n, inclusivo. Por ejemplo, $\{\ \}, \{5,7\}, \{2,5,7\}, \{2,5,7\}, \{2,5,6,7,9\}$ es una de estas secuencias, con $n = 5$. Determina el residuo cuando dividimos K entre 10 .

(A) 1 (B) 3 (C) 5 (D) 7 (E) 9

AMC 12A 2023#24

9.1.18 D

Determina todos los números primos p tales que $(x+y)^{19} - x^{19} - y^{19}$ sea un múltiplo de p para cualquier par de enteros positivos x, y.

JBMO 2022 SL NT 4

9.1.19 F

Probar que para todo entero positivo n, $n^{19} - n^7$ es divisible por 30.

OMEFL 2009#4

9.2 La función Phi de Euler. El Teorema de Euler.

Definición. La función Phi de Euler.

Dado un número natural $n>1$, la **función Phi de Euler**, que denotaremos por $\phi(n)$, indica el número de números naturales menores que n y coprimos con n. Definimos $\phi(1)=1$.

Por ejemplo, $\phi(30)=8$ porque el número de naturales coprimos con 30 son 1, 7, 11, 13, 17, 19, 23 y 29. De la misma manera vemos que

$$\phi(2)=1,\phi(3)=2,\phi(4)=2,\phi(5)=4,\ \phi(6)=2,\phi(7)=6...$$

Observamos p es primo si y solo si $\phi(p)=n-1$.

Con Mathematica: "**`EulerPhi[n]`**"

Proposición. La función Phi de Euler mediante el TFA.

Si la descomposición en factores primos de n es $n=p_1^{k_1}p_2^{k_2}...p_r^{k_r}$, entonces:

$$\phi(n)=\left(p_1^{k_1}-p_1^{k_1-1}\right)\left(p_2^{k_2}-p_2^{k_2-1}\right)...\left(p_r^{k_r}-p_r^{k_r-1}\right)=n\cdot\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$$

Ejemplos:

a) $\phi(360)=96$ porque

$$360=2^3 3^2 5\Rightarrow\phi(360)=360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=96$$

b) $\phi(1001)=720$ porque

$$1001=7\cdot11\cdot13\Rightarrow\phi(1001)=1001\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right)=720$$

Propiedad de la función Phi de Euler.

Fijemos un número n y un divisor suyo: Por ejemplo, $n=30$ y $d=5$.

Estudiemos el conjunto $S_d=\{\, m\le n\,,(m,n)=d\,\}$. En la siguiente tabla vemos que $S_5=\{\,5\,,20\,\}$

$1\le m\le n$	$(m,30)$	$(m,30)=5$	$\phi(6)=2$
1	1		
2	2		
3	3		
4	2		
5	5	$5=5\cdot 1$ ✔	1 ✔
6	6		
7	1		
8	2		
9	3		
10	10	$10=5\cdot 2$ ✈	2 ✈
11	1		
12	6		
13	1		
14	2		
15	15	$15=5\cdot 3$ ✈	3 ✈
16	2		
17	1		
18	6		
19	1		
20	10	$20=5\cdot 4$ ✈	4 ✈
21	3		
22	2		
23	1		
24	6		
25	5	$5=5\cdot 5$ ✔	5 ✔
26	2		
27	3		
28	2		
29	1		
30	30	$30=5\cdot 6$ ✈	6 ✈

Consideremos ahora $n/d=6$ y $\phi(6)$. El conjunto de números menores que 6 y coprimos con 6 es $\{1,5\}$, luego $\phi(6)=2$.

Vemos que existe una biyección perfecta entre S_5 y los coprimos de 6, y por tanto

$$|S_d|=\phi(n/d)$$

Por otro lado, todo número $m\le n$ pertenece a algún S_d con $d\,|\,n$, y por tanto:

$$n=\sum_{d|n}|S_d|=\sum_{d|n}\phi(n/d)$$

Existe también una biyección $d\,|\,n\leftrightarrow\frac{d}{n}\,|\,n$ y por tanto llegamos a la siguiente propiedad:

$$n=\sum_{d|n}\phi(d)$$

Teorema. El Teorema de Euler.

$$a^{\phi(n)} \equiv 1 \pmod{n} \text{ si } (a,n)=1$$

Observación: La condición $(a,n)=1$ es necesaria, pues si $(a,n)>1$, ya vimos en el capítulo 8 que la congruencia $ax \equiv 1 \pmod{n}$ no tiene solución, y por tanto no puede existir ningún k tal que $a^k \equiv 1 \pmod{n}$, pues en ese caso $x = a^{k-1}$ sería solución de la congruencia $a\,x \equiv 1 \pmod{n}$.

Nota histórica. La primera demostración del PTF fue dada por Euler en 1736. El propio Euler presentó en 1760 este teorema, que es una generalización del PTF porque si n es primo entonces $\phi(n) = p-1$, y $(a,p)=1 \Rightarrow p \nmid a$.

Ejemplo.

Tomando $n=30$ y $a=11$, $\phi(30)=8$ y $11^8 \equiv 1 \pmod{30}$

En efecto, $11^2 = 121 \equiv 1 \pmod{30} \Rightarrow 11^8 = \left(11^2\right)^4 \equiv 1^4 = 1 \pmod{30}$

Ejemplo 1.

Determina el residuo de 7^{1000} entre 24 aplicando el Teorema de Euler.

En primer lugar vemos que los divisores de 24 son 1, 2, 3, 4, 6, 8, 12 y 24, luego $\phi(24)=8$.

Luego, aplicando el Teorema de Euler, puesto que $(7,24)=1$, $7^8 \equiv 1 \pmod{24}$

Ahora, puesto que $1000 = 125 \cdot 8$, $7^{1000} = \left(7^8\right)^{125} \equiv 1^{125} = 1 \pmod{24}$

Ejemplo 2.

Determina los dos últimos dígitos de la expresión decimal de 3^{256}.

Solución.

Está claro que este problema implica estudiar $3^{256} \pmod{100}$, y aquí nos puede ayudar el Teorema de Euler:

$\phi(100) = \phi\left(2^2 5^2\right) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40$, y puesto que $(3,100)=1$, podemos aplicar el Teorema de Euler: $3^{40} \equiv 1 \pmod{100}$

Luego $3^{256} = 3^{406+16} \pmod{100} = \left(3^{40}\right)^6 3^{16} \pmod{100} = 3^{16} \pmod{100}$.

$3^8 = 6561 \equiv 61 \bmod(100) \Rightarrow 3^{16} = 3^8 3^8 \equiv 61 \cdot 61 = 3721 \equiv 21 \bmod(100)$

Por lo tanto, el número 3^{256} acaba en "21".

Ejemplo 3.

Determina $2^{98} \pmod{33}$, mediante dos técnicas: a) PTF & TCR y b) Teorema de Euler.

Solución:

a) Aplicando el PTF:

$$2^2 \equiv 1 \pmod 3 \Rightarrow 2^{98} = \left(2^2\right)^{49} \equiv 1^{49} = 1 \pmod 3$$

$$2^{10} \equiv 1 \pmod{11} \Rightarrow 2^{98} = 2^{90} \cdot 2^8 = \left(2^{10}\right)^9 \cdot 2^8 \equiv 2^8 = 256 \equiv 3 \pmod{11}$$

Así pues, debemos resolver el sistema

$$x \equiv 1 \pmod 3$$

$$x \equiv 3 \pmod{11}$$

Este sistema lo resolveremos aplicando el TCR:

$$\left.\begin{array}{l} 11y_1 \equiv 1 \pmod 3 \Leftrightarrow 2y_1 \equiv 1 \pmod 3 \Leftrightarrow y_1 = 5 \\ 3y_2 \equiv 1 \pmod{11} \Leftrightarrow y_2 = 4 \end{array}\right\} \Rightarrow x = 11 \cdot 5 \cdot 1 + 3 \cdot 4 \cdot 3 = 91 \equiv 25 \pmod{33}$$

b) Aplicando Teorema de Euler.

En primer lugar, $\phi(33) = 3 \cdot 11\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{11}\right) = 2 \cdot 10 = 20$.

Luego, aplicando el Teorema de Euler, $2^{20} \equiv 1 \pmod{33}$, y por tanto:

$$2^{98} = 2^{100} \cdot \left(2^2\right)^{-1} \equiv \left(2^{20}\right)^5 \cdot \left(2^2\right)^{-1} \equiv 4^{-1} \pmod{33}$$

Mediante cualquiera de las técnicas ya estudiadas determinamos el inverso modular de 4 y llegamos a $2^{98} \equiv 4^{-1} \equiv 25 \pmod{33}$.

9.2.1 F

¿Para cuántos enteros i, cumpliendo $1 \le i \le 1000$, existe un entero j, cumpliendo $1 \le j \le 1000$, tal que i es un divisor de $2^j - 1$?

9.2.2 M

Determina los ocho últimos dígitos de la expansión binaria de 27^{1986}.

9.2.3 D

Determina los tres últimos dígitos de $2008^{2007^{2006^{\cdots^{2^1}}}}$

Nota: $2008^{2007^{2006^{\cdots^{2^1}}}}$ se define recursivamente:

$$a_1 = 1,\ a_2 = 2^{a_1},\ a_3 = 3^{a_2},\ \ldots,\ a_{2008} = 2008^{\,a_{2007}}$$

9.2.4 [D]

Definimos $f(x)=x^{x^{x^x}}$. Determina los dos últimos dígitos de

$$f(17)+f(18)+f(19)+f(20)$$

PuMAC 2008

Nota: $f(x)$ se define recursivamente: $f_1(x)=x$, $f_2(x)=x^{f_1(x)}$,..., $f(x)=f_4(x)=x^{f_3(x)}$.

Indicación: Si $(a,n)=1$, entonces $a^b \equiv a^{b \bmod \phi(n)} \pmod n$ y podemos reducir el cálculo a determinar $b \pmod{\phi(n)}$.

9.2.5 [F]

Encontrar las tres últimas cifras del número 7^{2014}

OMEFL 2014 #2

9.2.6 [F]

Determina el número de enteros $1 \le i \le 1000$ para los cuales existe un entero $1 \le j \le 1000$ tal que i es divisor de 2^j-1.

Brilliant.org

9.2.7 [F]

Sea $p>5$ un número primo. Demuestra que $p^8 \equiv 1 \pmod{240}$.

9.2.8 [MD] **Problema solucionado paso a paso en vídeo**

Determinar todas las parejas (a, b) de enteros positivos para las que existen enteros positivos g y N tales que

$$mcd\left(a^n+b, b^n+a\right)=g$$

se cumple para todo $n \ge N$.
(Nota: $mcd(x,y)$ denota el máximo común divisor de x e y.)

IMO 2024 #2

Solución: https://youtu.be/MZD1hkIRBd4

9.3 Orden de un entero.

Definición. Orden de un entero.

Observando las tablas del apartado 9.1 vemos que si $(a,n)=1$, entonces siempre existe un $1 \le k \le n$ tal que $a^k \equiv 1 \pmod{n}$.

En efecto, consideremos la secuencia

$$\left(a^0, a^1, a^2, a^3, ..., a^n \right)$$

Esta secuencia consta de $n+1$ valores, y solo hay n valores diferentes en Z_n, luego forzosamente dos de ellos deberán ser iguales:

$$a^i \equiv a^j \pmod{n} \text{ para ciertos } 0 \le i < j \le n$$

Consideremos el valor $q = j - i \Rightarrow j = q + i$ y por tanto

$$a^i \equiv a^j = a^{q+i} = a^q \cdot a^i \pmod{n}$$

Puesto que $(a,n)=1 \Rightarrow (a^i,n)=1$, podemos cancelar el factor a^i en la igualdad anterior (es decir, multiplicaremos ambos lados por el inverso de a^i) para deducir que

$$1 \equiv a^q \pmod{n}$$

Definimos el **orden de un entero** a **módulo** n, y escribiremos $ord_n(a)$, como el menor valor k tal que $a^k \equiv 1 \pmod{n}$. Acabamos de ver que si $(a,n)=1$ este valor siempre existe.

Con Mathematica:

```
In[1]:= MultiplicativeOrder[3, 7]
        |orden multiplicativo
Out[1]= 6

In[2]:= MultiplicativeOrder[2, 5]
        |orden multiplicativo
Out[2]= 4
```

El Teorema de Euler indica que si $(a,n)=1$, la secuencia $\left(a, a^2, a^3, a^4, ...\right)$ siempre alcanza el 1 (y por lo tanto se vuelve periódica), y lo alcanza en $a^{\phi(n)}$. Naturalmente, $\phi(n)$ no es necesariamente el primer número k para el cual $a^k \equiv 1$.

Ejemplos.

$3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1 \pmod{7} \Rightarrow ord_7(3) = 6$.

$ord_5(2) = 4$ pues $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$, $2^4 = 16 \equiv 1 \pmod{5}$.

$ord_{12}(5) = 2$ pues $5^1 \equiv 5$, $5^2 = 25 = 2 \cdot 12 + 1 \equiv 1 \pmod{12}$.

Observación.

No todos los números tienen un definido un orden. Por ejemplo, si $n \mid a$, entonces $a^k \equiv 0 \pmod{n}$ para todo k.

El siguiente corolario nos indica cuando un entero tendrá un orden asociado.

Corolario.

Dado un entero $n>1$, $a \in Z$ tendrá orden módulo n si y solo si $(a,n)=1$.

Demostración. Si $(a,n)=1$, por la proposición anterior existirá un $1 \le k \le n$ tal que $a^k \equiv 1 \pmod{n}$, luego por el Principio de la buena ordenación, existirá un mínimo k cumpliendo tal condición, es decir, el número a tendrá un orden asociado.

Supongamos ahora que existe un entero positivo m tal que $a^m \equiv 1 \pmod{n}$. Entonces existirá un entero s tal que

$$a^m + sn = 1 \Rightarrow a \cdot a^{m-1} + sn = 1$$

Esta última expresión es una combinación lineal de a y n, luego

$$(a,n) \mid a \cdot a^{m-1} + sn = 1 \Rightarrow (a,n) = 1$$

Teorema. Teorema fundamental del orden.

Supongamos que $(a,n)=1$, y sea $d = ord_n(a)$.

Entonces, para cualquier entero k, $a^k \equiv 1 \pmod{n} \Leftrightarrow d \mid k$.

Demostración.

Supongamos que $a^k \equiv 1 \pmod{n}$. Entonces $k \ge d$ por definición de orden, y por tanto $k = dq + r$ para cierto $0 \le r < d$. Luego

$$1 = a^k = a^{dq+r} = a^{dq} \cdot a^r = \left(a^d\right)^q \cdot a^r \equiv 1^q \cdot a^r = a^r \pmod{n}$$

Pero $0 \le r < d$ y la única posibilidad que no contradiga la definición de orden es $r = 0$, y por tanto $k = dq \Rightarrow d \mid k$, tal y como queríamos ver.

Supongamos ahora que $d \mid k$. Entonces $k = dq$ y por tanto

$$a^k = a^{dq} = \left(a^d\right)^q \cdot a^r \equiv 1^q = 1 \pmod{n}$$

Corolario.

Supongamos que $(a,n)=1$, y sea $d = ord_n(a)$. Entonces

$$a^i \equiv a^j \pmod{n} \Leftrightarrow i \equiv j \pmod{d}$$

Demostración. Podemos suponer, sin pérdida de generalidad, que $i > j$.

Supongamos que $i \equiv j \pmod{d} \Rightarrow i = qd + j$, y por tanto

$$a^i = a^{qd+j} = \left(a^d\right)^q a^j \equiv 1^q a^j = a^j \pmod{n}$$

Supongamos ahora que $a^i \equiv a^j \pmod{n}$. Entonces tomando $q = i - j > 0$ y cancelando términos llegamos a $1 \equiv a^q = a^{i-j} \pmod{n} \Rightarrow d \mid i - j$ por el Teorema anterior, luego $d \mid i - j \Rightarrow i \equiv j \pmod{d}$.

Observación.

Este corolario nos dice que la sucesión de potencias a^k se va repitiendo en ciclos de longitud $d = ord_n(a)$. En particular, podemos aplicar este hecho a la función Phi de Euler: $ord_n(a) \mid \phi(n)$

Ejercicio resuelto.

Determina $ord_{33}(2)$

Solución: Vemos que $2^5 = 32 \equiv -1 \left(ord\ 33\right) \Rightarrow 2^{10} = \left(2^5\right)^2 \equiv \left(-1\right)^2 = 1 \left(ord\ 33\right)$. Luego, por el corolario anterior, $ord_{33}(2)$ debe ser un divisor de 10. Vamos probando, uno por uno, todos los divisores:
$2^1 = 2 \not\equiv 1 \left(\text{mod } 33\right)$, $2^2 = 4 \not\equiv 1 \left(\text{mod } 33\right)$, $2^5 = 32 \not\equiv 1 \left(\text{mod } 33\right)$, así que solo puede ser $2^{10} \equiv 1 \left(\text{mod } 33\right)$, y la solución es 10.

Problema resuelto.

Determina todos los enteros positivos n tales que $2^n - 1$ sea divisible entre 7.

IMO 1967 #1 (apartado a)

Solución: $7 \mid 2^n - 1 \Leftrightarrow 2^n - 1 \equiv 0 \ (\text{mod } 7) \Leftrightarrow 2^n \equiv 1 \ (\text{mod } 7)$
Puesto que $(2,7) = 1$, podemos aplicar el Teorema anterior:
$2^n \equiv 1 \ (\text{mod } 7) \Leftrightarrow ord_7(2) \mid n$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8 \equiv 1 \ (\text{mod } 7) \Rightarrow ord_7(2) = 3$
Luego, finalmente, $7 \mid 2^n - 1 \Leftrightarrow 3 \mid \text{n}$, es decir, para todos los múltiplos de 3.

Corolario.

Dados p primo y a entero con $p \nmid a$, entonces $ord_n(a) \mid p - 1$

Demostración. Puesto que p es primo y $p \nmid a$, podemos aplicar el PTF para garantizar que $a^{p-1} \equiv 1 \ (\text{mod } p)$, y aplicar ahora el teorema anterior.

Ejemplo.

Determinar $ord_{11}(8)$.

Solución.
Puesto que $11 \nmid 8$, aplicar el corolario anterior para asegurar que $ord_{11}(8) \mid 10$.
$ord_{11}(8) = 2$ no puede ser pues $8^2 = 64 \equiv 9 \not\equiv 1 \ (\text{mod } 11)$.
$ord_{11}(8) = 5$ tampoco puede ser:
$8^2 \equiv 9 \ (\text{mod } 11)$ y $8^3 = 512 \equiv 6 \ (\text{mod } 11)$, luego
$8^5 = 8^2 8^3 \equiv 9 \cdot 6 = 54 \ (\text{mod } 11) \equiv 10 \ (\text{mod } 11)$. Luego solo nos queda $ord_{11}(5) = 10$.

Ejemplo resuelto.

Determina $ord_{13}(2)$.

Solución. $\phi(13) = 12 \Rightarrow ord_{13}(2) \in \{1,2,3,4,6,12\}$
$2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16 \equiv 3 \ (\text{mod } 13)$, $2^6 = 32 \equiv 12 \ (\text{mod } 13)$, luego solo puede ser $ord_{13}(2) = 12$.

Problema resuelto.

Determina la última cifra de 7^{83}.

Solución. Está claro que debemos determinar $7^{83} \pmod{10}$.

$7^0 = 1 \equiv 1 \pmod{10}$, $7^2 = 49 \equiv -1 \pmod{10} \Rightarrow 7^4 \equiv (-1)^2 = 1 \pmod{10}$

Y puesto que el orden tiene que ser divisor de 10, solo puede ser $ord_{10} 7 = 4$.

Por otro lado, $83 \equiv 3 \pmod{4}$, luego $7^{83} \equiv 7^3 \equiv (-1) \cdot 7 \equiv 3 \pmod{10}$, y por tanto la última cifra es 3.

Problema resuelto.

Determina $ord_{29}(10)$.

Solución. Puesto que 29 es primo, aplicando el PTF, $10^{28} \equiv 1 \pmod{29}$, luego $ord_{29}(10) \mid 28$.

Vamos probando, uno por uno, todos los divisores de 28:

$10^1 = 10 \not\equiv 1 \pmod{29}$, $10^2 = 100 \equiv 13 \not\equiv 1 \pmod{29}$, $10^4 \equiv 24 \not\equiv 1 \pmod{29}$...

Finalmente $10^{28} \equiv 1 \pmod{29}$, y por tanto $ord_{29}(10) = 28$.

Así pues:

$$10^{28} \equiv 1 \pmod{29} \Rightarrow 10^{28} - 1 = \underbrace{99...99}_{28 nueves} \equiv 0 \pmod{29} \Rightarrow 29 \mid \underbrace{99...99}_{28 nueves}$$

Pero $29 \nmid \underbrace{99...99}_{n \text{ nueves}}$ si $n < 28$.

Ejercicio resuelto.

a) Determina, de forma directa, $ord_{17} 2$.

b) Aplicando el apartado anterior, calcula $2^{20} \pmod{17}$ y $2^{1024} \pmod{17}$.

Solución:

a) en módulo 17, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 16 \equiv -1$, $2^5 \equiv -2$, $2^6 \equiv -4$, $2^7 \equiv -8$, $2^8 \equiv -(-1) \equiv 1$. Así pues, $ord_{17} 2 = 8$.

b) $2^{20} = 2^{8+8+4} = 2^8 \cdot 2^8 \cdot 2^4 \equiv 2^4 \equiv -1 \pmod{17}$, $2^{1024} = 2^{8 \cdot 128} = \left(2^8\right)^{128} \equiv 1^{128} \equiv 1 \pmod{17}$

Problema resuelto.

Determina el menor factor primo impar de 2019^8+1

AIME I 2019 #14

Solución.

Buscamos el menor número primo p tal que $p \mid 2019^8+1$

$$p \mid 2019^8+1 \Leftrightarrow 2019^8+1 \equiv 0 \pmod{p} \Leftrightarrow 2019^8 \equiv -1 \pmod{p}$$

Entonces, elevando al cuadrado ambos lados, $2019^{16} \equiv 1 \pmod{p}$

Pero $2019^{16} \equiv 1 \pmod{p} \Rightarrow ord_p(2019) \in \{1,2,4,8,16\}$

Sin embargo, $ord_p(2019) \in \{1,2,4,8\} \Rightarrow 2019^8 \equiv 1 \pmod{p}$ y no -1, como queríamos, luego deducimos que $ord_p(2019) = 16$.

Puesto que $ord_p(2019) \mid \phi(p)$, $\phi(p)$ será un múltiplo de 16.

Puesto que por hipótesis p es primo, $\phi(p) = p \cdot \left(1-\frac{1}{p}\right) = p-1$

Y por tanto $p \equiv 1 \pmod{16}$. Los dos primeros primos que cumplen $p \equiv 1 \pmod{16}$ son 17 y 97.

Sin embargo, $2019^8 \not\equiv -1 \pmod{17}$, pero $2019^8 \equiv -1 \pmod{97}$, luego la solución es 97.

Fuente de esta solución: artofproblemsolving.com

Problema resuelto.

Determina el menor entero positivo n tal que, cuando ese escribe 3^n en base 143, sus últimas dos cifras en dicha base son 01.

AIME I 2018 #11

Solución:

Sabemos que decir que la expresión de 3^n en base 143 es $\overline{...d_3d_2d_101}_{143}$ es equivalente a

$$3^n = 1+0\cdot 143 + d_1\cdot 143^2 + d_2\cdot 143^3 + ... = 1+143^2(d_1+d_2\cdot 143+...) \Leftrightarrow 3^n \equiv 1 \left(\text{mod } 143^2\right)$$

Así pues, en este problema nos piden resolver la congruencia $3^n \equiv 1 \bmod \left(143^2\right)$ con solución n mínima, es decir, determinar el orden de 3 módulo 143^2.

Es importante remarcar que nos piden n mínimo, pues el Teorema de Euler nos garantiza que $3^{\phi(143^2)} \equiv 1 \left(\text{mod } 143^2\right)$ puesto que $\left(3,143^2\right)=1$, pero en este caso $\phi\left(143^2\right)=17160$ y veremos que no es el valor mínimo posible.

$143 = 11\cdot 13 \Rightarrow 143^2 = 11^2\cdot 13^2$, y puesto que $\left(11^2,13^2\right)=1$, para resolver la congruencia $3^n \equiv 1\left(\text{mod } 11^2\cdot 13^2\right)$ será suficiente resolver las congruencias $3^a \equiv 1\left(\text{mod } 11^2\right)$ y $3^b \equiv 1\left(\text{mod } 13^2\right)$ por separado.

Paso 1. Resolvemos la congruencia: $3^a \equiv 1 \pmod{11^2}$
Esta es sencilla. Se puede encontrar por tanteo:

$3^1 = 3 \equiv 3 \pmod{121}$ $\qquad$ $3^2 = 9 \equiv 9 \pmod{121}$

$3^3 = 27 \equiv 27 \pmod{121}$ $\qquad$ $3^4 = 81 \equiv 81 \pmod{121}$

$3^5 = 243 = 2 \cdot 121 + 1 \equiv 1 \pmod{121}$

El valor mínimo es $a = 5$.

Paso 2. Resolvemos la congruencia: $3^b \equiv 1 \pmod{13^2}$. Esta es mucho más complicada.

Paso 2.1. Por tanteo ("*bash*"). Si lo hacemos por tanteo nos vamos a pasar un buen rato calculando potencias hasta llegar al exponente 39 para encontrar $3^{39} \equiv 1 \pmod{13^2}$:

1→3	2→9	3→27	4→81	5→74
6→53	7→159	8→139	9→79	10→68
11→35	12→105	13→146	14→100	15→131
16→55	17→165	18→157	19→133	20→61
21→14	22→42	23→126	24→40	25→120
26→22	27→66	28→29	29→87	30→92
31→107	32→152	33→118	34→16	35→48
36→144	37→94	38→113	39→1	

Paso 2.2. Aplicando el Teorema de Euler. Una indicación nos la puede dar la función Phi de Euler: $\phi(13^2) = 2 \cdot 3 \cdot 13$, luego el orden de 3 módulo 156 será un divisor de $156 = 2 \cdot 3 \cdot 13$. Probando divisores encontramos la solución $39 = 3 \cdot 13$.

Paso 2.3. Aplicando el Teorema del binomio.
Observamos que $3^b \equiv 1 \pmod{13^2} \Rightarrow 3^b \equiv 1 \pmod{13}$.
En efecto: $3^b \equiv 1 \pmod{13^2} \Rightarrow 3^b = 13^2 k + 1 = 13(13k) + 1 \Rightarrow 3^b \equiv 1 \pmod{13}$

Y la congruencia $3^b \equiv 1 \pmod{13}$ tiene fácil solución: $3^3 = 27 = 2 \cdot 13 + 1 \equiv 1 \pmod{13}$.
Así pues, cualquier solución de $3^b \equiv 1 \pmod{13}$ será múltiple de 3.
Llegados a este punto podríamos aplicar la estrategia 2.2 anterior para llegar a la solución, pero en su lugar vamos a aplicar el desarrollo binomial.

El número b buscado será múltiplo de 3: $b = 3c$ para cierto entero c, con lo que la congruencia se transforma en:

$$3^{3c} \equiv 1 \pmod{13^2} \Leftrightarrow (3^3)^c \equiv 1 \pmod{13^2} \Leftrightarrow 27^c \equiv 1 \pmod{13^2}$$

Ahora aplicamos el desarrollo binomial:

$$27 = 2 \cdot 13 + 1 \Rightarrow 27^c = (2 \cdot 13 + 1)^c =$$

$$= \binom{c}{0}(2 \cdot 13)^c 1^0 + \binom{c}{1}(2 \cdot 13)^{c-1} 1^1 + \ldots + \binom{c}{c-1}(2 \cdot 13)^1 1^{c-1} + \binom{c}{c}(2 \cdot 13)^0 1^c$$

Y observamos que, trabajando módulo 13^2, cualquier potencia 13^c con $c \geq 2$ será (congruente con) cero.

Así pues, a todos los efectos prácticos:

$$27^c = \binom{c}{c-1}(2\cdot 13)^1 1^{c-1} + \binom{c}{c}(2\cdot 13)^0 1^c = c\cdot 26 + 1$$

Y por tanto, la congruencia exponencial $27^c \equiv 1 \pmod{13^2}$ se convierte en la congruencia lineal

$$26c + 1 \equiv 1 \pmod{13^2}$$

Que se resuelve fácilmente:

$$26c + 1 \equiv 1 \pmod{13^2} \Leftrightarrow 26c \equiv 0 \pmod{13^2} \Leftrightarrow 2\cdot 13c \equiv 0 \pmod{13^2}$$

Para que esta última congruencia se cumpla, es necesario y suficiente que c sea múltiplo de 13.

Así pues, finalmente llegamos a un resultado múltiplo de 3 y múltiplo de 13, y el valor mínimo posible es $c = 3\cdot 13 = 39$.

Paso 3. Juntamos las dos congruencias:

Hemos obtenido $3^5 \equiv 1 \bmod(11^2)$ y $3^{39} \equiv 1 \bmod(13^2)$, luego tomando el mínimo común múltiplo de ambos exponentes: $[5,39] = 5\cdot 39 = 195$, tendremos, aplicando 7.5d:

$$\left.\begin{array}{l} 3^{195} = 3^{5\cdot 39} = (3^5)^{39} \equiv 1^{39} = 1 \bmod(11^2) \\ 3^{195} = 3^{39\cdot 5} = (3^{39})^5 \equiv 1^5 = 1 \bmod(13^2) \\ (11^2, 13^2) = 1 \end{array}\right\} \Rightarrow 3^{195} \equiv 1 \bmod(11^2\cdot 13^2)$$

Que será el valor mínimo posible pues en todos los pasos hemos obtenido los valores mínimos posibles. La solución del problema es 159.

Fuentes:
https://artofproblemsolving.com/wiki/index.php/2018_AIME_I_Problems/Problem_11
https://youtu.be/e7JGgykuK3w Analyzing the Expression in Mod 143² (2018 AIME I Prob 11) "LetsSolveMathProblems"
https://youtu.be/b_Z_OGfyJyw 2018 AIME I Problem #11 ("Osman Nal")

9.3.1 M

Determina el número de enteros positivos múltiples de 1001 que se pueden expresar de la forma

$$10^j - 10^i$$

con i , j enteros cumpliendo $0 \leq i < j \leq 99$.

AIME 2001

9.3.2 F

Demuestra que, si p es un número primo, todo divisor primo de $2^p - 1$ es mayor que p.

9.4 Problemas.

9.4.1 MD

Demuestra que existen infinitas parejas (a,b) de números enteros positivos distintos y relativamente coprimos $a>1$ y $b>1$ tales que a^b+b^a es divisible entre $a+b$.

USAMO 2017 #1

9.4.2 MD

Sea S el conjunto de todos los números racionales que se pueden escribir como decimales periódicos de la forma $0.\overline{abcd}$, donde al menos uno de los dígitos a,b,c,d no es cero. Sea N el número de numeradores distintos que se encuentran en S cuando estos decimales se escriben en forma de fracción irreducible. Por ejemplo, 4 y 410 aparecen en S porque $0.\overline{3636}=\frac{4}{11}$ y $0.\overline{1230}=\frac{410}{3333}$. Determina el residuo cuando N se divide entre 1000.

AIME I 2022 #13

9.4.3 MD

Dado que $20^{22}+1$ tiene exactamente 4 divisores primos $p_1<p_2<p_3<p_4$, determina p_1+p_2.

SMT 2022 Discrete #8

9.4.4 MF

Seleccionamos al azar un entero N en el rango $1\le N\le 2020$. Determina la probabilidad que el residuo al dividir N^{16} entre 5 sea 1.

(A) 1/5 (B) 2/5 (C) 3/5 (D) 4/5 (E) 1

AMC 10B 2017 #14

9.4.5 MD

Determina el mayor entero positivo n que divide p^6-1 para todos los números primos $p>7$.

JBMO 2016 SL N #1

10 Ecuaciones diofánticas.

Las ecuaciones diofánticas son aquellas ecuaciones en las que solo son admitidas soluciones enteras, y son un problema transversal en la teoría de números. Estas ecuaciones ya han aparecido a lo largo de todo este libro como aplicación de las diversas técnicas presentadas, en sus respectivos apartados. Aquí se ofrece una presentación algo más sistemática de algunos modelos concretos de ecuaciones diofánticas, así como de algunas técnicas que pueden ser útiles para su resolución y un recopilatorio de algunas ecuaciones diofánticas aparecidas en el contexto de pruebas olímpicas.

10.1 Ecuaciones diofánticas lineales.

Definición. Ecuaciones diofánticas lineales.

Son las ecuaciones diofánticas que tienen la forma $a_1 x_1 + a_2 x_2 + ... + a_n x_n = b$, con $\{a_i\}$ enteros.

Ejemplo 1.

Por ejemplo, la ecuación $3x + 6y = 18$ tiene infinitas soluciones:

$x = 4$, $y = 1 \rightarrow 3 \cdot 4 + 6 \cdot 1 = 18$

$x = -6$, $y = 6 \rightarrow 3 \cdot (-6) + 6 \cdot 6 = 18$

$x = 10$, $y = -2 \rightarrow 3 \cdot 10 + 6 \cdot (-2) = 18$

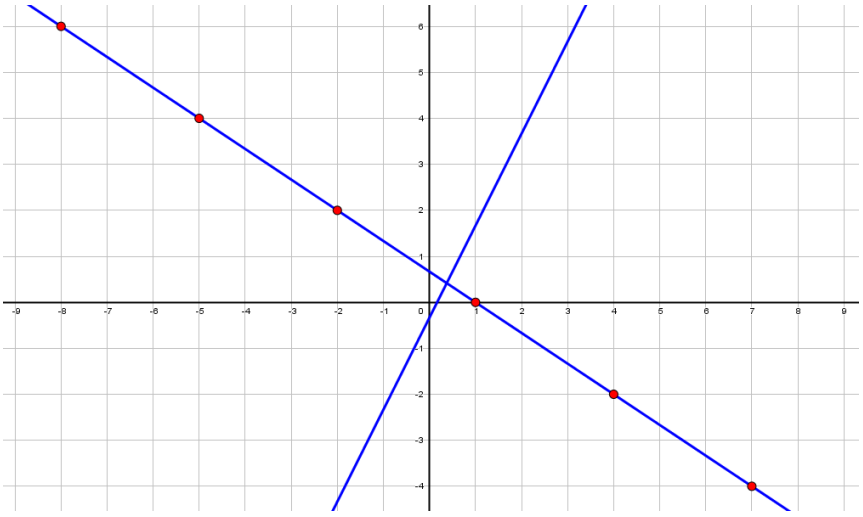
En general, cualquier valor $x = 2k$, $y = 3 - k \rightarrow 3(2k) + 6(3-k) = 6k + 18 - 3k = 18$

Sin embargo, la ecuación $2x + 10y = 17$ no tiene solución: Para cualquier x, y, la parte izquierda de la ecuación será par, mientras que la parte derecha es un impar.

Ejemplo 2.

Consideremos las siguientes ecuaciones diofánticas: $2x + 3y = 2$ y $6x - 3y = 1$.

Observamos que la primera tiene infinitas soluciones (-5,4), (-2,2), (1,0), (4,-2), (7,-4)… mientras que no parece existir ninguna solución para la segunda:



Esto se puede formalizar en el siguiente Teorema:

Teorema fundamental de las ecuaciones diofánticas lineales.

Una ecuación diofántica lineal $ax+by=c$ tendrá solución si y solo si $(a,b)\,|\,c$.

Si (x_0, y_0) es una solución particular de esta ecuación, entonces todas las soluciones son de la forma

$$x = x_0 + \left(\frac{b}{d}\right)k,\ y = y_0 - \left(\frac{a}{d}\right)k \text{ para cualquier } k \text{ entero.}$$

Ejemplo resuelto.

Resuelve la ecuación diofántica $172x+20y=1000$

Solución. $d=(172,20)=4$, y $4\,|\,1000$, luego esta ecuación tiene solución.

Probando números vemos que $172\cdot 5+20\cdot 7=1000$, luego $x_0=5, y_0=7$ es una solución particular de la ecuación.

Por el Teorema anterior, las soluciones de esta ecuación son todas las parejas de la forma

$$x = 5+\left(\frac{20}{4}\right)k = 5+5k = 5(1+k),\ y = 7-\left(\frac{172}{4}\right)k = 7-43k \text{ , con } k\in Z$$

o equivalentemente, tomando $q=1+k$,

$$x=5q,\ y=7-43(q-1)=7-43q+43=50-43q, \text{ con } q\in Z.$$

10.1.1 [F]

Resuelve la ecuación diofántica $7x-9y=3$

10.1.2 [F]

Un cliente compra una docena de piezas de fruta, manzanas y naranjas, por 1.32€. Si una manzana cuesta 3 céntimos más que una naranja, y se compraron más manzanas que naranjas, cuantas piezas de cada fueron compradas?

Resolución de ecuaciones diofánticas lineales mediante el Algoritmo de Euclides.

El Algoritmo de Euclides para el cálculo del máximo común divisor de dos números mediante sucesivas divisiones nos permite resolver ecuaciones diofánticas lineales. Lo veremos con el siguiente ejemplo:

Resuelve la ecuación diofántica $2173x+2491y=53$

Solución. Aplicamos el algoritmo de Euclides:

$$\left.\begin{array}{l}2491=1\cdot 2173+318\\2173=6\cdot 318+265\\318=1\cdot 265+53\\265=5\cdot 53+0\end{array}\right\} \Rightarrow (2173,2491)=53, \text{ y claramente } 53\,|\,53, \text{ luego hay solución.}$$

Deshaciendo los pasos del algoritmo de Euclides:

$$\left.\begin{array}{l}53=318-1\cdot 265\\265=2173-6\cdot 318\\318=2491-1\cdot 2173\end{array}\right\} \Rightarrow 53=318-1\cdot 265=2491-1\cdot 2173-1\cdot(2173-6\cdot 318)=$$

$$=2491-1\cdot 2173-2173+6\cdot(2491-1\cdot 2173)=$$

$$=2491-1\cdot 2173-2173+6\cdot 2491-6\cdot 2173=$$

$$=7\cdot 2491-8\cdot 2173$$

Luego $x=-8, y=7$ es una solución de la ecuación diofántica del enunciado.

El conjunto de soluciones de la ecuación serán las parejas de la forma:

$$x=-8+\frac{2491}{53}k=-8+47k\,,\ y=7-\frac{2173}{53}k=7-41k$$

10.1.3 [F]

Resuelve la ecuación diofántica $858x+253y=33$ mediante el algoritmo de Euclides.

10.1.4 [F]

Resuelve la ecuación diofántica $258x+147y=369$

10.1.5 [F]

Resuelve la ecuación diofántica $60x+33y=9$

10.1.6 [F]

Las medidas (en grados) de los ángulos interiores de un hexágono convexo forman una sucesión aritmética de enteros positivos. Sea m^o la medida del mayor de los ángulos interiores de este hexágono. El mayor valor posible de m^o es

(A) 165º (B) 167º (C) 170º (D) 175º (E) 179º

AHSME 1991 #12

10.1.7 [F]

Determina un número que, cuando se divide entre 10, deja un residuo de 9, cuando se divide entre 9 deja un residuo de 8, entre 8 el residuo es 7, y así sucesivamente, hasta que, finalmente, cuando se divide entre 2, deja un residuo de 1.

AHSME 1951 #37

10.1.8 [F]

Resuelve la ecuación diofántica lineal $19x+17y=1$.

10.2 Ternas pitagóricas.

Definición. Terna Pitagórica.

Definimos por **Terna Pitagórica** las ternas (x, y, z) de números enteros solución de la ecuación diofántica

$$x^2 + y^2 = z^2$$

Las ternas pitagóricas son un caso particular de la llamada **Ecuación de Fermat**:

$$x^n + y^n = z^n$$

Que fue resuelta por **Wiles** en 1994, más de 350 años después de que este problema fuera propuesto, demostrando que para $n > 2$ no existen soluciones que no sean la trivial $x = y = z = 0$.

Lema.

Si (x, y, z) es una terna pitagórica y $d = mcd(x, y, z)$, entonces:

a) $d = mcd(x, y) = mcd(y, z) = mcd(x, z)$

b) Si escribimos $x = d\,x'$, $y = d\,y'$, $z = d\,z'$, entonces (x', y', z') también es una terna pitagórica.

Demostración.

a) Demostraremos la primera igualdad. Está claro que

$$d \mid x, d \mid y, d \mid z \Rightarrow d \mid x, d \mid y$$

Por otro lado:

$$\left.\begin{array}{l} d \mid x \Rightarrow d^2 \mid x^2 \\ d \mid y \Rightarrow d^2 \mid y^2 \end{array}\right\} \Rightarrow d^2 \mid x^2 + y^2 = z^2 \Rightarrow d^2 \mid z^2 \Rightarrow d \mid z$$

b) Es trivial.

Definición. Terna pitagórica primitiva.

Una terna pitagórica (x, y, z) se dice que es primitiva si $mcd(x, y, z) = 1$, o equivalentemente $mcd(x, y) = mcd(y, z) = mcd(x, z) = 1$

Lema.

Sea (x, y, z) una terna pitagórica primitiva. Entonces uno y solo uno de los tres números es par, y siempre es x o y.

Demostración.

$$\left.\begin{array}{l} x\ par \Rightarrow x^2\ par \\ y\ imp \Rightarrow y^2\ imp \end{array}\right\} \Rightarrow z^2 = x^2 + y^2\ imp\ , \quad \left.\begin{array}{l} x\ imp \Rightarrow x^2\ imp \\ y\ par \Rightarrow y^2\ par \end{array}\right\} \Rightarrow z^2 = x^2 + y^2\ imp$$

Recordemos que todo cuadrado perfecto es 0 o 1 módulo 4. Luego

$$\left.\begin{array}{l} x\ imp \Rightarrow x^2\ imp \Rightarrow x^2 \equiv 1 \pmod 4 \\ y\ imp \Rightarrow y^2\ imp \Rightarrow y^2 \equiv 1 \pmod 4 \end{array}\right\} \Rightarrow z^2 = x^2 + y^2 \equiv 2 \pmod 4 \text{ absurdo.}$$

Puesto que estamos suponiendo ternas pitagóricas primitivas, el caso x,y ambos pares no se puede dar.

Teorema. Caracterización de las ternas pitagóricas.

Las ternas pitagóricas primitivas son todas las ternas de enteros que se pueden escribir de la forma

$$\begin{cases} x = m^2 - n^2 \\ y = 2mn \\ z = m^2 + n^2 \end{cases} \text{ (con } y \text{ par)} \quad \text{o bien} \quad \begin{cases} x = 2mn \\ y = m^2 - n^2 \text{ (con } x \text{ par)} \\ z = m^2 + n^2 \end{cases}$$

Donde $m > n > 0$ son números coprimos con paridad diferente.

Demostración.

Que las ternas de enteros anteriores son pitagóricas es fácil de comprobar:

$$x^2 + y^2 = z^2 \Leftrightarrow \left(m^2 - n^2\right)^2 + \left(2mn\right)^2 = \left(m^2 + n^2\right)^2$$

Simplificando:

$\left(m^2 - n^2\right)^2 + \left(2mn\right)^2 = \left(m^2 + n^2\right)^2 \Leftrightarrow \left(m^2 - n^2\right)^2 + 4m^2n^2 = \left(m^2 + n^2\right)^2$, que es una aplicación directa de la igualdad $(a-b)^2 + 4ab = (a+b)^2$.

Veamos que si una terna es pitagórica, necesariamente debe ser como las anteriores.

Vamos a demostrar la columna de la izquierda, es decir, cuando x es impar y y es par.

$x^2 + y^2 = z^2$ se puede escribir como

$$y^2 = z^2 - x^2 = (z+x)(z-x)$$

Y por tanto:

$$\left(\frac{y}{2}\right)^2 = \frac{y^2}{4} = \frac{z+x}{2} \cdot \frac{z-x}{2}$$

Teniendo en cuenta que $\frac{z+x}{2} + \frac{z-x}{2} = z$, $\frac{z+x}{2} - \frac{z-x}{2} = x$, y $mcd(x,z) = 1$, llegamos a

$$mcd\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1$$

Y por tanto, aplicando 5.2.26b, $\frac{z-x}{2}$ y $\frac{z+x}{2}$ son cuadrados perfectos, es decir:

$\frac{z-x}{2} = n^2$ y $\frac{z+x}{2} = m^2$ para ciertos enteros n y m.

Se cumple claramente que $m > n$ y son enteros coprimos.

También se cumple que m y n tienen diferente paridad, puesto que $z = m^2 + n^2$ es impar.

Y se cumple $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$, tal y como queríamos ver.

10.2.1 [D]

Calcula todos los números enteros a, b y c tales que $a^2 = 2b^2 + 3c^2$

OMEFL 2011#4

10.3 La ecuación diofántica $x^2 - y^2 = k$.

Lema.

Un elemento importante para resolver la ecuación $x^2 - y^2 = k$ es observar que, por cada posible factorización $a \cdot b = k$,

$$x^2 - y^2 = k \Leftrightarrow (x+y)(x-y) = n \cdot m = k \Leftrightarrow \begin{cases} x+y = n \\ x-y = m \end{cases}$$

Y el sistema de ecuaciones de la derecha tiene como única solución

Sumando las dos ecuaciones: $2x = n+m \Rightarrow x = \dfrac{n+m}{2}$

Restando las dos ecuaciones: $2y = n-m \Rightarrow y = \dfrac{n-m}{2}$

Aunque no todas las soluciones en x, y serán aceptables por no ser enteras: Está claro que $n+m$ y $n-m$ deben ser ambos pares, luego n, m deben tener la misma paridad.

10.3.1 Ejemplo 1.

Determina todas las soluciones enteras de la ecuación

$$x^2 - y^2 = 108$$

Solución.

$$x^2 - y^2 = 108 \Leftrightarrow (x+y)(x-y) = 2^2 3^3$$

Y por tanto

$$\begin{cases} x+y = 2^a 3^b \\ x-y = 2^{2-a} 3^{3-b} \end{cases} \quad \text{para ciertos } 0 \le a \le 2 \ , \ 0 \le b \le 3 .$$

Luego

$$\begin{cases} x = \dfrac{2^a 3^b + 2^{2-a} 3^{3-b}}{2} = 2^{a-1} 3^b + 2^{1-a} 3^{3-b} \\ y = \dfrac{2^a 3^b - 2^{2-a} 3^{3-b}}{2} = 2^{a-1} 3^b - 2^{1-a} 3^{3-b} \end{cases}$$

El único valor de a para el que x, y son enteros es $a = 1$, y en este caso:

$$\begin{cases} x+y = 2 \cdot 3^b \\ x-y = 2 \cdot 3^{3-b} \end{cases} \Rightarrow \begin{cases} x = 3^b + 3^{3-b} \\ y = 3^b - 3^{3-b} \end{cases}$$

Dando valores a n aparecen las cuatro soluciones posibles con $x > 0$:

$b = 0 \Rightarrow x = 28 \, , \ y = -26$

$b = 1 \Rightarrow x = 12 \, , \ y = -6$

$b = 2 \Rightarrow x = 12 \, , \ y = 6$

$b = 3 \Rightarrow x = 28 \, , \ y = 26$

Las soluciones son ocho:

$(x, y) = (\pm 28 \, , \pm 26)$, $(x, y) = (\pm 12 \, , \pm 6)$

10.3.2 Ejemplo 2.

Determina todas las soluciones enteras de la ecuación

$$x^2 - y^2 = 600$$

Solución.

$x^2 - y^2 = 600 \Leftrightarrow (x+y)(x-y) = 2^3 \cdot 3 \cdot 5^2$

Y por tanto

$$\begin{cases} x+y = 2^a \cdot 3^b \cdot 5^c \\ x-y = 2^{3-a} \cdot 3^{1-b} \cdot 5^{2-c} \end{cases} \quad \text{para ciertos } 0 \le a \le 3,\ 0 \le b \le 1,\ 0 \le c \le 2$$

Luego

$$\begin{cases} x = \dfrac{2^a \cdot 3^b \cdot 5^c + 2^{3-a} \cdot 3^{1-b} \cdot 5^{2-c}}{2} = 2^{a-1} \cdot 3^b \cdot 5^c + 2^{2-a} \cdot 3^{1-b} \cdot 5^{2-c} \\ y = \dfrac{2^a \cdot 3^b \cdot 5^c - 2^{3-a} \cdot 3^{1-b} \cdot 5^{2-c}}{2} = 2^{a-1} \cdot 3^b \cdot 5^c - 2^{2-a} \cdot 3^{1-b} \cdot 5^{2-c} \end{cases}$$

Luego $a = 1$ o $a = 2$. En total tenemos las siguientes combinaciones:

a=1 , b=0 ,c=0, x= 151, y= -149	;	a=1 , b=0 ,c=1, x= 35, y= -25
a=1 , b=0 ,c=2, x= 31, y= 19	;	a=1 , b=1 ,c=0, x= 53, y= -47
a=1 , b=1 ,c=1, x= 25, y= 5	;	a=1 , b=1 ,c=2, x= 77, y= 73
a=2 , b=0 ,c=0, x= 77, y= -73	;	a=2 , b=0 ,c=1, x= 25, y= -5
a=2 , b=0 ,c=2, x= 53, y= 47	;	a=2 , b=1 ,c=0, x= 31, y= -19
a=2 , b=1 ,c=1, x= 35, y= 25	;	a=2 , b=1 ,c=2, x= 151, y= 149

Que dan lugar a las siguientes 24 soluciones:

$(x, y) = (\pm 151, \pm 149), (\pm 35, \pm 25), (\pm 31, \pm 19), (\pm 53, \pm 47), (\pm 25, \pm 5), (\pm 77, \pm 73)$

10.3.3 Ejemplo 3.

Determina todas las soluciones enteras de la ecuación

$$x^2 - y^2 = 294$$

Solución.

$x^2 - y^2 = 294 \Leftrightarrow (x+y)(x-y) = 2 \cdot 3 \cdot 7^2$

Y por tanto

$$\begin{cases} x+y = 2^a \cdot 3^b \cdot 7^c \\ x-y = 2^{1-a} \cdot 3^{1-b} \cdot 7^{2-c} \end{cases} \quad \text{para ciertos } 0 \le a \le 1,\ 0 \le b \le 1,\ 0 \le c \le 2$$

Luego

$$\begin{cases} x = \dfrac{2^a \cdot 3^b \cdot 7^c + 2^{1-a} \cdot 3^{1-b} \cdot 7^{2-c}}{2} = 2^{a-1} \cdot 3^b \cdot 7^c + 2^{-a} \cdot 3^{1-b} \cdot 7^{2-c} \\ y = \dfrac{2^a \cdot 3^b \cdot 7^c - 2^{1-a} \cdot 3^{1-b} \cdot 7^{2-c}}{2} = 2^{a-1} \cdot 3^b \cdot 7^c - 2^{-a} \cdot 3^{1-b} \cdot 7^{2-c} \end{cases}$$

Y vemos que no existe ningún valor $0 \le a \le 1$ para el cual x, y sean enteros. Por lo tanto, esta ecuación no tiene ninguna solución entera.

10.3.4 Ejemplo 4.

Determina todas las soluciones enteras de la ecuación

$$x^2 - y^2 = 189$$

Solución.

$x^2 - y^2 = 189 \Leftrightarrow (x+y)(x-y) = 3^3 \cdot 7$

Y por tanto

$$\begin{cases} x + y = 3^a \cdot 7^b \\ x - y = 3^{3-a} \cdot 7^{1-b} \end{cases} \quad \text{para ciertos } 0 \le a \le 3 \ , \ 0 \le b \le 1$$

Luego

$$\begin{cases} x = \dfrac{3^a \cdot 7^b + 3^{3-a} \cdot 7^{1-b}}{2} \\ y = \dfrac{3^a \cdot 7^b - 3^{3-a} \cdot 7^{1-b}}{2} \end{cases}$$

Las soluciones son:

a=0 , b=0, x= 95, y= -94	;	a=0 , b=1, x= 17, y= -10
a=1 , b=0, x= 33, y= -30	;	a=1 , b=1, x= 15, y= 6
a=2 , b=0, x= 15, y= -6	;	a=2 , b=1, x= 33, y= 30
a=3 , b=0, x= 17, y= 10	;	a=3 , b=1, x= 95, y= 94

Que dan lugar a las siguientes 16 soluciones:

$$(x, y) = (\pm 95, \pm 94), (\pm 17, \pm 10), (\pm 33, \pm 30), (\pm 15, \pm 6)$$

10.3.5 Ejemplo 5.

Determina todas las soluciones enteras de la ecuación

$$x^2 - y^2 = 441$$

Solución.

$x^2 - y^2 = 189 \Leftrightarrow (x+y)(x-y) = 3^2 \cdot 7^2$

Y por tanto

$$\begin{cases} x + y = 3^a \cdot 7^b \\ x - y = 3^{3-a} \cdot 7^{1-b} \end{cases} \quad \text{para ciertos } 0 \le a \le 2 \ , \ 0 \le b \le 2$$

Luego

$$\begin{cases} x = \dfrac{3^a \cdot 7^b + 3^{2-a} \cdot 7^{2-b}}{2} \\ y = \dfrac{3^a \cdot 7^b - 3^{2-a} \cdot 7^{2-b}}{2} \end{cases}$$

Las soluciones son:

a=0 , b=0, x= 221, y= -220 ; a=0 , b=1, x= 35, y= -28
a=0 , b=2, x= 29, y= 20 ; a=1 , b=0, x= 75, y= -72
a=1 , b=1, x= 21, y= 0 ; a=1 , b=2, x= 75, y= 72
a=2 , b=0, x= 29, y= -20 ; a=2 , b=1, x= 35, y= 28
a=2 , b=2, x= 221, y= 220

En este caso observamos que el número de soluciones con $x>0$ es impar.
Las soluciones a la ecuación son las siguientes 18:

$$(x,y)=(\pm 221,\pm 220),(\pm 35,\pm 28),(\pm 29,\pm 20),(\pm 75,\pm 72),(\pm 21,0)$$

De las cuales son positivas las cinco siguientes:

$$(x,y)=(221,220),(35,28),(29,20),(75,72),(21,0)$$

Teorema.

El número r de soluciones enteras (x,y) de la ecuación $x^2-y^2=k$ queda determinado por su descomposición en factores primos $k=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n}$.

a) Si $p_1=2$ y $\alpha_1=1$, es decir, el número k es de la forma $k=2q$ con q impar, no hay solución posible: $r=0$.

b) Si con $p_1>2$, es decir, el número k es impar, entonces la fórmula

$$\prod_{i=1}^{n}(\alpha_i+1)$$

genera todas las soluciones de la forma (x,y) , $(x,-y)$, con $x>0$, luego

$$r=2\prod_{i=1}^{n}(\alpha_i+1)$$

c) Si $p_1=2$ y $\alpha_1>1$, es decir, el número k es de la forma $k=4q$, entonces la fórmula

$$(\alpha_1-1)\prod_{i=2}^{n}(\alpha_i+1)$$

genera todas las soluciones de la forma (x,y) , $(x,-y)$, con $x>0$, luego

$$r=2(\alpha_1-1)\prod_{i=2}^{n}(\alpha_i+1)$$

Demostración.

a) $x^2-y^2=2q \Leftrightarrow (x+y)(x-y)=2q$

Vemos que 2 y q son coprimos, y es imposible encontrar factorizaciones $2q=n\cdot m$ con la misma paridad.

b) Si $k=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n}$ con $p_1>2$, entonces

$$\begin{cases} x=\dfrac{p_1^{\beta_1}p_2^{\beta_2}\ldots p_n^{\beta_n}+p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}\ldots p_n^{\alpha_n-\beta_n}}{2} \\ y=\dfrac{p_1^{\beta_1}p_2^{\beta_2}\ldots p_n^{\beta_n}-p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}\ldots p_n^{\alpha_n-\beta_n}}{2} \end{cases} \quad \text{con } 0\le\beta_i\le\alpha_i$$

Y todas las combinaciones posibles son válidas pues los numeradores son siempre pares, pues son sumas y restas de números impares.

c) Si $k = 2^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, entonces

$$\begin{cases} x = \dfrac{2^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n} + 2^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} \ldots p_n^{\alpha_n-\beta_n}}{2} = 2^{\beta_1-1} p_2^{\beta_2} \ldots p_n^{\beta_n} + 2^{\alpha_1-\beta_1-1} p_2^{\alpha_2-\beta_2} \ldots p_n^{\alpha_n-\beta_n} \\ y = \dfrac{2^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n} - 2^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} \ldots p_n^{\alpha_n-\beta_n}}{2} = 2^{\beta_1-1} p_2^{\beta_2} \ldots p_n^{\beta_n} - 2^{\alpha_1-\beta_1-1} p_2^{\alpha_2-\beta_2} \ldots p_n^{\alpha_n-\beta_n} \end{cases}$$

con $0 \le \beta_i \le \alpha_i$

Pero para $\beta_1 = 0$ y $\beta_1 = \alpha_1$ los valores obtenidos de x, y no serán enteros, luego hay que descartarlos. Por lo tanto el exponente α_1 debe ser tratado de forma diferente.

Observación.

Si queremos determinar únicamente las soluciones no negativas, debemos diferenciar los siguientes casos:

a) Si k no es un cuadrado perfecto, es decir, algún α_i es impar y por tanto algún $\alpha_i + 1$ es par, el número de soluciones enteras será un número par (la mitad positivas y la mitad negativas). En particular:

a$_1$) Si $p_1 > 2$, es decir, k es impar, la fórmula $\prod_{i=1}^{n} (\alpha_i + 1)$ genera todas las soluciones (x, y) , $(x, -y)$ con $x > 0$, luego el número de soluciones positivas será

$$s = \frac{1}{2} \prod_{i=1}^{n} (\alpha_i + 1)$$

a$_2$) Si $p_1 = 2$ y $\alpha_1 > 1$, entonces el número de soluciones positivas será

$$s = \frac{1}{2} (\alpha_1 - 1) \prod_{i=2}^{n} (\alpha_i + 1)$$

b) Si k es un cuadrado perfecto, es decir, todos los α_i son pares y por tanto todos los $\alpha_i + 1$ son impares, aparecerá la solución $x = \sqrt{k}$, $y = 0$:

$$k = \left(\sqrt{k} + 0\right)\left(\sqrt{k} - 0\right)$$

Esta solución hará que el número total de soluciones sea impar.

Por ejemplo, en el Ejemplo 4,

$$x^2 - y^2 = 189 = 3^3 \cdot 7 \Rightarrow \frac{1}{2} \prod_{i=1}^{n} (\alpha_i + 1) = \frac{1}{2} (3+1)(1+1) = \frac{8}{2} = 4$$

Que son las cuatro soluciones ya encontradas anteriormente:

$$(x, y) = (95,94), (17,10), (33,30), (15,6)$$

10.3.6 Ejemplo.

Determina el número de soluciones enteras de la ecuación $x^2 - y^2 = 9$. ¿Cuántas de ellas no son negativas?

Solución.

Aplicando la fórmula del teorema anterior, $9 = 3^2 \rightarrow \prod_{i=1}^{n}(\alpha_i + 1) = 2 + 1 = 3$

Luego hay $3 \cdot 2 = 6$ soluciones enteras, de las cuales $\lceil 3/2 \rceil = \lceil 1.5 \rceil = 2$ no son negativas. Concretamente son: $x = 3, y = 0$; $x = 5, y = 4$

10.3.7 Ejemplo.

Determina el número de soluciones enteras de la ecuación $x^2 - y^2 = 400$. ¿Cuántas de ellas no son negativas?

Solución.

$400 = 2^4 \cdot 5^2 \Rightarrow (\alpha_1 - 1)\prod_{i=2}^{n}(\alpha_i + 1) = 3 \cdot 3 = 9.$

Luego hay $9 \cdot 2 = 18$ soluciones enteras, de las cuales $\lceil 9/2 \rceil = \lceil 4.5 \rceil = 5$ no son negativas.

Observación 2.

En el apartado 20.1 se introduce el número de divisores positivos de k, $\tau(k)$, y aplicando la fórmula de 20.4 se deduce que, si k es impar, se cumple:

$$\tau(k) = \frac{1}{2}r$$

Fuente: "On the Number of Solutions of the Diophantine Equation $x^2 - y^2 = N$", J.F.T. Rabago
INTERNATIONAL JOURNAL OF MATHEMATICS AND SCIENTIFIC COMPUTING
(ISSN: 2231-5330), VOL. 2, NO. 2, 2012 13

10.3.8 D

Dado un número entero positivo n, definimos λ(n) como el número de soluciones enteras positivas de la ecuación $x^2 - y^2 = n$. Diremos que el número n es "olímpico" si λ(n) = 2021. ¿Cuál es el menor entero positivo que es olímpico? ¿Y cuál es el menor entero positivo impar que es olímpico?

OME 2021 #2

10.3.9 M

Suponiendo que las raíces de la función $f(x) = x^2 - ax + 2a$ son valores enteros, determina la suma de todos los posibles valores de a.

(A) 7 (B) 8 (C) 16 (D) 17 (E) 18

AMC 10A 2015 #23

10.4 El método de la contradicción modular.

Una técnica muy potente para resolver ecuaciones diofánticas es pasar la ecuación a un módulo adecuado en el que los candidatos aceptables se reduzcan significativamente. También se puede demostrar que una ecuación no tiene solución si no tiene solución para algún módulo conveniente.

10.4.1 D

Determina todas las parejas de enteros (x, y) que satisfacen la ecuación

$$x^2 - y! = 2001$$

Nota: Cuando trabajamos con números factoriales es interesante tener en cuenta que $n! \equiv 0 \pmod{m}$ para todo $n \geq m$, y así reducir los valores aceptables significativamente.

10.4.2 F

Demuestra que para todo m, n enteros positivos, $3^m + 3^n + 1$ no puede ser un cuadrado perfecto.

USAMTS

10.4.3 D

Demuestra que 19^{19} no se puede escribir como $x^3 + y^4$, con x, y enteros.

10.4.4 F

Determina todas las soluciones de la ecuación $x^5 = y^2 + 4$ en enteros positivos.

10.4.5 F

¿Existe alguna pareja de enteros a, b para los cuales $a^5b + 3$ y $ab^5 + 3$ son cubos perfectos?

USAJMO 2013 #1

10.4.6 M

Demuestra que la ecuación

$$(x+1)^2 + (x+2)^2 + \ldots + (x+2001)^2 = y^2$$

no tiene soluciones enteras.

10.4.7 D

Determina todos los pares (p, q) de números primos tales que

$$p^3 - q^5 = (p+q)^2$$

Russian Mathematical Olympiad

10.4.8 M

Determina todos los enteros positivos a, b, c tales que

$$a^3 + b^3 + c^3 = 2001$$

10.5 La técnica del descenso infinito de Fermat.

Supongamos que queremos resolver una ecuación diofántica, y encontramos que, dada una solución $x_1 \geq 0$, entonces también será solución $x_2 \geq 0$, con $x_1 > x_2 \geq 0$.

Obtenemos así una sucesión infinita y decreciente de soluciones $x_1 > x_2 > \ldots > x_n \geq 0$, lo cual es imposible pues trabajamos con números naturales, llegando a contradicción.

Así pues, esta técnica nos permite demostrar que una determinada ecuación diofántica no tiene solución posible, o solo tiene la solución trivial $x = 0$.

Una definición más formal de esta técnica sería la siguiente: Supongamos que queremos demostrar una propiedad P para los enteros. Si la hipótesis de que se cumple para un cierto número entero positivo n_0 implica que también se cumple para otro entero positivo más pequeño $n_1 < n_0$, entonces ningún entero positivo satisface P.

Esta técnica se justifica formalmente en el principio de que todo conjunto finito de números naturales tiene un mínimo. Sea S el conjunto de números naturales que satisfacen P. Entonces S tiene un mínimo n, y la existencia de $m < n$ satisfaciendo P, es decir, $m \in S$ nos lleva a contradicción.

Este método se asocia a **Fermat** (1601-1665) porque este matemático fue el primero en utilizarlo explícitamente en sus razonamientos. Es interesante reseñar que Fermat, pese a ser proclamado padre de la Teoría de Números moderna, siempre se consideró a sí mismo un matemático amateur, y nunca se preocupó de publicar ninguno de sus resultados matemáticos, contentándose con enviarlos a su amigo el matemático **Marin Mersenne** (1588-1648).

Podemos leer en Cut the Knot que este método fue el utilizado por **Euclides** en Los Elementos VII.31 para demostrar que todo número compuesto tiene un divisor primo.

10.5.1 F

Determine todas las soluciones enteras de la ecuación

$$x^2 + y^2 = 3z^2$$

10.5.2 M

Determine todas las soluciones enteras de la ecuación

$$a^2 + b^2 + c^2 = a^2 b^2$$

USAMO 1976 #3

10.5.3 M

Resuelve la siguiente ecuación diofántica:

$$x^3 = 2y^3 + 4z^3$$

10.6 Resolución de ecuaciones diofánticas mediante factorización.

Fuente: An Introduction to Diophantine Equations A Problem-Based Approach (Andreescu, Cucurezeanu, Andrica) , página 4 en adelante.

El método más común para resolver una ecuación diofántica es escribirla como producto de expresiones más sencillas igual a un número:

$$f_1(x_1, x_2, ..., x_n) \cdot f_2(x_1, x_2, ..., x_n) \cdot ... \cdot f_m(x_1, x_2, ..., x_n) = a$$

Ahora, factorizando el número a, obtenemos todas las posibles expresiones $a = a_1 \cdot ... \cdot a_m$, convirtiendo la ecuación diofántica original en un conjunto de sistema de ecuaciones:

$$\begin{cases} f_1(x_1, x_2, ..., x_n) = a_1 \\ f_2(x_1, x_2, ..., x_n) = a_2 \\ ... \\ f_m(x_1, x_2, ..., x_n) = a_m \end{cases}$$

Ejemplo resuelto 1.

Determina todas las soluciones enteras de la ecuación

$$(x^2+1)(y^2+1) + 2(x-y)(1-xy) = 4(1+xy)$$

Solución:

Reescribimos la ecuación de la siguiente forma:

$$(x^2+1)(y^2+1) + 2(x-y)(1-xy) = 4(1+xy) \Leftrightarrow$$
$$x^2y^2 - 2xy + 1 + x^2 + y^2 - 2xy + 2(x-y)(1-xy) = 4 \Leftrightarrow$$
$$(xy-1)^2 + (x-y)^2 - 2(x-y)(xy-1) = 4 \Leftrightarrow$$
$$[xy - 1 - (x-y)]^2 = 4 \Leftrightarrow$$
$$xy - 1 - (x-y) = \pm 2 \Leftrightarrow$$
$$(x+1)(y-1) = \pm 2$$

Veamos los casos posibles:

$$\begin{cases} x+1=1 \\ y-1=2 \end{cases} \Leftrightarrow x=0, y=3 \qquad \begin{cases} x+1=-1 \\ y-1=2 \end{cases} \Leftrightarrow x=-2, y=3 \qquad \begin{cases} x+1=1 \\ y-1=-2 \end{cases} \Leftrightarrow x=0, y=-1$$

$$\begin{cases} x+1=-1 \\ y-1=-2 \end{cases} \Leftrightarrow x=-2, y=-1 \qquad \begin{cases} x+1=2 \\ y-1=1 \end{cases} \Leftrightarrow x=1, y=2 \qquad \begin{cases} x+1=-2 \\ y-1=1 \end{cases} \Leftrightarrow x=-3, y=2$$

$$\begin{cases} x+1=2 \\ y-1=-1 \end{cases} \Leftrightarrow x=1, y=0 \qquad \begin{cases} x+1=-2 \\ y-1=-1 \end{cases} \Leftrightarrow x=-3, y=0$$

Es fácil comprobar que las ocho soluciones encontradas satisfacen la ecuación del enunciado.

Ejemplo resuelto 2.

Determina todas las soluciones enteras positivas de la ecuación

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{pq}$$

Solución.

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{pq} \Leftrightarrow pq(x+y)=xy \Leftrightarrow$$
$$pqx+pqy-xy=0 \Leftrightarrow$$
$$(x-pq)(y-pq)-p^2q^2=0 \Leftrightarrow$$
$$(x-pq)(y-pq)=p^2q^2$$

Y probamos con todas las combinaciones posibles:

$$\begin{cases} x-pq=1 \\ y-pq=p^2q^2 \end{cases} \quad \begin{cases} x-pq=p \\ y-pq=pq^2 \end{cases} \quad \begin{cases} x-pq=p^2 \\ y-pq=q^2 \end{cases}$$
$$\begin{cases} x-pq=q \\ y-pq=p^2q \end{cases} \quad \begin{cases} x-pq=q^2 \\ y-pq=p^2 \end{cases} \quad \begin{cases} x-pq=pq \\ y-pq=pq \end{cases}$$
$$\begin{cases} x-pq=p^2q \\ y-pq=q \end{cases} \quad \begin{cases} x-pq=pq^2 \\ y-pq=p \end{cases} \quad \begin{cases} x-pq=p^2q^2 \\ y-pq=1 \end{cases}$$

Que llevan a las nueve soluciones posibles:

$$(1+pq, pq(1+pq)),\ (p(1+q), pq(1+q)),\ (q(1+p), pq(1+p))$$
$$(p(p+q), q(p+q)),\ (2pq, 2pq),\ (pq(1+q), p(1+q)),$$
$$(pq(1+p), q(1+p)),\ (q(p+q), p(p+q)),\ (pq(1+pq), 1+pq)$$

10.6.1 M

Determina todas los pares (x, y) de enteros no negativos para los cuales

$$(xy-7)^2=x^2+y^2$$

Indian Mathematical Olympiad

10.6.2 M

Resuelve la siguiente ecuación para soluciones enteras x, y:

$$x^2(y-1)+y^2(x-1)=1$$

Polish Mathematical Olympiad

10.6.3 F

Determina todas las parejas de enteros positivos no nulos (x, y) que satisfacen la ecuación

$$xy^2+2y^2-x-107=0$$

Kangourou Student 2021 #26

10.6.4 F

Las butacas de un teatro forman un rectángulo, ordenadamente por filas (butacas una al lado de la otra) y en columnas (una detrás de otra). Sabemos que la capacidad del teatro es la mínima que permite situar en cada fila exactamente 12 hombres, en cada columna exactamente 15 mujeres y dejar exactamente 7 butacas libres. Determina la capacidad del teatro.

(A) 635 (B) 754 (C) 736 (D) 650 (E) 680

Cangur B2 2022 #30

10.6.5 F **Problema solucionado paso a paso en vídeo .**

Un partido de fútbol entre equipos de North Berracan y South Berracan se juega en un estadio que tiene una serie rectangular de asientos para los espectadores. Hay 11 partidarios de North Berracan en cada fila y 14 partidarios de South Berracan en cada columna. Esto deja 17 asientos vacíos. ¿Cuál es el menor número posible de asientos en el estadio?

(A) 500 (B) 660 (C) 690 (D) 840 (E) 994

Kangaroo Student 2022 #30

Solución: https://youtu.be/x_mK2_JcgxE

10.6.6 MD

Determina todas las ternas de enteros positivos (x, y, z) que satisfacen la ecuación

$$2(x+y+z+2xyz)^2 = (2xy+2yz+2zx+1)^2 + 2023$$

USAJMO 2023 #1

Nota: Se presenta una solución incompleta.

10.6.7 M

Determina todos los enteros positivos x, y que satisfacen la ecuación $x(x-y)=8y-7$

10.7 Resolución de ecuaciones diofánticas aplicando desigualdades.

Este método consiste en aplicar algún tipo de desigualdad para reducir el número de casos aceptables. Para ello aplicaremos las técnicas estudiadas en el libro Desigualdades.

10.7.1 D

Determina todos los pares (x, y) de enteros para los que se verifica

$$x^3 + y^3 = (x + y)^2$$

10.7.2 M

Encontrar todas las soluciones enteras positivas de

$$\frac{1}{a+b} + \frac{1}{b+c} + \frac{1}{c+a} + \frac{1}{a+b+c-2} = 1$$

OMEFL 2017 #4

10.7.3 D

Sean a, b, n enteros positivos tales que $a > b$ y $ab - 1 = n^2$. Prueba que

$$a - b \geq \sqrt{4n - 3}$$

Indica justificadamente cuando se alcanza la igualdad.

OME 2013 #1

10.7.4 D

Determina todas las parejas de enteros positivos (x, y) que son solución de la ecuación

$$\frac{x^4 + y^3}{x^2 + y} = x + y$$

OMEC 2021 #3

10.7.5 M

Resuelve la siguiente ecuación para valores enteros positivos de x, y, z:

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{3}{5}$$

Romanian Mathematical Olympiad

10.7.6 D

Determina las soluciones enteras y positivas a, b, c de la ecuación

$$\left(1 + \frac{1}{a}\right)\left(1 + \frac{1}{b}\right)\left(1 + \frac{1}{c}\right) = 2$$

BMO 1995 Round 2 #1

10.7.7 [F]

a) Demostrar que

$$\frac{x^2}{(x-1)^2}+\frac{y^2}{(y-1)^2}+\frac{z^2}{(z-1)^2}\geq 1$$

Para todos los números reales x, y, z, todos diferentes de 1 y cumpliendo $xyz=1$.

b) Demostrar que la igualdad acontece para infinitas ternas de números racionales x, y, z, todos diferentes de 1 y cumpliendo $xyz=1$.

IMO 2008 #2

Nota: Solo el apartado b es un problema de Teoría de Números. El apartado a es un problema propio de Desigualdades.

10.8 Cuadrados perfectos. Potencias perfectas.

Cuadrados perfectos. Potencias perfectas.

Diremos que un entero n es un **cuadrado perfecto** cuando podamos encontrar otro entero m tal que $n = m^2$.

De la misma forma, diremos que n es un **cubo perfecto** cuando podamos encontrar otro entero m tal que $n = m^3$.

En general, si podemos escribir $n = m^k$ diremos que n es una **potencia perfecta de grado k**.

Los cuadrados perfectos son un tema recurrente en las competiciones matemáticas, y serán tratados a lo largo de este libro aplicando diversas técnicas.

Proposición. Potencias perfectas y congruencias.

Sea n un entero. Entonces:

a) $n^2 \equiv \{0, 1\} \pmod 3$ b) $n^2 \equiv \{0, 1\} \pmod 4$ c) $n^2 \equiv \{0, \pm 1\} \pmod 5$

d) $n^2 \equiv \{0, 1, 4\} \pmod 8$ e) $n^3 \equiv \{0, \pm 1\} \pmod 9$ f) $n^4 \equiv \{0, 1\} \pmod{16}$

Demostración. Basta estudiar caso por caso. Por ejemplo:

a) $0^2 = 0 \equiv 0 \pmod 3$, $1^2 = 1 \equiv 1 \pmod 3$, $2^2 = 4 \equiv 1 \pmod 3$, luego no hay ningún cuadrado que sea congruente con 2 módulo 3.

El siguiente problema es un problema motivador para que el estudiante analice la relación entre cuadrados perfectos y la cantidad de divisores de un número:

10.8.1

Veinte estudiantes aburridos se dedican a abrir y cerrar las taquillas de un vestuario, numeradas del 1 al 20. El primer estudiante abre todas las taquillas; el segundo estudiante cierra todas las taquillas numeradas 2, 4, 6, 8, 10, 12, 14, 16, 18; El tercer estudiante se dedica a las taquillas numeradas 3, 6, 9, 12, 15 y 18, si las encuentra abiertas, las cierra, y si las encuentra cerradas, las abre. En general, el estudiante número k se dedica a las taquillas múltiples de k: Si las encuentra abiertas, las cierra, y si las encuentra abiertas, las abre. Determina las taquillas que quedarán abiertas después de que hayan pasado los veiente estudiantes.

10.8.2 M

Determina todos los números primos p tales que $p^2 - p + 1$ es un cubo perfecto.

Balkan MO 2005 #2

10.8.3 M

Determina todos los números primos p, q para los cuales $p + q$ y $p + 7q$ son ambos cuadrados perfectos.

10.8.4 M

Determina todos los primos p y q para los que $p^2 + 7pq + q^2$ es un cuadrado perfecto.

10.8.5 MD

Determinar todos los números primos $p \geq 3$ tales que $(p+1)/2$ y $(p^2+1)/2$ son cuadrados perfectos.

OMEC 2022 #5

10.8.6 F

Sea n un entero positivo y sea d un divisor positivo de $2n^2$. Demuestra que n^2+d no es un cuadrado perfecto.

Kürschák Math Competition 1953

10.8.7 D

Determina todos los números primos p tales que $2p^4 - p^2 + 16$ sea un cuadrado perfecto.

Leningrad Math Olympiad 1980

10.8.8 MD

Demuestra que la ecuación $4xy - x - y = z^2$ no tiene soluciones en los enteros positivos.

(Euler)

10.8.9 M **Problema solucionado paso a paso en vídeo.**

Un número triangular es cualquier entero positivo que se puede expresar de la forma

$$t_n = 1+2+3+...+n,$$

para cierto entero positivo n. Los primeros tres números triangulares que son también cuadrados perfectos son: $t_1 = 1 = 1^2$, $t_8 = 36 = 6^2$ y $t_{49} = 1225 = 35^2$

Determina la suma de los dígitos del cuarto número triangular más pequeño que es también un cuadrado perfecto.

(A) 6 (B) 9 (C) 12 (D) 18 (E) 27

AMC 12A 2022 #16

Solución: https://youtu.be/2kJ1yQHWcCA

10.8.10 F

Describir todas las soluciones enteras positivas (m,n) de la ecuación

$$8m - 7 = n^2$$

y dar el primer valor de m (si existe) mayor que 1959.

OMEFL 2017 #1

10.8.11 MD

Determine todas las parejas de enteros (x, y) tales que $1 + 2^x + 2^{2x+1} = y^2$

IMO 2006 #4

10.8.12 M

Determina todas las soluciones enteras de la ecuación $3^x - 5^y = z^2$

Balkan MO 2009 #1

10.8.13 MD

Para cada entero $a_0 > 1$, se define la sucesión $a_0, a_1, a_2, \ldots$ tal que para cada $n \geq 0$:

$$a_{n+1} = \begin{cases} \sqrt{a_n} & \text{si } \sqrt{a_n} \text{ es entero,} \\ a_n + 3 & \text{en otro caso.} \end{cases}$$

Determinar todos los valores de a_0 para los que existe un número A tal que a $a_n = A$ para infinitos valores de n.

IMO 2017 #1

10.9 Ecuaciones de Frobenius. Problema de las monedas.

Definición. Ecuación de Frobenius. Número de Frobenius.

Llamaremos ecuación de Frobenius a toda ecuación diofántica de la forma

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

con a_i, x_i, b enteros , $a_i > 0$ y $x_i \geq 0$.

Llamaremos "Número de Frobenius" al mayor b para el cual la ecuación no tiene solución. Por ejemplo, la ecuación de Frobenius $4x + 9y = b$ tiene asociado el número de Frobenius 23.

En Mathematica:

```
In[1]:= FrobeniusNumber[{4, 9}]
        número de Frobenius
Out[1]= 23
```

El problema de las monedas.

Dados dos números positivos m, n, queremos estudiar las combinaciones lineales

$$am + bn$$

con coeficientes enteros no negativos $a, b \geq 0$.

Este problema se llama problema de las monedas de Frobenius o simplemente problema de Frobenius, pues este matemático alemán estudió las posibles sumas de dinero que se podían obtener acumulando ciertos tipos de moneda.

El teorema "Chicken McNugget".

Dados dos números positivos coprimos m, n, el mayor entero que no puede representarse como combinación lineal $am + bn$ con a, b enteros no negativos es

$$mn - m - n$$

Una consecuencia de este teorema es que existen exactamente

$$\frac{(m-1)(n-1)}{2}$$

enteros positivos que no se pueden representar de dicha forma.

Se dice que el origen de este teorema y de su curioso nombre viene de cuando McDonalds ofrecía sus *nuggets* en paquetes de 9 y de 20, y algunos aficionados a las matemáticas se preguntaron por la cantidad máxima que no se podían comprar en cajas completas (son 151).

Teorema de Frobenius.

Supongamos que a y b son enteros positivos.

a) Si $(a,b)=1$, el número de enteros positivos n que no se pueden escribir como $ax+by=n$, con $x,y\geq 0$, es exactamente $\frac{(a-1)(b-1)}{2}$.

b) Si $(a,b)>1$, todo número entero positivo de la forma $ax+by=n$ será múltiple de (a,b), luego existirán infinitos números que no se puedan escribir como $ax+by=n$.

c) Si $(a,b)=1$ y $n=ab-a-b$, la ecuación $ax+by=n$ no tiene solución con $x,y\geq 0$, pero sí la tiene para todo $n>ab-a-b$ (aunque puede tener solución para algunos $n<ab-a-b$ concretos)

10.9.1 MF

En un pueblo llamado Hamlet hay 3 personas por cada caballo, 4 ovejas por cada vaca, y 3 patos por cada persona. ¿Cuál de los siguientes valores no puede ser la suma de personas, caballos, ovejas, vacas y patos en Hamlet?

(A) 41 (B) 47 (C) 59 (D) 61 (E) 66

AMC 10B 2015 #15

10.9.2 D

Determina todos los posibles valores de enteros positivos n para los cuales 91 céntimos es el mayor valor que no se puede formar disponiendo de una infinita cantidad de sellos de 5, n y $n+1$ céntimos.

AIME II 2019 #14

10.9.3 F

Se propone un juego en el cual el jugador gana a puntos si gana o b puntos si pierde ($a,b\in IN, a>b$), y los puntos se van acumulando partida a partida. Se sabe que existen exactamente 35 puntuaciones no alcanzables y que una de ellas es 58. Determina a y b.

Putnam 1971 #A5

10.9.4 D **Problema solucionado paso a paso en vídeo**

Tomamos 94 ladrillos de medidas 4''×10''×19'' y los apilamos uno encima del otro hasta formar una torre de 94 ladrillos. Cada ladrillo puede estar orientado de cualquier forma, por lo que contribuye en 4'', 10'' o 19'' en la altura total de la torre. Determina el número de alturas diferentes de las torres que podemos formar con estos 94 ladrillos.

AIME 1994 #11

Solución: https://youtu.be/oMSDngxwt6U

10.9.5 M

En un país llamado Coinland hay tres tipos de moneda, de 6, de 10 y de 15. Determina la suma de los dígitos del mayor valor que es imposible obtener con estas monedas.

(A) 8 (B) 10 (C) 7 (D) 11 (E) 9

AMC 12B 2023 #16

10.10 Simon's Favorite Factoring Trick (SFFT).

El llamado **Simon's Favorite Factoring Trick** (SFFT) se encuentra en la página web

https://artofproblemsolving.com/wiki/index.php?title=Simon%27s_Favorite_Factoring_Trick

y es una técnica para factorizar expresiones como por ejemplo

$$xy+66x-88y=23333$$

en donde aparecen el producto de dos variables y una combinación lineal de estas dos variables.

Observamos que

$$xy+66x-88y=(x-88)(y+66)+88\cdot 66$$

Luego

$$23333=xy+66x-88y=(x-88)(y+66)+88\cdot 66 \Leftrightarrow 23333-88\cdot 66=(x-88)(y+66)$$

En general esta técnica se puede aplicar a cualquier expresión de la forma

$$xy+ax+by=c \Rightarrow (x+a)(x+b)=c+ab$$

y puede ser muy útil para resolver problemas de Teoría de Números.

más información y ejemplos resueltos en el link anterior.

10.10.1 MD

Una circunferencia de radio entero r está centrada en (r,r). Trazamos segmentos diferentes de longitud c_i conectando los puntos $(0,a_i)$ y $(b_i,0)$ para $1\le i\le 14$ todos tangentes a la circunferencia, con a_i, b_i y c_i todos enteros positivos y $c_1\le c_2\le ...\le c_{14}$. Determina la razón c_{14}/c_1 para el valor mínimo posible de r.

(A) 21/5 (B) 85/13 (C) 7 (D) 39/5 (E) 17

AMC 12A 2022#25

10.11 Ecuaciones diofánticas en competiciones olímpicas.

10.11.1 M

Determina todos los enteros no negativos a, b tales que $\sqrt{a} + \sqrt{b} = \sqrt{2009}$

BMO 2009 Round 2 #1

10.11.2 F

Resuelve la siguiente ecuación para $x, y, z \in IN$

$$\frac{1}{x} + \frac{2}{y} - \frac{3}{z} = 1$$

BMO 1988 #4

10.11.3 F

Determina todas las soluciones enteras positivas n, m, con n impar, de la ecuación

$$\frac{1}{m} + \frac{4}{n} = \frac{1}{12}$$

BMO 2001 Round 1 #1

10.11.4 F

Determina todos los pares (a, b) de enteros positivos tales que $\frac{1}{a} + \frac{1}{b} = \frac{3}{2018}$

Putnam 2018 A1

10.11.5 F

Determina justificadamente todos los pares de números enteros (x, y) que verifican la ecuación $x^2 - y^4 = 2009$.

OME 2009 #4

10.11.6 M

Determina $3x^2y^2$ si x, y son enteros que satisfacen $y^2 + 3x^2y^2 = 30x^2 + 517$.

AIME 1987 #5

10.11.7 F

Encuentra todos los primos p y q que satisfacen la ecuación $p + q = (p - q)^3$

Rusia, 2001

10.11.8 M

Determina todas las ternas de enteros positivos a, b, c tales que $abc = a + b + c + 1$.

México 2010

10.11.9 D

Calcular todos los pares de enteros (x, y) tales que $3^4 2^3 (x^2 + y^2) = x^3 y^3$.

OME 2019 #4

10.11.10 M

Determina todos las parejas de enteros positivos (x, y) tales que $x^3 - y^3 = xy + 61$

Russian Math Olympiad

10.11.11 M

Resuelve la siguiente ecuación para valores enteros $x, y \neq 0$:

$$(x^2 + y)(x + y^2) = (x - y)^3$$

USAMO 1987 #1

10.11.12 M

Determina todos los pares de enteros (x, y) tales que $x^6 + 3x^3 + 1 = y^4$

Romanian Math Olympiad

10.11.13 F

Encontrar todas las soluciones enteras posibles, x e y, de la ecuación

$$p(x + y) = xy$$

siendo p un cierto número primo.

OMEFL 2007 #2

10.11.14 D

Determina todos los $x, y, z \in IN$ tales que $3^x + 4^y = 5^z$.

IMO 1991 Shortlist

10.11.15 D

Determina todas las soluciones enteras de la ecuación $3^m - 2^n = 1$

10.11.16 D

Determina todos los pares de enteros (x, y) que satisfacen la ecuación

$$1 + x^2 y = x^2 + 2xy + 2x + y$$

BMO 2001 Round 2 #2

10.11.17 F

En una calle hay una fila de casas numeradas del 1 al n, donde n es un número de tres cifras. Exactamente 1/k de estos números empiezan con el dígito "2", donde k es un entero positivo. Determina los posibles valores de n.

BMO 2022 Round 1 #1

11 El problema de la primalidad. Encriptación RSA.

11.1 El test de primalidad de Fermat.

Al problema de como determinar si un número n es primo se lo conoce como problema de la primalidad. Un test de primalidad es un algoritmo que permite comprobar si un número n es primo o es compuesto. Existen dos tipos de test de primalidad:
- Determinista: determina si el número es primo o no lo es.
- Probabilístico: determina si un número es compuesto o si es "probablemente primo".
Determinar que el número es "probablemente" primo no te asegura que sea primo, pero existe una elevada probabilidad de que lo sea, y esta puede ser tan grande con se desee. O dicho de otro modo, la probabilidad de que un número "probablemente primo" sea compuesto es insignificante. Una característica de los test probabilísticos es que son mucho más rápidos que los deterministas.

Recordemos que el PTF afirma que, si p es primo, para todo número a coprimo con p se cumplirá $a^{p-1} \equiv 1 \pmod{p}$.
Por lo tanto, para demostrar que un número determinado n no es primo, bastará encontrar un número a, coprimo con n, para el cual $a^{p-1} \not\equiv 1 \pmod{p}$.

Naturalmente, no encontrar dicho número a no garantiza que n sea primo. Por ejemplo:

$n = 3215031751$ pasa el test para los valores $a = 2, 3, 5, 7$:

$$2^{3215031750} \equiv 1 \pmod{3215031751}$$
$$3^{3215031750} \equiv 1 \pmod{3215031751}$$
$$5^{3215031750} \equiv 1 \pmod{3215031751}$$
$$7^{3215031750} \equiv 1 \pmod{3215031751}$$

Y, sin embargo 3215031751 no es un número primo:

$$3215031751 = 151 \cdot 751 \cdot 28351$$

Esto no quiere decir que este método no sea efectivo. Entre todos los números n menores que 250 billones, solo este número pasa el test para los números primos 2, 3, 5 y 7 siendo un número compuesto.

Ejemplo resuelto.

Demostrar que 117 no es primo.

Solución.

Tomamos $a = 2$. Sabemos que $2^7 = 128 \equiv 11 \pmod{117}$, y que $121 \equiv 4 \pmod{117}$, luego:

$$\left(2^7\right)^{16} \equiv 11^{16} = \left(11^2\right)^8 = 121^8 \equiv 4^8 = \left(2^2\right)^8 = 2^{16} \pmod{117}$$

$$2^{117} = 2^{7 \cdot 16 + 5} = \left(2^7\right)^{16} 2^5 \equiv 2^{16} 2^5 \pmod{117} = 2^{21} \pmod{117}$$

Pero $2^{21} = \left(2^7\right)^3 \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 = 44 \pmod{117}$

Con lo que, finalmente llegamos a $2^{117} \equiv 44 \neq 2 \pmod{117}$, y por tanto 117 debe ser un número compuesto (de hecho: $117 = 13 \cdot 9$).

Ejemplo resuelto.

Demuestra, aplicando el PTF, que $2^{32}+1=4294967297$ no es un número primo.

Solución: Sea p un factor primo de $k=2^{32}+1$.

Este factor primo p estará acotado superiormente: $p<\left\lfloor\sqrt{2^{32}+1}\right\rfloor=2^{16}=65536$.

Por otro lado:

$p\mid k\Leftrightarrow k\equiv 0\pmod{p}\Leftrightarrow 2^{32}\equiv -1\pmod{p}\Rightarrow 2^{64}\equiv(-1)^2=1\pmod{p}$

Sea $d=ord_p(2)$. Está claro que $2^{64}\equiv 1\pmod{p}\Rightarrow d\mid 64=2^6\Rightarrow d=2^r$ para cierto $r\leq 6$.

Si $r<6\Rightarrow d\mid 32\Rightarrow 2^{32}\equiv 1\pmod{p}$, llegando a contradicción. Por lo tanto $r=6$ y $d=64$.

Ahora, aplicando el Corolario XXXX (página ????),

$$d=64\Rightarrow p\equiv 1\pmod{64}\Rightarrow p=64s+1$$

Con todo esto los candidatos a factor primo de k se han reducido a los primos de la forma $p=64s+1$. Vamos dando valores a s para ir obteniendo los diferentes valores de p asociados:

s=1 → p=65 no es primo.
s=2 → p=129 no es primo
s=3 → p=193 es primo pero no divide a k
s=4 → p=257 es primo pero no divide a k
s=5 → p=321 no es primo
s=6 → p=385 no es primo
s=7 → p=449 es primo pero no divide a k
s=8 → p=513 no es primo
s=9 → p=577 es primo pero no divide a k
s=10 → p=641, es primo y sí divide a k. En efecto: $k=p\cdot 6700417$

Así pues, hemos encontrado un factor de k, y por tanto hemos demostrado que no es un número primo.

Problema.

Aplicando el método anterior, comprueba si $2^{11}-1=2047$ es un número primo o compuesto.

Solución: Supongamos que p es un factor primo de $k=2^{11}-1$. Luego:

$p\mid k\Leftrightarrow k\equiv 0\pmod{p}\Leftrightarrow 2^{11}\equiv 1\pmod{p}$

Sea $d=ord_p(2)$. Está claro que $d\mid 11$ y por tanto solo puede ser $d=11$ o $d=1$.

Supongamos que $d=11$. Luego, por el Corolario XXXX, $p\equiv 1\pmod{11}$, es decir, p es de la forma $p=11s+1$ para cierto s. Vamos dando valores a s para ir obteniendo valores de p y comprobando si son primos, en cuyo caso comprobamos si son divisores de k:

s=1 → p=12 no es primo.
s=2 → p=23 es primo y divisor de k. En efecto, $k=2^{11}-1=89\cdot 23$

Así pues, hemos encontrado una factorización de k, y por tanto hemos demostrado que no es primo.

Algoritmo del Test de Primalidad de Fermat.

Input: número n.

Paso 1: Determinamos, al azar, un número $1 < a < n$

Paso 2: Determinamos (a, n) mediante el Algoritmo de Euclides.

Paso 3: Si $(a, n) \neq 1$, el número n no es primo, retornamos a.

(es muy poco probable que esto suceda)

Paso 4: Calculamos $r = a^{n-1} \pmod{n}$ mediante el EMO.

Paso 5: Si $r \neq 1$, el número n no es primo (aunque no sabemos su factorización)

Paso 6: Este test no ha sido decisivo. Se vuelve al Paso 1 para probar con otro número.

Ejemplo.

Vamos a demostrar que el número 527 es compuesto aplicando el método anterior.

Después de mucho calcular llegamos al resultado siguiente:

$$2^{40} \equiv 1 \pmod{527}$$

Por otro lado, $526 = 40 \cdot 13 + 6$, y por tanto

$$2^{526} = \left(2^{40}\right)^{13} \cdot 2^6 \equiv 1^{13} \cdot 2^6 = 2^6 = 64 \not\equiv 1 \pmod{527}$$

Por lo tanto podemos asegurar que el número 527 es compuesto (de hecho, $527 = 17 \cdot 31$).

Los números de Carmichael.

En ningún momento se ha dicho que, para todo número n compuesto, exista un a coprimo con n para el que $a^{n-1} \not\equiv 1 \pmod{n}$.

Existen números n para los cuales la identidad $a^{n-1} \equiv 1 \pmod{n}$ es cierta para todas las bases a coprimas con n y sin embargo son números compuestos.

Estos números son excepcionales (pero existen infinitos), y se llaman números **Carmichael**. El menor número Carmichael es 561.

11.2 Aplicación a la criptografía: El método RSA.

El método RSA fue descubierto/inventado en 1977 como el primer método de encriptación de clave pública de la historia. Su nombre deriva de las iniciales de los tres investigadores americanos que lo descubrieron: **Rivest**, **Shamir** y **Adleman**.

Este método se basa en la dificultad de factorizar números muy grandes. Los números utilizados en este sistema suelen tener más de 300 dígitos decimales, y intentar su factorización ocuparía miles de años para las más avanzadas computadoras que existen en la actualidad.

Descripción del método RSA.

Emisor: Alicia	Espacio público	Receptor: Bob
	¡Todo lo que pase por aquí será visto por el Enemigo!	1. El receptor selecciona dos números primos p y q muy grandes (de centenares de cifras) 2. Calcula $n = p \cdot q$ 3. Calcula $\varphi(n) = (p-1)(q-1)$ 4. Determina, al azar, un número aleatorio $1 < e < \varphi(n)$ coprimo con $\varphi(n)$ 5. La pareja (n,e) es la clave pública, que se envía al Emisor.
7. El emisor recibe la clave pública (n,e). Con ella encriptará el número secreto k de la siguiente forma:	El Enemigo puede ver la clave pública, pero no le servirá de nada (por eso se llama pública)	6. Determina $d = e^{-1} \pmod{\varphi(n)}$ La pareja (n,d) es la clave privada de desencriptación. ¡Los números p, q y d se deben mantener secretos, por eso no pueden salir de aquí!
8. Calcula $f(k) = k^e \pmod{n}$ y lo envía al Receptor. →	¡Aunque el Enemigo vea el número encriptado $f(k)$ y disponga de la clave pública (n,e) no podrá desencriptar el mensaje!	9. El receptor recibe $f(k)$ y lo desencripta de la siguiente manera: 10. Calcula $g(f(k)) = f(k)^d \pmod{n} = k$

Ejemplo.

Por su valor puramente didáctivo exponemos aquí dos ejemplos prácticos con números primos p y q muy pequeños.

Supongamos que el Emisor quiere enviar al Receptor el mensaje "16346", y el Enemigo puede escuchar cualquier información entre Emisor y Receptor.

1. El receptor selecciona dos números primos p y q muy grandes (de centenares de cifras), nosotros ahora, a efectos didácticos, tomaremos números no tan grandes:

$$p = 281 \text{ y } q = 167$$

2. Calcula $n = p \cdot q = 46927$

3. Calcula $\varphi(n) = (p-1)(q-1) = 46480$

4. Determina, al azar, un número aleatorio $1 < e < \varphi(n)$ coprimo con $\varphi(n)$:

$$e = 39423$$

5. La pareja $(n,e) = (\ 46927\ ,\ 39423\ )$ es la clave pública, que se envía al Emisor.

6. Determina $d = e^{-1} \pmod{\varphi(n)} = 26767$

La pareja $(n,d) = (\ 46927\ ,\ 26767\ )$ es la clave privada de desencriptación. Los números p, q, d se deben mantener secretos en todo momento.

7. Supongamos que el Emisor quiere enviar al Receptor el número secreto $k = 16346$.

8. El Emisor calcula

$$f(k) = k^e \pmod{n} = 16346^{\ 39423} \pmod{46927} = 21166$$

Envía al Receptor el número 21166

9. El receptor recibe 21166 y lo desencripta de la siguiente manera:

10. Calcula $21166^{\ d} \pmod{n} = 21166^{\ 26767} \pmod{46927} = 16346$

Obteniendo el número secreto desencriptado 16346.

Comentario.

El punto fundamental de la encriptación RSA es que el "Enemigo", aunque disponga de la clave pública (n,e) y del número encriptado k, no será capaz de desencriptarlo. Y esto es debido a que necesitaría determinar $d = e^{-1} \pmod{\varphi(n)}$, y desconoce $\varphi(n)$.

En efecto, $\varphi(n)$ es muy fácil de calcular si se conoce la factorización de n, recordemos que el receptor pudo calcular $\varphi(n)$ porque conocía desde un principio:

$$n = p \cdot q \Rightarrow \varphi(n) = (p-1)(p-1) = pq - p - q + 1 = n - p - q + 1$$

y la factorización de un número muy grande como es n es terriblemente complicada.

La seguridad del sistema RSA radica en la imposibilidad computacional de factorizar un número de 200 cifras, ya que, con los algoritmos actuales y las mejores computadoras requeriría siglos.

12 Números primos de Fermat y de Mersenne.

12.1 Números primos de Fermat.

12.1.1 Definición. Números de Fermat. Primos de Fermat.

Queremos estudiar los números primos de la forma 2^n+1. Ya vimos en el Tema 4 que si es primo entonces n debe ser una potencia de 2.

Definimos el n-ésimo **número de Fermat** como $F_n = 2^{2^n}+1,\ n \geq 0$.

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537,\ F_5 = 4294967297$$

El propio Fermat conjeturó que F_n era primo para todo n, sin embargo Euler demostró que $641 \mid F_5$. El razonamiento se encuentra en el Tema 4.

Así pues, no todo número de Fermat es primo. Llamaremos "**primos de Fermat**" a aquellos números de Fermat que sean primos. Es un problema abierto la existencia o no de infinitos primos de Fermat. Se conjetura que F_n es compuesto para $n \geq 5$.

12.1.2 Proposición.

Los números de Fermat son todos coprimos entre ellos: $(F_n, F_m)=1$ si $n \neq m$.

Demostración.

Supongamos que $m > n$, y sea d un divisor común de F_n y F_m. En primer lugar vemos que d debe ser impar, pues lo son todos los números de Fermat.

$$d \mid F_n = 2^{2^n}+1 \Leftrightarrow 2^{2^n}+1 \equiv 0 \pmod{d} \Leftrightarrow 2^{2^n} \equiv -1 \pmod{d}$$

Pero entonces

$$2^{2^m} = 2^{2^n 2^{m-n}} = \left(2^{2^n}\right)^{2^{m-n}} \equiv (-1)^{2^{m-n}} \equiv 1 \pmod{d}$$

Pero, por otro lado, $d \mid F_m = 2^{2^m}+1 \Leftrightarrow 2^{2^m}+1 \equiv 0 \pmod{d} \Leftrightarrow 2^{2^m} \equiv -1 \pmod{d}$, con lo cual llegamos a $1 \equiv -1 \pmod{d} \Leftrightarrow 2 \equiv 0 \pmod{d} \Leftrightarrow d \mid 2$, y puesto que d es impar, solo puede ser $d = 1$.

Nota: Un argumento alternativo podría ser aprovechar la identidad

$$F_n - 2 = F_0 F_2 \ldots F_{n-1}$$

Que se deduce de

$$2^{2^m} - 1 = (2-1)(2+1)\left(2^2+1\right)\ldots\left(2^{2^{n-1}}+1\right)$$

Y por tanto, si d divide F_n y F_m, con $m < n$, también dividirá a $2 = F_n - F_0 \ldots F_{n-1}$, y puesto que d es impar, llegamos a $d = 1$

12.2 Números primos de Mersenne.

12.2.1 Números de Mersenne. Primos de Mersenne.

Definimos los números de Mersenne como aquellos de la forma $M_n = 2^n - 1,\ n \geq 1$.

Está claro que si n es compuesto, también lo será M_n:

Si $n = ab \Rightarrow M_n = 2^{ab} - 1 = \left(2^a\right)^b - 1^b = \left(2^a - 1\right)\left(2^{a-1} + 2^{a-2} + ... + 2 + 1\right) \Rightarrow 2^a - 1 \mid M_n$

Por lo tanto, si M_n es primo, también lo será n.

Sin embargo, existen primos p para los cuales M_p es compuesto. Por ejemplo:

$$47 \mid M_{23},\ 167 \mid M_{83},\ 263 \mid M_{13}$$

Llamaremos "**primos de Mersenne**" a los números de Mersenne que sean primos. Es un problema abierto la existencia o no de infinitos primos de Mersenne.

12.2.2 Los mayores primos de Mersenne descubiertos hasta ahora.

El mayor número primo de Mersenne que se conoce es $2^{82589933}-1$, descubierto en diciembre del 2018.

Los primeros 38 primos de Mersenne son los siguientes:

2^2-1, 2^3-1, 2^5-1, 2^7-1, $2^{13}-1$, $2^{17}-1$, $2^{19}-1$, $2^{31}-1$, $2^{61}-1$, $2^{89}-1$, $2^{107}-1$, $2^{127}-1$, $2^{521}-1$, $2^{607}-1$, $2^{1279}-1$, $2^{2203}-1$, $2^{2281}-1$, $2^{3217}-1$, $2^{4253}-1$, $2^{4423}-1$, $2^{9689}-1$, $2^{9941}-1$, $2^{11213}-1$, $2^{19937}-1$, $2^{21701}-1$, $2^{23209}-1$, $2^{44497}-1$, $2^{86243}-1$, $2^{110503}-1$, $2^{132049}-1$, $2^{216091}-1$, $2^{756839}-1$, $2^{859433}-1$, $2^{1257787}-1$, $2^{1398269}-1$, $2^{2976221}-1$, $2^{3021377}-1$, $2^{6972593}-1$.

13 Número y suma de los divisores de un entero.

13.1 Número de divisores de un entero.

13.1.1 Definición. Número de divisores de un entero.

Dado un número entero n, definimos $\tau(n)$ como el número de enteros positivos divisores de n.

Ejemplos: Los divisores positivos de 6 son $\{1, 2, 3, 6\}$, luego $\tau(6) = 4$.
Los divisores positivos de 20 son $\{1, 2, 4, 5, 10, 20\}$, luego $\tau(20) = 6$.
$\tau(1) = 1$, $\tau(2) = 2$, $\tau(3) = 2$, $\tau(4) = 3$, $\tau(5) = 2$, $\tau(6) = 4$, $\tau(7) = 2$, $\tau(8) = 4$, $\tau(9) = 3$, $\tau(10) = 4$
Problema motivador: #1.2.1.
Con Mathematica:

```
In[1]:= Divisors[1729]
Out[1]= {1, 7, 13, 19, 91, 133, 247, 1729}
```

13.1.2 Proposición.

Para cualquier entero positivo n,
a) $\tau(n) \geq 1$ y $\tau(n) = 1 \Leftrightarrow n = 1$.
b) Para todo $n \geq 2$, $\tau(n) \geq 2$ y $\tau(n) = 2 \Leftrightarrow$ n es primo.
c) $\tau(n) \leq 2\sqrt{n}$

Demostración. a) y b) se deducen de la propia definición de $\tau(n)$.
c) Cada divisor positivo a de n tiene asociado su divisor complementario $b = n/a$.
Puesto que $a \cdot b = a(n/a) = n$, se tiene que cumplir $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$. Así pues, existirán como mucho $2\sqrt{n}$ divisores de n.

13.1.3 Teorema.

La función $d(n)$ es **multiplicativa**, es decir, si $n = ab$, con $(a,b) = 1$, entonces

$$\tau(n) = \tau(a)\,\tau(b)$$

13.1.4 Corolario.

a) Si $n = p^a$ para cierto p primo, entonces los divisores de n son

$$\{1, p, p^2, p^3, \ldots, p^a\}$$

y por tanto $\tau(n) = a + 1$

b) Si $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ es la descomposición en factores primos de n, entonces los divisores d de n son todos los números que se pueden escribir como

$$d = p_1^{b_1} p_2^{b_2} \ldots p_r^{b_r} \text{ con } 0 \leq b_i \leq a_i,$$

y

$$\tau(n) = (a_1 + 1)(a_2 + 1)\ldots(a_r + 1)$$

Por ejemplo: $\tau(2904) = d(2^3 \cdot 3 \cdot 11^2) = (3+1)(1+1)(2+1) = 24$

13.1.5 F

Demostrar que $\tau(n)$ es impar si y solo si n es un cuadrado perfecto.

13.1.6 F

Demostrar que $\sigma(n)$ es primo si y solo si $n = p^{q-1}$ con p, q primos.

13.1.7 MF

Si tomamos aleatoriamente un divisor de 10^{99}, ¿Cuál es la probabilidad de que sea múltiplo de 10^{88}?

AIME 1998#5

13.1.8 F

Determina todos los enteros positivos n tales que $\tau(n) = 6$.

13.1.9 F

Determina el número de enteros positivos que son divisores de al menos uno de los siguientes números: 10^{10}, 15^7, 18^{11}.

AIME II 2005#4

13.1.10 D

Sea $\tau(n)$ el número de enteros positivos de n. Determina la suma de los seis enteros positivos n más pequeños tales que

$$\tau(n) + \tau(n+1) = 7$$

AIME 1 2019#9

13.1.11 F

¿Cuántos divisores positivos de 2004^{2004} son divisibles por exactamente 2004 enteros positivos?

AIME II 2004#8

13.1.12 F

Joey, Chloe y su hija Zoe cumplen años el mismo día. Joey es un año mayor que Chloe y Zoe cumple hoy su primer año. Hoy es el primero de los nueve aniversarios en los que la edad de Chloe será múltiple de la edad de Zoe. Determina la suma de los dos dígitos de la edad de Joey que tendrá la próxima vez que sea múltiple de la edad de Zoe.

(A) 7 (B) 8 (C) 9 (D) 10 (E) 11

AMC 12B 2018#14

13.1.13 [F]

Sea N un entero positivo. Supongamos que existen exactamente 2005 pares ordenados (x, y) de enteros positivos tales que

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{N}$$

Demuestra que N es un cuadrado perfecto.

BMO 2005 Round 2 #1

13.1.14 Proposición. Producto de los divisores de un entero.

Una propiedad interesante de $\tau(n)$ es que el producto de todos los divisores de n es igual a la raíz cuadrada de $n^{\tau(n)}$:

$$\prod_{d|n} d = \sqrt{n^{\tau(n)}}$$

Demostración.

La clave está en observar que los divisores de un número van por parejas: Dado un divisor d, tenemos su divisor complementario $d' = n/d$, de forma que $d \cdot d' = n$. Sean $d_1, d_2, ..., d_{\tau(n)}$ todos los divisores de n. Si multiplicamos dos veces dichos divisores, los factores se pueden reorganizar agrupando $\tau(n)$ parejas cuyo resultado sea n, luego:

$$\left(\prod_{d|n} d\right)^2 = \prod_{d|n} d \cdot \prod_{d|n} d = d_1.d_2...d_{\tau(n)} \cdot d_1.d_2...d_{\tau(n)} = n^{\tau(n)} \Leftrightarrow \left(\prod_{d|n} d\right)^2 = n^{\tau(n)}$$

13.1.15 Corolario.

De la proposición anterior se deduce que $n^{\tau(n)}$ es un cuadrado perfecto. Esto es obvio si $\tau(n)$ es par, pero no estaba tan claro si $\tau(n)$ es impar. Pero en el problema 13.1 anterior ya demostramos que si $\tau(n)$ es impar, n es un cuadrado perfecto, y por tanto también lo es $n^{\tau(n)}$.

13.1.16 Ejemplo.

El producto de todos los divisores de 16 es

$$\prod_{d|n} d \,|16 = \sqrt{16^{\tau(n)}} = \sqrt{16^5} = 4^5 = 1024$$

En efecto, $1 \cdot 2 \cdot 4 \cdot 8 \cdot 16 = 1024$.

13.1.17 MD

Denotamos por $d(n)$ el número de enteros positivos que dividen a n, incluyendo 1 y n. Por ejemplo: $d(1)=1$, $d(2)=2$, $d(12)=6$ (esta función es conocida como la función divisor). Sea

$$f(n)=\frac{d(n)}{\sqrt[3]{n}}$$

Existe un único entero positivo N tal que $f(N)>f(n)$ para todo entero positivo $n\neq N$. Determina la suma de los dígitos de N.

(A) 5 (B) 6 (C) 7 (D) 8 (E) 9

AMC 12A 2021#25

13.2 Suma de los divisores de un entero.

13.2.1 Definición. Suma de los divisores de un entero.

Dado un número entero n, definimos $\sigma(n)$ como la suma de todos los enteros positivos divisores de n, incluyendo 1 y el propio n.

$$\sigma(n) = \sum_{d|n} d$$

Está claro que $\sigma(n) \geq n+1$, y $\sigma(n) = n+1$ si y solo si n es primo.

Ejemplos.

Los divisores positivos de 6 son $\{1, 2, 3, 6\}$, luego $\sigma(6) = 1+2+3+6 = 12$.

Los divisores positivos de 20 son $\{1, 2, 4, 5, 10, 20\}$, luego

$\sigma(20) = 1+2+4+5+10+20 = 42$.

13.2.2 Teorema.

La función $\sigma(n)$ es multiplicativa.

13.2.3 Proposición.

a) Si $n = p^a$ para cierto primo p, entonces $\sigma(n) = 1 + p + p^2 + ... + p^a$.

b) Si $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$ es la descomposición en factores primos de n, entonces

$$\sigma(n) = \left(1 + p_1 + p_1^2 + ... + p_1^{a_1}\right)\left(1 + p_2 + p_2^2 + ... + p_2^{a_2}\right)...\left(1 + p_r + p_r^2 + ... + p_r^{a_r}\right) =$$
$$= \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} ... \frac{p_r^{a_r+1} - 1}{p_r - 1}$$

Demostración.

a) Aplicando la propia definición de $\sigma(n)$.

b) Basta tener en cuenta que $\sigma(n)$ es multiplicativa y aplicar la serie geométrica:

$$x^n + x^{n-1} + x^{n-2} + ... + x + 1 = \frac{x^{n+1} - 1}{x - 1}$$

Por ejemplo:

$$180 = 2^2 \cdot 3^2 \cdot 5 \Rightarrow \sigma(180) = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = \frac{7}{1} \cdot \frac{26}{2} \cdot \frac{24}{4} = 7 \cdot 13 \cdot 6 = 546$$

13.2.4 Problema resuelto.

Sea n un entero positivo tal que $24|n+1$. Demuestra que entonces se cumple $24|\sigma(n)$.

Putnam 1969

Solución.

$$24|n+1 \Rightarrow \begin{cases} n+1 \equiv 0 \pmod 3 \Leftrightarrow n \equiv -1 \pmod 3 \\ n+1 \equiv 0 \pmod 8 \Leftrightarrow n \equiv -1 \pmod 8 \end{cases}$$

Observamos que los divisores de un número van en parejas: Si d_1 es divisor entonces su complementario $d_2 = \frac{n}{d_1}$ también es divisor.

Por un lado, haciendo módulo 3:

$d_1 \cdot d_2 = d_1 \frac{n}{d_1} = n \equiv -1 \pmod 3$, y las únicas opciones son:

$d_1 \equiv 1 \pmod 3$ y $d_2 \equiv 2 \pmod 3$ o viceversa.

En todo caso se cumple $d_1 + d_2 \equiv 0 \pmod 3$.

Y por otro lado, haciendo módulo 8:

$d_1 \cdot d_2 = d_1 \frac{n}{d_1} = n \equiv -1 \pmod 8$, y las únicas opciones son:

$d_1 \equiv 1 \pmod 8$ y $d_2 \equiv 7 \pmod 8$ o viceversa.

$d_1 \equiv 3 \pmod 8$ y $d_2 \equiv 5 \pmod 8$ o viceversa.

En todo caso se cumple $d_1 + d_2 \equiv 0 \pmod 8$.

Así pues, $d_1 + d_2 \equiv 0 \pmod 3$ y $d_1 + d_2 \equiv 0 \pmod 8$, luego $d_1 + d_2 \equiv 0 \pmod{24}$, y por tanto el sumatorio $\sigma(n)$ se puede reordenar por parejas divisibles entre 24, y por tanto: $\sigma(n) = \sum_{d|n} d$ será divisible entre 24.

13.2.5 [F]

Los únicos factores primos de un número n son 2 y 3. Si la suma de todos los divisores de n (incluyendo el propio n) es 1815, determina n.

PUMaC 2011/NT #A1

13.3 Números perfectos.

13.3.1 Definición de número perfecto.

Los antiguos griegos clasificaban los enteros positivos en tres clases, en función de la suma de sus divisores:

"Números perfectos" si $\sigma(n) = 2n$

"Números abundantes" si $\sigma(n) > 2n$

"Números deficientes" si $\sigma(n) < 2n$

Los primeros números perfectos son: $6, 28, 496, 8128$.

Si utilizamos la notación clásica en la que se cuentan solo los divisores propios, es decir, todos menos el propio n, tiene más sentido la idea de "número perfecto" como aquel que es igual a la suma de todos sus divisores (propios).

13.3.2 Teorema. Caracterización de los números pares perfectos.

Un número par n es perfecto si y solo si existen números primos p, q tales que

$$n = 2^{p-1}q \quad \text{con} \quad q = 2^p - 1$$

Así pues, cada número par perfecto está asociado a un primo de Mersenne, que fueron introducidos en el Tema 19.

Demostración.

$\Rightarrow$ Supongamos que n se puede escribir de esta forma.

Está claro que q es impar , $2n = 2^p q$ y que $q+1 = 2^p$.

$\sigma\left(2^{p-1}\right) = \dfrac{2^{p-1+1}-1}{2-1} = 2^p - 1$, $\sigma(q) = q+1$

Luego $\sigma(n) = \sigma\left(2^{p-1}\right)\sigma(q) = \left(2^p - 1\right)(q+1) = 2^p q + 2^p - (q+1) = 2n$

Y por tanto n es perfecto.

$\Leftarrow$ Supongamos ahora que n es perfecto, es decir, que $\sigma(n) = 2n$. Puesto que además estamos suponiendo que n es par, podemos escribir $n = 2^{k-1}m$ con m impar y $k \geq 2$.

Luego $2^k m = 2n = \sigma(n) = \sigma\left(2^{k-1}m\right) = \sigma\left(2^{k-1}\right)\sigma(m) = \left(2^k - 1\right)\sigma(m)$

Donde hemos utilizado que $\sigma\left(2^{k-1}\right) = \dfrac{2^{k-1+1}-1}{2-1} = 2^k - 1$.

De la igualdad $2^k m = \left(2^k - 1\right)\sigma(m)$ se deduce que $2^k - 1 \mid 2^k m$, y puesto que $\left(2^k - 1, 2^k\right) = 1$, el Lema de Euclides implica que $2^k - 1 \mid m$, y por tanto

$m = \left(2^k - 1\right)l$ para cierto entero l impar.

$2^k\left(2^k - 1\right)l = 2^k m = 2n = \sigma(n) = \sigma\left(2^{k-1}(2^k - 1)l\right) = \sigma\left(2^{k-1}\right)\sigma\left((2^k - 1)l\right) =$

$= \left(2^k - 1\right)\sigma\left((2^k - 1)l\right) \Rightarrow 2^k l = \sigma\left((2^k - 1)l\right)$ (*)

Si $l>1$ entonces $1, l, (2^k-1)l$ son factores diferentes de $(2^k-1)l$, y por tanto, por la definición de σ, tenemos que $1+l+(2^k-1)l \le \sigma((2^k-1)l)$

Luego $2^k l = \sigma((2^k-1)l) \ge 1+l+(2^k-1)l = 1+l+2^k l-l = 1+2^k l$ absurdo.

Así pues, $l=1$, y $n=2^{k-1}(2^k-1)$. Ahora solo falta demostrar que k es primo.

De (*) tenemos que $2^k = \sigma(2^k-1) = 1+2^k-1+\sum_{\substack{d|(2^k-1)\\ 1<d<2^k-1}} d \Rightarrow \sum_{\substack{d|(2^k-1)\\ 1<d<2^k-1}} d = 0$

Es decir, 2^k-1 no tiene divisores propios, es decir, es un número primo. Ya vimos en el Tema 15 que si un número de Mersenne es primo entonces k es primo, y con esto acabamos la demostración.

13.3.3 Observación.

Acabamos de ver que todo número perfecto par está asociado a un primo de Mersenne. Es un problema abierto la existencia o no de infinitos números perfectos pares, y apenas sabemos nada de los números perfectos impares, ni tan solo si existe alguno.

14 Encriptación mediante Curvas Elípticas. Encriptación bitcoin.

En 1985, Neal Koblitz y Victor Miller propusieron independientemente la criptografía basada en curvas elípticas. Es la técnica utilizada para el bitcoin entre otras criptomonedas.

14.1 Curvas elípticas sobre cuerpos en general.

Trabajar con números reales, es decir, en el plano $IR \times IR$, nos permite visualizar las operaciones que realizamos, con lo que "vemos qué estamos haciendo", pero es un plano teórico, es un primer paso para tomar confianza con los métodos y fórmulas utilizadas para pasar después a trabajar sobre cuerpos finitos, que es como trabajan las computadoras.

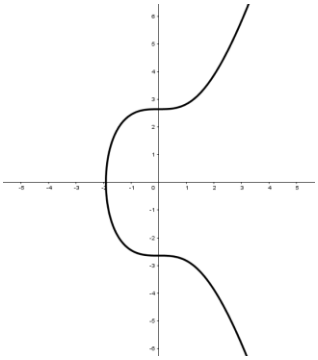
Una curva elíptica es una curva en el plano con ecuación

$$y^2 = x^3 + a\,x + b$$

La curva elíptica utilizada por Bitcoin, Ethereum y muchas otras criptomonedas es la curva **secp256k1**, cuya ecuación es:

$$y^2 = x^3 + 7$$

Es decir, es un caso particular de curva elíptica tomando $a = 0$ y $b = 7$. Su representación gràfica sobre los reales es la siguiente:



Hay que dejar muy claro que esta representación de la curva es sobre el cuerpo IR, y por lo tanto se presenta como una colección de puntos ordenados siguiendo una trayectoria suave y contínua, pero en criptografía se utilizan cuerpos finitos, y en estos cuerpos esta misma curva se presenta como una nube de puntos con poca o ninguna continuidad visible.

Curvas elípticas no singulares.

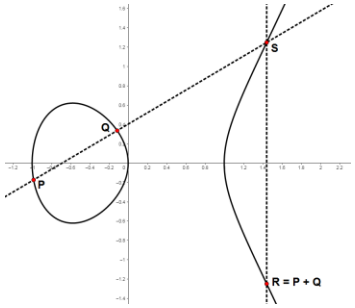
Diremos que una curva elíptica $y^2 = x^3 + a\,x + b$ es no singular cuando su discriminante sea distinto de cero:

$$4a^2 + 27b^2 \neq 0$$

Suma de puntos en una curva elíptica.

Sean $P=(x_1,y_1)$ y $Q=(x_2,y_2)$ con $P\neq\pm Q$ dos puntos de una curva elíptica. Definimos el punto $R=P+Q$, al que llamaremos suma de P y Q, de la siguiente forma:

1) Trazamos la recta r que pasa por P y Q.
2) Determinamos el tercer punto S de corte de esta recta con la curva elíptica.
3) Trazamos el simétrico de S respecto del eje X.



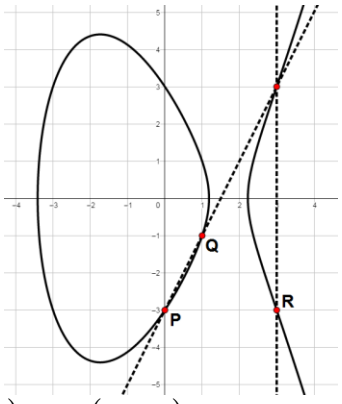
Con coordenadas:

Si $P=(x_1,y_1)$ y $Q=(x_2,y_2)$ con $P\neq\pm Q$, las coordenadas de $R=(x_3,y_3)$ son:

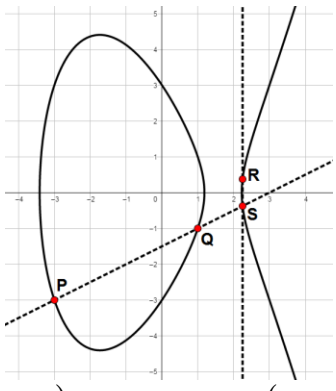
$$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2\ ,\ y_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3)-y_1$$

Ejemplo.

Dada la curva elíptica $y^2=x^3-9x+9$



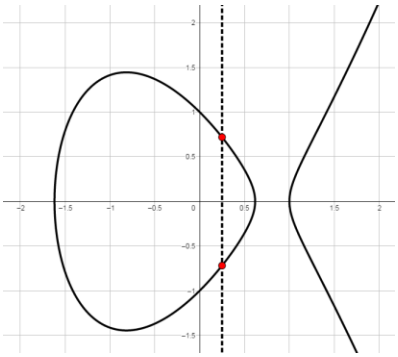
$$P=(0,-3),Q=(1,-1)\Rightarrow R=P+Q=(3,-3)$$



$$P=(-3,-3),Q=(1,-1)\Rightarrow R=P+Q=(9/4,3/8)=(2.25,0.375)$$

El punto del infinito.

Si $P=(x_1,y_1)$ y $Q=(x_2,y_2)$ con $x_1=x_2$, la recta $r=PQ$ es vertical y no tiene ningún otro punto de corte con la curva. Para evitar esta excepción, añadiremos a nuestro conjunto de puntos un punto al que denotaremos por O y que llamaremos "elemento cero" o "punto del infinito", que será, por definición, el punto de intersección entre una recta vertical y la curva.



Multiplicación escalar de puntos en una curva elíptica.

Cuando $Q=P$, la recta $r=PQ$ se convierte en la recta tangente por el punto P a la curva elíptica, y esto nos justifica definir el punto $R=2P=P+P$ de la siguiente forma:

1) Trazamos la recta r tangente a la curva elíptica por el punto P.
2) Determinamos el tercer punto S de corte de esta recta con la curva elíptica.
3) Trazamos el simétrico de S respecto del eje X.

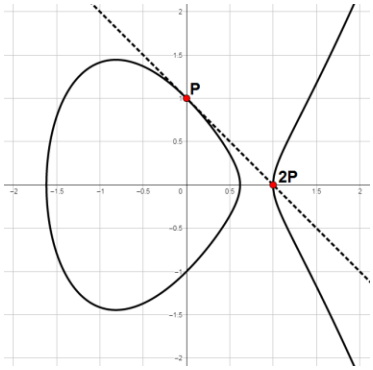
Con coordenadas:

Si $P=(x_1,y_1)$ y la curva elíptica es $y^2=x^3+ax+b$, las coordenadas de $2P=(x_3,y_3)$ son:

$$x_3=\left(\frac{3x_1^2+a}{2y_1}\right)^2-2x_1\ ,\ y_3=\left(\frac{3x_1^2+a}{2y_1}\right)(x_1-x_3)-y_1$$

Ejemplo.

Sea $P=(0,1)$ de la curva elíptica $y^2=x^3-2x+1$, entonces $2P=(1,0)$



Múltiplos de un punto. Orden de un punto.

Una vez que hemos definido $2P=P+P$, podemos definir $3P=P+2P$, $4P=P+3P$,... a los que llamaremos múltiplos del punto P.

Dado un punto P, definimos su orden como el menor natural n tal que $nP=O$, si es que existe.

Método efectivo para calcular múltiplos de un punto. El método del "dobla y suma".

La misma técnica para optimizar la exponenciación que explicamos en el apartado 12.2 se puede aplicar perfectamente al problema de optimizar la multiplicación de puntos.

Supongamos que queremos calcular $227P$ para cierto punto P dado. No es nada efectivo ir calculado, una tras otra, las 226 multiplicaciones

$$2P = P + P \to 3P = P + 2P \to 4P = P + 3P \to \ldots \to 227P = P + 226P$$

Es mucho más efectivo aprovechar los cálculos anteriores para ir calculando las potencias de dos:

$$2P = P + P$$
$$4P = 2P + 2P = 2(2P)$$
$$8P = 4P + 4P = 2(4P)$$
$$16P = 8P + 8P = 2(8P)$$
$$\ldots$$

Y ahora, puesto que la descomposición binaria de 227 es 11100011, tenemos

$$227P = 2^7P + 2^6P + 2^5P + 2^1P + 2^0P$$

En total, entre potencias $2^k P$ y las sumas anteriores hemos reducido el cálculo a 8 operaciones.

Este método se llama "**dobla y suma**" y permite calcular puntos nP con n enormes en un número reducido de operaciones. Por ejemplo, aunque el número n fuera tan grande como el número de átomos del universo, del orden de $10^{82} \cong 2^{275}$, este método permitiría determinar nP en apenas 275 operaciones.

El problema del logaritmo discreto en curvas elípticas (ECDLP).

Planteamos ahora el problema inverso:

Dados dos puntos P y Q, determinar el valor de n tal que $Q = nP$

Llamaremos a resolver este problema el "**logarítmo discreto de P**".

Acabamos de ver que, dado un punto P y un número natural n, es fácil y rápido determinar el punto nP mediante la técnica de "dobla y suma". Pero el problema inverso, dado un punto P y el punto nP, es terriblemente lento determinar el valor de n, pues no podemos aplicar el truco anterior y debemos tenemos que ir probando múltiplo a múltiplo:

$$P \to 2P \to 3P \to 4P \to \ldots$$

La terrible dificultad de encontrar el logarítmo discreto se llama "**Elliptic Curve Discrete Logarithm Problem**" (ECDLP), y es el fundamento de la encriptación mediante curvas elípticas.

Este problema es similar a otros logaritmos discretos estudiamos anteriormente, y la ventaja del ECDLP respecto de los anteriores es que parece ser mucho más duro, y por tanto mucho más seguro.

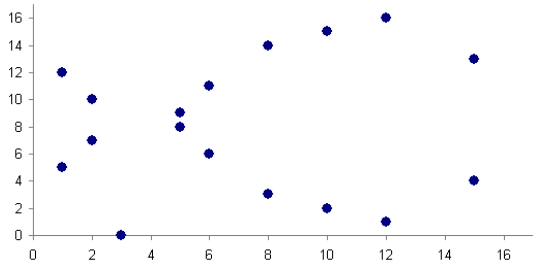
Una vez introducidas estas ideas, pasaremos a desarrollarlas en planos sobre cuerpos finitos.

14.2 Curvas elípticas sobre cuerpos finitos.

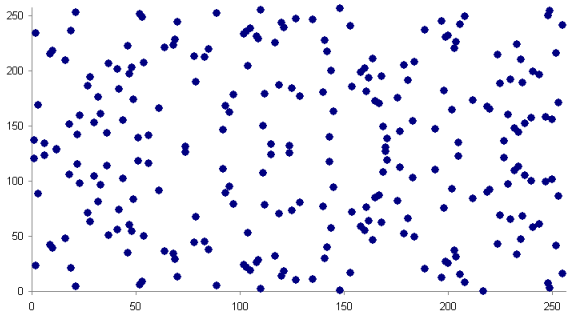
La curva **secp256k1**, sobre F_{17} consta de los siguientes 17 puntos:

(1,5) ; (1,12) ; (2,7) ; (2,10) ; (3,0) ; (5,8) ; (5,9) ; (6,6) ; (6,11) ; (8,3) ; (8,14) ;(10,2); (10,15) ; (12,1) ; (12,16) ; (15,4) ; (15,13)

Y su representación gráfica es:



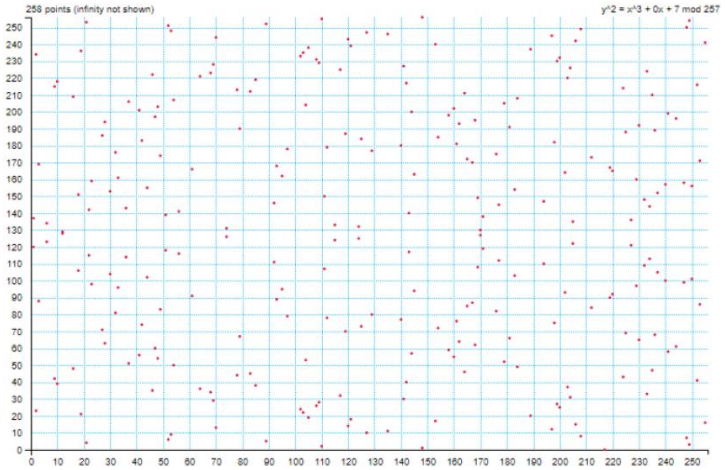
Esta misma curva, sobre F_{257} consta de 257 puntos y su representación en un sistema X-Y es una nube de puntos:



El bitcoin trabaja sobre $F_{2^{28}+1}$, y sobre este cuerpo la curva **secp256k1** es ya una nube de

115792089237316195423570985008687907852837564279074904382605163141518161494337

puntos totalmente dispersos, imposible de representar visualmente. Una muestra sería la siguiente:



Práctica de Python.

Crea un programa de Python que genere todos los puntos de la curva **secp256k1** módulo un cuerpo F_p dado:

```
#
# Generador de puntos de la curva secp256k1 módulo p por Brute-Force
#
p=257
Total=0
for x in range (0,p):
    for y in range (0,p):
        v=y**2-x**3-7
        if v%p==0:
            print(x,",",y)
            Total=Total+1
print("Total de puntos:",Total)
```

Exporta estos puntos generados por Python a una hoja de Excel mediante las opciones de "importar dados" de la hoja de cálculo, para representarlos mediante una nube de puntos.

Comprueba, mediante este programa, los resultados obtenidos en los ejemplos anteriores, y genera la nube de puntos asociada a la curva **secp256k1** para el caso del cuerpo F_{23}.

La encriptación bitcoin.

Para encriptar bitcoin se utiliza la curva elíptica **secp256k1**, cuya ecuación es:

$$y^2 = x^3 + 7$$

Sobre el campo finito Z_p, con $p = 2^{256} - 2^{32} - 977$.

Aquí se eligió p para estar relativamente cerca de 2^{256}, aunque no es el primo más grande menor de 2^{256}; hay muchos primos entre p y 2^{256}. Otros factores también entraron en la elección de p.

El punto base elegido para el bitcoin es, en notación hexadecimal:

x = 79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798
y = 483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8

Este punto base se eligió para tener un módulo grande, y de hecho su orden es aproximadamente 2^{256}. Específicamente, su orden, escrito en hexadecimal, es

n = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141

El siguiente programa Python nos permite comprobar que, efectivamente, este punto pertenece a la curva dada:

```
x = 0x79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798
y = 0x483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
p = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFC2F
print( (y*y-x*x*x-7)%p == 0 )
```

Cuyo output es, obviamente, "True".

Otro ejemplo real de los parámetros utilizados en ECDH por Google.com son los de la curva **P-384**: $x^2=y^3+ax+b \bmod(p)$, con:

a=115792089210356248762697446949407573530086143415290314195533631308867097853948
b=105836372515214212932612978004726840911444101599372555483525631403946740129 1
p=115792089210356248762697446949407573530086143415290314195533631308867097853951

Múltiples de un punto.

Tomemos la curva $y^2 = x^3 + 2x + 3 \pmod{97}$ y el punto $P = (3,6)$. Los múltiplos nP generan una sucesión cíclica de orden 5, es decir, el orden del punto P es 5:

$$1P = P = (3,6), 2P = (80,10), 3P = (80,87), 4P = (3,91), 5P = O, 6P = P, 7P = 2P, ...$$

Además, está claro que estos cinco puntos forman un grupo cerrado con la suma: La suma de dos múltiplos de P es también un múltiplo de P. Es lo que se llama un "subgrupo" del grupo general de la suma de puntos.

Un resultado conocido de la Teoría de Grupos es que el orden de cualquier subgrupo de un grupo dado es un divisor del orden de dicho grupo.

Por ejemplo, la curva $y^2 = x^3 - x + 3 \pmod{37}$ tiene orden 42. Por lo tanto, todos sus subgrupos tendrán orden 1, 2, 3, 6, 7, 14, 21 o 42. En particular:

$$P = (2,3), 2P = (23,14), 3P = (21,17), 4P = (21,20), 5P = (23,23), 6P = (2,34), 7P = O$$

Y por tanto el orden de (2 , 3) es 7.

Para los propósitos de la criptografía ECC, interesa encontrar puntos que tengan el mayor orden posible.

14.3 Protocolo de intercambio de claves Diffie-Hellmann en Curvas Elipticas (ECDH).

Supongamos que Alicia y Bob desean generar una clave secreta común R que solo ellos deben conocer, pero se tienen que comunicar a través de un espacio público no seguro.

Alicia	Espacio público	Bob
	¡Todo lo que pase por aquí será visto por el Enemigo!	
Alicia y Bob pactan los siguientes datos públicos: 1. La curva elíptica $y^2 = x^3 + ax + b \pmod{p}$ usada , es decir, los parámetros a , b , p 2. Un punto generador G de esta curva. Alicia envía a Bob estos datos a, b, p, G →		Bob recibe a, b, p, G
Determina, al azar, un número aleatorio α Es su clave privada.		Determina, al azar, un número aleatorio β Es su clave privada.
Recibe $Q = \beta G$ ←		Computa $Q = \beta G$ y lo envía a Alicia
Computa $P = \alpha G$ Y lo envía a Bob →		Recibe $P = \alpha G$
Computa $R = \alpha(\beta G)$		Computa $R = \beta(\alpha G)$
Puesto que $\alpha(\beta G) = \beta(\alpha G)$, Alicia y Bob pueden compartir esta clave secreta R, que en ningún momento será transmitida por el espacio público ni podrá ser calculada por nadie más.	El enemigo solo puede ver $Q = \beta G$ y $P = \alpha G$ pero con ellos no es capaz de determinar ni α ni β, y por tanto no es capaz de determinar R, gracias al "Problema del Logaritmo Discreto en ECDH".	

Soluciones.

5.1.1

a) $7 \equiv 7$ b) $23 \equiv 23$ c) $29 \equiv 5$ d) $168 \equiv 0$ e) $773 \equiv 5$

5.1.2

a) $15 \equiv 15$ b) $21 \equiv 21$ c) $30 \equiv 6$ d) $200 \equiv 8$ e) $1441 \equiv 1$

5.1.3

a) 9 b) 23 c) 0 d) 14

5.1.4

a) 5 b) 9 c) 13 d) 15

5.1.5

a) 1 b) 11 c) 14 d) 1 e) 3 f) 0 g) 8 h) 16

5.1.6

a) 2 b) 6 c) 3 d) 4 e) 8

5.1.7

$2023 = 289 \cdot 7 + 0$, luego volverá a a ser jueves (C)

5.2.1

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

5.2.2

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

5.6.1

Si $n \geq 6$, está claro que los factores 3 y 6 están dentro de $n!$, luego $6 \cdot 3 = 9 \cdot 2 \mid n!$.
Por lo tanto, solo nos tenemos que ocupar de $1!+2!+3!+4!+5! = 153 = 17 \cdot 9$
Así pues:

$$\left.\begin{array}{l} 1!+2!+3!+\ldots+5! \equiv 0 \pmod 9 \\ 6!+7!+\ldots+n! \equiv 0 \pmod 9 \end{array}\right\} \Rightarrow 1!+2!+3!+\ldots+n! \equiv 0+0=0 \pmod 9$$

Y por tanto el residuo al dividirlo entre 9 es 0.

5.6.2

Por ejemplo: $6^2 \equiv 4^2 \pmod 5$, pero sin embargo, $6 \not\equiv 4 \pmod 5$

5.6.3

$$\left.\begin{array}{l} 2^5 = 32 \equiv 4 = 2^2 \pmod 7 \\ 2^4 = 16 \equiv 2 \pmod 7 \end{array}\right\} \Rightarrow 2^{50} = \left(2^5\right)^{10} = \left(2^2\right)^{10} \pmod 7 = \left(2^5\right)^4 \pmod 7 = \left(2^2\right)^4 \pmod 7 =$$

$$= \left(2^4\right)^2 \pmod 7 = 2^2 \pmod 7 = 4 \pmod 7, \text{ luego el residuo es 4.}$$

$41 = 6 \pmod 7 = -1 \pmod 7 \Rightarrow 41^{65} \pmod 7 = (-1)^{65} \pmod 7 = -1 \pmod 7 = 6 \pmod 7$, luego el residuo es 6.

5.6.4

$$2^{11} = 2048 = 1 \pmod{89} \Rightarrow 2^{44} = 2^{4\cdot 11} = \left(2^{11}\right)^4 = 1^4 \bmod 89 = 1 \bmod 89 \Rightarrow$$

$$2^{44} - 1 \pmod{89} = 1 - 1 \pmod{89} = 0 \pmod{89} \Rightarrow 89 \mid 2^{44} - 1$$

$$2^{12} = 4096 = 22 \pmod{97} \Rightarrow 2^{24} = 2^{12}2^{12} = 22 \cdot 22 \pmod{97} =$$

$$= 484 \pmod{97} = 96 \pmod{97} = -1 \pmod{97} \Rightarrow$$

$$2^{48} = \left(2^{24}\right)^2 \pmod{97} = (-1)^2 \pmod{97} = 1 \pmod{97} \Rightarrow$$

$$2^{48} - 1 \pmod{97} = 1 - 1 \pmod{97} = 0 \pmod{97} \Rightarrow 97 \mid 2^{48} - 1$$

5.6.5

$$9 \equiv -1 \bmod 10 \Rightarrow 9^{1003} \equiv (-1)^{1003} \bmod 10 = -1 \bmod 10 = 9 \bmod 10$$

$$7^2 = 49 \equiv -1 \bmod 10 \Rightarrow 7^{902} = \left(7^2\right)^{451} \equiv (-1)^{451} \bmod 10 = -1 \bmod 10 = 9 \bmod 10$$

$$3^2 = 9 \equiv -1 \bmod 10 \Rightarrow 3^{801} = 3 \cdot 3^{800} = 3 \cdot \left(3^2\right)^{400} = 3 \bmod 10 \cdot \left(3^2\right)^{400} \bmod 10 =$$

$$= 3 \bmod 10 \cdot (-1)^{400} \bmod 10 = 3 \bmod 10 \cdot 1 \bmod 10 = 3 \bmod 10$$

Luego $9^{1003} - 7^{902} + 3^{801} \bmod 10 = 9 - 9 + 3 \bmod 10 = 3 \bmod 10$, luego acaba en 3

5.6.6

$$\left.\begin{array}{l} 11^{n+2} = 11^n \cdot 11^2 \\ 11^2 = 121 = -12 \bmod 133 \end{array}\right\} \Rightarrow 11^{n+2} = -12 \cdot 11^n \bmod 133$$

$$\left.\begin{array}{l} 12^{2n+1} = 12^{2n} \cdot 12 = \left(12^2\right)^n \cdot 12 \\ 12^2 = 144 = 11 \bmod 133 \end{array}\right\} \Rightarrow 12 \cdot 11^n \bmod 133$$

$$a_n = 11^{n+2} + 12^{2n+1} = -12 \cdot 11^n + 12 \cdot 11^n \bmod 133 = 0 \bmod 133 \Rightarrow 133 \mid 11^{n+2} + 12^{2n+1}$$

5.6.7

Está claro que 2137^2 acaba en 9, luego:

$$2137^2 = 9 \bmod 10 = -1 \bmod 10 \Rightarrow \left(2137^2\right)^{376} = (-1)^{376} = 1 \bmod 10$$

Por otro lado, está claro también que $2137 = 7 \bmod 10$

Por lo tanto

$$2137^{753} = 2137^{752} \cdot 2137 = 2137^{2\cdot 376} \cdot 2137 = \left(2137^2\right)^{376} \cdot 2137 = 1 \cdot 7 \bmod 10 = 7 \bmod 10,$$

Luego acaba en 7.

Nota: Este problema también se puede resolver sin congruencias, observando en qué dígito van acabando las potencias de 2137^n:

$$n=0\to 1$$
$$n=1\to 7$$
$$n=2\to 9$$
$$n=3\to 3$$

Y para exponentes mayores entramos en un bucle.

5.6.8

Primera versión.

Estudiamos el dígito de las unidades de 3^{1001}:

$3^0=1, 3^1=3, 3^2=9, 3^3=27, 3^4=81, 3^5=253, 3^6=759...$

Vemos que se va repitiendo en grupos de 4: $\{1,3,9,7\}$, y puesto que $1001=1 \bmod 4$, 3^{1001} acabará como 3^1, es decir en 3.

El mismo análisis hacemos para estudiar el dígito de las unidades de 7^{1002}:

$7^0=1, 7^1=7, 7^2=49, 7^3=343, 7^4=2401, ...$

Vemos que se va repitiendo en grupos de 4: $\{1,7,9,3\}$, y puesto que $1002=2 \bmod 4$, 7^{1002} acabará como 7^2, es decir en 9.

Finalmente, estudiemos el dígito de las unidades de 13^{1003}:

$13^0=1, 13^1=13, 13^2=169, 13^3=2197, 13^4=28561, ...$

Vemos que se va repitiendo en grupos de 4: $\{1,3,9,7\}$, y puesto que $1003=3 \bmod 4$, 13^{1003} acabará como 13^3, es decir en 7.

El producto de un número acabado en 3, un número acabado en 9 y un número acabado en 7 es un número acabado en 9.

Segunda versión.

Vamos a aprovechar el hecho de que toda potencia de un número acabado en 1 acaba siempre en 1. En nuestro caso, cualquier potencia de $7\cdot 13=91$ acaba en 1, y cualquier potencia de $3^4=81$ acaba en 1. Luego:

$$3^{1001}7^{1002}13^{1003}=13\cdot 3^{1001}7^{1002}13^{1002}=13\cdot 3^{1001}(7\cdot 13)^{1002}=13\cdot 3^{1001}91^{1002}=$$
$$=13\cdot 3\cdot 3^{1000}91^{1002}=13\cdot 3\cdot 3^{4\cdot 250}91^{1002}=13\cdot 3\cdot \left(3^4\right)^{250}91^{1002}=$$
$$=13\cdot 3\cdot 81^{250}91^{1002}=39\cdot 3\cdot 81^{250}91^{1002}$$

Que claramente acabará en 9.

Fuente de esta versión: The Contest Problem Book V 198S-1988, pág. 62

5.6.9

Para $k=1$: $18^3 = 5832 \equiv 833 \cdot 7 + 1 \Rightarrow 18^6 = \left(18^3\right)^2 \equiv 1^2 = 1 \pmod{7}$

Para $k=2$: $18^3 = 5832 \equiv 12 \cdot 49 + 1 \Rightarrow 18^6 = \left(18^3\right)^2 \equiv 1^2 = 1 \pmod{49}$

Para $k=3$: $18^3 = 5832 \equiv 2 \cdot 2401 + 1 \Rightarrow 18^6 = \left(18^3\right)^2 \equiv 1^2 = 1 \pmod{2401}$

Observación: Sin embargo, para $k=4$ cambia la pauta: $18^3 \equiv 1030 \pmod{7^4}$

5.6.10

Si n es impar, entonces $n = 2k+1$, y por tanto $n^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$

k o $k+1$ es par, luego $k(k+1)$ es par, y por tanto $4k(k+1)$ es un múltiplo de 8. Luego $n^2 = 4k(k+1) + 1 \equiv 0 + 1 = 1 \pmod{8}$.

5.6.11

$0 \equiv n^2 + 3n + 2 = (n+1)(n+2) \pmod{6}$

La tabla de congruencias módulo 6 es suficientemente pequeña para enunciar todas las combinaciones posibles:

$0 \equiv 2 \cdot 3 \equiv 5 \cdot 6 \equiv 6 \cdot 1 \pmod{6}$, y por tanto: $(n+1) \equiv 2,5,6 \pmod{6} \Rightarrow n \equiv 1,4,5 \pmod{6}$

Y cumpliendo la condición $1 \le n \le 25$, tenemos:

$n \equiv 1 \pmod{6} \Rightarrow n = 1,7,13,19,25$

$n \equiv 4 \pmod{6} \Rightarrow n = 4,10,16,20$

$n \equiv 5 \pmod{6} \Rightarrow n = 5,11,17,23$

En total, $5 + 4 + 4$ posibilidades.

5.6.12

Primera versión.

Vemos el comportamiento de $2^n + 6 \cdot 9^n$ para los primeros valores de n:

Antes de nada, observamos que $6 \equiv -1 \pmod{7}$

$n = 1 \rightarrow 2^1 = 2 \qquad 6 \cdot 9^1 \equiv -9 \equiv -2 \pmod{7} \qquad \rightarrow 2^n + 6 \cdot 9^n \equiv 2 - 2 = 0 \pmod{7}$

$n = 2 \rightarrow 2^2 = 4 \qquad 6 \cdot 9^2 \equiv -81 \equiv -4 \pmod{7} \qquad \rightarrow 2^n + 6 \cdot 9^n \equiv 4 - 4 = 0 \pmod{7}$

$n = 3 \rightarrow 2^3 = 8 \equiv 1 \pmod{7} \quad 6 \cdot 9^3 \equiv -729 \equiv -1 \pmod{7} \rightarrow 2^n + 6 \cdot 9^n \equiv 1 - 1 = 0 \pmod{7}$

Y, a partir de este valor, se van repitiendo la pauta:

$n = 4 \rightarrow 2^4 = 2^3 2 \equiv 1 \cdot 2 \pmod{7} \equiv 2 \pmod{7}$

$6 \cdot 9^4 \equiv -9^3 \cdot 9 \equiv -1 \cdot 9 \equiv -9 \pmod{7} \rightarrow 2^n + 6 \cdot 9^n \equiv 2 - 2 = 0 \pmod{7}$

$n = 5 \rightarrow 2^5 = 2^3 2^2 \equiv 1 \cdot 2^2 \pmod{7} \equiv 2^2 \pmod{7}$

$6 \cdot 9^5 \equiv -9^3 \cdot 9^2 \equiv -1 \cdot 9^2 \equiv -9^2 \pmod{7} \rightarrow 2^n + 6 \cdot 9^n \equiv 4 - 4 = 0 \pmod{7}$

$n = 6 \rightarrow 2^6 = 2^3 2^3 \equiv 1 \cdot 2^3 \pmod{7} \equiv 2^3 \pmod{7}$

$6 \cdot 9^6 \equiv -9^3 \cdot 9^3 \equiv -1 \cdot 9^3 \equiv -9^3 \pmod{7} \rightarrow 2^n + 6 \cdot 9^n \equiv 1 - 1 = 0 \pmod{7}$

Y siempre llegamos al mismo resultado: $2^n + 6 \cdot 9^n \equiv 0 \pmod{7}$.

Segunda versión.

Partimos de la igualdad $9 \equiv 2 \pmod{7}$, luego $9^n \equiv 2^n \pmod{7}$, y por tanto:

$2^n + 6 \cdot 9^n \equiv 9^n + 6 \cdot 9^n = 7 \cdot 9^n \equiv 0 \cdot 9^n = 0 \pmod{7}$

5.6.13

Primera versión.

Vamos a calcular $6^{83}+8^{83} \pmod{49}$ directamente, mediante el método de las potencias de dos:

$6^1 = 6 \pmod{49}$

$6^2 = 36 \pmod{49}$

$6^4 \equiv 36 \cdot 36 = 1296 \equiv 22 \pmod{49}$

$6^8 \equiv 22 \cdot 22 = 484 \equiv 43 \pmod{49}$

$6^{16} \equiv 43 \cdot 43 = 1849 \equiv 36 \pmod{49}$

$6^{32} \equiv 36 \cdot 36 = 1296 \equiv 22 \pmod{49}$

$6^{64} \equiv 22 \cdot 22 = 484 \equiv 43 \pmod{49}$

$83 = 64+16+2+1 \Rightarrow 6^{83} = 6^{64}6^{16}6^2 6 \equiv 43 \cdot 36 \cdot 36 \cdot 6$

$\equiv 43 \cdot 22 \cdot 6 \equiv 15 \cdot 6 = 41 \pmod{49}$

$8^1 = 8 \pmod{49}$

$8^2 = 64 = 15 \pmod{49}$

$8^4 \equiv 15 \cdot 15 = 225 \equiv 29 \pmod{49}$

$8^8 \equiv 29 \cdot 29 = 841 \equiv 8 \pmod{49}$

$8^{16} \equiv 8 \cdot 8 = 64 \equiv 15 \pmod{49}$

$8^{32} \equiv 15 \cdot 15 = 225 \equiv 29 \pmod{49}$

$8^{64} \equiv 29 \cdot 29 = 841 \equiv 8 \pmod{49}$

$83 = 64+16+2+1 \Rightarrow 8^{83} = 8^{64}8^{16}8^2 8 \equiv 8 \cdot 15 \cdot 15 \cdot 8 \equiv$

$\equiv 15 \cdot 29 = 435 \equiv 43 \pmod{49}$

Finalmente, $6^{83}+8^{83} \equiv 41+43 = 84 \equiv 35 \pmod{49}$

Segunda versión.

Aplicando el Teorema del Binomio:

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}a^1 b^{n-1} + b^n$$

Aplicado a nuestro caso, y teniendo en cuenta que $n = 83$ es impar, y por tanto $(-1)^n = -1$,

$$6^n = (7-1)^n = 7^n - \binom{n}{1}7^{n-1} + \binom{n}{2}7^{n-2} + \ldots + \binom{n}{n-1}7 - 1$$

$$8^n = (7+1)^n = 7^n + \binom{n}{1}7^{n-1} + \binom{n}{2}7^{n-2} + \ldots + \binom{n}{n-1}7 + 1$$

Y por tanto:

$$6^n+8^n=7^n+\binom{n}{2}7^{n-2}+\binom{n}{4}7^{n-4}+\ldots+\binom{n}{n-3}7^3+\binom{n}{n-1}7=$$

$$=2\left(7^n+\binom{n}{2}7^{n-2}+\binom{n}{4}7^{n-4}+\ldots+\binom{n}{n-3}7^3+7n\right)=$$

$$=2\cdot 7^2\left(7^{n-2}+\binom{n}{2}7^{n-4}+\binom{n}{4}7^{n-6}+\ldots+\binom{n}{n-3}7\right)+14n=49k+14n$$

En particular, para $n=83$, $a_{83}=6^{83}+8^{83}=49k+14\cdot 83\equiv 14\cdot 83 \pmod{49}$
Luego solo nos queda calcular este último residuo:

$$14\cdot 83=1162=49\cdot 23+35\Rightarrow 14\cdot 83\equiv 35\,(\mathrm{mod}\,49)$$

Fuente de la segunda versión: The Contest Problem Book V 1983-1988 (George Berzsenyi, 1997).

Tercera versión.
Aplicando el Teorema de Euler (que se introducirá en el apartado 13.2)
$49=7^2\Rightarrow \phi(49)=49\left(1-\frac{1}{7}\right)=42$, y $a^{42}\equiv 1\,(\mathrm{mod}\,49)$ si $(a,n)=1$.
En nuestro caso $(6,49)=(8,49)=1$, y por tanto:

$$6^{42}\equiv 1\,(\mathrm{mod}\,49)\Rightarrow 6^{83}=6^{2\cdot 42-1}=\left(6^{42}\right)^2 6^{-1}\equiv 6^{-1}\,(\mathrm{mod}\,49)$$

$$8^{42}\equiv 1\,(\mathrm{mod}\,49)\Rightarrow 8^{83}=8^{2\cdot 42-1}=\left(8^{42}\right)^2 8^{-1}\equiv 8^{-1}\,(\mathrm{mod}\,49)$$

$$6^{83}+8^{83}\equiv 6^{-1}+8^{-1}=\frac{1}{6}+\frac{1}{8}=\frac{8+6}{48}=\frac{14}{-1}=-14\equiv 35\,(\mathrm{mod}\ 49)$$

Fuente de esta versión: https://artofproblemsolving.com/wiki/index.php/1983_AIME_Problems/Problem_6

5.6.14

$$9\times 99\times 999\times\ldots\times\underbrace{99\ldots9}_{999\,nueves}=9\times 99\times(1000-1)\times(10000-1)\times\ldots\times\left(\underbrace{100\ldots00}_{999\,ceros}-1\right)=$$

$$=9\times 99\times(10^3-1)\times(10^4-1)\times\ldots\times\left(10^{999}-1\right)$$

Y observamos que si $k\geq 3\Rightarrow 10^k$ es múltiplo de 1000, y por tanto $10^k\equiv 0\,(\mathrm{mod}\,1000)$, luego $10^k-1\equiv 0-1=-1\,(\mathrm{mod}\,1000)$
Y por tanto:

$$(10^3-1)\times(10^4-1)\times\ldots\times\left(10^{999}-1\right)\equiv(-1)^{999-3+1}=(-1)^{997}=-1\,(\mathrm{mod}\,1000)$$

Y, finalmente,

$$9\times 99\times(10^3-1)\times(10^4-1)\times\ldots\times\left(10^{999}-1\right)\mathrm{mod}(1000)=9\cdot 99(-1)\ \mathrm{mod}(1000)=$$

$$=-891\ \mathrm{mod}(1000)=109\ \mathrm{mod}(1000)$$

5.6.15
Calculamos directamente los primeros valores de $f(n)$:

$$f(0)=0\ ,\ f(1)=2\ ,\ f(3)=6\ ,\ f(4)=14\ ,\ f(5)=30\ ,\ f(6)=62$$

Analizando cómo se obtiene $f(n)$ llegamos a la conclusión de que

$$f(n) = 2f(n-1) - 2(n-1) + 2n = 2f(n-1) + 2$$

Que es el típico comportamiento de una función exponencial. Mirando los primeros valores vemos que un buen candidato puede ser $f(n) = 2^n - 2$.

Lo vamos a demostrar por inducción:

Para $n = 1,2,3$ es cierto.

Suponiendo que $f(n) = 2^n - 2$, entonces

$$f(n+1) = 2f(n) + 2 = 2(2^n - 2) + 2 = 2^{n+1} - 4 + 2 = 2^{n+1} - 2.$$

Luego es cierto para todo n.

$f(100) = 2^{100} - 2$, y queremos determinar $2^{100} - 2 \pmod{100}$.

Calculamos $2^{100} \pmod{100}$ con el "Método de las potencias de 2":

$$2^2 = 4 \pmod{100}$$

$$2^4 = 16 \pmod{100}$$

$$2^8 \equiv 16 \cdot 16 = 256 \equiv 56 \pmod{100}$$

$$2^{16} \equiv 56 \cdot 56 = 3136 \equiv 36 \pmod{100}$$

$$2^{32} \equiv 36 \cdot 36 = 1296 \equiv 96 \equiv -4 \pmod{100}$$

$$2^{64} \equiv (-4) \cdot (-4) = 16 \pmod{100}$$

Luego

$$2^{100} = 2^{64+32+4} = 2^{64}2^{32}2^4 \equiv 16 \cdot (-4) \cdot 16 \pmod{100} \equiv 56 \cdot (-4) \pmod{100}$$

$$\equiv -224 \pmod{100} \equiv -24 \pmod{100} \equiv -24 \pmod{100} \equiv 76 \pmod{100}$$

Finalmente: $2^{100} - 2 \equiv 76 - 2 \pmod{100} \equiv 74 \pmod{100}$, y el residuo pedido es 74.

5.6.16

Queremos determinar $k^2 + 2^k \pmod{10}$. Estudiemos los residuos $2^n \pmod{10}$:

$$2^1 = 2 \pmod{10}$$

$$2^2 = 4 \pmod{10}$$

$$2^3 = 8 \pmod{10}$$

$$2^4 \equiv 4 \cdot 4 = 16 \equiv 6 \pmod{10}$$

$$2^5 \equiv 6 \cdot 2 = 12 \equiv 2 \pmod{10}$$

$$2^6 \equiv 2 \cdot 2 = 4 \pmod{10}$$

$$2^7 \equiv 4 \cdot 2 = 8 \pmod{10}$$

$$2^8 \equiv 8 \cdot 2 = 6 \pmod{10}$$

...

En general: $2^n \pmod{10}$ genera un ciclo $(2,4,8,6)$, y en particular, para todo $n = 4k$ múltiplo de 4, $2^{4k} \equiv 6 \pmod{10}$.

En particular, en nuestro caso:

$$\left.\begin{array}{l} 4 \mid 2008 \Rightarrow 4 \mid 2008^2 \\ 2^{2008} = 2^{2\cdot 4\cdot 251} = \left(2^2\right)^{4\cdot 251} = 4^{4\cdot 251} \Rightarrow 4 \mid 2^{2008} \end{array}\right\} \Rightarrow 4 \mid 2008^2 + 2^{2008} = k$$

k es un múltiplo de 4, y por tanto $2^k \equiv 6 \pmod{10}$.

También vemos que 2008 es múltiplo de 4, luego $2^{2008} \equiv 6 \pmod{10}$.

Por otro lado, $2008 \equiv 8 \pmod{10} \Rightarrow 2008^2 \equiv 8^2 = 64 \equiv 4 \pmod{10}$

Y por tanto $k = 2008^2 + 2^{2008} \equiv 4 + 6 = 10 \equiv 0 \pmod{10} \Rightarrow k^2 \equiv 0^2 = 0 \pmod{10}$

Finalmente, $k^2 + 2^k \pmod{10} \equiv 0 + 6 = 6 \pmod{10}$, y el dígito de las unidades es 6.

Fuente de la solución: https://artofproblemsolving.com/wiki/index.php/2008_AMC_12A_Problems/Problem_15

5.6.17

n y $107n$ tienen las dos últimas cifras iguales si y solo si

$107n \equiv n \pmod{100} \Leftrightarrow 7n \equiv n \pmod{100} \Leftrightarrow 6n \equiv 0 \pmod{100} \Leftrightarrow 6n = 100k$

$\Leftrightarrow 3n = 50k$

De aquí deducimos que n es un múltiplo de 50. El múltiplo de 50 más pequeño es $n = 50$ y ya satisface la condición del enunciado, pues $107 \cdot 50$ acaba en 50.

5.6.18

Pasando a módulo 3 la ecuación se convierte en $x^2 + y^2 \equiv 0$

Hacemos la tabla $x^2 + y^2 \pmod 3$

	$x=0$	$x=1$	$x=2$
$y=0$	0	1	1
$y=1$	1	2	2
$y=2$	1	2	2

Vemos que la única posibilidad es $x \equiv 0$, $y \equiv 0$, es decir, x, y múltiplos de 3. Pero entonces: $3z^2 = x^2 + y^2 = (3x')^2 + (3y')^2 = 9x'^2 + 9y'^2 = 9\left(x'^2 + y'^2\right) \Rightarrow z^2 = 3\left(x'^2 + y'^2\right)$, es decir, z^2 es múltiplo de 3, y por tanto z es múltiplo de 3.

Pero entonces $x^2 + y^2 = 3z^2 \Leftrightarrow (3x')^2 + (3y')^2 = 3(3z')^2 \Leftrightarrow 9\left(x'^2 + y'^2\right) = 9 \cdot 3z'^2 \Leftrightarrow x'^2 + y'^2 = 3z'^2$

Este proceso lo puedo repetir una y otra vez, y esto solo puede ocurrir si $x = y = z = 0$.

5.6.19

$(n+18)^2 = n^2 + 36n + 324$.

Realizamos la división sintética $n^2 + 36n + 324$ entre $n+2$ obtenemos un cociente igual a $n+34$ y un residuo igual a 256, luego $(n+18)^2 \equiv 256 \pmod{n+2}$

Así pues

$n+2 \mid (n+18)^2 \Leftrightarrow (n+18)^2 \equiv 0 \pmod{n+2} \Leftrightarrow 256 \equiv 0 \pmod{n+2}$

$\Leftrightarrow n+2 \mid 256 = 2^8$

Luego $n+2$ es una potencia 2^k, $0 \le k \le 8$

$1 \Rightarrow n = -1$, $2^1 = 2 \Rightarrow n = 0$, $2^2 = 4 \Rightarrow n = 2$, $2^3 = 8 \Rightarrow n = 6$, $2^4 = 16 \Rightarrow n = 14$,

$2^5 = 32 \Rightarrow n = 30$, $2^6 = 64 \Rightarrow n = 62$, $2^7 = 128 \Rightarrow n = 126$, $2^8 = 256 \Rightarrow n = 254$

Se comprueba que todos estos valores satisfacen la condición del enunciado.

5.6.20

Observamos la secuencia de potencias $2^n \pmod 7$:

$2^1 \equiv 2 \pmod 7$

$2^2 \equiv 4 \pmod 7$

$2^3 \equiv 1 \pmod 7$

...

Siempre es 1, 2 o 4 y por tanto $2^n + 1$ será congruente con 2 , 3 o 5, nunca con 0.

5.6.21

$7^2 = 49 \equiv -1 \pmod{10}$, luego $7^4 \equiv (-1)^2 = 1 \pmod{10}$, y por tanto

$7^7 = 7 \cdot 7^3 \cdot 7^4 \equiv 7 \cdot (-1) \cdot 1 \equiv -7 \pmod{10}$

Y por tanto $\left(7^7\right)^7 \equiv (-7)^7 \equiv (-1)^7 (7)^7 \equiv -(-7) \equiv 7 \pmod{10}$

Así pues, por cada pareja de potencias de 7 el resultado es 7, y como elevamos 1000 veces, que es par, el resultado es 7.

5.6.22

Está claro que pasando estos números a módulo 3 solo pueden haber tres diferentes, luego forzosamente encontraremos una pareja equivalente, digamos, por ejemplo, que

$a \equiv b \pmod 3 \Leftrightarrow 3 \mid a - b$

Y ya tenemos un factor divisible entre 3 en el producto del enunciado.

De la misma forma, pasando a módulo 2 solo pueden haber 2 números diferentes, luego puede suceder uno de los siguientes dos casos:

a) $\begin{cases} a \equiv b \pmod 2 \Rightarrow 2 \mid a - b \\ b \equiv c \pmod 2 \Rightarrow 2 \mid b - c \end{cases}$

b) $\begin{cases} a \equiv b \pmod 2 \Rightarrow 2 \mid a - b \\ c \equiv d \pmod 2 \Rightarrow 2 \mid c - d \end{cases}$

En todo caso, encontramos dos factores diferentes múltiples de 2, con lo que el resultado será múltiple de 4. Puesto que 3 y 4 son coprimos, el producto del enunciado será múltiple de $3 \cdot 4 = 12$.

5.6.23

Primera versión.

Aplicando el criterio de divisibilidad del 3 y del 9.

$$0 + 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 45$$

Agrupando dígitos en grupos, vemos que la suma de dígitos de N es:

$7 \cdot 45 + 10 \cdot (2 + 3 + 4 + 5 + 6 + 7 + 8) + 1 + 9 + 9 + 0 + 9 + 1 + 9 + 2 = 705$

705 es divisible entre 3 pero no entre 9, luego $k = 1$.

Segunda versión.
Aplicamos el criterio general $N \equiv S(N) \equiv S(S(N)) = S(705) = 12 \equiv 3 \pmod 9$, y por tanto es divisible entre 3 pero no entre 9, luego $k = 1$.

5.6.24
Supongamos que el año N es de 365 días, es decir, no es bisiesto.
$300 \equiv 6 \pmod 7$
y el día 200 del año $N+1$ es el día $300 + 65 + 200 = 765 \equiv 5 \pmod 7$, lo cual no puede ser.
Por lo tanto deducimos que el año N es bisiesto, de 366 días. Ahora sí es coherente:
$300 + 66 + 200 = 765 \equiv 6 \pmod 7$

El día 100 del año $N-1$ es el día -265 respecto al primero, y $-265 \equiv 1 \pmod 7$, que corresponde a un jueves.

5.6.25
$n^2 + 3n + 2 = (n+1)(n+2)$
$6 \mid (n+1)(n+2) \Leftrightarrow (n+1)(n+2) \equiv 0 \pmod 6$
Las únicas posibilidades son:
$n+1 \equiv 0 \pmod 6 \Leftrightarrow n \equiv -1 \equiv 5 \pmod 6 \Rightarrow n = 5, 11, 17, 23$
$n+2 \equiv 0 \pmod 6 \Leftrightarrow n \equiv -2 \equiv 4 \pmod 6 \Rightarrow n = 4, 10, 16, 22$
$\left.\begin{matrix} n+1 \equiv 2 \pmod 6 \\ n+2 \equiv 3 \pmod 6 \end{matrix}\right\} \Leftrightarrow \left.\begin{matrix} n \equiv 1 \pmod 6 \\ n \equiv 1 \pmod 6 \end{matrix}\right\} \Rightarrow n \equiv 1 \pmod 6 \Rightarrow n = 1, 7, 13, 19, 25$
$\left.\begin{matrix} n+1 \equiv 3 \pmod 6 \\ n+2 \equiv 2 \pmod 6 \end{matrix}\right\} \Leftrightarrow \left.\begin{matrix} n \equiv 2 \pmod 6 \\ n \equiv 0 \pmod 6 \end{matrix}\right\}$ no existe.

5.6.26
Aplicando el criterio de divisibilidad del 3, $7 + 4 + A + 5 + 2 + B + 1 = A + B + 19$ es múltiple de 3, y $3 + 2 + 6 + A + B + 4 + C = A + B + C + 15$ es múltiple de 3, luego su resta también lo será:
$A + B + 19 - (A + B + C + 15) = 4 - C \equiv 0 \pmod 3 \Leftrightarrow C \equiv 4 \equiv 1 \pmod 3$
Los únicos dígitos aceptables son $C = 1,4,7$ y su suma es 12.

5.6.27
Sabemos que $n = \overline{c_k}\,\overline{c_{k-1}}\,\overline{c_{k-2}} \ldots \overline{c_1}\,\overline{c_0}$ es equivalente a
$$n = c_k 10^k + c_{k-1} 10^{k-1} + c_{k-2} 10^{k-2} + \ldots + c_1 10 + c_0$$
Es decir,
$n = p(10)$ con $p(x) = c_k x^k + c_{k-1} x^{k-1} + c_{k-2} x^{k-2} + \ldots + c_1 x + c_0$.

Y que las suma de sus cifras será $S = p(1)$.
Por otro lado, $9 = 10 - 1 \Rightarrow 9 \mid 10 - 1 \Rightarrow 9 \mid p(10) - p(1) = n - S \Rightarrow n \equiv S \pmod 9$

Luego $9 \mid n \Leftrightarrow n \equiv 0 \pmod 9 \Leftrightarrow S \equiv 0 \pmod 9 \Leftrightarrow 9 \mid S$

Sabemos que $n = \overline{c_k}\,\overline{c_{k-1}}\,\overline{c_{k-2}} \ldots \overline{c_1}\,\overline{c_0}$ es equivalente a
$$n = c_k 10^k + c_{k-1} 10^{k-1} + c_{k-2} 10^{k-2} + \ldots + c_1 10 + c_0$$

Es decir,

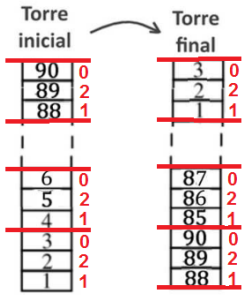
$n = p(10)$ con $p(x) = c_k x^k + c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + \ldots + c_1 x + c_0$.

Y que la suma alternada de sus cifras es $T = p(-1)$.

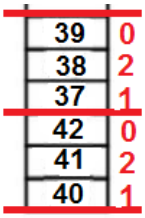
Por otro lado, $10 \equiv -1 \pmod{11} \Rightarrow p(10) \equiv p(-1) \pmod{11}$, es decir $n \equiv T \pmod{11}$.
Luego $11 | n \Leftrightarrow n \equiv 0 \pmod{11} \Leftrightarrow T \equiv 0 \pmod{11} \Leftrightarrow 11 | T$

5.6.28

Pasamos los números del 1 al 90 a módulo 3, y vemos que se separan entre el 0 y el 1:



Puesto que $39 \equiv 0 \pmod{3}$ y $40 \equiv 1 \pmod{3}$, al colocarse en la segunda columna quedarán separados de la siguiente forma:



Y por tanto habrá 4 números entre ellos (E).

5.6.29

Estudiando como se construye esta pirámide de números es fácil ver que la suma S_n de los números de la fila n, es igual a

$$S_n = 2S_{n-1} + n$$

Luego S_n será una función cercana a una potencia de 2. En efecto,

$$S_n = 2^n - n$$

Para determinar la cifra de las unidades de S_{2023} vemos que las potencias de 2 van haciendo un ciclo de 4 valores:

$$2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32, 2^6 = 64, \ldots$$

$$2023 = 4 \cdot 500 + 3$$

Luego 2^{2023} acaba igual que 2^3, en ocho, y por tanto S_{2023} acaba igual que 8-3, es decir, en 5 (C).

5.6.30

En primer lugar vemos que

$$A_0 = 2^0 + 3^2 + 5^2 = 35 = 5 \cdot 7$$

Veamos que 5 no es un divisor de A_1.

$$A_1 = 2^3 + 3^8 + 5^8 = 2^3 + \left(3^2\right)^8 + 5^8 = 8 + 9^8 + 5^8 \equiv 3 + (-1)^8 + 0^8 = 4 \neq 0 \pmod 5$$

Así pues, 5 no puede ser un divisor común.

Veamos que 7 sí es un divisor común de todos los A_n.

$$A_n = 2^{3n} + 3^2 \cdot 3^{6n} + 5^2 \cdot 5^{6n} = \left(2^3\right)^n + 3^2 \cdot 3^{6n} + 5^2 \cdot 5^{6n} = \left(2^3\right)^n + 3^2 \cdot \left(3^6\right)^n + 5^2 \cdot \left(5^6\right)^n =$$

$$\equiv 1^n + 2 \cdot 1^n + 4 \cdot 1^n = 1 + 2 + 4 = 0 \pmod 7 \Rightarrow 7 \mid A_n$$

En donde hemos calculado las sucesivas potencias modulares de la siguiente forma:

$$3^1 \equiv 3, 3^2 \equiv 9 \equiv 2,\ 3^3 \equiv 3 \cdot 2 \equiv 6 \equiv -1,\ 3^6 \equiv (-1)^2 = 1 \pmod 7$$

$$5^1 \equiv 5, 5^2 \equiv 25 \equiv 4,\ 5^3 \equiv 5 \cdot 4 \equiv 20 \equiv 6 \equiv (-1),\ 3^6 \equiv (-1)^2 = 1 \pmod 7$$

Así pues, el máximo común divisor es 7.

5.6.31

Queremos ver que $7^n \equiv 3 \pmod{10} \Rightarrow 7^n \equiv 43 \pmod{100}$

Vamos viendo el comportamiento de las potencias de 7 módulo 100:

$$7^0 = 1$$
$$7^1 = 7$$
$$7^2 = 49 \equiv 9 \pmod{10}$$
$$7^3 \equiv 63 \equiv 3 \pmod{10}$$
$$7^4 \equiv 21 \equiv 1 \pmod{10}$$

Vemos que hay un bucle de longitud 4, y que $7^n \equiv 3 \pmod{10} \Leftrightarrow n \equiv 3 \pmod 4$.

Veamos ahora como son las potencias de 7 módulo 100:

$$7^0 = 1$$
$$7^1 = 7$$
$$7^2 = 49$$
$$7^3 = 343 \equiv 43 \pmod{100}$$
$$7^4 \equiv 301 \equiv 1 \pmod{10}$$

Vemos que también hay un bucle de longitud 4, y que $7^n \equiv 43 \pmod{100} \Leftrightarrow n \equiv 3 \pmod 4$, luego $7^n \equiv 3 \pmod{10} \Leftrightarrow n \equiv 3 \pmod 4 \Leftrightarrow 7^n \equiv 43 \pmod{100}$.

5.6.32

$$2222 \equiv 3 \pmod 7$$
$$3^2 = 9 \equiv 2 \pmod 7$$
$$3^3 \equiv 6 \equiv -1 \pmod 7$$

$$5555 = 3 \cdot 1851 + 2$$
$$2222^{5555} \equiv 3^{5555} \equiv 3^{3 \cdot 1851 + 2} = \left(3^3\right)^{1851} 3^2 \equiv (-1)^{1851} 2 \equiv -2 \equiv 5 \pmod 7$$

$$5555 \equiv 4 \pmod 7$$
$$4^2 = 16 \equiv 2 \pmod 7$$
$$4^3 \equiv 8 \equiv 1 \pmod 7$$

$$2222 = 3 \cdot 740 + 2$$
$$5555^{2222} \equiv 4^{2222} \equiv 4^{3 \cdot 740 + 2} = \left(4^3\right)^{740} 4^2 \equiv (1)^{1851} 2 \equiv 2 \pmod 7$$

$2222^{5555}+5555^{2222}\equiv 5+2\equiv 0 \pmod 7$

5.6.33

$$a_n=\frac{n^2-2}{n^2-n+2}=1+\frac{n-4}{n^2-n+2}$$

Vemos que la sucesión está bien definida pues el denominador es siempre superior o igual a 2.

Los valores diferentes de (a_n) serán los mismos que de $b_n=\dfrac{n-4}{n^2-n+2}$

$b_4=0$ y es el único cero de la sucesión.

Si $n\neq 4$, los valores diferentes de (b_n) serán los mismos que de $c_n=\dfrac{1}{b_n}=\dfrac{n^2-n+2}{n-4}$.

$$c_n=\frac{n^2-n+2}{n-4}=n+3+\frac{14}{n-4}$$

Veamos los elementos iguales de la sucesión c_n:

$$c_n=c_m\Leftrightarrow n+3+\frac{14}{n-4}=m+3+\frac{14}{m-4}\Leftrightarrow n+\frac{14}{n-4}=m+\frac{14}{m-4}$$
$$\Leftrightarrow n-m=\frac{14}{m-4}-\frac{14}{n-4}=14\left(\frac{1}{m-4}-\frac{1}{n-4}\right)=14\frac{n-4-m+4}{(m-4)(n-4)}=14\frac{n-m}{(m-4)(n-4)}$$
$$\Leftrightarrow 1=14\frac{1}{(m-4)(n-4)}\Leftrightarrow (m-4)(n-4)=14=7\cdot 2$$

Llegamos a una ecuación diofántica, que tiene dos soluciones positivas:

$$\begin{matrix} m-4=1\Rightarrow m=5 \\ n-4=14\Rightarrow n=18 \end{matrix}\quad,\quad \begin{matrix} m-4=2\Rightarrow m=6 \\ n-4=7\Rightarrow n=11 \end{matrix}$$

Luego $a_5=a_{18}$ y $a_6=a_{11}$, y el número de valores distintos es 98.

Observación.

En la solución oficial se sigue el siguiente razonamiento:

$$\frac{n-4}{n^2-n+2}=\frac{m-4}{m^2-m+2}\Leftrightarrow (n-m)(nm-4n-4m+2)=0\Leftrightarrow$$
$$nm-4n-4m+2+14=14\Leftrightarrow (n-4)(m-4)=14$$

Llegando a las mismas dos soluciones: $(5,18)$ y $(6,11)$.

5.6.34

Antes de nada, observamos que el conjunto de números que al dividirlos entre 3 da residuo 1 es cerrado por la multiplicación, es decir:

$$\left.\begin{matrix} a=3a'+1 \\ b=3b'+1 \end{matrix}\right\}\Rightarrow ab=(3a'+1)(3b'+1)=9a'b'+3a'+3b'+1=3(3a'b'+a'+b')+1$$

Su producto también dará resto 1 al dividirlo entre 3.

Vamos a resolver este problema por reducción al absurdo.
Sea K_1 el conjunto de números primos que al dividirlos entre 3 dan resto 1, y K_2 el conjunto de números primos que al dividirlos entre 3 dan resto 2.
Todo número primo pertenece a K_1 o K_2, puesto que no puede ser múltiplo de 3.
Supongamos que el conjunto K_2 es finito:

$$K_2 = \{ p_1 , p_2 , \dots , p_n \}$$

Y consideremos el número $k = 3p_1p_2 \dots p_n + 2$.
No puede ser primo pues entonces pertenecería a K_2 lo cual es absurdo pues
$k > p_1, \dots, p_n$
Luego será producto de primos. Al menos uno de estos factores primos de k no será de la forma $3k+1$, pues, por la observación anterior, si todos los factores de k son de la forma $3k+1$, su producto también sería de la forma $3k+1$, pero k da resto 2 al dividirlo entre 3, no da resto 1.
Luego existirá un factor primo p_i de k que pertenece al conjunto K_2, lo cual es absurdo pues cuando dividimos $k = 3p_1p_2 \dots p_n + 2$ entre p_i da resto 2, no 0.
Con esto llegamos a contradicción, y por tanto el conjunto K_2 no puede ser finito.

Observación: En las soluciones oficiales (SE, pág. 1080) se presenta una variación ligeramente diferente.

5.6.35
Una raíz cuadrada de un entero es irracional o es un entero, luego se trata de determinar si $3n^2 + 2n + 2$ es un cuadrado perfecto para algún $n \geq 1$.

Supongamos que existe un entero $k > 0$ tal que
$3n^2 + 2n + 2 = k^2 \Leftrightarrow 3n^2 + 2n + 2 - k^2 = 0 \Leftrightarrow$

$$n = \frac{-2 \pm \sqrt{4 - 4 \cdot 3 \cdot (2 - k^2)}}{2 \cdot 3} = \frac{-2 \pm \sqrt{12k^2 - 20}}{2 \cdot 3} = \frac{-2 \pm \sqrt{4(3k^2 - 5)}}{2 \cdot 3} = \frac{-2 \pm 2\sqrt{3k^2 - 5}}{2 \cdot 3} =$$

$$= \frac{-1 \pm \sqrt{3k^2 - 5}}{3}$$

Pero entonces n es un múltiplo de 3, y por tanto $3n^2 + 2n + 2$ es de la forma $3q + 2$, y no puede ser un cuadrado perfecto como ya vimos en el problema 3.16.

5.6.36
Estudiando los primeros primos vemos, en efecto, una sucesión de 7 números seguidos cumpliendo la condición:

$$29 = 29 , 30 = 2 \cdot 3 \cdot 5 , 31 = 31 , 32 = 2^5 , 33 = 3 \cdot 11 , 34 = 2 \cdot 17 , 35 = 5 \cdot 7$$

Vamos a demostrar que no puede haber más.
Cada 8 números naturales habrá uno que dividido entre 8 dé residuo 4:

$$n = 8k + 4 = 2^2(2k + 1)$$

La descomposición factorial de dicho número tiene seguro el factor 2 elevado al cuadrado, pues el paréntesis es impar, y por lo tanto no puede ser divisible entre 2. Así pues, dicho número no puede cumplir la condición del enunciado.

5.6.37

Se demuestra por inducción sobre n.

Para $n=1$, $S_1 = 5 = 5^1$.

Para $n=2$, $S_2 = 75 = 5^2 \cdot 3$

Supongamos que es cierto hasta $n-1$, es decir, existe un S_{n-1} con $n-1$ dígitos todos impares divisible entre 5^{n-1}.

Para cualquier número impar $1 \le k \le 9$, el valor

$$S_n = k \cdot 10^{n-1} + S_{n-1}$$

Consiste en añadir el dígito k a la izquierda del número anterior. Por lo tanto, si S_{n-1} tiene todo sus dígitos impares, también los tendrá S_n.

Vamos a demostrar que existe un número impar $1 \le k \le 9$ para el cual, además, S_n sea divisible entre 5^n.

Puesto que $5^{n-1} \mid S_{n-1}$, podemos escribir $S_{n-1} = a \cdot 5^{n-1}$, y por tanto

$S_n = k \cdot 10^{n-1} + S_{n-1} = k \cdot 10^{n-1} + a \cdot 5^{n-1} = 5^{n-1}\left(k \cdot 2^{n-1} + a\right)$

$5^n \mid S_n \Leftrightarrow 5 \mid k \cdot 2^{n-1} + a \Leftrightarrow k \cdot 2^{n-1} + a \equiv 0 \pmod 5$

Y en efecto, basta tomar $k \equiv -3^{n-1} a \pmod 5$

En efecto, $-3^{n-1} a \cdot 2^{n-1} + a \equiv -6^{n-1} a + a \equiv -1^{n-1} a + a \equiv -a + a \equiv 0 \pmod 5$

Como estamos trabajando en módulo 5, si el valor de k obtenido es par, podemos sumarle 5 para que sea impar.

Nota: Se puede demostrar que el valor de k es único, y por lo tanto existe un único S_n para cada n.

5.6.38

Sea $F_k^n = 1 + \dfrac{2^k - 1}{n}$

Vamos a demostrar la identidad del enunciado por inducción sobre k.

Para $k=1$ es fácil:

$F_1^n = 1 + \dfrac{2^1 - 1}{n} = 1 + \dfrac{2-1}{n} = 1 + \dfrac{1}{n} = 1 + \dfrac{1}{m_1}$, la solución es $m_1 = n$.

Supongamos que es cierto hasta hasta k, y veamos que también se cumple para $k+1$:

$$F_k^{n/2}\cdot\left(1+\frac{1}{2^{k+1}+n-2}\right)=\left(1+\frac{2^k-1}{n/2}\right)\left(1+\frac{1}{2^{k+1}+n-2}\right)=$$
$$=\left(\frac{2^k-1+n/2}{n/2}\right)\left(\frac{2^{k+1}+n-2+1}{2^{k+1}+n-2}\right)=\left(\frac{2^{k+1}-2+n}{n}\right)\left(\frac{2^{k+1}+n-2+1}{2^{k+1}+n-2}\right)=$$
$$=\frac{2^{k+1}+n-1}{n}=\frac{2^{k+1}-1}{n}+1=F_{k+1}^n$$

$F_{k+1}^n=F_k^{n/2}\cdot\left(1+\frac{1}{2^{k+1}+n-2}\right)$, y por tanto, si n es par, ya está demostrado, pues es cierto para $F_k^{n/2}$ y basta multicarlo por $\left(1+\frac{1}{m_{k+1}}\right)$ con $m_{k+1}=2^{k+1}+n-2$.

Si n es impar,
$$F_k^{(n+1)/2}\cdot\left(1+\frac{1}{n}\right)=\left(1+\frac{2^k-1}{(n+1)/2}\right)\left(1+\frac{1}{n}\right)=$$
$$=\left(1+\frac{2^{k+1}-2}{n+1}\right)\left(1+\frac{1}{n}\right)=\left(\frac{2^{k+1}-2+n+1}{n+1}\right)\left(\frac{n+1}{n}\right)=\frac{2^{k+1}-1+n}{n}=\frac{2^{k+1}-1}{n}+1=F_{k+1}^n$$

Es decir, $F_{k+1}^n=F_k^{(n+1)/2}\cdot\left(1+\frac{1}{n}\right)$
Y se demuestra por inducción, pues $(n+1)/2$ es entero, tomando $m_{k+1}=n$..

Sea par o impar, queda demostrado el enunciado.

5.6.39
Pasamos a módulo n:
$$n\mid a_i(a_{i+1}-1)\Leftrightarrow a_i(a_{i+1}-1)\equiv 0\ (\text{mod } n)\Leftrightarrow a_ia_{i+1}-a_i\equiv 0\ (\text{mod } n)\Leftrightarrow$$
$$a_ia_{i+1}\equiv a_i\ (\text{mod } n)$$

Tomando el primer elemento a_1, vemos que:
$$\left.\begin{aligned}a_1a_2&\equiv a_1\ (\text{mod } n)\\ a_2a_3&\equiv a_2\ (\text{mod } n)\end{aligned}\right\}\Rightarrow a_1a_2a_3\equiv a_1a_2\equiv a_1\ (\text{mod } n)$$

Y después
$$\left.\begin{aligned}&a_3a_4\equiv a_3\ (\text{mod } n)\\ &a_1a_2a_3a_4\equiv a_1a_2a_3\equiv a_1\ (\text{mod } n)\end{aligned}\right\}\Rightarrow a_1a_2a_3a_4\equiv a_1a_2a_3\equiv a_1\ (\text{mod } n)$$

Hasta que, finalmente,
$$a_1...a_{k-1}\equiv a_1\ (\text{mod } n)$$

Pero si, además, $n\mid a_k(a_1-1)\Leftrightarrow a_ka_1\equiv a_1\ (\text{mod } n)$, en cierta manera lo que hacemos es completar el círculo, es decir:

$$a_1 \equiv a_1 a_k \equiv a_1 ... a_{k-1} a_k \pmod{n}$$

Pero esto lo podríamos haber hecho con todos y cada uno de los elementos a_j, es decir:

$$a_1 \equiv a_2 \equiv ... \equiv a_k \equiv a_1 ... a_{k-1} a_k \pmod{n}$$

Lo cual es absurdo, pues $1 \le a_j \le n$ y son todos diferentes.

Fuente de la solución: "Mathematical Excalibur May-Sep. 2009"

5.6.40

Buscamos un número entero n con $10^4 \le n < 10^5$ y que cumpla $n^2 = m \cdot 10^5 + n$ para un cierto entero m.

$n^2 = m \cdot 10^5 + m \Leftrightarrow n^2 - n = 10^5 m \Leftrightarrow n^2 - n = n(n-1)$ es divisible entre 10^5

Puesto que n y $n-1$ son coprimos, $2^5 5^5 = 10^5 \mid n(n-1)$ si y solo si n o $n-1$ es divisible entre 2^5 y el otro es divisible entre 2^5.

O, equivalentemente, queremos un número k divisible entre $5^5 = 3125$ y que cumpla $k \equiv \pm 1 \pmod{32}$

$$\left.\begin{array}{l} 3125 \mid k \Leftrightarrow k = 3125\, q \\ 3125 \equiv 21 \pmod{32} \end{array}\right\} \Rightarrow k \equiv \pm 1 \pmod{32} \Leftrightarrow 3125\, q \equiv \pm 1 \pmod{32} \Leftrightarrow 21 q \equiv \pm 1 \pmod{32}$$

Puesto que 21 y 32 son coprimos, la ecuación $21q \equiv \pm 1 \pmod{32}$

Tiene por solución $q = 3$. En efecto $21 \cdot 3 = 63 = 2 \cdot 32 - 1$

Por otro lado, la condición $10^4 \le k < 10^5$ obliga a que $4 \le q \le 31$, y por tanto tomaremos el valor $q = 32 - 3 = 29$

$$21(32-3) \equiv 21(-3) \equiv -(-)1 \equiv 1 \pmod{32}$$

Así pues, $k = 3125 \cdot 29 = 90625$.

En efecto, $90625^2 = 8212890625$

Fuente de la solución: https://math.stackexchange.com/questions/1692048/a-five-digit-number-whose-square-has-its-last-five-digits-equal-to-the-number

Observación: La solución oficial se puede considerar como un buen ejemplo de lo que no debe ser la solución a un problema.

5.6.41

Primera versión. Mediante aritmética modular.

Buscamos conjuntos ordenados (a,b,c,d), con $a \neq 0$, tales que

$$7 \mid \overline{0abcd} \Leftrightarrow 7 \mid 10000 \cdot 0 + 1000 \cdot a + 100 \cdot b + 10 \cdot c + d \qquad (1)$$
$$7 \mid \overline{a0bcd} \Leftrightarrow 7 \mid 10000 \cdot a + 1000 \cdot 0 + 100 \cdot b + 10 \cdot c + d \qquad (2)$$
$$7 \mid \overline{ab0cd} \Leftrightarrow 7 \mid 10000 \cdot a + 1000 \cdot b + 100 \cdot 0 + 10 \cdot c + d \qquad (3)$$
$$7 \mid \overline{abc0d} \Leftrightarrow 7 \mid 10000 \cdot a + 1000 \cdot b + 100 \cdot c + 10 \cdot 0 + d \qquad (4)$$
$$7 \mid \overline{abcd0} \Leftrightarrow 7 \mid 10000 \cdot a + 1000 \cdot b + 100 \cdot c + 10 \cdot d + 0 \qquad (5)$$

Puesto que: $10000 \equiv 4 \pmod 7$, $1000 \equiv 6 \pmod 7$, $100 \equiv 2 \pmod 7$ y $10 \equiv 3 \pmod 7$, las condiciones del enunciado se pueden escribir como:

$$10000 \cdot 0 + 1000 \cdot a + 100 \cdot b + 10 \cdot c + d \equiv 0 \pmod 7 \Leftrightarrow 6a + 2b + 3c + d \equiv 0 \pmod 7$$
$$10000 \cdot a + 1000 \cdot 0 + 100 \cdot b + 10 \cdot c + d \equiv 0 \pmod 7 \Leftrightarrow 4a + 2b + 3c + d \equiv 0 \pmod 7$$
$$10000 \cdot a + 1000 \cdot b + 100 \cdot 0 + 10 \cdot c + d \equiv 0 \pmod 7 \Leftrightarrow 4a + 6b + 3c + d \equiv 0 \pmod 7$$
$$10000 \cdot a + 1000 \cdot b + 100 \cdot c + 10 \cdot 0 + d \equiv 0 \pmod 7 \Leftrightarrow 4a + 6b + 2c + d \equiv 0 \pmod 7$$
$$10000 \cdot a + 1000 \cdot b + 100 \cdot c + 10 \cdot d + 0 \equiv 0 \pmod 7 \Leftrightarrow 4a + 6b + 2c + 3d \equiv 0 \pmod 7$$

Restando la primera de la segunda llegamos a
$2a \equiv 0 \pmod 7 \Rightarrow a = 0, 7$, y solo puede ser $a = 7$
Restando la tercera de la segunda llegamos a
$2b \equiv 0 \pmod 7 \Rightarrow b = 0, 7$
Restando la tercera de la cuarta llegamos a
$c \equiv 0 \pmod 7 \Rightarrow c = 0, 7$
Restando la quinta de la cuarta llegamos a
$2d \equiv 0 \pmod 7 \Rightarrow d = 0, 7$

Así pues, las soluciones posibles son los todos los números de cuatro cifras que se forman con los dígitos 0 y 7, es decir, los siete números: 7000, 7007, 7070, 7077, 7700, 7707 y 7777.

Segunda versión. Sin aritmética modular.
El tratamiento sería similar. Por ejemplo:

$$x = \overline{0abcd} = 10000 \cdot 0 + 1000 \cdot a + 100 \cdot b + 10 \cdot c + d$$
$$y = \overline{a0bcd} = 10000 \cdot a + 1000 \cdot 0 + 100 \cdot b + 10 \cdot c + d$$
$$\left.\begin{array}{l} 7 \mid x \\ 7 \mid y \end{array}\right\} \Rightarrow 7 \mid y - x = 9000\,a$$

Y puesto que 7 no es divisor de 9000, se llega a $7 \mid a$, es decir, $a = 0, 7$. Y como no puede ser cero puesto que estamos suponiendo un número de cuatro cifras, solo queda $a = 7$.
Y con un argumento similar se deducen los otros tres dígitos.

5.6.42
a)
$2n-1$ y $2n+1$ son coprimos.

$$\left.\begin{array}{l} 2n-1 = k \cdot a \\ 2n+1 = k \cdot b \end{array}\right\} \Rightarrow 2n+1-(2n-1) = 2 = kb - ka = k(b-a)$$

Y esto es imposible para cualquier $k > 1$, pues entonces tendríamos $k = 2$ y los números $2n-1$ y $2n+1$ serían pares, lo cual es absurdo.

b)

Está claro que podemos reducir nuestra búsqueda a divisores comunes primos.
Sea p un divisor común de n^2-1 y $3n+1$
Puesto que $n^2-1=(n+1)(n-1)$, $p\mid n^2-1$ si y solo si $p\mid n+1$ o $p\mid n-1$. (ver 5.5)
Supongamos que $p\mid n+1$.

$$\left.\begin{array}{l} p\mid n+1 \\ p\mid 3n+1 \end{array}\right\} \Rightarrow p\mid 3n+1-(n+1)=2n \Rightarrow p\mid n$$

Sabemos que dos números consecutivos son coprimos, luego es imposible que p sea divisor de n y de $n+1$.
Supongamos que $p\mid n-1$.

$$\left.\begin{array}{l} p\mid n-1 \\ p\mid 3n+1 \end{array}\right\} \Rightarrow p\mid 3n+1-(n-1)=2n+2=2(n+1) \Rightarrow p\mid n+1$$

Luego $p\mid n-1$ y $p\mid n+1$, lo cual es absurdo por el apartado a).

Fuente de esta solución: F.J.G.C. en Facebook.

5.6.43
$2^{2001}+3^{2001}$ es divisible entre 7 equivale a demostrar que $2^{2001}+3^{2001}\equiv 0 \pmod 7$.

Veamos la sucesión de potencias de 2 módulo 7:

$$2^1=2\equiv 2 \pmod 7$$
$$2^2=4\equiv 4 \pmod 7$$
$$2^3=8\equiv 1 \pmod 7$$

Puesto que $2001=667\cdot 3$, se tiene $2^{2001}=\left(2^3\right)^{667}\equiv 1^{667}=1 \pmod 7$.

Veamos la sucesión de potencias de 3 módulo 7:

$$3^1=3\equiv 3 \pmod 7$$
$$3^2=9\equiv 2 \pmod 7$$
$$3^3=27\equiv 6 \pmod 7$$
$$3^4\equiv 6\cdot 3=18\equiv 4 \pmod 7$$
$$3^5\equiv 4\cdot 3=12\equiv 5 \pmod 7$$
$$3^6\equiv 5\cdot 3=15\equiv 1 \pmod 7$$

Puesto que $2001=333\cdot 6+3$, se tiene $3^{2001}=\left(3^6\right)^{333}\cdot 3^3\equiv 1^{333}\cdot 6=6 \pmod 7$.
Luego, finalmente, $2^{2001}+3^{2001}\equiv 1+6=7\equiv 0 \pmod 7$, tal y como queríamos ver.

5.6.44
Mediante una división sintética vemos que

$$n^3+100=(n+10)\left(n^2-10n+100\right)-900$$

Luego

$$0\equiv n^3+100=(n+10)\left(n^2-10n+100\right)-900\equiv -900 \pmod{n+10}$$
$$\Leftrightarrow 0\equiv -900 \pmod{n+10} \Leftrightarrow n+10\mid -900$$

El mayor n positivo para el que esto ocurre es $n+10=900\Leftrightarrow n=890$

5.6.45

Para $n=2$ es cierto:

$$n^6-1=63=3^2\cdot 7\,,\ (n^3-1)(n^2-1)=7\cdot 3$$

y está claro que todos los factores primos del primero son factores primos del segundo.

Veamos que para $n>2$ no se cumple nunca.
Aplicando las fórmulas de factorización, tenemos

$$n^6-1=(n^3-1)(n^3+1)=(n^3-1)(n+1)(n^2-n+1)$$
$$(n^3-1)(n^2-1)=(n^3-1)(n-1)(n+1)$$

Luego nuestro problema se reduce a determinar los enteros $n>2$ para los cuales

$$p\mid n^2-n+1\Rightarrow p\mid (n^3-1)(n^2-1)$$

Si $p\mid n^2-n+1$ entonces $p\mid n^3+1$, puesto que $n^3+1=(n+1)(n^2-n+1)$
Por otro lado, $n^2-n+1=n(n-1)+1$ es un número impar, luego $p\geq 3$.
Luego $p\nmid n^3-1$, puesto que $(n^3+1,n^3-1)=(n^3+1-(n^3-1),n^3-1)=(2,n^3-1)\leq 2$
Así pues, la única posibilidad aceptable es $p\mid n^2-1$.
Por otro lado,

$$\left.\begin{array}{l} p\mid n^3+1 \\ p\mid n^2-1 \end{array}\right\}\Rightarrow p\mid n^3+1+n^2-1=n^2(n+1)$$

Y puesto que $p\nmid n$ (ya que $p\mid n\Rightarrow p\mid n^6\Rightarrow p\nmid n^6-1$), deducimos que $p\mid n+1$.
De la misma forma,

$$\left.\begin{array}{l} p\mid n^2-1 \\ p\mid n^2-n+1 \end{array}\right\}\Rightarrow p\mid n^2-1-(n^2-n+1)=n-2$$

De $p\mid n+1$ y $p\mid n-2$ deducimos que $p=3$, es decir, $n^2-n+1=3^k$ para cierto entero positivo k.
$n^2-n+1=3^k\Leftrightarrow n^2-n+1-3^k=0$, luego su discriminante debe ser un cuadrado perfecto:
$\Delta=(-1)^2-4\cdot 1\cdot(1-3^k)=1-4(1-3^k)=1-4+4\cdot 3^k=-3+4\cdot 3^k=3(4\cdot 3^k-1)$
Pero para $k>1$ el número $4\cdot 3^k-1$ no es divisible entre 3, por lo tanto el único caso aceptable es $k=1\Rightarrow n^2-n+1=3\Rightarrow n=2$.

Fuente de esta solución: "Baltic Way 2002-2006 Problems and Solutions" Rasmus Villemoes

5.6.46
Primera versión.
Estos conjuntos son de la forma

$$\{10k+1,10k+2,10k+3,\ldots,10k+10\}\quad 0\leq k\leq 99$$

En cada uno de ellos hay 10 números consecutivos, luego está claro que cada uno contendrá al menos un múltiplo de 7, es imposible que contenga tres, y contendrá dos múltiplos de 7 cuando lo sea el primero, el segundo o el tercero.

Primer caso:
$10k+1\equiv 0\pmod 7\Leftrightarrow 10k\equiv -1\equiv 6\pmod 7\Leftrightarrow 5k\equiv 3\pmod 7$
Estudiando los valores $5k\pmod 7$:

k	0	1	2	3	4	5	6
5k	0	5	10≡3	15≡1	20≡6	25≡4	30≡2

Vemos que esto sucede para $k \equiv 2 \pmod 7$

Segundo caso:
$10k + 2 \equiv 0 \pmod 7 \Leftrightarrow 10k \equiv -2 \equiv 5 \pmod 7 \Leftrightarrow 2k \equiv 1 \pmod 7$
Estudiando los valores $2k \pmod 7$:

k	0	1	2	3	4	5	6
2k	0	2	4	6	8≡1	10≡3	12≡5

Vemos que esto sucede para $k \equiv 4 \pmod 7$

Tercer caso:
$10k + 3 \equiv 0 \pmod 7 \Leftrightarrow 10k \equiv -3 \equiv 4 \pmod 7 \Leftrightarrow 5k \equiv 2 \pmod 7$
Estudiando los valores $5k \pmod 7$:

k	0	1	2	3	4	5	6
5k	0	5	10≡3	15≡1	20≡6	25≡4	30≡2

Vemos que esto sucede para $k \equiv 2 \pmod 7$

Así pues, buscamos todos los valores de k , $0 \le k \le 99$ tales que $k \equiv 2,4,6 \pmod 7$.
Puesto que $99 = 7 \cdot 14 + 1$, existirán $14 \cdot 3 = 42$ conjuntos aceptables posibles (B)

Segunda versión.
Hemos visto que hay 100 conjuntos, y en cada conjunto hay 1 o dos múltiplos de 7. Entre el 0 y el 1000 hay un total de $\lfloor 1000 / 7 \rfloor = 142$ múltiplos de 7, luego los conjuntos con dos múltiplos de 7 serán 142-100=42.

5.6.47
Sean a y b enteros tales que

$$\begin{cases} 3x + 4y = a^2 \\ 4x + 3y = b^2 \end{cases}$$

Sumando las dos ecuaciones:

$$a^2 + b^2 = 3x + 4y + 4x + 3y = 7x + 7y = 7(x + y)$$

Así pues, $a^2 + b^2$ es un múltiplo de 7. Pero si hacemos toda la tabla $a^2 + b^2 \pmod 7$:

	0	1	2	3	4	5	6
0	0	1	4	2	2	4	1
1	1	2	5	3	3	5	2
2	4	5	1	6	6	1	5
3	2	3	6	4	4	6	3
4	2	3	6	4	4	6	3
5	4	5	1	6	6	1	5
6	1	2	5	3	3	5	2

Vemos que la única posibilidad es $a \equiv b \equiv 0 \pmod 7$, es decir, que a y b sean ambos múltiplos de 7: $a = 7n$, $b = 7m$ para ciertos enteros n y m.

También lo podríamos haber demostrado observando que los cuadrados módulo 7 son 0, 1, 2 y 4, y la única manera de obtener 0 sumando dos de estos números es 0 + 0.

Resolviendo el sistema inicial tenemos

$$x=\frac{4b^2-3a^2}{7}=\frac{4(7m)^2-3(7n)^2}{7}=\frac{7^2\left(4m^2-3n^2\right)}{7}=7\left(4m^2-3n^2\right),$$

$$y=\frac{4a^2-3b^2}{7}=\frac{4(7n)^2-3(7m)^2}{7}=\frac{7^2\left(4n^2-3m^2\right)}{7}=7\left(4n^2-3m^2\right)$$

Es decir, que x e y son múltiplos de 7, tal y como queríamos ver.

5.6.48

Si $a=1$ la ecuación queda de la forma $2+7^b=c^2+4\Leftrightarrow 7^b=c^2+2\Rightarrow 0\equiv c^2+2\pmod 7$, en donde tenemos en cuenta que $b\geq 1$.
Pero vemos que en módulo 7 la expresión de la derecha nunca es cero:

c	$c^2+2 \pmod 7$
0	4
1	5
2	1
3	6
4	6
5	1
6	5

Luego no hay solución posible.

Si $a=2$ la ecuación queda de la forma $4+7^b=c^2+4\Leftrightarrow 7^b=c^2$.
Aquí está claro que b debe ser par y c una potencia de 7, concretamente $b=2k, c=7^k$. Está claro que cualquier combinación de esta forma satisfacerá la condición del enunciado. Luego hay infinitas soluciones.

Si $a>2$ entonces 2^a es un múltiplo de 9. Luego, pasando la expresión a módulo 8 nos queda

$$7^b\equiv c^2+4 \pmod 8\Leftrightarrow (-1)^b\equiv c^2+4 \pmod 8\Rightarrow \begin{cases} c^2+4\equiv 1 \pmod 8 \\ c^2+4\equiv -1 \pmod 8 \end{cases}.$$

Pero haciendo la tabla $c^2+4 \pmod 8$ vemos que no hay ningún valor compatible con esta condición:

c	$c^2+4 \pmod 8$
0	4
1	5
2	0
3	5
4	4
5	5
6	0
7	5

Luego no hay solución posible.

Así pues, las únicas soluciones aceptables son todas las de la forma $a=2, b=2k, c=7^k$, $k \geq 1$.

5.6.49

Vamos a resolver este problema por inducción. Sea a_n este número.

$$a_1 = 5 = 5^1 \cdot 1$$
$$a_2 = 75 = 5^2 \cdot 3$$
$$a_3 = 375 = 5^3 \cdot 5$$
$$a_4 = 9374 = 5^4 \cdot 15$$

Y vemos la pauta de construcción. Supongamos resuelto el problema hasta $a_n = \overline{k_n k_{n-1} \ldots k_1}$.
Por hipótesis de inducción, a_n será múltiple de 5^n, es decir, $a_n = 5^n \cdot k_n$
Tomemos los siguientes candidatos para a_{n+1}, que construimos añadiendo una cifra impar al anterior:

$$\overline{1k_n k_{n-1} \ldots k_1} = 1 \cdot 10^n + a_n = 1 \cdot (2 \cdot 5)^n + 5^n \cdot k_n = 5^n (1 \cdot 2^n + k_n)$$
$$\overline{3k_n k_{n-1} \ldots k_1} = 3 \cdot 10^n + a_n = 3 \cdot (2 \cdot 5)^n + 5^n \cdot k_n = 5^n (3 \cdot 2^n + k_n)$$
$$\overline{5k_n k_{n-1} \ldots k_1} = 5 \cdot 10^n + a_n = 5 \cdot (2 \cdot 5)^n + 5^n \cdot k_n = 5^n (5 \cdot 2^n + k_n)$$
$$\overline{7k_n k_{n-1} \ldots k_1} = 7 \cdot 10^n + a_n = 7 \cdot (2 \cdot 5)^n + 5^n \cdot k_n = 5^n (7 \cdot 2^n + k_n)$$
$$\overline{9k_n k_{n-1} \ldots k_1} = 9 \cdot 10^n + a_n = 9 \cdot (2 \cdot 5)^n + 5^n \cdot k_n = 5^n (9 \cdot 2^n + k_n)$$

Está claro que todos estos números son divisibles entre 5^n, pero además, los cinco paréntesis de la derecha tienen todos diferentes residuos módulo 5. En efecto, si

$a \cdot 2^n + k_n \equiv b \cdot 2^n + k_n \pmod 5 \Rightarrow a \cdot 2^n \equiv b \cdot 2^n \pmod 5 \Rightarrow a \equiv b \pmod 5$ y esto nunca ocurre, pues los números 1, 3, 5, 7 y 9 tienen todos residuos diferentes módulo 5. Así pues, uno de ellos tiene que tener residuo cero módulo 5, es decir, uno de ellos debe ser divisible entre 5, lo que dará lugar a un candidato divisible entre 5^{n+1}, tal y como queríamos ver.

Fuente de esta solución: Soluciones oficiales (USAMO, pág 84)

5.7.1

$1^{-1} = 1 \pmod 7,\ 2^{-1} = 4 \pmod 7,\ 3^{-1} = 5 \pmod 7,\ 4^{-1} = 2 \pmod 7,\ 5^{-1} = 3 \pmod 7,$
$6^{-1} = 6 \pmod 7$

5.7.2

Escribimos la tabla de multiplicar de Z_6 y marcamos los unos:

×	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	[1]	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	[1]	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	[1]	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	[1]

Podemos ver claramente que los valores invertibles son 1, 5, 7 y 11, cuyos repectivos inversos son ellos mismos: 1, 5, 7 y 11.

5.7.3

$244 = 2 \cdot 117 + 10$

$117 = 11 \cdot 10 + 7$

$10 = 1 \cdot 7 + 3$

$7 = 2 \cdot 3 + 1$

$1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (10 - 7) = 7 - 2 \cdot 10 + 2 \cdot 7 = 3 \cdot 7 - 2 \cdot 10 = 3 \cdot (117 - 11 \cdot 10) - 2 \cdot 10 =$
$= 3 \cdot 117 - 33 \cdot 10 - 2 \cdot 10 = 3 \cdot 117 - 35 \cdot 10 = 3 \cdot 117 - 35 \cdot (244 - 2 \cdot 117) =$
$= 3 \cdot 117 - 35 \cdot 244 + 70 \cdot 117 = 73 \cdot 117 - 35 \cdot 244$

Luego

$$1 = 73 \cdot 117 - 35 \cdot 244 \equiv 73 \cdot 117 \pmod{244} \Rightarrow 117^{-1} = 73 \pmod{244}$$

6.1.1

a) Resolvemos la congruencia sumando 4 a ambos lados de la igualdad:
$x - 4 \equiv 0 \pmod 5 \Rightarrow x - 4 + 4 \equiv 0 + 4 \pmod 5 \Rightarrow x \equiv 4 \pmod 5$
b) Resolvemos la congruencia sumando 1 a ambos lados de la igualdad:
$x - 1 \equiv 1 \pmod 5 \Rightarrow x - 1 + 1 \equiv 1 + 1 \pmod 5 \Rightarrow x \equiv 2 \pmod 5$
c) Resolvemos la congruencia restando 3 a ambos lados de la igualdad:
$x + 3 \equiv 1 \pmod 5 \Rightarrow x + 3 - 3 \equiv 1 - 3 \pmod 5 \Rightarrow x \equiv -2 \equiv -2 + 5 = 3 \pmod 5$
d) Resolvemos la congruencia restando 12 a ambos lados de la igualdad:
$x + 12 \equiv 3 \pmod 5 \Rightarrow x + 12 - 12 \equiv 3 - 12 \pmod 5 \Rightarrow\Rightarrow x \equiv -9 \equiv -9 + 10 = 1 \pmod 5$

6.1.2

Observamos la tabla de multiplicar de Z_5:

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

a) El inverso multiplicativo de 3 es 2, luego multiplicamos a ambos lados por 2:
$3x \equiv 1 \pmod 5 \Rightarrow 2 \cdot 3x \equiv 2 \cdot 1 \pmod 5 \Rightarrow 1x \equiv 2 \pmod 5 \Rightarrow x \equiv 2 \pmod 5$

b) De la misma manera: $3x \equiv 2 \pmod 5 \Leftrightarrow 2 \cdot 3x \equiv 2 \cdot 2 = 4 \pmod 5 \Leftrightarrow x \equiv 4 \pmod 5$
c) El inverso multiplicativo de 2 es 3, luego:
$2x \equiv 3 \pmod 5 \Leftrightarrow 3 \cdot 2x \equiv 3 \cdot 3 \pmod 5 \Leftrightarrow x \equiv 9 \equiv 4 \pmod 5$

d) $12 \equiv 2 \pmod 5 \Rightarrow 12x \equiv 2x \pmod 5$ y la congruencia queda:
$2x \equiv 4 \pmod 5 \Rightarrow 3 \cdot 2x \equiv 3 \cdot 4 \pmod 5 \Rightarrow x \equiv 12 \equiv 2 \pmod 5$
e)
$2x - 4 \equiv 2 \pmod 5 \Leftrightarrow 2x - 4 + 4 \equiv 2 + 4 \pmod 5 \Leftrightarrow 2x \equiv 6 \equiv 1 \pmod 5 \Leftrightarrow$
$3 \cdot 2x \equiv 3 \cdot 1 \pmod 5 \Leftrightarrow x \equiv 3 \pmod 5$

6.1.4
$d = (9,30) = 3$, y $3 \mid 21$, luego la ecuación anterior tendrá 3 soluciones diferentes.

Encontramos la primera solución por tanteo:
$x_0 = 9$, pues $9 \cdot 9 = 81 = 2 \cdot 30 + 21$.
Luego el resto de soluciones serán:
$x_1 = 9 + \frac{30}{3} \cdot 1 = 9 + 10 = 19$, efectivamente: $9 \cdot 19 = 171 = 5 \cdot 30 + 21$
$x_2 = 9 + \frac{30}{3} \cdot 2 = 9 + 20 = 29$, efectivamente: $9 \cdot 29 = 261 = 8 \cdot 30 + 21$

6.1.5
$(3,10) = 1$, luego la congruencia lineal anterior tendrá una única solución módulo 10.
Aunque no sea la más elegante, una manera de resolverla es ir probando números del 1 al 9:
$3 \cdot 1 = 3 \not\equiv 7 \bmod 10$, $3 \cdot 2 = 6 \not\equiv 7 \bmod 10$, $3 \cdot 3 = 9 \not\equiv 7 \bmod 10$,
$3 \cdot 4 = 12 \equiv 2 \not\equiv 7 \bmod 10$, $3 \cdot 5 = 15 \equiv 5 \not\equiv 7 \bmod 10$, $3 \cdot 6 = 18 \equiv 8 \not\equiv 7 \bmod 10$,
$3 \cdot 7 = 21 \equiv 1 \not\equiv 7 \bmod 10$, $3 \cdot 8 = 24 \equiv 4 \not\equiv 7 \bmod 10$, $3 \cdot 9 = 27 \equiv 7 \bmod 10$.

Luego la solución es $x = 9$.

6.2.1
Primera versión.
Un número n da residuo 5 cuando lo dividimos entre 6, 7, 8 y 9 si $n - 5$ es divisible entre 6, 7, 8 y 9. Luego $n - 5$ será divisible entre el mínimo común múltiplo de 6, 7, 8 y 9, que es 504. Así pues, $n - 5 = 504a \Rightarrow n = 504a + 5$ para cierto a.
Vamos dando valores de $a = 0, 1, 2, 3...$ y vemos que para $a = 4$, $n = 504 \cdot 4 + 5 = 2021$ ya es demasiado grande. Luego hay 4 números (D).

Segunda versión. (un método más general)

Nos vamos a entrar en las divisiones entre 7, 8 y 9, por ser los tres coprimos.
Sea n un número que, dividido entre 7, da residuo 5. Luego n se podrá escribir de la forma $n = 7a + 5$ para cierto entero a.
Pero este mismo número da residuo 5 cuando lo dividimos entre 8, luego $n = 7a + 5 = 8b + 5$ para cierto entero b.
Luego $7a + 5 = 8b + 5 \Rightarrow 7a = 8b \Rightarrow 7 \mid 8b$, y puesto que $(7,8) = 1$, se deduce que $7 \mid b$, es decir, $b = 7k$ para cierto entero k. Así pues, $n = 8b + 5 = 8 \cdot 7k + 5 = 56k + 5$.
Este número da residuo 5 cuando lo dividimos entre 9, es decir:
$n = 56k + 5 = 9c + 5$ para cierto entero c, luego
$56k + 5 = 9c + 5 \Rightarrow 56k = 9c \Rightarrow 9 \mid 56k$
De nuevo, puesto que $(9,56) = 1$, se deduce que $9 \mid k$, es decir, $k = 9q$ para cierto entero q.
Así pues,

$$n = 56k + 5 = 56 \cdot 9q + 5 = 504q + 5$$

Con esto ya hemos conseguido una criba suficientemente fina para determinar todos los candidatos posibles. Puesto que $6 = 2 \cdot 3$, y el 2 lo hemos incluido en el 8, y el 3 en el 9, no nos tenemos que preocupar por él. O dicho de otro modo, $n = 504q + 5 = 84 \cdot 6q + 5$, y todos estos números darán 5 como residuo al dividirlos entre 6.
Puesto que $2021 = 504 \cdot 4 + 5$, los valores de q aceptables estarán entre 0 y 3, es decir, habrán 4 números cumpliendo las condiciones del enunciado (D).

6.2.2
$N = 9a + 1 = 10b + 3 \Rightarrow 9a = 10b + 2 = 9b + b + 2 \Rightarrow 9 \mid b + 2 \Rightarrow b + 2 = 9k \Rightarrow b = 9k - 2$
Luego $n = 10b + 3 = 10(9k - 2) + 3 = 90k - 20 + 3 = 90k - 17$

Vemos que el único valor aceptable de dos dígitos es para $k = 1 \rightarrow N = 90 \cdot 1 - 17 = 73$, y el residuo de 73 al dividirlo entre 11 es 7 (E).

6.2.3
$n = 6a + 2 = 9b + 5 = 11c + 7$
para ciertos enteros a, b, y c.

$$101 \le 11c + 7 \le 999 \Leftrightarrow 94 \le 11c \le 992 \Leftrightarrow 8 < \frac{94}{11} \le c \le \frac{992}{11} < 91 \Leftrightarrow 9 \le c \le 90$$

Puesto que $6a + 2 = 11c + 7 \Rightarrow 6a = 11c + 5 = 6c + 5c + 5 = 6c + 5(c + 1)$

Luego $c + 1$ tiene que ser un múltiple de 6.

De la misma manera, puesto que

$$9b + 5 = 11c + 7 \Rightarrow 9b = 11c + 2 = 9b + 2c + 2 = 9b + 2(c + 1)$$

Luego $c + 1$ tiene que ser un múltiple de 9.
Así pues, $c + 1$ será un multiple del mínimo común múltiple de 6 y 9, es decir, 18.
Así pues, $c + 1 = 18k$ para cierto k, y por tanto $c = 18k - 1$, y
$n = 11c + 7 = 11(18k - 1) + 7 = 198k - 11 + 7 = 198k - 4$
Para $k = 0 \rightarrow 198k - 4 = -4$,
$k = 1 \rightarrow 198 \cdot 1 - 4 = 194$
$k = 2 \rightarrow 198 \cdot 2 - 4 = 392$

...

$k=5\rightarrow 198\cdot 5-4=986$

$k=6\rightarrow 198\cdot 6-4=1184$ es excesivo.

Luego hay 5 casos aceptables (E).

6.3.4

$y\mid x\Leftrightarrow x\equiv 0\pmod{y}$

$y+1\mid x+1\Leftrightarrow x+1\equiv 0\pmod{y+1}\Leftrightarrow x\equiv -1\pmod{y+1}\Leftrightarrow x\equiv y\pmod{y+1}$

Puesto que $(y,y+1)=1$, aplicando el TCR sabemos que el sistema

$$\begin{cases} x\equiv 0\pmod{x} \\ x\equiv y\pmod{y+1} \end{cases}$$

tendrá solución única $y\equiv a\pmod{y(y+1)}$. Esta solución es $x\equiv y\pmod{y(y+1)}$.

En efecto, está claro que $x\equiv y\pmod{x(x+1)}\Rightarrow x\equiv y\pmod{x+1}$, y

$x\equiv y\pmod{x(x+1)}\Rightarrow x=ay(y+1)+y=(ay+a+1)y\equiv 0\pmod{y}$

Ahora vamos a ir observando los casos uno por uno:

a) $y=1\Rightarrow x\equiv 1\pmod{2}\Leftrightarrow 1<2a+1\leq 100\Leftrightarrow 1\leq a\leq 49\Rightarrow 49$ casos.

b) $y=2\Rightarrow x\equiv 2\pmod{6}\Leftrightarrow 1<6a+2\leq 100\Leftrightarrow 1\leq a\leq 16\Rightarrow$ 16 casos.

c) $y=3\Rightarrow x\equiv 3\pmod{12}\Leftrightarrow 1<12a+3<100\Leftrightarrow 1\leq a\leq 8\Rightarrow$ 8 casos.

d) $y=4\Rightarrow x\equiv 4\pmod{20}\Leftrightarrow 1<20a+4<100\Leftrightarrow 1\leq a\leq 4\Rightarrow 4$ casos.

e) $y=5\Rightarrow x\equiv 5\pmod{30}\Leftrightarrow 1<30a+5<100\Leftrightarrow 1\leq a\leq 3\Rightarrow 3$ casos.

f) $y=6\Rightarrow x\equiv 6\pmod{42}\Leftrightarrow 1<42a+6<100\Leftrightarrow 1\leq a\leq 2\Rightarrow 2$ casos.

g) $y=7\Rightarrow x\equiv 7\pmod{56}\Leftrightarrow 1<56a+7<100\Leftrightarrow 1\leq a\leq 1\Rightarrow 1$ caso.

h) $y=8\Rightarrow x\equiv 8\pmod{72}\Leftrightarrow 1<72a+8<100\Leftrightarrow 1\leq a\leq 1\Rightarrow 1$ caso.

i) $y=9\Rightarrow x\equiv 9\pmod{72}\Leftrightarrow 1<90a+9<100\Leftrightarrow 1\leq a\leq 1\Rightarrow 1$ caso.

Para $y=10\Rightarrow x\equiv 10\pmod{110}\Leftrightarrow 1<110a+10<100\Rightarrow a=0\Rightarrow x=y=10$ y ya no se cumple $y>x$.

El total es 49+16+8+4+3+2+1+1+1=85 casos.

6.4.4

En primer lugar vemos que si $n\equiv 0\pmod{2}$, es decir, n es par entonces $n\pmod{4}=2$, pues $n\equiv 1,3\pmod{4}$ implicaría n impar, y $n\not\equiv 0\pmod{4}$ porque no se pueden repetir los módulos. Con el mismo argumento, $n\equiv 0\pmod{2}\Rightarrow n\not\equiv 3,5\pmod{6}$.

De la misma forma, $n\equiv 1\pmod{2}\Rightarrow n\not\equiv 0,2\pmod{4}$, $n\equiv 1\pmod{2}\Rightarrow n\not\equiv 0,2\pmod{4}$.

También vemos que $n\equiv 5\pmod{6}\Rightarrow n=6k+5\Rightarrow n\equiv 2\pmod{3}$.

Haciendo el árbol de todas las posibles combinaciones, y descartando las ramas incompatibles anteriores, vemos que solo quedan tres combinaciones aceptables:

a) $n\equiv 0\pmod{2}, n\equiv 1\pmod{3}, n\equiv 2\pmod{4}, n\equiv 3\pmod{5}, n\equiv 4\pmod{6}$

b) $n\equiv 1\pmod{2}, n\equiv 2\pmod{3}, n\equiv 3\pmod{4}, n\equiv 0\pmod{5}, n\equiv 5\pmod{6}$

c) $n\equiv 1\pmod{2}, n\equiv 2\pmod{3}, n\equiv 3\pmod{4}, n\equiv 4\pmod{5}, n\equiv 5\pmod{6}$

a)

$n \equiv 4 \pmod 6 \Rightarrow n \equiv 0 \pmod 2, n \equiv 1 \pmod 3$, luego el sistema a resolver es:
$n \equiv 2 \pmod 4, n \equiv 3 \pmod 5, n \equiv 4 \pmod 6$.
$n \equiv 2 \pmod 4 \Leftrightarrow n = 4a + 2$
$n \equiv 3 \pmod 5 \Leftrightarrow n = 5b + 3$
$n \equiv 4 \pmod 6 \Leftrightarrow n = 6c + 4$
Resolvemos el sistema de la segunda con la tercera congruencia:
$$\left.\begin{array}{l} n = 5b + 3 \\ n = 6c + 4 \end{array}\right\} \Rightarrow 5b + 3 = 6c + 4 \Leftrightarrow 5n - 6c = 1 \Rightarrow \begin{cases} b \equiv 5 \pmod 6 \Rightarrow b = 6b'+5 \\ c \equiv 4 \pmod 5 \Rightarrow c = 5c'+4 \end{cases} \Rightarrow$$
$$\left.\begin{array}{l} n = 5b + 3 = 5(6b'+5) + 3 = 30b'+28 \\ n = 6c + 4 = 6(5c'+4) + 4) = 30c'+28 \end{array}\right\}$$
Y ahora resolvemos con la primera congruencia:
$$\left.\begin{array}{l} n = 4a + 2 \\ n = 30c'+28 \end{array}\right\} \Rightarrow 4a + 2 = 30c'+28 \Leftrightarrow 4a - 30b' = 26 \Rightarrow \begin{cases} a = 15a'+14 \\ b' = 2b''+1 \end{cases} \Rightarrow$$
$$\left.\begin{array}{l} n = 4(15a'+14) + 2 = 60a'+58 \\ n = 30(2b''+1) + 28 = 60b''+58 \end{array}\right\} \Rightarrow n = 60k + 58$$
Los números de la forma $n = 60k + 58$ entre 1 y 999 corresponden a los valores entre
$$\left.\begin{array}{l} k = 0 \Rightarrow n = 58 \\ k = 15 \Rightarrow n = 60 \cdot 15 + 58 = 958 \end{array}\right\} \Rightarrow \text{ 16 números en total.}$$

b)
$n \equiv 5 \pmod 6 \Rightarrow n \equiv 1 \pmod 2, n \equiv 2 \pmod 3$, luego el sistema a resolver es:
$n \equiv 3 \pmod 4, n \equiv 0 \pmod 5, n \equiv 5 \pmod 6$.
$n \equiv 3 \pmod 4 \Leftrightarrow n = 4a + 3$
$n \equiv 0 \pmod 5 \Leftrightarrow n = 5b$
$n \equiv 5 \pmod 6 \Leftrightarrow n = 6c + 5$
Tomando la segunda y la tercera congruencia:
$$\left.\begin{array}{l} n = 5b \\ n \equiv 6c + 5 \end{array}\right\} \Rightarrow 5b = 6c + 5 \Rightarrow 5b - 6c = 5 \Rightarrow \begin{cases} b = 6b'+1 \\ c = 5c' \end{cases} \Rightarrow$$
$$\left.\begin{array}{l} n = 5(6b'+1) = 30b'+5 \\ n \equiv 6(5c') + 5 = 30c'+5 \end{array}\right\}$$
Ahora tomamos este resultado con la primera congruencia:
$$\left.\begin{array}{l} n = 4a + 3 \\ n \equiv 30c'+5 \end{array}\right\} \Rightarrow 4a + 3 = 30c'+5 \Rightarrow 4a - 30c' = 2 \Rightarrow \begin{cases} a = 15a'+8 \\ c' = 2c''+1 \end{cases} \Rightarrow$$
$$\left.\begin{array}{l} n = 4(15a'+8) + 3 = 60a'+32 + 3 = 60a'+35 \\ n \equiv 30(2c''+1) + 5 = 60c''+30 + 5 = 60c''+35 \end{array}\right\} \Rightarrow n = 60k + 35$$
Los números de la forma $n = 60k + 35$ entre 1 y 999 corresponden a los valores entre
$$\left.\begin{array}{l} k = 0 \Rightarrow n = 35 \\ k = 16 \Rightarrow n = 60 \cdot 16 + 35 = 995 \end{array}\right\} \Rightarrow \text{ 17 números en total.}$$

c)
$n \equiv 1 \pmod 2, n \equiv 2 \pmod 3, n \equiv 3 \pmod 4, n \equiv 4 \pmod 5, n \equiv 5 \pmod 6$

$n \equiv 5 \pmod 6 \Rightarrow n \equiv 1 \pmod 2, n \equiv 2 \pmod 3$, luego el sistema a resolver es:

$n \equiv 3 \pmod 4, n \equiv 4 \pmod 5, n \equiv 5 \pmod 6$.

$n \equiv 3 \pmod 4 \Leftrightarrow n = 4a + 3$

$n \equiv 4 \pmod 5 \Leftrightarrow n = 5b + 4$

$n \equiv 5 \pmod 6 \Leftrightarrow n = 6c + 5$

Tomando la segunda y la tercera congruencia:

$$\left.\begin{array}{l} n = 5b + 4 \\ n \equiv 6c + 5 \end{array}\right\} \Rightarrow 5b + 4 = 6c + 5 \Rightarrow 5b - 6c = 1 \Rightarrow \begin{cases} b = 6b' + 5 \\ c = 5c' + 4 \end{cases} \Rightarrow$$

$$\left.\begin{array}{l} n = 5(6b' + 5) + 4 = 30b' + 29 \\ n \equiv 6(5c' + 4) + 5 = 30c' + 29 \end{array}\right\}$$

Ahora tomamos este resultado con la primera congruencia:

$$\left.\begin{array}{l} n = 4a + 3 \\ n \equiv 30c' + 29 \end{array}\right\} \Rightarrow 4a + 3 = 30c' + 29 \Rightarrow 4a - 30c' = 26 \Rightarrow \begin{cases} a = 15a' + 14 \\ c' = 2c'' + 1 \end{cases} \Rightarrow$$

$$\left.\begin{array}{l} n = 4(15a' + 14) + 3 = 60a' + 59 \\ n \equiv 30(2c'' + 1) + 29 = 60c'' + 59 \end{array}\right\} \Rightarrow n = 60k + 59$$

Los números de la forma $n = 60k + 59$ entre 1 y 999 corresponden a los valores entre

$$\left.\begin{array}{l} k = 0 \Rightarrow n = 59 \\ k = 15 \Rightarrow n = 60 \cdot 15 + 59 = 959 \end{array}\right\} \Rightarrow \text{ 16 números en total.}$$

En total hay 16+17+16=49 números que satisfacen la condición del enunciado.

6.6.2

Sea $n = \overline{a}\overline{b}\overline{c}\overline{d}$.

$7 \mid 1\overline{b}\overline{c}\overline{d} \Leftrightarrow 7 \mid 1000 + 100b + 10c + d \Leftrightarrow 1000 + 100b + 10c + d \equiv 0$

$\Leftrightarrow 6 + 2b + 3c + d \equiv 0$

$7 \mid \overline{a}1\overline{c}\overline{d} \Leftrightarrow 7 \mid 1000a + 100 + 10c + d \Leftrightarrow 1000a + 100 + 10c + d \equiv 0$

$\Leftrightarrow 6a + 2 + 3c + d \equiv 0$

$7 \mid \overline{a}\overline{b}1\overline{d} \Leftrightarrow 7 \mid 1000a + 100b + 10 + d \Leftrightarrow 1000a + 100b + 10 + d \equiv 0$

$\Leftrightarrow 6a + 2b + 3 + d \equiv 0$

$7 \mid \overline{a}\overline{b}\overline{c}1 \Leftrightarrow 7 \mid 1000a + 100b + 10c + 1 \Leftrightarrow 1000a + 100b + 10c + 1 \equiv 0$

$\Leftrightarrow 6a + 2b + 3c + 1 \equiv 0$

Con lo que nuestro problema se reduce a resolver el siguiente sistema de cuatro congruencias (que siempre serán módulo 7):

$$\begin{cases} 6 + 2b + 3c + d \equiv 0 \\ 6a + 2 + 3c + d \equiv 0 \\ 6a + 2b + 3 + d \equiv 0 \\ 6a + 2b + 3c + 1 \equiv 0 \end{cases}$$

Restando la primera a la segunda:

$$6a - 2b \equiv 4 \Leftrightarrow 3a - b \equiv 2 \Leftrightarrow b \equiv 3a - 2$$

Substituyendo en la tercera:

$$6a+2(3a-2)+3+d\equiv 0 \Leftrightarrow$$
$$6a+6a-4+3+d\equiv 0 \Leftrightarrow$$
$$12a-1+d\equiv 0 \Leftrightarrow$$
$$d\equiv 1-12a\equiv 1-5a$$

Substituyendo en la cuarta:

$$6a+2(3a-2)+3c+1\equiv 0 \Leftrightarrow$$
$$6a+6a-4+3c+1\equiv 0 \Leftrightarrow$$
$$12a-3+3c\equiv 0 \Leftrightarrow 4a+c\equiv 1 \Leftrightarrow c\equiv 1-4a$$

Finalmente, subtituyendo en la primera:

$$2(3a-2)+3(1-4a)+1-5a\equiv 1 \Leftrightarrow$$
$$6a-4+3-12a+1-12a\equiv 1 \Leftrightarrow$$
$$-18a\equiv 1 \Leftrightarrow -4a\equiv 1 \Leftrightarrow 3a\equiv 1 \Leftrightarrow a\equiv 5$$

Puesto que sabemos que $0<a\leq 9$ llegamos a $a=5$

Luego

$$b\equiv 3\cdot 5-2\equiv 13\equiv 6\Rightarrow b=6$$
$$c\equiv 1-4a\equiv 1-4\cdot 5\equiv -19\equiv 2\Rightarrow b=2,9$$

Puesto que buscamos el máximo, tomaremos $b=9$

$$d\equiv 1-12\cdot 5\equiv 1-60\equiv -59\equiv 4\Rightarrow d=4$$

El número buscado es 5694, y la respuesta correcta es $5+694=699$.

7.1.7

$\alpha(\alpha-1)+3$ es divisible por p es equivalente a $\alpha(\alpha-1)+3\equiv 0 \pmod{p}$, es decir, nuestro problema se reduce a demostrar que la congruencia $x(x-1)+3\equiv 0 \pmod{p}$ tiene solución si y solo si la congruencia $y(y-1)+25\equiv 0 \pmod{p}$ tiene solución.

Supongamos, en primer lugar, que $p>3$. Completando cuadrados en la primera congruencia cuadrática:

$$x(x-1)+3\equiv 0 \pmod{p} \Leftrightarrow$$
$$x^2-x+3\equiv 0 \pmod{p} \Leftrightarrow$$
$$4x^2-4x+12\equiv 0 \pmod{p} \Leftrightarrow$$
$$(2x)^2-2\cdot 2x+1^2-1^2+12\equiv 0 \pmod{p} \Leftrightarrow$$
$$(2x-1)^2-1^2+12\equiv 0 \pmod{p} \Leftrightarrow$$
$$(2x-1)^2\equiv -11 \pmod{p}$$

y esta congruencia tendrá solución cuando -11 sea un residuo cuadrático módulo p.

Completando cuadrados en la segunda congruencia cuadrática:

$$y(y-1)+25\equiv 0\pmod{p}\Leftrightarrow$$
$$y^2-y+25\equiv 0\pmod{p}\Leftrightarrow$$
$$4y^2-4y+100\equiv 0\pmod{p}\Leftrightarrow$$
$$(2y)^2-2\cdot 2y+1^2-1^2+100\equiv 0\pmod{p}\Leftrightarrow$$
$$(2y-1)^2-1^2+100\equiv 0\pmod{p}\Leftrightarrow$$
$$(2x-1)^2\equiv -99=3^2(-11)\pmod{p}$$

y esta congruencia tendrá solución cuando -11 sea un residuo cuadrático módulo p, es decir, las dos congruencias tendrán soluciones o no en los mismos casos.

Si $p=2$,
$x(x-1)+3\equiv 0\pmod 2$ no tiene solución porque entonces o bien $x\equiv 0\pmod 2$ o bien $x-1\equiv 0\pmod 2$, y en todo caso $x(x-1)\equiv 0\pmod 2$ y por tanto
$x(x-1)+3\equiv x(x-1)+1\equiv 1\not\equiv 0\pmod 2$
Lo mismo sucede con la segunda congruencia. Así pues, ninguna de las dos tiene solución.

Si $p=3$,
$$0\equiv x(x-1)+3\equiv x(x-1)\pmod 3\Leftrightarrow\begin{cases}x\equiv 0\pmod 3\\ x\equiv 1\pmod 3\end{cases}$$
$$0\equiv y(y-1)+25\equiv y(y-1)+1\pmod 3\Leftrightarrow y\equiv 2\pmod 3$$

Es decir, ambas congruencias tienen solución (el enunciado no exige que tengan las mismas soluciones).

7.2.3
Primera versión.
$$2005=5\ (\text{mod}\ 1000)$$
$$2005^2=25\ (\text{mod}\ 1000)$$
$$2005^3=25\cdot 2005=25\cdot 5=125\ (\text{mod}\ 1000)$$
$$2005^4=125\cdot 2005=125\cdot 5=625\ (\text{mod}\ 1000)$$
$$2005^5=625\cdot 2005=625\cdot 5=125\ (\text{mod}\ 1000)$$
$$2005^6=125\cdot 2005=125\cdot 5=625\ (\text{mod}\ 1000)$$

Vemos la pauta: $n\geq 3\Rightarrow\begin{cases}2005^n=125\ (\text{mod}\ 1000)\ \text{si n es impar}\\ 2005^n=625\ (\text{mod}\ 1000)\ \text{si n es par}\end{cases}$

En $N=2005^{11}+2005^{12}+\ldots+2005^{2006}$ hay 1996 sumandos: 998 pares y 998 impares, luego, tabajando módulo 1000, tenemos:
$N=998\cdot 125+998\cdot 625=998(125+625)=998\cdot 750$
Haciendo esta última multiplicación (no hace falta hacerla entera) vemos que acaba en 500.

Segunda versión.
Ante todo vemos que $2005\equiv 5\ (\text{mod}1000)$

Por un lado calculamos el sumatorio módulo 125:
Si $k \geq 3 \Rightarrow 5^k \equiv 10 (\text{mod } 125)$, luego el sumatorio es cero.

Por otro lado, calculamos el sumatorio módulo 8:

Observamos que $5^2 \equiv 1 (\text{mod } 8)$
Luego $5^k \equiv 1 (\text{mod } 8)$ si es par, y $5^k \equiv 5 (\text{mod } 8)$ si k es impar, luego

$$5^{11} + 5^{12} + ... + 5^{2006} \equiv \frac{1996}{2}(1+5) = 1996 \cdot 3 = 5988 \equiv 4 (\text{mod } 8)$$

Ahora aplicamos el Teorema Chino del Residuo:

$$\left.\begin{array}{l} x \equiv 0 (\text{mod } 125) \\ x \equiv 4 (\text{mod } 8) \end{array}\right\} \Rightarrow \begin{cases} N = 125 \cdot 8 \\ N_1 = 8 \\ N_2 = 125 \rightarrow 125\, y \equiv 1 (\text{mod } 8) \Rightarrow y = 5 \\ x = 8 \cdot 0 \cdot y_1 + 125 \cdot 5 \cdot 4 = 2500 \equiv 500 \ (\text{mod } 1000) \end{cases}$$

7.2.4
Si x no es divisible entre tres entonces $x \equiv 1 \text{ mod } 3$ o $x \equiv 2 \text{ mod } 3$.
$x \equiv 1 \text{ mod } 3 \Rightarrow x = 3k+1 \Rightarrow x^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3k(3k+2) + 1 \Rightarrow x^2 \equiv 1 \text{ mod } 3$
$x \equiv 2 \text{ mod } 3 \Rightarrow x = 3k+2 \Rightarrow x^2 = (3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1 + 1 \Rightarrow x^2 \equiv 1 \text{ mod } 3$
En todo caso, $x^2 \equiv 1 \text{ mod } 3$.

Si x es impar, $x = 2k+1 \Rightarrow x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$, aquí k o k+1 es par, y por tanto $4k(k+1)$ es múltiplo de 8, y por lo tanto $x^2 \equiv 1 \text{ mod } 8$.
Así pues,

$$\begin{cases} x^2 \equiv 1 (\text{mod } 3) \\ x^2 \equiv 1 (\text{mod } 8) \end{cases}$$

Y ahora aplicamos el Teorema chino del residuo:

$N = 8 \cdot 3 = 24$
$N_1 = 3 \rightarrow 3y_1 \equiv 1 \text{ mod } 8 \Rightarrow y_1 = 3$
$N_2 = 8 \rightarrow 8y_2 \equiv 1 \text{ mod } 38 \Rightarrow y_2 = 5$
$x = 3 \cdot 3 \cdot 1 + 8 \cdot 5 \cdot 1 = 9 + 40 = 49$
$x = 49 \equiv 1 (\text{mod } 24)$

7.2.7
Queremos resolver la congruencia cuadrática $x^2 + 7x + 89 \equiv 0 (\text{mod } 77)$.
Puesto que $77 = 7 \cdot 11$, resolveremos las dos congruencias por separado:
i)
$x^2 + 7x + 89 \equiv 0 (\text{mod } 7) \Leftrightarrow x^2 - 2 \equiv 0 (\text{mod } 7) \Leftrightarrow x^2 \equiv 2 (\text{mod } 7)$
La resolvemos por tanteo: $x \equiv 3, 4 (\text{mod } 7)$
ii)

$x^2+7x+89\equiv 0\pmod{11}\Leftrightarrow x^2-4x+1\equiv 0\pmod{11}$

$\Leftrightarrow (x-2)^2-3\equiv 0\pmod{11}\Leftrightarrow (x-2)^2\equiv 3\pmod{11}$

La congruencia $y^2\equiv 3\pmod{11}$ tiene por soluciones $y\equiv 5,6\pmod{11}$, luego

$x-2\equiv 5\pmod{11}\Leftrightarrow x\equiv 7\pmod{11}$

$x-2\equiv 6\pmod{11}\Leftrightarrow x\equiv 8\pmod{11}$

Ahora resolvemos los cuatro sistemas de congruencias que determinan las soluciones anteriores mediante el Teorema Chino del Residuo.

a) $\begin{cases} x\equiv 3\pmod 7 \\ x\equiv 7\pmod{11}\end{cases}$

$N=7\cdot 11=77$

$N_1=11\to 11y_1\equiv 1\pmod 7\Rightarrow y_1=2$

$N_2=7\to 7y_2\equiv 1\pmod{11}\Rightarrow y_2=8$

$x=2\cdot 11\cdot 3+8\cdot 7\cdot 7=458\equiv 73\pmod{77}$

b) $\begin{cases} x\equiv 3\pmod 7 \\ x\equiv 8\pmod{11}\end{cases}$

$x=2\cdot 11\cdot 3+8\cdot 7\cdot 8=514\equiv 52\pmod{77}$

c) $\begin{cases} x\equiv 4\pmod 7 \\ x\equiv 7\pmod{11}\end{cases}$

$x=2\cdot 11\cdot 4+8\cdot 7\cdot 7=480\equiv 18\pmod{77}$

d) $\begin{cases} x\equiv 4\pmod 7 \\ x\equiv 8\pmod{11}\end{cases}$

$x=2\cdot 11\cdot 4+8\cdot 7\cdot 8=536\equiv 74\pmod{77}$

y la menor solución positiva será 18 .

7.3.1

Sabemos que $n=\overline{c_k}\,\overline{c_{k-1}}\,\overline{c_{k-2}}\ldots\overline{c_1}\,\overline{c_0}$ es equivalente a

$$n=c_k10^k+c_{k-1}10^{k-1}+c_{k-2}10^{k-2}+\ldots+c_110+c_0$$

Es decir,

$n=p(10)$ con $p(x)=c_kx^k+c_{k-1}x^{k-1}+c_{k-2}x^{k-2}+\ldots+c_1x+c_0$.

Y que las suma de sus cifras será $S=p(1)$.

Por otro lado, $9=10-1\Rightarrow 9\mid 10-1\Rightarrow 9\mid p(10)-p(1)=n-S\Rightarrow n\equiv S\ (\text{mod } 9)$

Luego $9\mid n\Leftrightarrow n\equiv 0\ (\text{mod } 9)\Leftrightarrow S\equiv 0\ (\text{mod } 9)\Leftrightarrow 9\mid \text{S}$

7.3.2

Sabemos que $n=\overline{c_k}\,\overline{c_{k-1}}\,\overline{c_{k-2}}\ldots\overline{c_1}\,\overline{c_0}$ es equivalente a

$$n=c_k10^k+c_{k-1}10^{k-1}+c_{k-2}10^{k-2}+\ldots+c_110+c_0$$

Es decir,

$n=p(10)$ con $p(x)=c_kx^k+c_{k-1}x^{k-1}+c_{k-2}x^{k-2}+\ldots+c_1x+c_0$.

Y que la suma alternada de sus cifras es $T = p(-1)$.

Por otro lado, $10 \equiv -1 \pmod{11} \Rightarrow p(10) \equiv p(-1) \pmod{11}$, es decir $n \equiv T \pmod{11}$.
Luego $11 | n \Leftrightarrow n \equiv 0 \pmod{11} \Leftrightarrow T \equiv 0 \pmod{11} \Leftrightarrow 11 | T$

7.4.3
Aplicando el Teorema de Wilson, sabemos que

$$-1 \pmod{17} \equiv 16! = 16 \cdot 15 \cdot 14! \Rightarrow 14! \equiv (-1) \cdot 15^{-1} \cdot (-1) \pmod{17}$$

Ya solo queda calcular $15^{-1} \pmod{17}$ mediante el ADE:

$$17 = 15 + 2 \Rightarrow 2 = 17 - 15$$

$$15 = 7 \cdot 2 + 1 \Rightarrow 1 = 15 - 7 \cdot 2 = 15 - 7(17 - 15) = 8 \cdot 15 - 7 \cdot 17 \Rightarrow 15^{-1} \equiv 8 \pmod{17}$$

Así pues, $14! \equiv 8 \pmod{17}$, y el residuo de la división es 8.

7.4.4
Aplicando el Teorema de Wilson, $2016! \equiv -1 \pmod{2017}$ y por otro lado, $2015! \equiv 1 \pmod{p}$
Luego $2016! - 2015! \equiv -1 - (-1) = -2 \equiv 2015 \pmod{2017}$

7.4.5
Multiplicando por 23! a ambos lados de la igualdad obtenemos

$$2 \cdot 3 \cdot \ldots \cdot 23 + 1 \cdot 3 \cdot \ldots \cdot 23 + 1 \cdot 2 \cdot 4 \cdot \ldots \cdot 23 + \ldots + 1 \cdot 2 \cdot 4 \cdot \ldots \cdot 22 = a$$

Todos los sumandos de la izquierda tienen el factor 13 y por tanto se anulan al hacer módulo 13, menos $1 \cdot 2 \cdot 3 \cdot \ldots \cdot 12 \cdot 14 \cdot \ldots \cdot 23$, por lo tanto todo se reduce a calcular
$1 \cdot 2 \cdot 3 \cdot \ldots \cdot 12 \cdot 14 \cdot \ldots \cdot 23 \pmod{13}$

Y aquí aplicamos el Teorema de Wilson:

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot 12 = 12! \equiv -1 \pmod{13},$$

$$14 \cdot 15 \cdot 16 \cdot \ldots \cdot 23 \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 10 \equiv 12^{-1} \cdot 11^{-1} \cdot 12! \equiv (-1)^{-1} \cdot 11^{-1} \cdot (-1) \equiv$$

$$\equiv (-1) \cdot 11^{-1} \cdot (-1) \equiv 11^{-1} \pmod{13}$$

Determinamos $11^{-1} \pmod{13}$ mediante el ADE:

$$13 = 11 + 2 \Rightarrow 2 = 13 - 11$$

$$11 = 2 \cdot 5 + 1 \Rightarrow 1 = 11 - 2 \cdot 5 = 11 - (13 - 11) \cdot 5 = 6 \cdot 11 - 5 \cdot 13 \Rightarrow 11^{-1} \equiv 6 \pmod{13}$$

Así pues, finalmente:

$$a \equiv (-1) \cdot 11^{-1} \equiv -6 \equiv 7 \pmod{13}$$

7.4.6
Se cumple $i \equiv -(p - i) \pmod{p}$, por lo tanto:

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot (p-2) \equiv (-1)^{(p-1)/2} (p-1)(p-3) \cdot \ldots \cdot 2 \pmod{p}$$

Y multiplicando ambos lados por $1 \cdot 3 \cdot 5 \cdot \ldots \cdot (p-2)$ llegamos a:

$$1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{(p-1)/2} (p-1)! \pmod{p}$$

Y finalmente aplicamos el Teorema de Wilson:

$$(-1)^{(p-1)/2}(p-1)!\equiv(-1)^{(p-1)/2}(-1)=(-1)^{(p-1)/2+1}=(-1)^{(p+1)/2}\pmod{p}$$

tal y como queríamos ver.

Fuente de esta solución: Mathematical Excalibur, Vol. 22, No. 3, Feb. 19 – Apr. 19.

7.4.7

Vamos a estudiar la tabla de todos los valores $1\le n\le 102$ para observar qué valores $x\equiv n^2+n=n(n+1)\pmod{103}$ generan:

n	$n(n+1)$
1	$1\cdot 2=2$
2	$2\cdot 3=6$
3	$3\cdot 4=12$
…	…
99	$99\cdot 100\equiv(-4)(-3)=3\cdot 4=12$
100	$100\cdot 101\equiv(-3)(-2)=2\cdot 3=6$
101	$101\cdot 102\equiv(-2)(-1)=1\cdot 2=2$

Vemos que los valores de x que vamos obteniendo van por parejas, puesto que $-n\equiv 103-n\pmod{103}$, luego solo trabajaremos hasta la mitad:

n	$n(n+1)$
1	$1\cdot 2=2$
2	$2\cdot 3=6$
3	$3\cdot 4=12$
…	…
49	$49\cdot 50$
50	$50\cdot 51$
51	$51\cdot 52$

Pero observamos que, en módulo 103, $1\equiv -102$, $2\equiv -101$, $3\equiv -100$,…, $51\equiv -52$

Luego la tabla anterior la podemos escribir como

n	$n(n+1)$
1	$-102\cdot 2=2$
2	$-101\cdot 3=6$
3	$-100\cdot 4=12$
…	…
49	$-54\cdot 50$
50	$-53\cdot 51$
51	$-52\cdot 52$

Es decir, que el producto que buscamos es

$2\cdot 3\cdot 4\cdot \ldots \cdot 50\cdot 51\cdot (-52)\cdot (-53)\cdot \ldots \cdot (-101)\cdot (-102)\cdot 52 =$

$2\cdot 3\cdot 4\cdot \ldots \cdot 50\cdot 51\cdot 52\cdot 53\cdot \ldots \cdot 101\cdot 102\cdot (-1)^{102-52+1}\cdot 52 =$

$102!\cdot (-1)^{102-52+1}\cdot 52 = 102!\cdot (-1)\cdot 52$

Ahora aplicamos el Teorema de Wilson (10.4.2): $102!\equiv -1 \pmod{103}$

Para concluir que el producto es $(-1)(-1)\cdot 52 \pmod{103} = 52 \pmod{103}$

Observación: En las soluciones oficiales (Compendium SMT, pág. 1078) se presenta una solución más formal en términos algebraicos.

7.6.1

$$\frac{(a-b)(b-c)(c-a)}{2}+2=2016^n \Leftrightarrow (a-b)(b-c)(c-a)+4=2\cdot 2016^n$$

Hacemos un cambio de variable:

$$\left.\begin{array}{l} b-a=x \\ c-b=y \end{array}\right\} \Rightarrow c-a=b-a+c-b=x+y$$

Luego tenemos la expresión equivalente

$$xy(x+y)+4=2\cdot 2016^n$$

Ahora, si $n>0$,

$$7\mid 2016 \Rightarrow 7\mid 2\cdot 2016^n \Rightarrow xy(x+y)+4\equiv 0 \pmod 7 \Leftrightarrow$$
$$\Leftrightarrow 3xy(x+y)+12\equiv 0 \pmod 7 \Leftrightarrow 3xy(x+y)\equiv -12 \pmod 7$$
$$\Leftrightarrow 3xy(x+y)\equiv 2 \pmod 7$$
$$\Leftrightarrow (x+y)^3-x^3-y^3\equiv 2 \pmod 7$$

Aplicando el PTF (o simplemente observando la tabla de valores $x^3 \pmod 7$ con $0\le x\le 6$) vemos que $x\not\equiv 0 \Rightarrow 1\equiv x^6=x^3\cdot x^3 \pmod 7 \Rightarrow \pm 1\equiv x^3 \pmod 7$.

Luego es imposible encontrar una combinación $(x+y)^3-x^3-y^3\equiv 2 \pmod 7$ a no ser que uno de los tres elementos: $x+y$, x o y sea 0 módulo 7, es decir, sea divisible entre 7.

Pero entonces $xy(x+y)$ es múltiple de 7, con lo que $xy(x+y)+4$ no puede ser múltiple de 7, llegando a contradicción.

La única posibilidad válida es $n=0 \Rightarrow xy(x+y)+4=2 \Rightarrow xy(x+y)=-2$.

$$\left.\begin{array}{l} x=2 \\ y=-1 \\ x+y=1 \end{array}\right\} \Rightarrow \left.\begin{array}{l} b-a=2 \\ c-b=-1 \end{array}\right\} \Rightarrow \begin{cases} a=k \\ b=2+k \\ c=-1+2+k=1+k \end{cases}$$

Observando las demás soluciones posibles llegamos al resultado final:

$(a,b,c)=(k,k+2,k+1)$ y todas sus permutaciones cíclicas.

7.7.1

Queremos resolver la congruencia $30n^3+143n^2+117n-56\equiv 0 \pmod{13}$.

Lo primero que hacemos es pasar los coeficientes a módulo 13:

$$30n^3+143n^2+117n-56\equiv 0\pmod{13}\Leftrightarrow 4n^3+0n^2+0n-4\equiv 0\pmod{13}\Leftrightarrow$$
$$4n^3-4\equiv 0\pmod{13}\Leftrightarrow 4\left(n^3-1\right)\equiv 0\pmod{13}\Leftrightarrow n^3-1\equiv 0\pmod{13}\Leftrightarrow$$
$$n^3\equiv 1\pmod{13}$$

Esta última congruencia la podemos resolver directamente:

$1^3\equiv 1,\ 2^3\equiv 8,\ 3^3\equiv 1,\ 4^3\equiv -1,\ 5^3\equiv 8,\ 6^3\equiv 8,\ 7^3\equiv 5,\ 8^3\equiv 5,\ 9^3\equiv 1,\ 10^3\equiv -1,$
$11^3\equiv 5,\ 12^3\equiv -1$

y por tanto $n^3\equiv 1\pmod{13}\Leftrightarrow n\equiv 1,3,9\pmod{13}$.

Aunque es mucho más elegante seguir el siguiente razonamiento:

Sabemos que $2^{12}\equiv 1\pmod{13}$ por el PTF, y sabemos que 2 es una raíz primitiva módulo 13. Por lo tanto:

$\left(2^a\right)^3\equiv 1\pmod{13}\Leftrightarrow 2^{3a}\equiv 2^{12}\pmod{13}\Leftrightarrow 12\mid 3a\Leftrightarrow 4\mid a\Leftrightarrow a=4,8,12$

$a=4\Rightarrow 2^a=2^4=16\equiv 3\pmod{13}$

$a=8\Rightarrow 2^a=2^8=256\equiv 9\pmod{13}$

$a=12\Rightarrow 2^a=2^{12}\equiv 1\pmod{13}$

Puesto que $2021\equiv 6\pmod{13}$, el primer valor $2021+k\equiv 1,3,9\pmod{13}$ será para $k=3$, y la solución del problema será 2024 .

8.2.1

$3^2=9\ (\text{mod } 191)$ $\qquad 3^4=\left(3^2\right)^2=81\ (\text{mod } 191)$

$3^8=\left(3^4\right)^2=6561\equiv 67\ (\text{mod } 191)$ $\qquad 3^{16}=\left(3^8\right)^2=4489\equiv 96\ (\text{mod } 191)$

$3^{32}=\left(3^{16}\right)^2=9216\equiv 48\ (\text{mod } 191)$ $\qquad 3^{64}=\left(3^{32}\right)^2=2304\equiv 12\ (\text{mod } 191)$

$3^{128}=\left(3^{64}\right)^2=144\ (\text{mod } 191)$

Y ahora, puesto que $172=128+32+8+4$,

$3^{172}\ (\text{mod } 191)=3^{128}3^{32}3^8 3^4\ (\text{mod } 191)=144\cdot 48\cdot 67\cdot 81\ (\text{mod } 191)=170\ (\text{mod } 191)$

8.6.1

Primera versión.

$$1^3+2^3+3^3+\ldots+n^3=\frac{n^2(n+1)^2}{4}$$

Queremos resolver la congruencia $\dfrac{n^2(n+1)^2}{4}\equiv 17 \bmod (n+5)$

$$\frac{n^2(n+1)^2}{4}\equiv 17 \bmod (n+5)\Leftrightarrow \frac{n^2(n+1)^2}{4}=k(n+5)+17$$
$$\Leftrightarrow n^2(n+1)^2=4k(n+5)+4\cdot 17=4k(n+5)+68\Rightarrow$$
$$n^2(n+1)^2\equiv 68 \bmod (n+5)$$

Pero observamos que

$$n \equiv -5 \bmod (n+5) \Rightarrow n^2 \equiv (-5)^2 \bmod (n+5)$$
$$n+1 \equiv -4 \bmod (n+5) \Rightarrow (n+1)^2 \equiv (-4)^2 \bmod (n+5)$$

Y por tanto

$$n^2(n+1)^2 \equiv (-5)^2(-4)^2 = 25 \cdot 16 = 400 \bmod (n+5)$$

Luego

$$400 \equiv 68 \bmod (n+5) \Leftrightarrow 400 - 68 \equiv 0 \bmod (n+5) \Leftrightarrow 332 \equiv 0 \bmod (n+5)$$
$$\Leftrightarrow n+5 \mid 332 = 2^2 \cdot 83$$

Con las condiciones del enunciado estamos suponiendo implícitamente que $n+5 > 17$, luego las únicas posibilidades son $n+5 = 83,166,332 \Rightarrow n = 78,161,327$.

Comprobamos estas soluciones, y vemos que se cumple para 78 y para 161, pero no para 327:

$$n = 327 \Rightarrow \frac{n^2(n+1)^2}{4} \equiv 100 \bmod (n+5)$$

Luego las soluciones son $n = 78,161$.

Observación. Las comprobaciones exigen cálculo manual con números grandes. Por ejemplo:

$$n = 327 \Rightarrow \begin{cases} n^2 = 106929 \\ (n+1)^2 = 107584 \end{cases}$$

Segunda versión. Mediante aritmética modular.

$$\frac{n^2(n+1)^2}{4} \equiv 17 \bmod (n+5) \Leftrightarrow$$
$$n^2(n+1)^2 \equiv 68 \bmod (n+5) \Leftrightarrow$$
$$n^2(n+1)^2 - 68 \equiv 0 \bmod (n+5) \Leftrightarrow$$
$$n+5 \mid n^2(n+1)^2 - 68 = n^4 + 2n^3 + n^2 - 68$$

Realizando la división sintética tenemos que

$$n^4 + 2n^3 + n^2 - 68 = (n^3 - 3n^2 + 16n - 80)(n+5) + 332 \Rightarrow$$
$$\frac{n^4 + 2n^3 + n^2 - 68}{n+5} = n^3 - 3n^2 + 16n - 80 + \frac{332}{n+5}$$

Y por tanto

$$n+5 \mid n^2(n+1)^2 - 68 \Leftrightarrow \frac{332}{n+5} \in Z$$

Y se sigue igual que en la primera versión.

Tercera versión.

Con un cambio de variable: $m=n+5 \Rightarrow \begin{cases} n=m-5 \\ n+1=m-4 \end{cases}$

Y por tanto

$$\frac{n^2(n+1)^2}{4} \equiv 17 \bmod (n+5) \Leftrightarrow \frac{(m-5)^2(m-4)^2}{4} \equiv 17 \bmod m \Leftrightarrow$$

$$\frac{(-5)^2(-4)^2}{4} \equiv 17 \bmod m \Leftrightarrow \frac{400}{4} \equiv 17 \bmod m \Leftrightarrow 400 \equiv 4 \cdot 17 \bmod m \Leftrightarrow$$

$$400 \equiv 68 \bmod m \Leftrightarrow 400-68 \equiv 0 \bmod m \Leftrightarrow 332 \equiv 0 \bmod m \Leftrightarrow m \mid 332 \Leftrightarrow n+5 \mid 332$$

Y se sigue igual que en la primera versión.

Fuente de estas soluciones: https://artofproblemsolving.com/wiki/index.php?title=2020_AIME_II_Problems/Problem_10&oldid=125812

8.6.2

Estamos estudiando la función $n \mapsto \left(\left\lfloor \frac{n}{4} \right\rfloor, \left\lfloor \frac{n}{5} \right\rfloor, \left\lfloor \frac{n}{6} \right\rfloor \right)$, y queremos ver en qué casos es inyectiva, es decir, la imagen determina unívocamente la antiimagen.

Para que un entero n quede unívocamente determinado por esta terna se pueden cumplir varias situaciones:

A)

$$\begin{cases} n-1 \to (a-1, b, c) \\ n \to (a, b, c) \\ n+1 \to (a, b+1, c) \end{cases}$$

La única posibilidad de que

$$\left\lfloor \frac{n}{4} \right\rfloor = a, \left\lfloor \frac{n-1}{4} \right\rfloor = a-1$$

es que se cumpla $n=4k$.

La única posibilidad de que

$$\left\lfloor \frac{n}{5} \right\rfloor = b, \left\lfloor \frac{n+1}{5} \right\rfloor = b+1$$

Es que se cumpla $n=5q-1$

Luego se dará esta situación cuando

$$\begin{cases} n=4k \\ n=5q-1 \end{cases} \Leftrightarrow \begin{cases} n \equiv 0 \pmod 4 \\ n \equiv 4 \pmod 5 \end{cases} \Leftrightarrow n \equiv 4 \pmod{20}$$

B)

$$\begin{cases} n-1 \to (a-1, b, c) \\ n \to (a, b, c) \\ n+1 \to (a, b, c+1) \end{cases}$$

De nuevo, tenemos $n=4k$.

La única posibilidad de que

$$\left\lfloor \frac{n}{6} \right\rfloor = c, \left\lfloor \frac{n+1}{6} \right\rfloor = c+1$$

es que se cumpla $n=6q-1$

Luego se dará esta situación cuando

$$\begin{cases} n=4k \\ n=6q-1 \end{cases} \Leftrightarrow \begin{cases} n\equiv 0 \pmod 4 \\ n\equiv -1 \pmod 6 \end{cases}$$

Este sistema no tiene solución.

C)

$$\begin{cases} n-1\rightarrow (a,b-1,c) \\ n\rightarrow (a,b,c) \\ n+1\rightarrow (a,b,c+1) \end{cases}$$

Con los mismos razonamientos, aquí nos encontramos con $n=5k$ y $n=6q-1$

$$\begin{cases} n=5k \\ n=6q-1 \end{cases} \Leftrightarrow \begin{cases} n\equiv 0 \pmod 5 \\ n\equiv -1 \pmod 6 \end{cases} \Leftrightarrow n\equiv 5 \pmod{30}$$

D)

$$\begin{cases} n-1\rightarrow (a,b-1,c) \\ n\rightarrow (a,b,c) \\ n+1\rightarrow (a+1,b,c) \end{cases}$$

Se dará esta situación cuando

$$\begin{cases} n=4k-1 \\ n=5q \end{cases} \Leftrightarrow \begin{cases} n\equiv -1 \pmod 4 \\ n\equiv 0 \pmod 5 \end{cases} \Leftrightarrow n\equiv 15 \pmod{20}$$

E)

$$\begin{cases} n-1\rightarrow (a,b,c-1) \\ n\rightarrow (a,b,c) \\ n+1\rightarrow (a+1,b,c) \end{cases}$$

Se dará esta situación cuando

$$\begin{cases} n=4k-1 \\ n=6q \end{cases} \Leftrightarrow \begin{cases} n\equiv -1 \pmod 4 \\ n\equiv 0 \pmod 6 \end{cases}$$

Este sistema de congruencias no es compatible.

F)

$$\begin{cases} n-1\rightarrow (a,b,c-1) \\ n\rightarrow (a,b,c) \\ n+1\rightarrow (a,b+1,c) \end{cases}$$

Se dará esta situación cuando

$$\begin{cases} n=5k-1 \\ n=6q \end{cases} \Leftrightarrow \begin{cases} n\equiv -1 \pmod 5 \\ n\equiv 0 \pmod 6 \end{cases} \Leftrightarrow n\equiv 24 \pmod{30}$$

Así pues, se cumplirá el enunciado cuando n sea de una de las cuatro formas siguientes:

$$\begin{cases} n\equiv 4 \pmod{20}\rightarrow 30 \\ n\equiv 5 \pmod{30}\rightarrow 20 \\ n\equiv 15 \pmod{20}\rightarrow 30 \\ n\equiv 24 \pmod{30}\rightarrow 20 \end{cases}$$

De todos estos casos, debemos tener en cuenta que el grupo

$$\begin{cases} n \equiv 5 \pmod{30} \\ n \equiv 15 \pmod{20} \end{cases}$$

tiene 10 repeticiones

Y el grupo

$$\begin{cases} n \equiv 24 \pmod{30} \\ n \equiv 4 \pmod{20} \end{cases}$$

Tiene 10 repeticiones,
Por lo tanto, el total será $30+20+30+20-10-10=80$ casos.

Observaciones: Una vez entendemos la mecánica profunda del problema, vemos que todo se desarrolla en módulo 30 y módulo 20, luego podemos pasar resolver el problema en módulo 60, y después multiplicar por 3 el recuento obtenido. Al reducir el problema a 60 casos, incluso se puede hacer un recuento "por fuerza bruta", uno por uno.

Podemos leer en www.artofproblemsolving.com que este problema recibió una queja formal porque, en realidad, se podía haber incluido el caso $n=600$, y por tanto el resultado sería 81. Esta queja fue aceptada.

8.6.3

Observamos que $A_0 = 2^0 + 3^2 + 5^2 = 2+9+25 = 35 = 5\cdot 7$, luego el máximo común divisor buscado será un divisor de 35, es decir: 1, 5, 7 o 35.
Veamos que $5 \nmid A_n$ para algún n.

$$5 \mid A_n \Leftrightarrow A_n \equiv 0 \pmod 5 \Leftrightarrow 2^{3n} + 3^{6n+2} + 5^{6n+2} \equiv 0 \pmod 5 \Leftrightarrow 2^{3n} + 3^{6n+2} \equiv 0 \pmod 5$$

$$\Leftrightarrow \left(2^3\right)^n + 3^2 \cdot \left(3^6\right)^n \equiv 0 \pmod 5$$

$$2^3 = 8 \equiv 3 \Rightarrow \left(2^3\right)^n \equiv 3^n$$

$$3^6 = (3^3)^2 \equiv 2^2 = 4 \equiv -1 \Rightarrow \left(3^6\right)^n \equiv (-1)^n \Rightarrow 3^2 \cdot \left(3^6\right)^n \equiv (-1)(-1)^n = (-1)^{n+1}$$

Así pues, $A_n \equiv \left(2^3\right)^n + 3^2 \cdot \left(3^6\right)^n \equiv 3^n + (-1)^{n+1} \pmod 5$.
Luego, en particular,

$$A_1 \equiv 3^1 + (-1)^2 = 3+1 = 4 \not\equiv 0 \pmod 5$$

Veamos que $7 \mid A_n$ para todo n.

$$A_n = 2^{3n} + 3^{6n+2} + 5^{6n+2} = \left(2^3\right)^n + 3^2 \cdot \left(3^6\right)^n + 5^2 \cdot \left(5^6\right)^n = (*)$$

$$2^3 = 8 \equiv 1 \pmod 7$$

$$3^2 = 9 \equiv 2 \pmod 7$$

$$3^6 = \left(3^3\right)^2 \equiv (-1)^2 = 1 \pmod 7$$

$$5^2 = 25 \equiv 4 \pmod 7$$

$$5^6 = \left(5^3\right)^2 = 125^2 \equiv (-1)^2 = 1 \pmod 7$$

Luego

$$(*) \equiv 1^n + 2\cdot 1^n + 4 \cdot 1^n = 1+2+4 = 7 \equiv 0 \pmod 7$$

Así pues, finalmente, $\left(A_0, A_1, \ldots, A_{1999}\right) = 7$

8.6.4

Primera versión. Mediante factorización.

Opción A: Aplicamos Binomio de Newton:

$$2^{606}-1=\left(2^3\right)^{202}-1^{202}=\left(2^3-1\right)\left(\left(2^3\right)^{201}+\left(2^3\right)^{200}+\left(2^3\right)^{199}+...\right)$$

y por tanto está claro que es divisible entre 7, y queda descartado.

Opción E: Aplicando la identidad "suma de potencias":

$$2^{607}+3^{607}=\left(2+3\right)\left(2^{606}-2^{605}\cdot 3+2^{604}\cdot 3^2-...\right)$$

y por tanto está claro que es divisible entre 5, y queda descartado.

Opción D: Con el mismo razonamiento:

$$2^{607}+1=2^{607}+1^{607}=\left(2+1\right)\left(2^{606}-2^{605}+2^{604}-...\right)$$

y por tanto está claro que es divisible entre 3, y queda descartado.

Opción B: Aplicando la identidad "suma de cubos"

$$2^{606}+1=\left(2^{202}\right)^3+1^3=\left(2^{202}+1\right)\left(\left(2^{202}\right)^2-2^{202}+1\right)$$

El primer factor se puede escribir de la siguiente manera:

$$2^{202}+1=\left(2^2\right)^{101}+1=4^{101}+1$$

Vemos como se comportan los números de la forma 4^n+1

$$n=1\rightarrow 4^1+1=5$$
$$n=2\rightarrow 4^2+1=17$$
$$n=3\rightarrow 4^3+1=65$$
$$n=4\rightarrow 4^4+1=257$$
$$n=4\rightarrow 4^5+1=1025$$

Y observamos que si n es impar, 4^n+1 es múltiple de 5, que es nuestro caso, luego también se puede descartar.

Este último resultado se puede demostrar mediante aritmética modular:

$$4^n+1 \pmod 5=(-1)^n+1\equiv -1+1\equiv 0 \pmod 5 \text{ si n es impar.}$$

La única opción sin descartar es C.

Segunda versión. Mediante exponenciación modular.

Vamos a estudiar la sucesión de potencias 2^n, 2^n-1 y 2^n+1:

n	2^n	2^n-1	2^n+1
1	2	1	3
2	4	3	5
3	8	7	9
4	16	15	17
5	32	31	33
6	64	63	65
7	128	127	129
8	256	255	267
9	512	511	513
10	1024	1023	1025

Observamos que los todos los números de la forma 2^n+1, con n impar, son todos múltiplos de 3. Es el caso D. En efecto,

$$2 \equiv -1 \pmod 3 \Rightarrow 2^n \equiv (-1)^n \pmod 3$$

y en el caso n impar,

$$2^n \equiv (-1)^n \equiv -1 \pmod 3 \Rightarrow 2^n + 1 \equiv -1 + 1 \equiv 0 \pmod 3$$

Observamos que los todos los números de la forma $2^n - 1$, con n par, son todos múltiplos de 3. Es el caso A. En efecto,

$$2 \equiv -1 \pmod 3 \Rightarrow 2^n \equiv (-1)^n \pmod 3$$

y en el caso n par,

$$2^n \equiv (-1)^n \equiv 1 \pmod 3 \Rightarrow 2^n + 1 \equiv 1 - 1 \equiv 0 \pmod 3$$

Observamos que algunos de los números de la forma $2^n + 1$, con n par, son múltiplos de 5.

$$2^n + 1 \equiv 2^{2k} + 1 \equiv \left(2^2\right)^k + 1 \equiv 4^k + 1 \equiv (-1)^k + 1 \pmod 5$$

y en el caso k impar,

$$(-1)^k + 1 \equiv (-1) + 1 \equiv 0 \pmod 5$$

Por lo tanto si podemos escribir n de la forma $n = 2k = 2(2q+1) = 4q + 2$, la potencia será múltiple de 5, y quedará descartado. Y el número de la opción B se adapta a este patrón. En efecto, $606 - 2 = 604 = 4 \cdot 151 \Rightarrow 606 = 4 \cdot 151 + 2$.

Finalmente, para descartar la opción E, vamos a trabajar módulo 5:

$$3 \equiv -2 \pmod 5 \Rightarrow 3^n \equiv (-2)^n \pmod 5$$

Y por tanto, si n es impar, $(-2)^n \equiv -2^n \pmod 5$ y por tanto

$$2^n + 3^n \equiv -2^n + 2^n \equiv 0 \pmod 5.$$

En el caso de la opción E tenemos que 607 es impar, por lo tanto este número será divisible entre 5 y quedará descartado.
La única opción aceptable es C.

Observación. El número de la opción C, $2^{607} - 1$, es el número 14 de Mersenne, que se trabajan en el apartado 19.2 de este mismo libro.

8.6.5

Este problema es equivalente a resolver la congruencia $2^n + 5^n \equiv n \pmod{1000}$.

Puesto que $1000 = 2^3 \cdot 5^3$, podemos dividir este problema en dos, con lo que nos queda el siguiente sistema de congruencias:

$$\begin{cases} 2^n + 5^n \equiv n \pmod{2^3} \\ 2^n + 5^n \equiv n \pmod{5^3} \end{cases}$$

Ahora bien, es fácil comprobar que no se cumple para $n \le 2$. Pero si $n \ge 3$, está claro que $2^n \equiv 0 \pmod{2^3}$ y $5^n \equiv 0 \pmod{5^3}$, con lo cual nuestro sistema se reduce al siguiente:

$$\begin{cases} 5^n \equiv n \pmod{2^3} \\ 2^n \equiv n \pmod{5^3} \end{cases}$$

Veamos ahora estas congruencias por separado. La primera es fácil:

$5^2 = 25 \equiv 1 \pmod{2^3}$, luego $5^n \equiv \begin{cases} 1 \text{ si n es par} \\ 5 \text{ si n es impar} \end{cases} \pmod{2^3}$

Así pues, si n es par, $5^n \equiv 1 \pmod{2^3}$, pero para n par nunca se cumple $n \equiv 1 \pmod{2^3}$, pues $n \equiv 1 \pmod{2^3} \Rightarrow n = 8k+1$ que es impar. Luego n debe ser impar, y en particular $n = 8a+5$ para cierto $a \geq 0$.

Veamos ahora la segunda congruencia: $2^n \equiv n \pmod{5^3}$. Esta congruencia es mucho más difícil.

Aquí utilizaremos la propiedad $2^n \equiv n \pmod{5^3} \Rightarrow \begin{cases} 2^n \equiv n \pmod{5} \\ 2^n \equiv n \pmod{5^2} \end{cases}$

Primera reducción.

$2^{8a+5} \equiv 8a+5 \pmod{5^3}$.

$2^{8a+5} = \left(2^8\right)^a \cdot 2^5 = 256^a \cdot 32 \equiv 32 \cdot 6^a \pmod{5^3}$

$2^{8a+5} \equiv 8a+5 \pmod{5^3} \Leftrightarrow 32 \cdot 6^a \equiv 8a+5 \pmod{5^3}$

Resolvemos $32 \cdot 6^a \equiv 8a+5 \pmod{5}$

$32 \cdot 6^a \equiv 8a+5 \pmod{5} \Leftrightarrow 7 \cdot 1^a \equiv 3a \pmod{5}$

$\Leftrightarrow 7 \equiv 3a \pmod{5} \Leftrightarrow 3^{-1} \cdot 7 \equiv a \pmod{5} \Leftrightarrow a \equiv 2 \cdot 7 = 14 \equiv 4 \equiv -1 \pmod{5} \Rightarrow$

$a = 5b-1$

Y por tanto $n = 8(5b-1)+5 = 40b-8+5 = 40b-3$

Segunda reducción.

Volvamos a la congruencia $2^n \equiv n \pmod{5^3}$:

$2^n \equiv n \pmod{5^3} \Leftrightarrow 2^{40b-3} \equiv 40b-3 \pmod{5^3} \Leftrightarrow 2^{40b} \equiv 2^3(40b-3) \pmod{5^3}$

$\Leftrightarrow 2^{40b} \equiv 320b-24 \pmod{5^3}$

Estudiamos ahora la congruencia $2^{40b} \equiv 320b-24 \pmod{5^2}$

$2^{40b} \equiv 320b-24 \pmod{5^2} \Leftrightarrow \left(2^{10}\right)^{4b} \equiv 20b+1 \pmod{5^2}$

Por otro lado, observamos que $2^{10} = 1024 = -1 \pmod{5^2}$, así pues:

$\left(2^{10}\right)^{4b} \equiv 20b+1 \pmod{5^2} \Leftrightarrow (-1)^{4b} \equiv 20b+1 \pmod{5^2}$

$\Leftrightarrow 1 \equiv 20b+1 \pmod{5^2} \Leftrightarrow 0 \equiv 20b \pmod{5^2} \Leftrightarrow b = 5c$

Así pues, $n = 8(5b-1)+5 = 8(5 \cdot 5c-1)+5 = 200c-3$.

Tercera reducción.

Volvemos a la congruencia $2^n \equiv n \pmod{5^3}$:

$2^{200c-3} \equiv 200c-3 \pmod{5^3} \Leftrightarrow \left(2^{100}\right)^{2c} 2^{-3} \equiv 200c-3 \pmod{5^3}$

$\phi(125)=100 \Rightarrow 2^{100}\equiv 1\left(\text{mod } 5^3\right)\Rightarrow \left(2^{100}\right)^{2c}\equiv 1\left(\text{mod } 5^3\right)$, luego aplicando Teorema de Euler,
$\left(2^{100}\right)^{2c}2^{-3}\equiv 200c-3\left(\text{mod } 5^3\right)\Leftrightarrow \left(2^3\right)^{-1}\equiv 200c-3\left(\text{mod } 5^3\right)$
$\Leftrightarrow 47\equiv 200c-3\left(\text{mod } 5^3\right)\Leftrightarrow 50\equiv 200c\left(\text{mod } 5^3\right)\Leftrightarrow c\equiv 4\left(\text{mod } 5\right)\Leftrightarrow c\equiv 5d+4$

Finalmente,

$$n=200c-3=200(5d+4)-3=1000d+800-3=1000d+797$$

Y el valor más pequeño lo encontraremos para $d=0\Rightarrow n=797$.

9.1.1

Primera versión: Mediante el método de las potencias de dos.

Vamos calculando $1032^{(2^n)}\,(\text{mod } 100)$:

$$1032^{1}\equiv 32\ (\text{mod } 100)$$
$$1032^{2}\equiv 32\cdot 32=24\ (\text{mod } 100)$$
$$1032^{4}\equiv 24\cdot 24=76\ (\text{mod } 100)$$
$$1032^{8}\equiv 76\cdot 76=76\ (\text{mod } 100)$$
$$\ldots$$

Observamos que $1032^{(2^n)}\equiv 76\,(\text{mod } 100)$ para todo $n\geq 2$.

Por otro lado,

$1032=1024+4+2\Rightarrow 1032^{1032}=1032^{1024+8}=1032^{1024}\cdot 1032^{8}\Rightarrow$

$1032^{1032}\,(\text{mod } 100)=1032^{2^{10}}\cdot 1032^{2^3}\,(\text{mod } 100)\equiv 76\cdot 76\,(\text{mod } 100)\equiv 76\,(\text{mod } 100)$

Segunda versión: Mediante el Teorema Chino del Residuo.

$1032\equiv 0\ (\text{mod } 4)\Rightarrow 1032^{1032}\equiv 0\ (\text{mod } 4)$

$1032\equiv 7\ (\text{mod } 25)\Rightarrow 1032^{2}\equiv 49\equiv -1\ (\text{mod } 25)\Rightarrow$

$\Rightarrow 1032^{1032}=1032^{2\cdot 516}=\left(1032^{2}\right)^{516}\equiv (-1)^{516}\equiv 1\ (\text{mod } 25)$

Nos queda el siguiente sistema de congruencias que resolveremos mediante el Teorema Chino del Residuo:

$$\begin{cases}1032^{1032}\equiv 0\ (\text{mod } 4)\\ 1032^{1032}\equiv 1\ (\text{mod } 25)\end{cases}$$

$$\left.\begin{array}{l}N=4\cdot 25=100\\ N_1=25\rightarrow 25y_1\equiv 1\,(\text{mod } 4)\\ N_2=4\rightarrow 4y_2\equiv 1\,(\text{mod } 25)\Rightarrow y_2=19\end{array}\right\}\Rightarrow x=25\cdot y_1\cdot 0+4\cdot 19\cdot 1=76$$

Y por tanto: $1032^{1032}\equiv 76\ (\text{mod } 4\cdot 25)$, tal como queríamos ver.

9.1.2

Queremos determinar $2003^{2002^{2001}} \pmod{1000}$.

Puesto que $2003 \equiv 3 \pmod{1000}$, está claro que $2003^{2002^{2001}} \equiv 3^{2002^{2001}} \pmod{1000}$

Vamos a estudiar las potencias $3^n \pmod{1000}$. Para ello vamos a utilizar el siguiente argumento:

$$3^{2k} \equiv \left(3^2\right)^k \pmod{1000} \equiv 9^k = (10-1)^k \pmod{1000}$$

Para estudiar las potencias $(10-1)^k$ vamos a aplicar el Binomio de Newton:

$$(10-1)^k = \binom{k}{0} 10^0 (-1)^k + \binom{k}{1} 10^1 (-1)^{k-1} + \binom{k}{2} 10^2 (-1)^{k-2} + \binom{k}{3} 10^3 (-1)^{k-3} + \ldots$$

Todos los sumandos a partir del cuarto son múltiples de 1000, y por tanto se pueden despreciar. Así pues,

$$(10-1)^k \equiv (-1)^k + 10k(-1)^{k-1} + 50k(k-1)(-1)^{k-2} \pmod{1000}$$

En particular, tomando $k = 2n$,

$$(10-1)^{2n} \equiv (-1)^{2n} + 10 \cdot 2n(-1)^{2n-1} + 50 \cdot 2n(2n-1)(-1)^{2n-2} \pmod{1000}$$
$$\equiv 1 - 20n + 100n(2n-1) \pmod{1000}$$

Es decir:

$$3^{4n} \equiv 1 - 20n + 100n(2n-1) \pmod{1000} \quad (*)$$

En particular, para $n = 25$:

$$3^{100} = 3^{4 \cdot 25} \equiv 1 - 20 \cdot 25 + 100 \cdot 25 \cdot (2 \cdot 25 - 1) \equiv 1 - 500 + 100 \cdot 25 \cdot 49$$
$$\equiv 1 - 500 + 2500 \cdot 49 \equiv 1 + 500 \cdot 48 \equiv 1 + 1000 \cdot 24 \equiv 1 \pmod{1000}$$

Puesto que $3^{100} \equiv 1 \pmod{1000}$, tenemos que determinar $2002^{2001} \pmod{100}$ para resolver nuestro problema.

$$2002 \equiv 2 \pmod{100} \Rightarrow 2002^{2001} \equiv 2^{2001} \pmod{100}$$

Utilizando que $2^{2001} \equiv 4 \cdot 2^{1999} \pmod{4 \cdot 25}$, aplicaremos la "Simplificación de congruencias lineales", con lo que tenemos que calcular $\equiv 2^{1999} \pmod{25}$, y para determinar esta congruencia utilizaremos el siguiente resultado:

$$2^{10} = 1024 \equiv -1 \pmod{25} \Rightarrow 2^{1999} = 2^{2000-1} = 2^{200 \cdot 10 - 1} = \left(2^{10}\right)^{200} \cdot 2^{-1} \equiv (-1)^{200} \cdot 2^{-1} \equiv$$
$$\equiv 1 \cdot 2^{-1} \equiv 2^{-1} \equiv 13 \pmod{25}$$

Ahora:

$$2^{2001} \equiv 4 \cdot 2^{1999} \pmod{4 \cdot 25} \equiv 4 \cdot 13 \equiv 52 \pmod{4 \cdot 25}$$

En donde en el último paso hemos utilizado que $2 \cdot 13 = 26 \equiv 1 \pmod{25}$.

Así pues, finalmente,

$$3^{2002^{2001}} \pmod{1000} \equiv 3^{52} \pmod{1000}$$

Volviento a utilizar (*),

$$3^{52} = 3^{4\cdot 13} \equiv 1 - 20\cdot 13 + 100\cdot 13(2\cdot 13 - 1) = 1 - 260 + 100\cdot 13\cdot 25 =$$
$$= 1 - 260 + 32500 \equiv 1 - 260 + 500 \equiv 241 \pmod{1000}$$

Las tres últimas cifras de $2003^{2002^{2001}}$ son 241.

Fuente: Soluciones oficiales (Compendium CMO, pág. 115)

9.1.3

a) Aplicando PTF, $3^6 \equiv 1 \pmod 7 \Rightarrow 3^{31} = 3^{5\cdot 6+1} = \left(3^6\right)^5 3 \equiv 1^5 \cdot 3 = 3 \pmod 7$

b) 4 , c) 9

9.1.4

Aplicando el PTF, $2^{12} \equiv 1 \pmod{13}$, luego

$2^{1000} = 2^{12\cdot 83+4} = \left(2^{12}\right)^{83} \cdot 2^4 \equiv 1^{83} \cdot 2^4 = 2^4 \pmod{13} = 16 \pmod{13} \equiv 3 \pmod{13}$

El residuo es 3.

9.1.5

Por el PTF, $11^{16} \equiv 1 \pmod{17}$.

$104 = 16\cdot 6 + 8$, luego $11^{104} = 11^{16\cdot 6+8} = \left(11^{16}\right)^6 11^8 \equiv (1)^6 11^8 = 11^8 \pmod{17}$

$11^2 = 121 \equiv 2 \pmod{17} \Rightarrow 11^8 = \left(11^2\right)^4 \equiv 2^4 \pmod{17} = 16 \pmod{17} = -1 \pmod{17}$

Finalmente: $11^{104} \equiv -1 \pmod{17} \Leftrightarrow 11^{104} + 1 \equiv 0 \pmod{17} \Leftrightarrow 17 \mid 11^{104} + 1$

9.1.6

El número a no puede ser múltiplo de 5, pues en ese caso $mcd(a,35) \neq 1$. Luego podemos aplicar el PTF para garantizar que $a^4 \equiv 1 \pmod 5$, y por tanto:

$a^4 \equiv 1 \pmod 5 \Rightarrow a^{12} = \left(a^4\right)^3 \equiv 1^3 = 1 \pmod 5$

De la misma manera, a no puede ser múltiplo de 7, y de nuevo aplicamos el PTF para garantizar que $a^6 \equiv 1 \pmod 7$, y por tanto:

$a^6 \equiv 1 \pmod 7 \Rightarrow a^{12} = \left(a^6\right)^2 \equiv 1^2 = 1 \pmod 7$

Luego:

$$\left.\begin{array}{l} a^{12} \equiv 1 \pmod 5 \\ a^{12} \equiv 1 \pmod 7 \end{array}\right\} \Rightarrow a^{12} \equiv 1 \pmod{[5,7]} \Rightarrow a^{12} \equiv 1 \pmod{35}$$

pues $[5,7] = mcm(5,7) = 5\cdot 7 = 35$ ya que $mcd(5,7) = 1$

9.1.7

Sabemos que $4^k \equiv 4 \pmod 6$ para todo k (se demuestra fácilmente por inducción sobre k)

Observamos que la secuencia a_n parece dar siempre residuo 4 módulo 7:

$a_1 = 4 \equiv 4 \pmod 7$

$a_2 = 4^4 = 256 = 7 \cdot 36 + 4 \equiv 4 \pmod 7$

Veamos que, en general, si $k \equiv 4 \pmod 6 \Rightarrow 4^k \equiv 4 \pmod 7$. En efecto:
Por el PTF, $4^6 \equiv 1 \pmod 7$ luego

$k \equiv 4 \pmod 6 \Rightarrow k = 6j + 4 \Rightarrow 4^k = 4^{6j+4} = \left(4^6\right)^j 4^4 \equiv 4^4 \equiv 4 \pmod 7$

Luego $a_n \equiv 4 \pmod 7$ para todo n, en particular, para $n = 100$.

9.1.8

Queremos ver $(a,42) = 1 \Rightarrow a^6 - 1 \equiv 0 \bmod(3 \cdot 7 \cdot 8) \Leftrightarrow a^6 \equiv 1 \bmod(3 \cdot 7 \cdot 8)$

Aplicamos tres veces el PTF:

$(a,42) = 1 \Rightarrow 3 \nmid a \Rightarrow a^2 \equiv 1 \bmod(3) \Rightarrow a^6 = \left(a^2\right)^3 \equiv 1^3 = 1 \bmod(3)$

$(a,42) = 1 \Rightarrow 7 \nmid a \Rightarrow a^6 \equiv 1 \bmod(7)$

$(a,42) = 1 \Rightarrow 2 \nmid a \Rightarrow a \equiv 1 \bmod(2) \Rightarrow a^6 \equiv 1^6 = 1 \bmod(2)$

Y ahora:

$$\left.\begin{array}{l} a^6 \equiv 1 \bmod(3) \\ a^6 \equiv 1 \bmod(7) \\ a^6 \equiv 1 \bmod(2) \end{array}\right\} \Rightarrow a^6 \equiv 1 \bmod([3,7,2]) = a^6 \equiv 1 \bmod(3 \cdot 7 \cdot 8)$$

9.1.9

Vemos que $7 \nmid 2,3,4,5,6$ y por tanto podemos aplicar el PTF:

$2^6 \equiv 1 \pmod 7 \Rightarrow 2^{20} = 2^{3 \cdot 6 + 2} = \left(2^6\right)^2 2^2 \pmod 7 \equiv 1^2 2^2 \pmod 7 = 4 \pmod 7$

$3^6 \equiv 1 \pmod 7 \Rightarrow 3^{30} = 3^{6 \cdot 5} = \left(3^6\right)^5 \pmod 7 \equiv 1^5 = 1 \pmod 7$

$4^6 \equiv 1 \pmod 7 \Rightarrow 4^{40} = 4^{6 \cdot 6 + 4} = \left(4^6\right)^6 \cdot 4^4 \pmod 7 \equiv 1^6 \cdot 4^4 \pmod 7 = 4^4 \pmod 7 \equiv 4 \pmod 7$

En donde hemos aplicado que $4^2 = 16 \equiv 2 \pmod 7 \Rightarrow 4^4 = \left(4^2\right)^2 \equiv 2^2 = 4 \pmod 7$

$5^6 \equiv 1 \pmod 7 \Rightarrow 5^{50} = 5^{8 \cdot 6 + 2} = \left(5^6\right)^8 \cdot 5^2 \pmod 7 \equiv 1^8 \cdot 5^2 = 5^2 = 25 \equiv 4 \pmod 7$

$6^6 \equiv 1 \pmod 7 \Rightarrow 6^{60} = 5^{10 \cdot 6} = \left(5^6\right)^{10} \pmod 7 \equiv 1 \pmod 7$

Finalmente, $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \equiv 4 + 1 + 4 + 4 + 1 = 14 \equiv 0 \pmod 7$

9.1.10

Primera versión.

Aplicando el PTF a nuestro caso:

$$\left.\begin{array}{l} 133^5 \equiv 133 \equiv 3 \pmod 5 \\ 110^5 \equiv 110 \equiv 0 \pmod 5 \\ 84^5 \equiv 84 \equiv 4 \pmod 5 \\ 27^5 \equiv 27 \equiv 2 \pmod 5 \end{array}\right\} \Rightarrow 133^5 + 110^5 + 84^5 + 27^5 \equiv 3 + 0 + 4 + 2 \equiv 4 \pmod 5$$

$n^5 \equiv n \pmod 5 \Rightarrow n \equiv 4 \pmod 5$

Por otro lado:

$$\left.\begin{array}{l} 133 \equiv 1 \pmod 3 \Rightarrow 133^5 \equiv 1^5 = 1 \pmod 3 \\ 110 \equiv -1 \pmod 3 \Rightarrow 110^5 \equiv (-1)^5 = -1 \pmod 3 \\ 84 \equiv 0 \pmod 3 \Rightarrow 84^5 \equiv 0 \pmod 3 \\ 27 \equiv 0 \pmod 3 \Rightarrow 27^5 \equiv 0 \pmod 3 \end{array}\right\} \Rightarrow 133^5 + 110^5 + 84^5 + 27^5 \equiv 1 - 1 \equiv 0 \pmod 3$$

Por el PTF, $n^3 \equiv n \pmod 3 \Rightarrow n^5 \equiv n^2 n^3 \equiv n^2 n = n^3 \equiv n \pmod 3$, luego $n \equiv 0 \pmod 3$

Está claro que $n^5 = 133^5 + 110^5 + 84^5 + 27^5 > 133^5 \Rightarrow n > 133$

El primer número $n > 133$ que cumple $n \equiv 4 \pmod 5$ y $n \equiv 0 \pmod 3$ es 144, y el siguiente es 176.

Enseguida (????) vemos que 176 es ya demasiado grande, por lo tanto la solución debe ser $n = 144$.

Segunda versión.

$$\left.\begin{array}{l} 133 \equiv 3 \pmod{10} \Rightarrow 133^5 \equiv 3^5 = 243 \equiv 3 \pmod{10} \\ 110 \equiv 0 \pmod{10} \Rightarrow 110^5 \equiv 0 \pmod{10} \\ 84 \equiv 4 \pmod{10} \Rightarrow 84^5 \equiv 4^5 \equiv 4 \pmod{10} \\ 27 \equiv 7 \pmod{10} \Rightarrow 27^5 = 7^5 \equiv 7 \pmod{10} \end{array}\right\} \Rightarrow n^5 \equiv 2 + 0 + 4 + 7 \equiv 4 \pmod{10}$$

Pero por otro lado,

$n^2 \equiv n \pmod 2 \Rightarrow n^5 \equiv n^2 n^2 n \equiv n^3 \equiv n^2 n \equiv n^2 \equiv n \pmod 2$, y por tanto:

$$\left.\begin{array}{l} n^5 \equiv n \pmod 2 \\ n^5 \equiv n \pmod 5 \end{array}\right\} \Rightarrow n^5 \equiv n \pmod{10}$$

Así pues, $n^5 \equiv n \equiv 4 \pmod{10}$, y por lo tanto el número n buscado acaba en 4.

Observamos que $133, 110, 84$ son números muy próximos a múltiplos de 27:

$$\left.\begin{array}{l} 133 \approx 5 \cdot 27 \Rightarrow 133^5 \approx 5^5 \cdot 27^5 \\ 110 \approx 4 \cdot 27 \Rightarrow 110^5 \approx 4^5 \cdot 27^5 \\ 84 \approx 3 \cdot 27 \Rightarrow 84^5 \approx 3^5 \cdot 27^5 \end{array}\right\} \Rightarrow n^5 = 133^5 + 110^5 + 84^5 + 27^5 \approx 27^5 \left(5^5 + 4^5 + 3^5 + 1\right)$$

$$n^5 \approx 27^5 \left(5^5 + 4^5 + 3^5 + 1\right) = 27^5 \cdot 4393 \Rightarrow 4393 \approx \frac{n^5}{27^5} = \left(\frac{n}{27}\right)^5$$

Como antes, sabemos que $n > 133$, y sabemos que acaba en 4, luego los candidatos son 134, 144, 154, 164…

Está claro que $n = 134$ nos vamos a quedar cortos.

Probando (y utilizado mucho, pero mucho cálculo !!!!) con $n=144$:

$n=144 \Rightarrow \frac{144}{27}=\frac{16}{3} \Rightarrow \left(\frac{16}{3}\right)^5=\frac{1048576}{243} \approx 4315$, que se aproxima bastante a 4393.

Puesto que estamos trabajando con potencias quintas, que crecen de forma muy rápida, está claro que el siguiente candidato $n=154$ ya no será muy próximo al valor buscado, por lo que podemos asegurar que $n=144$ es la solución del problema.

Nota: El enunciado lleva implícito que este número existe. Ninguna de las dos soluciones demuestra que $133^5+110^5+84^5+27^5 \equiv 144^5$, son buenos argumentos que justifican que $n=154$ es un buen candidato para este resultado.

Fuente de esta solución: https://artofproblemsolving.com/wiki/index.php/1989_AIME_Problems/Problem_9

9.1.11

$p \mid 29^p+1 \Leftrightarrow 29^p+1 \equiv 0 \pmod p \Leftrightarrow 29^p \equiv -1 \pmod p \Rightarrow$

$\left(29^p\right)^2 \equiv (-1)^2=1 \pmod p \Leftrightarrow \left(29^2\right)^p \equiv 1 \pmod p$

Pero, aplicando el PTF, sabemos que $a^p \equiv a \pmod p$ para todo a, luego

$1 \equiv \left(29^2\right)^p \equiv 29^2 \pmod p \Leftrightarrow 1 \equiv 29^2 \pmod p \Leftrightarrow 29^2-1 \equiv 0 \pmod p \Leftrightarrow$

$p \mid 29^2-1=840=2^3 \cdot 3 \cdot 5 \cdot 7 \Rightarrow p=2,3,5,7$

De los cuatro candidatos posibles, los tres primeros son satisfactorios:

$p=2 \Rightarrow 29^2 \equiv 29 \equiv 1=-1 \pmod 2$

$p=3 \Rightarrow 29^3 \equiv 29 \equiv 2=-1 \pmod 3$

$p=5 \Rightarrow 29^5 \equiv 29 \equiv 4=-1 \pmod 5$

(en donde seguimos aplicando PTF : $a^p \equiv a \pmod p$)

Pero el cuarto primo no es satisfactorio: $p=7 \Rightarrow 29^7 \equiv 29 \equiv 1 \not\equiv -1 \pmod 7$

Luego las soluciones son tres: $p=2,3,5$.

9.1.12

Vamos a demostrar que solo el 1 es coprimo con toda la sucesión

$$a_n=2^n+3^n+6^n-1\ ,\ n \geq 1$$

Es decir, para todo $k>1$, existe un m tal que $(k,a_m)>1$.

Para ello es suficiente demostrarlo para los números primos.

En efecto, supongamos que se cumple para todo primo p.

Supongamos que no es cierto para cierto $k>1$ compuesto. Sea p uno de los factores primos de k.

$$(k,a_n)=1 \text{ para todo } n \geq 1.$$

$\left.\begin{matrix} p \mid k \\ (k,a_n)=1 \end{matrix}\right\} \Rightarrow (p,a_n)=1$ para todo $n \geq 1$, contradiciendo la hipótesis.

Para $p=2,3$, está claro que $p \mid a_2=48$.

Si $p>3$, por el Pequeño teorema de Fermat,

$$2^{p-1}\equiv 1\,(\text{mod } p)\Rightarrow 3\cdot 2^{p-1}\equiv 3\,(\text{mod } p)$$
$$3^{p-1}\equiv 1\,(\text{mod } p)\Rightarrow 2\cdot 3^{p-1}\equiv 2\,(\text{mod } p)$$
$$6^{p-1}\equiv 1\,(\text{mod } p)$$

y por tanto

$$6a_{p-2}=6\cdot 2^{p-2}+6\cdot 3^{p-2}+6\cdot 6^{p-2}-6=$$
$$=3\cdot 2^{p-1}+2\cdot 3^{p-1}+6^{p-1}-6\equiv 3+2+1-6\equiv 0\,(\text{mod } p)\Rightarrow p\mid 6a_{p-2}$$

Y por el Corolario al Lema de Euclides, llegamos a $p\mid a_{p-2}\Rightarrow (p,a_{p-2})=p>1$.

Fuente de la solución: Soluciones oficiales (Compendium IMO , pág. 821)

9.1.13

Aplicando el PTF sabemos que $x^{10}\equiv 1\pmod{11}$, luego
$4\equiv x^{103}=\left(x^{10}\right)^{10}x^3\equiv 1^{10}x^3=x^3\pmod{11}$, luego el problema se reduce a resolver la congruencia $x^3\equiv 4\pmod{11}$.
Probando valores del 2 al 10 encontramos la única solución posible: $5^3=125\equiv 4\pmod{11}$.

9.1.14

Observamos que $385=5\cdot 7\cdot 11$, y también que
$385\mid n^{60}-1\Leftrightarrow n^{60}-1\equiv 0\pmod{385}\Leftrightarrow n^{60}\equiv 1\pmod{385}$

Queremos demostrar $5,7,11\nmid n\Rightarrow n^{60}\equiv 1\pmod{385}$

El PTF nos garantiza que

$$5,7,11\nmid n\Rightarrow\begin{cases}n^4\equiv 1\pmod 5\\ n^6\equiv 1\pmod 7\\ n^{10}\equiv 1\pmod{11}\end{cases}$$

Luego

$$\left.\begin{aligned}&n^4\equiv 1\pmod 5\Rightarrow n^{60}=\left(n^4\right)^{15}\equiv 1\pmod 5\\ &n^6\equiv 1\pmod 7\Rightarrow n^{60}=\left(n^6\right)^{10}\equiv 1\pmod 7\\ &n^{10}\equiv 1\pmod{11}\Rightarrow n^{60}=\left(n^{10}\right)^{6}\equiv 1\pmod{11}\end{aligned}\right\}\Rightarrow n^{60}\equiv 1\pmod{5\cdot 7\cdot 11}$$

tal y como queríamos ver.

9.1.15

El problema equivale a determinar los primos p para los cuales
$29^p+1\equiv 0\,(\text{mod } p)\Leftrightarrow 29^p\equiv -1\,(\text{mod } p)$

Por el PTF sabemos que se cumple $29^p \equiv 29 \pmod{p}$, luego nuestro problema se reduce a determinar los primos p para los cuales

$$29 \equiv -1 \pmod{p} \Leftrightarrow 30 \equiv 0 \pmod{p} \Leftrightarrow p \mid 30 = 2 \cdot 3 \cdot 5 \Leftrightarrow p = 2,3,5$$

9.1.16

$9 \cdot \underbrace{111...1}_{p-1} = \underbrace{999...9}_{p-1} = 10^{p-1} - 1$

Si $p \geq 7$ entonces $p \nmid 10 = 2 \cdot 5$, y por tanto, aplicando el PTF, $10^{p-1} - 1 \equiv 1 - 1 = 0 \pmod{p}$.

Así pues, $9 \cdot \underbrace{111...1}_{p-1} \equiv 0 \pmod{p}$.

Puesto que $p \geq 7 \Rightarrow (9, p) = 1$, podemos cancelar el 9 y llegar a $\underbrace{111...1}_{p-1} \equiv 0 \pmod{p}$, tal y como queríamos ver.

9.1.17

Fijamos un n, y consideremos una sucesión $A_1 \subset A_2 \subset A_3 \subset ... \subset A_n$.

Cada uno de los diez números del conjunto $\{1,2,3,...,10\}$ puede ser colocado por primera vez en una de las $n+1$ siguientes posiciones: En ningún A_i, en A_1, en A_2,..., o en A_n. Luego hay $(n+1)^{10}$ maneras de colocarlos.

Así pues, $K = \sum_{n=1}^{10} (n+1)^{10} = \sum_{n=2}^{11} n^{10} = \sum_{n=1}^{11} n^{10} - 1$, y queremos calcular $K \pmod{10}$

En primer lugar calculamos $K \pmod{5}$. Aquí aplicaremos el PTF: $n^5 \equiv n \pmod{5}$, por lo que $n^{10} = (n^5)^2 \equiv n^2 \pmod{5}$

Y por tanto

$$K = \sum_{n=1}^{11} n^{10} - 1 \equiv \sum_{n=1}^{11} n^2 - 1 \equiv \frac{11 \cdot 12 \cdot 23}{6} - 1 = 11 \cdot 2 \cdot 23 - 1 = 505 \equiv 0 \pmod{5}$$

Ahora calculamos $K \pmod{2}$. Aquí aplicaremos que solo nos interesa la paridad:

$K = \sum_{n=2}^{11} n^{10} = 2^{10} + 3^{10} + 4^{10} + ... + 11^{10}$, hay 5 pares y 5 impares, que sumados generan un impar, luego es impar, y por tanto $K \equiv 1 \pmod{2}$

Finalmente, aplicando el Teorema chino del Residuo (o por simplemente por observación)

$$\left.\begin{array}{l} K \equiv 0 \pmod{5} \\ K \equiv 1 \pmod{2} \end{array}\right\} \Rightarrow K \equiv 5 \pmod{10}$$

Fuente de esta solución: Dr. Ebrahimian en Youtube

9.1.18

Tomando $x = y = 1$,

$$(x+y)^{19} - x^{19} - y^{19} = 2^{19} - 1^{19} - 1^{19} = 2^{19} - 2 = 2\left(2^{18} - 1\right) = 2\left(\left(2^9\right)^2 - 1^2\right) =$$

$$= 2\left(2^9 - 1\right)\left(2^9 + 1\right) = 2 \cdot 511 \cdot 513 = 2 \cdot 7 \cdot 73 \cdot 3 \cdot 19 = 2 \cdot 3 \cdot 7 \cdot 19 \cdot 73$$

Luego los candidatos posibles son 2, 3, 7, 19 y 73.

El 73 lo descartamos porque, tomando $x=2, y=1$, $(x+y)^{19}-x^{19}-y^{19}=3^{19}-2^{19}-1$ y este número no es un múltiplo de 73. En efecto,

$3^4=81\equiv 8\Rightarrow 3^8\equiv 8^2\equiv 64\equiv -9\Rightarrow 3^{16}\equiv(-9)^2\equiv 81\equiv 8\Rightarrow 3^{19}=3^3\cdot 3^{16}\equiv 27\cdot 8=216\equiv 70 \pmod{73}$

$2^8=256\equiv 37\Rightarrow 2^{16}\equiv 37^2\equiv 55\Rightarrow 2^{19}=2^3\cdot 2^{16}\equiv 8\cdot 55=440\equiv 2 \pmod{73}$

Por lo que $3^{19}-2^{19}-1\equiv 70-2-1\equiv 67\not\equiv 0 \pmod{73}$

El 19 es válido porque es una aplicación directa del PTF:

$$(x+y)^{19}\equiv x+y \pmod{19}$$

$$\left.\begin{array}{l} x^{19}\equiv x \pmod{19} \\ y^{19}\equiv y \pmod{19} \end{array}\right\}\Rightarrow x^{19}+y^{19}\equiv x+y \pmod{19}$$

El 7 es válido. En efecto, aplicando el PTF, sabemos que $a^7\equiv a \pmod{7}$ para cualquier valor de a, luego

$$a^{19}=a^5\cdot a^7\cdot a^7\equiv a^5\cdot a\cdot a\equiv a^7\equiv a \pmod{7}$$

y por tanto

$$(x+y)^{19}\equiv x+y\equiv x^{19}+y^{19} \pmod{7}$$

Un razonamiento alternativo sería el siguiente:

Si $7\mid a$ es trivial. $a^{19}\equiv 0^{19}\equiv 0\equiv a \pmod{7}$.

Si $7\nmid a$, aplicando el PTF, $7\mid a^6-1$, pero, por otro lado, $6\mid 18\Rightarrow a^6-1\mid a^{18}-1$, y por tanto

$7\mid a^{18}-1\Rightarrow 7\mid a\left(a^{18}-1\right)\Rightarrow a^{19}\equiv a \pmod{7}$

El 3 es válido. En efecto, aplicando el PTF, $a^3\equiv a \pmod{3}$ para cualquier valor de a, luego

$$a^{19}=a\cdot\left(a^6\right)^3\equiv a\cdot a^6\equiv a\cdot a^3\cdot a^3\equiv a\cdot a\cdot a\equiv a^3\equiv a \pmod{3}$$

y por tanto

$$(x+y)^{19}\equiv x+y\equiv x^{19}+y^{19} \pmod{3}$$

De nuevo, un razonamiento alternativo sería el siguiente:

Si $3\mid a$ es trivial. $a^{19}\equiv 0^{19}\equiv 0\equiv a \pmod{3}$.

Si $3\nmid a$, aplicando el PTF, $3\mid a^2-1$, pero, por otro lado, $2\mid 18\Rightarrow a^2-1\mid a^{18}-1$, y por tanto

$$3\mid a^{18}-1\Rightarrow 3\mid a\left(a^{18}-1\right)\Rightarrow a^{19}\equiv a \pmod{3}$$

Finalmente, 2 es válido. En efecto, a^{19} tiene la misma paridad que a.

Fuente de esta solución: Soluciones oficiales.

9.2.1

$i\mid 2^j-1\Leftrightarrow 2^j-1\equiv 0 \pmod{i}\Leftrightarrow 2^j\equiv 1 \pmod{i}$

Si $i=1$, $2\equiv 0 \pmod{1}, 1\equiv 0 \pmod{1}$, y por lo tanto, trivialmente $2^j\equiv 1 \pmod{i}$ para $j=1$.

Si $i=2$, $2\equiv 0 \pmod{1}, 1\not\equiv 0 \pmod{1}$, y por lo tanto, trivialmente $2^j\equiv 0\not\equiv 0 \pmod{i}$ para todo j, luego no se cumple la condición del enunciado.

Supongamos que $i\geq 3$.

Aplicando el Teorema de Euler, sabemos que si $(2,i)=1$, es decir, si i es impar, entonces $2^{\phi(i)} \equiv 1 \pmod{i}$, y por tanto basta tomar $j=\phi(i)$, que sabemos cumplirá $1 \le \phi(i) < i$.

Si $(2,i) \neq 1$, es decir, si i es par, no existirá ningún j tal que $2^j \equiv 1 \pmod{i}$, pues entonces:

$$2^j \equiv 1 \pmod{i} \Leftrightarrow 2 \cdot 2^{j-1} \equiv 1 \pmod{i}$$

Y por tanto $x = 2^{j-1}$ sería solución para la congruencia $2x \equiv 1 \pmod{i}$, pero ya vimos en en el Tema 9 que no tiene solución.
Tomando $j=1$, es imposible, pues $2 \not\equiv 1 \pmod{i}$.
Luego se cumple para todos los $1 \le i \le 1000$ impares, es decir, para 500 números.

9.2.2

Estudiar los ocho últimos dígitos de la expansión binaria de 27^{1986} es equivalente a determinar (en binario) $27^{1986} \pmod{256}$

$$\phi(256) = \phi(256) = 256\left(1-\frac{1}{2}\right) = 128,$$

Puesto que $256 \nmid 27$, podemos aplicar el Teorema de Euler para garantizar que $27^{128} \equiv 1 \pmod{256}$.

Por otro lado, $27^{1986} = 27^{15 \cdot 128+66} = \left(27^{128}\right)^{15} 27^{66} \equiv 1^{15} 27^{66} = 27^{66} \pmod{256}$

Calcularemos $27^{66} \pmod{256}$ con el "método de las potencias de dos":

$27^2 = 729 \Rightarrow 729 \equiv 217 \equiv -39 \pmod{256} \Rightarrow 27^{64} = (-39)^{32} \pmod{256}$

$(-39)^2 = 1521 \equiv 241 \equiv -15 \pmod{256} \Rightarrow (-39)^{32} = \left((-39)^2\right)^{16} \equiv (-15)^{16} \pmod{256}$

$(-15)^2 = 225 \equiv (-31) \pmod{256} \Rightarrow (-15)^{16} = \left((-15)^2\right)^8 \equiv (-31)^8 \pmod{256}$

$(-31)^2 = 961 \equiv 193 \equiv (-63) \pmod{256} \Rightarrow (-31)^8 = \left((-31)^2\right)^4 \equiv (-63)^4 \pmod{256}$

$(-63)^2 = 3969 \equiv 129 \pmod{256} \Rightarrow (-63)^4 = \left((-63)^2\right)^2 \equiv 129^2 \pmod{256}$

$129^2 \equiv 1 \pmod{256}$

Por lo anterior: $27^{66} = 27^{64} 27^2 \equiv 1 \cdot 217 = 217 \pmod{256}$
Y la expresión binaria de 217 es "11011001"

9.2.3

Queremos determinar $a_{2008} \pmod{1000}$, donde n se ha definido recursivamente:

$$a_1 = 1,\ a_2 = 2^{a_1},\ a_3 = 3^{a_2},\ \ldots,\ a_{2008} = 2008^{a_{2007}}$$

Por un lado, $2008 = 251 \cdot 8 \Rightarrow 2008 \equiv 0 \pmod{8} \Rightarrow n = 2008^{a_{2007}} \equiv 0 \pmod{8}$.

Por otro lado, $2008 = 16 \cdot 125 + 8 \Rightarrow 2008 \equiv 8 \pmod{125}$

$\phi(125) = \phi(5^3) = 5^3\left(1-\frac{1}{5}\right) = 5^3 \frac{4}{5} = 100$, luego, aplicando el Teorema de Euler, para cualquier número a, con $(a,125)=1$, se cumple $a^{100} \equiv 1 \pmod{125}$.

Observamos que
$2007 \equiv 7 \pmod{100} \Rightarrow 2007^{4k} \equiv 7^{4k} = 2401^k \equiv 1^k = 1 \pmod{100}$

$a_{2006} = 2006^{a_{2005}} = (2 \cdot 1003)^{a_{2005}} = 2^{a_{2005}} \cdot 1003^{a_{2005}}$ es múltiplo de 4, pues seguro que $a_{2005} \geq 2$,
Y por tanto $a_{2007} = 2007^{a_{2006}} \equiv 1 \pmod{100} \Rightarrow a_{2007} = 100k + 1$ para cierto k, luego
$a_{2008} = 2008^{a_{2007}} \equiv 2008^{100k+1} = 2008^{100k} \cdot 2008 \equiv 2008 \equiv 8 \pmod{125}$

Finalmente aplicamos el Teorema Chino del Residuo:

$$\begin{cases} n \equiv 0 \pmod 8 \\ n \equiv 8 \pmod{125} \end{cases}$$

$$\left.\begin{array}{l} N = 8 \cdot 125 \\ N_1 = 125 \rightarrow 125\, y_1 \equiv 1 \pmod 8 \\ N_2 = 8 \rightarrow 8 y_2 \equiv 1 \pmod{125} \Rightarrow y_2 = 47 \end{array}\right\} \Rightarrow n = 125 \cdot y_1 \cdot 0 + 8 \cdot 47 \cdot 8 = 3008 \equiv 8 \pmod{1000}$$

Así pues, la solución al problema es "008".

Fuente de la solución: Olympiad Number Theory Through Challenging Problems (Justin Stevens, 3E) pág.49

9.2.4

Queremos calcular $f(17) + f(18) + f(19) + f(20) \pmod{100}$, donde $f(x)$ se ha definido recursivamente: $f_1(x) = x$, $f_2(x) = x^{f_1(x)}$,..., $f(x) = f_4(x) = x^{f_3(x)}$.

$\phi(25) = \phi(5^2) = 25\left(1 - \frac{1}{5}\right) = 20 \Rightarrow a^{20} \equiv 1 \pmod{25}$ si $(a,25) = 1$

Los calcularemos por separado.

Primera parte: $f(20) \pmod{100}$

$20^2 = 400 \equiv 0 \pmod{100} \Rightarrow 20^k \equiv 0 \pmod{100}$ para todo k par, y puesto que $f_3(20) = 20^{f_2(20)}$ es par, está claro que $f(20) = 20^{f_3(20)} \equiv 0 \pmod{100}$.

Segunda parte: $f(19) \pmod{100}$

$$\left.\begin{array}{l} f(19) = 19^{f_3(19)} \equiv (-1)^{f_3(19)} \pmod 4 \\ f_3(19) = 19^{f_2(19)} \text{ es impar} \end{array}\right\} \Rightarrow f(19) \equiv -1 \pmod 4$$

$f_2(19) = 19^{f_1(19)}$ es claramente impar, luego
$f_3(19) \pmod{\phi(25)} = f_3(19) \pmod{20} = 19^{f_2(19)} \pmod{20} = -1 \pmod{20}$, y por tanto:
$f(19) = 19^{f_3(19)} \equiv 19^{f_3(19) \pmod{\phi(25)}} \equiv 19^{-1} \equiv 4 \pmod{25}$, pues $19 \cdot 4 = 76 = 3 \cdot 25 + 1$

Resolvemos el sistema $\left.\begin{array}{l} f(19) = -1 \pmod 4 \\ f(19) = 4 \pmod{25} \end{array}\right\}$ mediante el Teorema Chino del Residuo:

$$\left.\begin{array}{l} N = 4 \cdot 25 = 100 \\ N_1 = 25 \rightarrow 25\, y_1 \equiv 1 \pmod 4 \Rightarrow y_1 = 1 \\ N_2 = 4 \rightarrow 4 y_2 \equiv 1 \pmod{25} \Rightarrow y_2 = 19 \end{array}\right\} \Rightarrow f(19) = 25 \cdot 1 \cdot (-1) + 4 \cdot 19 \cdot 4 = 279 \equiv 79 \pmod{100}$$

Tercera parte: $f(18) \pmod{100}$

$f_3(18) = 18^{f_2(19)} = (2\cdot 9)^{f_2(19)} = 2^{f_2(19)}\cdot 9^{f_2(19)} = 2k$

Y por tanto $f(18) = 18^{f_3(19)} = 2^{f_3(18)} = 2^{2k} = 4^k \equiv 0 \pmod 4$

$18^4 \equiv 1 \pmod{25}$ (!!!!)

$f_3(18) = 18^{f_2(18)} = (2\cdot 9)^{f_2(18)} = 2^{f_2(18)}\cdot 9^{f_2(18)}$ es múltiplo de 4

$f_4(18) = 18^{f_3(18)} \equiv 1^{f_3(18)} = 1 \pmod{25}$

Resolvemos el sistema

$$\left.\begin{array}{l} f(18) \equiv 0 \pmod 4 \\ f(18) \equiv 1 \pmod{25} \end{array}\right\}$$

mediante el Teorema Chino del Residuo:

$$\left.\begin{array}{l} N = 4\cdot 25 = 100 \\ N_1 = 25 \to 25y_1 \equiv 1 \pmod 4 \Rightarrow y_1 = 1 \\ N_2 = 4 \to 4y_2 \equiv 1 \pmod{25} \Rightarrow y_2 = 19 \end{array}\right\} \Rightarrow f(18) = 25\cdot 1\cdot 0 + 4\cdot 19\cdot 1 = 279 \equiv 76 \pmod{100}$$

Cuarta parte: $f(17) \pmod{100}$

$17 \equiv 1 \pmod 4 \Rightarrow f(17) = 17^{f_3(17)} \equiv 1 \pmod 4$

$f(17) = 17^{f_3(17)} \equiv 17^{f_3(17) \bmod \phi(25)} \pmod{25} = (**)$

$f_3(17) \pmod{\phi(25)} = f_3(17) \pmod{20} = 17^{f_2(17)} \pmod{20} \equiv 17^{f_2(17) \bmod \phi(20)} \pmod{20} = (*)$

$\phi(20) = 8$, luego: $f_2(17) \pmod{\phi(20)} = f_2(17) = 17^{17} \equiv 1^{17} = 1 \pmod 8$

$(*) = 17^1 = 17 \pmod{20}$

$(**) = 17^{17} \pmod{25}$

Vamos a calcular esta última potencia por el "método de las potencias de dos":

$17^2 = 289 \equiv 14 \pmod{25}$

$17^4 \equiv 14\cdot 14 = 196 \equiv -4 \pmod{25}$

$17^8 \equiv (-4)\cdot(-4) = 16 \pmod{25}$

$17^{17} \equiv 17^{2\cdot 8+1} = (17^8)^2 \cdot 17 \equiv 16^2 \cdot 17 = 256\cdot 17 \equiv 6\cdot 17 = 102 \equiv 2 \pmod{25}$

Así pues, $f(17) = 2 \pmod{25}$.

Como antes, aplicamos el Teorema Chino del Residuo para determinar $f(17) \pmod{100}$

$$\left.\begin{array}{l} f(17) \equiv 1 \pmod 4 \\ f(17) \equiv 2 \pmod{25} \end{array}\right\}$$

$$\left.\begin{array}{l} N = 4\cdot 25 = 100 \\ N_1 = 25 \to 25y_1 \equiv 1 \pmod 4 \Rightarrow y_1 = 1 \\ N_2 = 4 \to 4y_2 \equiv 1 \pmod{25} \Rightarrow y_2 = 19 \end{array}\right\} \Rightarrow f(17) = 25\cdot 1\cdot 1 + 4\cdot 19\cdot 2 = 177 \equiv 77 \pmod{100}$$

Y finalmente,

$f(17) + f(18) + f(19) + f(20) \pmod{100} \equiv 77 + 76 + 79 + 0 = 232 \pmod{100} \equiv 32 \pmod{100}$

Fuente de la solución: Olympiad Number Theory Through Challenging Problems (Justin Stevens, 3E) pág.50

9.2.5

Queremos determinar $7^{2014} \pmod{1000}$.

Primera versión.
Aplicamos el Teorema de Euler:
$\phi(1000)=400$, y puesto que $(7,1000)=1$, aplicando el Teorema de Euler:

$$1\equiv 7^{\phi(1000)}=7^{400} \bmod (1000)$$

Luego $7^{2014}=7^{400\cdot 5+14}=7^{400\cdot 5}\cdot 7^{14}=\left(7^{400}\right)^5\cdot 7^{14}\equiv 1\cdot 7^{14}=7^{14} \bmod (1000)$

$7^2=49\rightarrow 7^3=343\rightarrow 7^4=2401\equiv 401\rightarrow 7^5\equiv 2807\equiv 807\rightarrow$
$\rightarrow 7^6\equiv 5649\equiv 649\rightarrow 7^7\equiv 4543\equiv 543$

$7^{14}=\left(7^7\right)^2\equiv 543^2=***849$ (no hace falta hacer toda la multiplicación)
$7^{2014}\equiv 7^{14} \bmod (1000)\equiv 849 \bmod (1000)$

Fuente de esta versión: Solución oficial (Ver SE, página 333)

Nota: En la Solución oficial (SE, página 333) se presenta otra solución alternativa.

Segunda versión.
Como es habitual en este tipo de problemas (ver Problemas #11.5 y #9.3), calcularemos por separado $7^{2014} \pmod 8$ y $7^{2014} \pmod{125}$ para después determinar $7^{2014} \pmod{1000}$ mediante el Teorema Chino del Residuo.

a) $7^{2014} \pmod 8$
$7^2=49\equiv 1 \pmod 8\Rightarrow 7^{2014}=\left(7^2\right)^{1007}\equiv 1^{1007}=1 \pmod 8$

b) $7^{2014} \pmod{125}$
$\phi(125)=\phi(5^3)=5^3\left(1-\frac{1}{5}\right)=5^3\frac{4}{5}=100$, luego, aplicando el Teorema de Euler, para cualquier número a, con $(a,125)=1$, se cumple $a^{100}\equiv 1 \pmod{125}$.

En nuestro caso se cumple $(2014,125)=1$, luego $7^{100}\equiv 1 \pmod{125}$
Y por tanto $7^{1000}=\left(7^{100}\right)^{10}\equiv 1^{10}=1 \pmod{125}$
$7^{2000}=\left(7^{1000}\right)^2\equiv 1^2=1 \pmod{125}$
$7^2=49 \pmod{125}$
$7^3=343=93 \pmod{125}$
$7^4=651=151=26 \pmod{125}$
$7^5=182=57 \pmod{125}$
$7^6=219=24 \pmod{125}$
$7^7=168=43 \pmod{125}$

Y por tanto $7^{14}=\left(7^7\right)^2\equiv 43^2=1849\equiv 99 \pmod{125}$

Y por último: $7^{2014} = 7^{2000} \cdot 7^{14} \equiv 1 \cdot 99 = 99 \pmod{125}$

Finalmente, aplicamos el Teorema chino del Residuo:

c)

$7^{2014} \equiv 1 \pmod 8$

$7^{2014} \equiv 99 \pmod{125}$

$N = 8 \cdot 125 = 1000$

$N_1 = 125 \to 125 y_1 \equiv 1 (\mathrm{mod}\, 8) \Rightarrow y_1 = 5$

$N_2 = 8 \to 8 y_2 \equiv 1 (\mathrm{mod}\, 125) \Rightarrow y_2 = 47 \quad (*)$

$x = 125 \cdot 5 \cdot 1 + 8 \cdot 47 \cdot 99 = 37849 \equiv 849 \pmod{1000}$

Nota: Esta segunda versión no es operativa en un contexto de una competición en la que no se pueden usar calculadoras, pues, por ejemplo, el paso (*) anterior exige demasiado cálculo.

9.2.6

Está claro que $2^j - 1$ es siempre impar, luego i no puede ser par.

Si i es impar, tenemos que, aplicando el Teorema de Euler,

$2^{\phi(i)} \equiv 1 \pmod i \Leftrightarrow 2^{\phi(i)} - 1 \equiv 0 \pmod i \Leftrightarrow i \mid 2^{\phi(i)} - 1$

Puesto que, por definición, $\phi(i) \le i \le 1000$, las condiciones del problema se cumplen para todo i impar, y la solución es 500.

9.2.7

$240 = 2^4 \cdot 3 \cdot 5.$

Aplicando el PTF:

$$p > 5 \Rightarrow p \nmid 5 \Rightarrow p^8 = \left(p^4\right)^2 \equiv 1^2 = 1 \pmod 5$$
$$p > 5 \Rightarrow p \nmid 3 \Rightarrow p^8 = \left(p^2\right)^4 \equiv 1^4 = 1 \pmod 3$$

Por otro lado, aplicando el Teorema de Euler:

$$\left.\begin{array}{l} \phi\left(2^4\right) = 8 \\ \left(2^4, p\right) = 1 \end{array}\right\} \Rightarrow p^8 \equiv 1 \pmod{2^4}$$

Finalmente, puesto que $(8, 5, 3) = 1$,

$$\left.\begin{array}{l} p^8 \equiv 1 \pmod 5 \\ p^8 \equiv 1 \pmod 3 \\ p^8 \equiv 1 \pmod{2^4} \end{array}\right\} \Rightarrow p^8 \equiv 1 \pmod{2^4 \cdot 3 \cdot 5}$$, tal y como queríamos ver.

9.2.8

Primera parte.

Dados dos enteros positivos a, b, sea $q = ab + 1$.

Está claro que (aplicando ADE) $(a, ab+1) = 1$, luego podemos aplicar el Teorema de Euler:

$$a^{\phi(q)} \equiv 1 \pmod q$$

Luego

$$1 \equiv a^{\phi(q)-1} = a \cdot a^{\phi(q)-1} \pmod{q} \Rightarrow a^{\phi(q)-1} = a^{-1} \pmod{q}$$

Pero entonces

$$a^{\phi(q)-1} + b \equiv a^{-1} + b = a^{-1}(1+ab) \equiv 0 \pmod{q}$$

Pero todo esto lo podemos hacer también con b, luego

$$b^{\phi(q)-1} + a \equiv 0 \pmod{q}$$

Así pues, dados dos enteros positivos a, b, hemos encontrado un $n_0 = \phi(ab+1) - 1$ tal que

$$\begin{cases} ab+1 \mid a^{n_0} + b \\ ab+1 \mid \mathrm{b}^{n_0} + a \end{cases} \Rightarrow ab+1 \mid \left(a^{n_0} + b \, , b^{n_0} + a \right)$$

Segunda parte.

Esto mismo sucede para todo n de la forma $n = n_0 + k\,\phi(q)$. En efecto,

$$a^{n_0+k\phi(q)} + b = a^{n_0} \cdot \left(a^{\phi(q)}\right)^k + b \equiv a^{n_0} \cdot 1^k + b \equiv a^{n_0} + b \equiv 0 \pmod{q}$$

y de la misma forma se demuestra que $b^{n_0+k\phi(q)} + a \equiv 0 \pmod{q}$.

Tercera parte.

Supongamos que se cumplen las condiciones del enunciado. Es decir, dados dos enteros positivos a y b, $x_n = \left(a^{n_0} + b \, , b^{n_0} + a \right)$ es constante para todo $\mathrm{n} \geq \mathrm{N}$.

Aprovechando el resultado de la segunda parte, tomando un k suficientemente grande sabemos que

$$ab+1 \mid x_n \text{ y } x_n = x_{n+1} = x_{n+2}.$$

Veamos qué pasa con x_{n+1}:

$$\left.\begin{array}{l} ab+1 \mid x_n \\ x_n = x_{n+1} \end{array}\right\} \Rightarrow ab+1 \mid x_{n+1} \Rightarrow \left.\begin{array}{l} ab+1 \mid a^{n+1} + b \Rightarrow 1 + b \equiv 0 \pmod{q} \Rightarrow b \equiv -1 \pmod{q} \\ ab+1 \mid b^{n+1} + a \Rightarrow 1 + a \equiv 0 \pmod{q} \Rightarrow a \equiv -1 \pmod{q} \end{array}\right\}$$

En donde hemos utilizado que

$$a^{n+1} + b = a^{\phi(p)-1+1} + b = a^{\phi(p)} + b \equiv 1 + b \pmod{q}$$

Y de la misma manera $b^{n+1} + a = b^{\phi(p)-1+1} + a = b^{\phi(p)} + a \equiv 1 + a \pmod{q}$

Veamos, finalmente, qué pasa con x_{n+2}:

$$\left.\begin{array}{l} ab+1 \mid x_n \\ x_n = x_{n+1} = x_{n+2} \end{array}\right\} \Rightarrow ab+1 \mid x_{n+2} \Rightarrow \left.\begin{array}{l} ab+1 \mid a^{n+2} + b \Rightarrow a + b \equiv 0 \pmod{q} \\ ab+1 \mid b^{n+2} + a \Rightarrow b + a \equiv 0 \pmod{q} \end{array}\right\}$$

En donde hemos utilizado que

$$a^{n+2} + b = a^{\phi(p)-1+2} + b = a^{\phi(p)+1} + b = a \cdot a^{\phi(p)} + b \equiv a + b \pmod{q}$$

Y de la misma manera $b^{n+2} + a \equiv b + a \pmod{q}$

Luego

$$0 \equiv a + b \equiv -1 + -1 \equiv -2 \pmod{q} \Rightarrow 0 \equiv -2 \pmod{q} \Rightarrow$$

$$0 \equiv 2 \pmod{q} \Rightarrow 2 = q = ab+1 \Rightarrow a = b = 1$$

La única solución posible es $a = b = 1$, y en efecto para este caso se cumplen las condiciones del enunciado: $x_n = (1^n + 1, 1^n + 1) = (2, 2) = 2$ constante.

Fuente: Soluciones oficiales y "IMO 2024 Solution Notes" de Evan Chen.

9.3.1

$$\left.\begin{array}{l} 1001 \mid 10^j - 10^i = 10^j\left(10^{j-i}-1\right) \\ (1001\,,10^j) = 1 \end{array}\right\} \Rightarrow 1001 \mid 10^{j-i}-1 \Leftrightarrow 10^{j-i} \equiv 1 \pmod{1001}$$

Observamos que $ord_{1001}(10) = 6$, pues

$10^3 = 1000 \equiv -1 \pmod{1001} \Rightarrow 10^6 \equiv (-1)^2 = 1 \pmod{1001}$

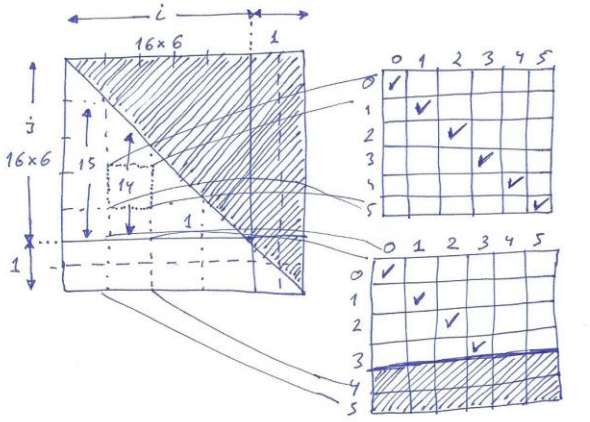
y $10^1, 10^2, 10^4, 10^5 \not\equiv 1 \pmod{1001}$.

Con lo que llegamos a $6 \mid j-i$.

Con lo anterior, hemos reducido nuestro problema a contar todas las parejas $0 \le i < j \le 99$ cumpliendo $j \equiv i \pmod 6$.

Vemos que $99 = 16 \cdot 6 + 3$

Dibujamos un esquema de 99 filas (valores de j) por 99 columnas (valores de i), podemos eliminar todos los pares de la diagonal hacia arriba porque $i < j$, vemos que quedarán completos $15+14+13+...+2+1 = 15 \cdot 16/2 = 120$ bloques, y en cada uno hay 6 pares aceptables, y en la parte inferior quedarán 16 medios bloques, con 4 pares aceptables en cada uno. Luego hay un total de $6 \cdot 120 + 4 \cdot 16 = 784$ pares (i, j) aceptables.



Fuente: Olympiad Number Theory Through Challenging Problems (Justin Stevens, pág. 62)

9.3.2

Sean p, q primos.

$$q \mid 2^p - 1 \Leftrightarrow 2^p - 1 \equiv 0 \pmod q \Rightarrow ord(2,q) \mid p \Rightarrow ord(2,q) = \begin{cases} 1 \\ p \end{cases}$$

$ord(2,q) = 1 \Rightarrow 2 = 1 \pmod q$, lo cual es absurdo, luego solo puede ser $ord(2,q) = p$.

Pero, por otro lado, por el PTF, y puesto que $q \nmid 2$, tenemos que

$2^{q-1} \equiv 1 \pmod q$, y por tanto $p = ord(2,q) \mid q-1 \Rightarrow p \le q-1 \Rightarrow p < q$

También se puede aplicar el Teorema de Euler:

$p = ord(2,q) \mid \phi(q) = q-1 \Rightarrow p \le q-1 \Rightarrow p < q$

9.4.1

Primera versión.

Sea $n = a + b$.

$a + b \mid a^b + b^a \Leftrightarrow a^b + b^a \equiv 0 \pmod{n} \Leftrightarrow a^{n-a} + (n-a)^a \equiv 0 \pmod{n} \Leftrightarrow$

$a^{n-a} \equiv -(-a)^a \pmod{n}$

Supongamos que a es impar. Entonces la condición anterior es equivalente a:

$$a^{n.-a} \equiv a^a \pmod{n} \Leftrightarrow 1 \equiv \frac{a^a}{a^{n-a}} \pmod{n} \Leftrightarrow 1 \equiv a^{2a-n} \pmod{n}$$

Aplicando el Teorema de Euler, puesto que $(a,b) = 1 \Rightarrow (a,n) = 1$, sabemos que

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Luego basta con resolver $\varphi(n) = 2a - n \Leftrightarrow a = \frac{\varphi(n) + n}{2}$.

Veamos que para $n = 2p$ con p primo y $p \equiv 1 \pmod{4}$ se cumple esta condición.

$$n = 2p \Rightarrow \varphi(n) = 2p\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{p}\right) = p - 1$$

Luego:

$$a = \frac{\varphi(n) + n}{2} = \frac{p - 1 + 2p}{2} = \frac{3p - 1}{2}$$

Observamos que la condición $p \equiv 1 \pmod{4}$ garantiza que a es par, puesto que

$p \equiv 1 \pmod{4} \Rightarrow 3p - 1 \equiv 2 \pmod{4}$

Y por tanto, deducimos que $a + b = n = 2p \Rightarrow b = 2p - \frac{3p-1}{2} = \frac{4p - 3p + 1}{2} = \frac{p+1}{2}$

Queda solamente garantizar que a y b así definidos son coprimos. En efecto:

$$\left(\frac{3p-1}{2}, \frac{p+1}{2}\right) = \frac{(3p-1, p+1)}{2} = \frac{(p-3, 4)}{2} = \frac{2}{2} = 1$$

tal y como queríamos ver.

Segunda versión.

Veamos que todo par de la forma $a = 2n - 1$, $b = 2n + 1$, con $n \geq 2$ satisface la condición del enunciado.

En primer lugar vemos que $(a,b) = 1$ aplicando el Algoritmo de Euclides:

$$(a,b) = (2n+1, 2n-1) = (2n-1, 2n-1+2) = (2n+1, 2) = 1$$

Observamos que

$a^2 = (2n-1)^2 = 4n^2 - 4n + 1 \equiv 1 \pmod{4n}$

$b^2 = (2n+1)^2 = 4n^2 + 4n + 1 \equiv 1 \pmod{4n}$

$a^b + b^a = a^{2n+1} + b^{2n-1} = a \cdot a^{2n} + b^{2n-2+1} = a \cdot a^{2n} + b \cdot b^{2(n-1)} =$

$= a \cdot (a^2)^n + b \cdot (b^2)^{n-1} \equiv a \cdot 1^n + b \cdot 1^{n-1} \equiv a + b \equiv 4n \equiv 0 \pmod{4n} \equiv 0 \pmod{a+b}$

tal y como queríamos ver.

Fuente de estas soluciones: www.artofproblemsolving.com

9.4.2

Sabemos por aritmética básica que $0.\overline{abcd} = \dfrac{abcd}{9999}$, luego este problema nos pide encontrar todos los denominadores distintos posibles para todas las fracciones simplificadas equivalentes a las fracciones de la forma $\dfrac{n}{9999}$, con $1 \le n \le 9999$.

Caso 1.
El bloque principal de numeradores consta de todos los números $1 \le n \le 9999$ coprimos con 9999, es decir, $(n, 9999) = 1$.

Esta cantidad la podemos calcular fácilmente como aplicación directa de la función Phi de Euler:

$$9999 = 3^2 \cdot 11 \cdot 101 \Rightarrow \varphi(9999) = 9999\left(1-\frac{1}{3}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{101}\right) = 6000$$

Pero vemos que también pueden aparecer numeradores n con $(n, 9999) > 1$. Por ejemplo:

$$\frac{605}{9999} = \frac{11^2 \cdot 5}{3^2 \cdot 11 \cdot 101} = \frac{11 \cdot 5}{3^2 \cdot 101} = \frac{55}{909}$$

Tenemos una fracción simplificada cuyo numerador es múltiplo de 11.

Caso 2: Numeradores n múltiplos de 3 pero no de 11 ni de 101.
Si en el numerador queda un múltiplo de 3 es que proviene de haber simplificado un múltiplo de 9, y por tanto el numerador original $1 \le abcd \le 9999$ era múltiple de 9. Así pues, podemos asegurar que $n \le 1111$.

Entre 1 y 1111 hay 370 múltiplos de 3:
de $3 \cdot 1 = 3$ a $3 \cdot 370 = 1110 \rightarrow 370$ números
a los que debemos quitar los múltiplos de 3 y 11, es decir, los múltiplos de 33:
de $33 \cdot 1 = 33$ a $33 \cdot 33 = 1089 \rightarrow 33$ números
y debemos quitar los múltiplos de 3 y 101, es decir, los múltiplos de 303:
de $303 \cdot 1 = 303$ a $303 \cdot 3 = 909 \rightarrow 3$ números

Puesto que $11 \cdot 101 = 1111$, y este número no aparece, no hay casos superpuestos.

Así pues, tenemos $370 - 33 - 3 = 334$ casos.

Caso 3: Numeradores múltiplos de 11, pero no de 3 ni de 101.

Si una fracción simplificada tiene numerador múltiplo de 11 es que proviene de una fracción sin simplificar $\frac{abcd}{9999}$, con $1 \le abcd \le 9999$, y $abcd$ múltiplo de $11^2 = 121$. Luego podemos garantizar que $n \le 909$.

Los múltiplos de 11:

de $11 \cdot 1 = 11$ a $11 \cdot 82 = 902 \rightarrow 82$ números.

A los que debemos quitar los múltiples de 11 y 3, es decir, múltiples de 33:

de $33 \cdot 1 = 33$ a $33 \cdot 27 = 891 \rightarrow 27$ números.

y debemos quitar también los múltiples de 11 y 101, que está claro que no existen.

Asi pues, tenemos $82 - 27 = 55$ casos.

Caso 4: Numeradores múltiplos de 101, pero no de 3 ni de 11.

Seguimos con el mismo razonamiento: Si una fracción simplificada tiene numerador múltiplo de 101 es que proviene de una fracción sin simplificar $\frac{abcd}{9999}$, con $1 \le abcd \le 9999$, y $abcd$ múltiplo de $101^2 = 10201$, lo cual es imposible.

Caso 5: Numeradores múltiplos de 3 y de 11, pero no de 101.

Son fracciones de la forma $\frac{n}{101}$. Son tres casos: $\frac{33}{101}, \frac{66}{101}, \frac{99}{101}$.

Así pues, N consta de $6000 + 334 + 55 + 3 = 6392$ números diferentes, y la respuesta correcta al problema es 392.

Fuente de esta solución: https://artofproblemsolving.com/wiki/index.php/2022_AIME_I_Problems/Problem_13

9.4.3

Sea p un divisor primo de $20^{22} + 1$, luego:

$$20^{22} + 1 \equiv 0 \pmod{p} \Leftrightarrow 20^{22} \equiv -1 \pmod{p} \Rightarrow 20^{44} \equiv 1 \pmod{p}$$

Sea $d = ord_p(20)$.

Está claro que $(20, p) = 1$, puesto que en caso contrario

$$p \mid 20 \Rightarrow 20 \equiv 0 \pmod{p} \Rightarrow 20^{22} \equiv 0 \pmod{p} \Rightarrow 20^{22} + 1 \equiv 1 \not\equiv -1 \pmod{p}$$

Luego,/ por el Teorema Fundamental del Orden (ver 13.3)

$d \mid 44$ y $d \nmid 22$ puesto que $20^{22} \equiv -1 \not\equiv 1 \pmod{p}$.

Los dos únicos candidatos posibles son $d = 4$ o $d = 11$. Estudiemos estos dos casos por separado:

Primer caso: $d = 4$.

$$20^4 \equiv 1 \pmod{p} \Rightarrow 0 \equiv 20^4 - 1 = (20^2 - 1)(20^2 + 1) = (20 - 1)(20 + 1)(20^2 + 1) =$$
$$= 19 \cdot 3 \cdot 7 \cdot 401 \pmod{p}$$

$$\left.\begin{array}{l} 20 \equiv -1 \pmod{3,7,19} \Rightarrow 20^2 \equiv 1 \pmod{3,7,19} \Rightarrow 20^{22} = (20^2)^{11} \equiv 1 \pmod{3,7,19} \\ 20^{22} \equiv -1 \pmod{p} \end{array}\right\} \Rightarrow p \neq 3,7,19$$

El único candidato que queda es $p=401$. Veamos que, en efecto, $20^{22}\equiv -1\pmod{401}$:

$$20^{22}=\left(20^2\right)^{11}=400^{11}\equiv(-1)^{11}\equiv -1\pmod{401}$$

Segundo caso: $d=44$.

Aplicando el Pequeño Teorema de Fermat, y puesto que hemos visto que $(20,p)=1$, se cumple

$$20^{p-1}\equiv 1\pmod{p}$$

Luego $44\mid p-1$, es decir: $p=45,89,133,177,221,265,309,353,397...$ y entre ellos los primos son:

$$p=89,353,397...$$

Tomemos como candidato $p-1=88\Rightarrow p=89$.

$2^6\equiv 64\equiv -25\pmod{89}\Rightarrow 20^{22}\equiv(2^2\cdot 5)^{22}=2^4\cdot 5^{22}\equiv\left(2^6\right)^7\cdot 2^2\cdot 5^{22}\equiv(-25)^7\cdot 2^2\cdot 5^{22}\equiv -5^{14}\cdot 2^2\cdot 5^{22}\equiv$

$\equiv -5^{36}\cdot 2^2\equiv(*)$

Por otro lado, $5^4=625\equiv 7\cdot 89+2$, luego:

$$(*)\equiv -\left(5^4\right)^9\cdot 2^2\equiv -(2)^9\cdot 2^2\equiv -2^{11}=-2048=-23\cdot 89-1\equiv -1\pmod{89}$$

Así pues, ya tenemos dos primos $89<401$ aceptables para las condiciones del enunciado.

Ahora ya solo nos queda comprobar que $p=353$ y $p=397$ no son aceptables. En efecto:

Supongamos que $p=397$:

$$20^{22}=\left(20^2\right)^{11}=400^{11}\equiv 3^{11}=3^6\cdot 3^5=729\cdot 243\equiv(-65)\cdot 243=-13\cdot 5\cdot 243\equiv -13\cdot 1215\equiv$$
$$\equiv -13\cdot 24\equiv -312\equiv 85\not\equiv -1\pmod{397}$$

Supongamos que $p=353$:

$$20^{22}=\left(2^2\cdot 5\right)^{22}=2^{44}\cdot 5^{22}$$
$$2^{44}=\left(2^{10}\right)^4\cdot 2^4=1024^4\cdot 2^4\equiv 70^4\cdot 2^4=\left(70^2\right)^2=4900^2\equiv(-42)^2=42^2=1764\equiv -1\,(\text{mod }353)$$

Por lo tanto,

$$20^{22}\equiv -1\pmod{353}\Leftrightarrow 5^{22}\equiv 1\pmod{353}\Leftrightarrow 0\equiv 5^{22}-1=\left(5^{11}-1\right)\left(5^{11}+1\right)\pmod{353}$$

Pero

$$5^{11}=5^4\cdot 5^4\cdot 5^3=625^2\cdot 125=(-81)^2\cdot 125=3^8\cdot 125=3^7\cdot 375\equiv 3\cdot 729\cdot 22=66\cdot 729=$$
$$\equiv 66\cdot 23=1518\equiv 106\not\equiv 1,-1$$

Finalmente, la solución del problema es $89+401=490$.

Fuente de esta solución: "Math Gold Medalist" en Youtube: https://youtu.be/gMrpXTtr86s

9.4.4

Primera versión.

Sea $N = 5a + b$, para ciertos enteros $a \geq 0$ y $0 \leq b < 5$.
Luego, aplicando el Binomio de Newton,

$$N^{16} = (5a + b)^{16} = \sum_{k=0}^{16} (5a)^{16-k} b^k$$

Todos los elementos de este sumatorio serán múltiples de 5 excepto el último, por tanto:

$$N^{16} \equiv b^{16} \pmod 5$$

Veamos caso por caso:

$$b = 0 \Rightarrow N^{16} \equiv 0^{16} \equiv 0 \pmod 5$$
$$b = 1 \Rightarrow N^{16} \equiv 1^{16} \equiv 1 \pmod 5$$
$$b = 2 \Rightarrow N^{16} \equiv 2^{16} = \left(2^2\right)^8 = 4^8 \equiv (-1)^8 = 1 \pmod 5$$
$$b = 3 \Rightarrow N^{16} \equiv 3^{16} = \left(3^2\right)^8 = 9^8 \equiv (-1)^8 = 1 \pmod 5$$
$$b = 4 \Rightarrow N^{16} \equiv 4^{16} \equiv (-1)^{16} = 1 \pmod 5$$

Todo esto se puede razonar directamente en el contexto de la aritmética modular, sin necesidad de utilizar el Binomio de Newton:

$$N \equiv 0 \pmod 5 \Rightarrow N^{16} \equiv 0^{16} \equiv 0 \pmod 5$$
$$N \equiv 1 \pmod 5 \Rightarrow N^{16} \equiv 1^{16} \equiv 1 \pmod 5$$
$$N \equiv 2 \pmod 5 \Rightarrow N^{16} \equiv 2^{16} = \left(2^2\right)^8 = 4^8 \equiv (-1)^8 = 1 \pmod 5$$
$$N \equiv 3 \pmod 5 \Rightarrow N^{16} \equiv 3^{16} = \left(3^2\right)^8 = 9^8 \equiv (-1)^8 = 1 \pmod 5$$
$$N \equiv 4 \pmod 5 \Rightarrow N^{16} \equiv 4^{16} = (-1)^{16} = 1 \pmod 5$$

Así pues, aplicando la fórmula de LaPlace habitual,

$$P = \frac{\text{Casos favorables}}{\text{Casos posibles}} = \frac{4}{5}$$

En donde hemos tenido en cuenta que $2020 = 5 \cdot 404$, es decir, los cinco casos son equiprobables.

Segunda versión.

Aplicando el Pequeño Teorema de Fermat, sabemos que para todo $N \not\equiv 0 \pmod 5$ se cumplirá $N^4 \equiv 1 \pmod 5$, luego:

$N \not\equiv 0 \pmod 5 \Rightarrow N^{16} = \left(N^4\right)^4 \equiv 1^4 = 1 \pmod 5$.

Por otro lado, está claro que $N \equiv 0 \pmod 5 \Rightarrow N^{16} \equiv 0^{16} = 0 \pmod 5$, y llegamos al mismo resultado:

$$P = \frac{\text{Casos favorables}}{\text{Casos posibles}} = \frac{4}{5}$$

9.4.5

Utilizaremos la igualdad

$$p^6 - 1 = (p-1)(p+1)\left(p^2 - p + 1\right)\left(p^2 + p + 1\right)$$

En particular, para

$$p=11\Rightarrow p^6-1=10\cdot 12\cdot(121-11+1)(121+11+1)=10\cdot 12\cdot 111\cdot 133=$$

$$=2^3\cdot 3^2\cdot 5\cdot 7\cdot 19\cdot 37$$

$$p=13\Rightarrow p^6-1=2^3\cdot 3^2\cdot 7\cdot 61\cdot 157$$

Vemos que $n=2^3\cdot 3^2\cdot 7$ es el mayor divisor común de estos números, y podemos especular que sea el mayor divisor de todos. Para ello lo vamos a ver por separado $2^3\mid p^6-1$, $3^2\mid p^6-1$, $7\mid p^6-1$, y puesto que $(2^3,3^2,7)=1$, se deduce que $504=2^3\cdot 3^2\cdot 7\mid p^6-1$.

Para $n=7$ basta aplicar el PTF.

Para $n=8$, si p es primo es impar, y por tanto

$$p=2k+1\Rightarrow p^2-1=(2k+1)^2-1=4k^2+4k+1-1=4k(k+1).$$

Aquí vemos que k o $k+1$ es par, por lo que $4k(k+1)$ siempre es múltiplo de 8, es decir,

$$8\mid p^2-1$$

Sabemos que

$$2\mid 6\Rightarrow p^2-1\mid p^6-1$$

Luego

$$8\mid p^2-1\mid p^6-1\Rightarrow 8\mid p^6-1$$

Para $n=9$, podemos aplicar el Teorema de Euler: $\phi(9)=6$, luego

$$(k,9)=1\Rightarrow k^6\equiv 1 \pmod 9$$

En particular, se cumple para todo $k=p>7$ primo.

Una manera alternativa de demostrarlo es tener en cuenta la factorización

$$p^6-1=(p-1)(p+1)(p^2-p+1)(p^2+p+1)$$

Y que todo número primo $p>3$ se puede escribir como $p=3k\pm 1$.

Si $p=3k+1$

$p-1$ es múltiplo de 3

$p^2+p+1=(3k+1)^2+3k+1+1=9k^2+6k+1+3k+1+1=9k^2+9k+3$ es múltiplo de 3

Luego $9\mid(p-1)(p^2+p+1)$

Si $p=3k-1$

$p+1$ es múltiplo de 3

$p^2-p+1=(3k-1)^2-3k+1+1=9k^2-6k+1-3k+1+1=9k^2-9k+3$ es múltiplo de 3

Luego $9\mid(p+1)(p^2-p+1)$.

Fuente de esta solución: Soluciones oficiales.

10.1.1

Sabemos que existirá solución pues $(7,9)=1$.

$7x-9y=3\Rightarrow 7x=3+9y=3(1+3y)\Rightarrow 3\mid x\Rightarrow x=3k\Rightarrow$

$7\cdot 3k-9y=3\Rightarrow 7k-3y=1\Rightarrow 7k=1+3y$

Claramente una solución de esta última ecuación es $y=2,k=1$, luego $y=2,x=3,k=3$ será una solución particular de la ecuación del enunciado.

En general, las soluciones serán de la forma $y = 2 + 9k, x = 3 + 7k$, con $k \in Z$

10.1.2

Sean N_a y N_b la cantidad de manzanas y naranjas compradas, respectivamente.

Sean P_a y P_b el precio de cada manzana y de cada naranja, respectivamente, en céntimos.

Tenemos las siguientes condiciones:

$$\begin{cases} N_a + N_b = 12 \\ P_a = P_b + 3 \\ N_a > N_b \\ P_a N_a + P_b N_b = 132 \end{cases}$$

Luego

$(P_b + 3)N_a + P_b(12 - N_a) = 132 \Leftrightarrow P_b N_a + 3N_a + 12P_b - P_b N_a = 132 \Leftrightarrow$

$3N_a + 12P_b = 132 \Leftrightarrow N_a + 4P_b = 44$

Esta última ecuación diofántica tiene solución pues $d = mcd(1,4) = 1$, y $1 | 44$.

Una solución particular de esta ecuación es $N_a = 4, P_b = 10$, pero no satisface la condición $N_a > N_b$. El resto de soluciones son de la forma

$N_a = 4 + \frac{4}{1}k, P_b = 10 - k$

$k = 0 \rightarrow N_a = 4, P_b = 10 \rightarrow N_b = 8$

$k = 1 \rightarrow N_a = 8, P_b = 9 \rightarrow N_b = 4, P_a = 12$

$k = 2 \rightarrow N_a = 12, P_b = 8 \rightarrow N_b = 0, P_a = 11$

Las soluciones posibles son 4 naranjas a 9 céntimos, (con 8 manzanas a 12 céntimos) o 12 manzanas a 11 céntimos (y sin ninguna naranja)

10.1.3

Aplicamos el algoritmo de Euclides:

$$\left.\begin{array}{l} 858 = 3 \cdot 253 + 99 \\ 253 = 2 \cdot 99 + 55 \\ 99 = 1 \cdot 55 + 44 \\ 55 = 1 \cdot 44 + 11 \\ 44 = 4 \cdot 11 \end{array}\right\} \Rightarrow (858,253) = 11, \text{ y } 11 | 33, \text{ luego la ecuación tiene solución.}$$

Deshacemos los pasos del algoritmo de Euclides:

$$\left.\begin{array}{l} 11 = 55 - 44 \\ 44 = 99 - 55 \\ 55 = 253 - 2 \cdot 99 \\ 99 = 858 - 3 \cdot 253 \end{array}\right\} \Rightarrow 11 = 55 - 44 = 253 - 2 \cdot 99 - (99 - 55) = 253 - 2 \cdot 99 - 99 + 55 =$$

$$= 253 - 3 \cdot 99 + 253 - 2 \cdot 99 = 2 \cdot 253 - 5 \cdot 99 = 2 \cdot 253 - 5(858 - 3 \cdot 253) =$$

$$= 2 \cdot 253 - 5 \cdot 858 + 15 \cdot 253 = -5 \cdot 858 + 17 \cdot 253$$

Y multiplicando ambos lados por 3 obtenemos la solución deseada:

$$11 = -5 \cdot 858 + 17 \cdot 253 \Rightarrow 33 = -15 \cdot 858 + 51 \cdot 253 \Rightarrow x = -15, y = 51$$

El conjunto general de soluciones serán todas las parejas de la forma:

$$x = -15 + \frac{253}{11}k = -15 + 23k = 8 + 23k,\ y = 51 - \frac{858}{11}k = 51 - 78k$$

10.1.4

Calculamos el (858,253) mediante el algoritmo de Euclides:

$$\left.\begin{array}{l} 258 = 147 + 111 \\ 147 = 111 + 36 \\ 111 = 36 \cdot 3 + 3 \\ 36 = 3 \cdot 12 \end{array}\right\} \Rightarrow (858,253) = 3, \text{ y } 3 \mid 369, \text{ luego la ecuación tiene solución.}$$

Deshaciendo los pasos del algoritmo de Euclides:

$$\left.\begin{array}{l} 3 = 111 - 3 \cdot 36 \\ 36 = 147 - 111 \\ 111 = 258 - 147 \end{array}\right\} \Rightarrow 3 = 111 - 3 \cdot 36 = 258 - 147 - 3(147 - 111) = 258 - 147 - 3 \cdot 147 + 3 \cdot 111 =$$

$$= 258 - 4 \cdot 147 + 3 \cdot 111 = 258 - 4 \cdot 147 + 3(258 - 147) = 258 - 4 \cdot 147 + 3 \cdot 258 - 3 \cdot 147 =$$

$$= 4 \cdot 258 - 7 \cdot 147$$

Multiplicando por 123 tenemos $369 = 123 \cdot 3 = 492 \cdot 258 - 861 \cdot 147$

luego una solución concreta es $x = 492,\ y = -861$, y el conjunto de soluciones es

$$x = 492 + 49k,\ y = -861 - 86k$$

10.1.5

$x = 15 + 11k,\ y = -27 - 20k$

10.1.6

La sucesión será de la forma $a, a+k, a+2k, a+3k, a+4k, a+5k$ para un cierto ángulo inicial a, y sabemos que los ángulos internos de un hexágono suman $(6-2) \cdot 180^o = 720^o$, así pues:

$$a + a + k + a + 2k + a + 3k + a + 4k + a + 5k = 720 \Leftrightarrow 6a + 15k = 720 \Leftrightarrow 2a + 5k = 240$$

Esta última ecuación diofántica tendrá solución pues $mcm(2,5) = 1$.

Una solución es $a = 100$, $k = 8$, con lo que el conjunto de soluciones será de la forma:

$$\begin{cases} a = 100 + 5n \\ b = 8 - 2n \end{cases}, \text{ con } n \in Z$$

Tenemos, además, la restricción $0 < a < 180$, luego

$$0 < 100 + 5n < 180 \Leftrightarrow -100 < 5n < 80 \Leftrightarrow -20 < n < 16$$

El valor máximo se toma con $n = 15 \Rightarrow a = 100 + 5 \cdot 15 = 175^{\circ}$.

10.1.7

Primera versión.

Sea n dicho número.

$$\left.\begin{array}{l} n = 10a + 9 \\ n = 9b + 8 \end{array}\right\} \Rightarrow 10a + 9 = 9b + 8 \Rightarrow 10a - 9b = -1$$

Esta ecuación diofántica tiene por solución

$$\left.\begin{array}{l} a = -1 - 9k \\ b = -1 - 10k \end{array}\right\} \Rightarrow n = 10(-1 - 9k) + 9 = -90k - 1, \text{ o equivalentemente, } n = 90c - 1$$

Añadimos una condición más:

$$\left.\begin{array}{l} n = 90c - 1 \\ n = 8d + 7 \end{array}\right\} \Rightarrow 90c - 1 = 8d + 7 \Rightarrow 90c - 8d = 8 \Rightarrow 45c - 4d = 4$$

Esta ecuación diofántica tiene por solución:

$$\left.\begin{array}{l} c = 4e \\ d = 45e - 1 \end{array}\right\} \Rightarrow n = 90(4e) - 1 = 360e - 1$$

Añadimos una condición más:

$$\left.\begin{array}{l} n = 360e - 1 \\ n = 7f + 6 \end{array}\right\} \Rightarrow 360e - 1 = 7f + 6 \Rightarrow 360e - 7f = 7$$

Esta ecuación diofántica tiene por solución:

$$\left.\begin{array}{l} e = 7g \\ d = -1 - 360g \end{array}\right\} \Rightarrow n = 360(7g) - 1 = 2520g - 1$$

Con este resultado ya podemos buscar candidatos, y vemos que con $g = 1 \rightarrow n = 2519$ ya cumple todas las condiciones del enunciado.

Segunda versión.

Sea n el número buscado. Este número se puede escribir como

$$n = 10a_9 + 9 = 9a_8 + 8 = 8a_7 + 7 = \ldots = 2a_1 + 1$$

Pero entonces:

$n + 1 = 10(a_9 + 1) = 9(a_8 + 1) = 8(a_7 + 1) = \ldots = 2(a_1 + 1)$, es decir:

$2,3,4,5,6,7,8,9 \mid n + 1 \Rightarrow 2520 = (2,3,4,5,6,7,8,9) \mid n + 1 \Rightarrow n + 1 = 2520k \Rightarrow n = 2520k - 1$

De nuevo, comprobamos que, con $k = 1$, $n = 2519$ cumple todas las condiciones exigidas.

10.1.8

$$\left.\begin{array}{l} 19 = 17 \cdot 1 + 2 \rightarrow 2 = 19 - 17 \\ 17 = 8 \cdot 2 + 1 \rightarrow 1 = 17 - 8 \cdot 2 \end{array}\right\} \Rightarrow 1 = 17 - 8(19 - 17) = 17 - 8 \cdot 19 + 8 \cdot 17 = -8 \cdot 19 + 9 \cdot 17$$

10.2.1
Para resolver este problema vamos a utilizar que todo cuadrado perfecto es 0 o 1 módulo 3 (ver Problema 3.22).

Entre el conjunto de todas las soluciones posibles, tomaremos aquella tal que $|a|+|b|+|c|$ sea mínimo.

Pasando a módulo 3, $a^2 = 2b^2 + 3c^2 \equiv 2b^2 \pmod 3$.
Puesto que b^2 es 0 o 1 módulo 3, $2b^2$ será 0 o 2 módulo 3. Puesto que es un cuadrado perfecto, no podrá ser 2 módulo 3, por lo que la única posibilidad es que sea 0 módulo 3:

$$b^2 \equiv 0 \pmod 3 \Leftrightarrow 3 \mid b^2 \Rightarrow 3 \mid b$$

$$\left.\begin{array}{l} 3 \mid b \Rightarrow 3 \mid 2b^2 \\ 3 \mid 3c^2 \end{array}\right\} \Rightarrow 3 \mid a^2 = 2b^2 + 3c^2 \Rightarrow 3 \mid a$$

$$\left.\begin{array}{l} 3 \mid b \Rightarrow b = 3b' \Rightarrow b^2 = 9b'^2 \\ 3 \mid a \Rightarrow a = 3a' \Rightarrow a^2 = 9a'^2 \end{array}\right\} \Rightarrow 3c^2 = 2b^2 - a^2 = 2 \cdot 9b'^2 - 9a'^2 = 9\left(2b'^2 - a'^2\right) \Rightarrow 9 \mid 3c^2 \Rightarrow 3 \mid c^2$$

$$3 \mid c^2 \Rightarrow 3 \mid c \Rightarrow c = 3c'$$

Luego $2b'^2 + 3c'^2 = 2\left(\frac{b}{3}\right)^2 + 3\left(\frac{c}{3}\right)^2 = 2\frac{b^2}{9} + 3\frac{c^2}{9} = \frac{1}{9}\left(2b^2 + 3c^2\right) = \frac{1}{9}a^2 = \left(\frac{a}{3}\right)^2 = a'^2$

Es decir, la terna (a', b', c') también es solución de la ecuación del enunciado, pero

$$|a'| + |b'| + |c'| = \left|\frac{a}{3}\right| + \left|\frac{b}{3}\right| + \left|\frac{c}{3}\right| < |a| + |b| + |c|$$

Contradiciendo la hipótesis de que esta suma era mínima.
Así pues, no existe ninguna solución a esta ecuación que no sea la trivial $a = b = c = 0$

Fuente de la solución: Solución oficial (OME, página 247)

10.3.8
Siguiendo los razonamientos de los teoremes de este apartado, distinguiremos los siguientes casos:
a) Si n no es un cuadrado perfecto.
a_1) Si n es impar.
El número de soluciones positivas será

$$\lambda(n) = \frac{1}{2}\prod_{i=1}^{n}(\alpha_i + 1)$$

Luego

$$43 \cdot 47 = \frac{1}{2}\prod_{i=1}^{n}(\alpha_i + 1) \Rightarrow 2 \cdot 43 \cdot 47 = \prod_{i=1}^{n}(\alpha_i + 1)$$

Y el valor de n más pequeño lo encontraremos tomando los factores primos más pequeños con los exponentes más pequeños posibles (y en orden inverso):

$$n = 3^{47-1}\,5^{43-1}\,7^{2-1} = 3^{46}\,5^{42}\,7$$

a_2) Si n es par.
El número total de soluciones será

$$\lambda(n) = \frac{1}{2}(\alpha_1 - 1)\prod_{i=2}^{n}(\alpha_i + 1) = 2021 = 43\cdot 47 \Rightarrow (\alpha_1 - 1)\prod_{i=2}^{n}(\alpha_i + 1) = 2\cdot 43\cdot 47$$

Y el número n más pequeño que podemos conseguir será

$$n = 2^{47+1}\,3^{43-1}\,5^{2-1} = 2^{48}\,3^{42}\,5$$

b) Si n es un cuadrado perfecto.
b_1) Si n es impar.

La fórmula $\prod_{i=1}^{n}(\alpha_i + 1)$ determina el total de soluciones con x positiva, que pueden ser de la forma (x, y) o $(x,-y)$. Entre ellas tenemos la solución la solución $\left(\sqrt{n}, 0\right)$, que no se contempla en este problema, luego:

$$\prod_{i=1}^{n}(\alpha_i + 1) = 2\cdot 2021 + 1 = 13\cdot 311$$

Y el número n más pequeño que podemos conseguir será $n = 3^{310}\cdot 5^{12}$

b_2) Si n es par.

La fórmula $(\alpha_1 - 1)\prod_{i=2}^{n}(\alpha_i + 1)$ determina el total de soluciones con x positiva, que pueden ser de la forma (x, y) o $(x,-y)$. Entre ellas tenemos la solución la solución $\left(\sqrt{n}, 0\right)$, que no se contempla en este problema, luego:

$$(\alpha_1 - 1)\prod_{i=2}^{n}(\alpha_i + 1) = 2\cdot 2021 + 1 = 13\cdot 311$$

Los valores de n que vamos obteniendo: $2^{14}p^{310}$, $2^{312}p^{12}$, 2^{4044} son todos mayores que el encontrado en el apartado a_2 (falta por comprobar).

Así pues, el menor número olímpico es $n = 2^{48}\,3^{42}\,5$ y si exigimos que además sea impar es $n = 3^{46}\,5^{42}\,7$.

Fuente: Soluciones oficiales (OME, pág. 886)

10.3.9

Las raíces de $f(x) = x^2 - a\,x + 2a$ son $x = \dfrac{a \pm \sqrt{a^2 - 8a}}{2}$

Luego $a^2 - 8a$ debe ser un cuadrado perfecto: $a^2 - 8a = b^2$

$$a^2 - 8a = b^2 \Leftrightarrow a^2 - 8a + 16 = b^2 + 16 \Leftrightarrow (a-4)^2 = b^2 + 16 \Leftrightarrow$$
$$(a-4)^2 - b^2 = 16 \Leftrightarrow (a - 4 + b)(a - 4 - b) = 16$$

Resolvemos todas las combinaciones posibles:

$$\begin{cases} a-4+b=1 \\ a-4-b=16 \end{cases} \Rightarrow \begin{cases} a=25/2 \\ b=-15/2 \end{cases} \qquad \begin{cases} a-4+b=2 \\ a-4-b=8 \end{cases} \Rightarrow \begin{cases} a=9 \\ b=-3 \end{cases}$$

$$\begin{cases} a-4+b=4 \\ a-4-b=4 \end{cases} \Rightarrow \begin{cases} a=8 \\ b=0 \end{cases} \qquad \begin{cases} a-4+b=8 \\ a-4-b=2 \end{cases} \Rightarrow \begin{cases} a=9 \\ b=3 \end{cases}$$

$$\begin{cases} a-4+b=16 \\ a-4-b=1 \end{cases} \Rightarrow \begin{cases} a=25/2 \\ b=15/2 \end{cases} \qquad \begin{cases} a-4+b=-1 \\ a-4-b=-16 \end{cases} \Rightarrow \begin{cases} a=-9/2 \\ b=15/2 \end{cases}$$

$$\begin{cases} a-4+b=-2 \\ a-4-b=-8 \end{cases} \Rightarrow \begin{cases} a=-1 \\ b=3 \end{cases} \qquad \begin{cases} a-4+b=-4 \\ a-4-b=-4 \end{cases} \Rightarrow \begin{cases} a=0 \\ b=0 \end{cases}$$

$$\begin{cases} a-4+b=-8 \\ a-4-b=-2 \end{cases} \Rightarrow \begin{cases} a=-1 \\ b=-3 \end{cases} \qquad \begin{cases} a-4+b=-16 \\ a-4-b=-1 \end{cases} \Rightarrow \begin{cases} a=-9/2 \\ b=-15/2 \end{cases}$$

Las soluciones aceptables son 9, 8, 0 y -1 , luego la respuesta correcta es $9+8+0+(-1)=16$ (C)

Observación.
Una manera mucho más elegante de resolver la ecuación

$$(a-4+b)(a-4-b)=16$$

Es la siguiente:

$$(a-4+b)(a-4-b)=u\cdot v \Rightarrow \begin{cases} a-4+b=u \\ a-4-b=v \end{cases} \Rightarrow 2(a-4)=u+v \Rightarrow a=\frac{u+v}{2}+4$$

Luego

$$u=1,\ v=16 \Rightarrow a=\frac{17}{2}+4 \qquad u=2,\ v=8 \Rightarrow a=\frac{10}{2}+4=9$$

$$u=4,\ v=4 \Rightarrow a=\frac{8}{2}+4=8 \qquad u=-1,\ v=-16 \Rightarrow a=\frac{-17}{2}+4$$

$$u=-2,\ v=-8 \Rightarrow a=\frac{-10}{2}+4=-1 \qquad u=-4,\ v=-4 \Rightarrow a=\frac{-8}{2}+4=0$$

Fuente de esta solución: https://artofproblemsolving.com/wiki/index.php/2015_AMC_10A_Problems/Problem_23

10.4.1
Supongamos que $y\geq 7$. Pasando a módulo 7 , $y!\equiv 0$, $2001\equiv -1$ y la ecuación se convierte en

$$x^2\equiv -1\equiv 6 \pmod 7$$

Pero en Z_7 esta ecuación no tiene solución. En efecto:

$$0^2\equiv 0,\ 1^2\equiv 1,\ 2^2\equiv 4,\ 3^2=9\equiv 2,\ 4^2=16\equiv 2,\ 5^2=25\equiv 4,\ 6^2=36\equiv 1$$

Así pues, $y\leq 6$. Ahora tenemos que ir estudiando los casos uno a uno:
$y=6\Rightarrow x^2-6!=2001\Rightarrow x^2=2721$ no es ningún cuadrado. Esto se puede deducir fácilmente viendo 2721 que es divisible entre 3 pero no entre 9.

$y=5 \Rightarrow x^2-5!=2001 \Rightarrow x^2=2121$ no es ningún cuadrado. Como en el caso anterior, esto se puede deducir fácilmente viendo que 2121 es divisible entre 3 pero no entre 9.
$y=4 \Rightarrow x^2-4!=2001 \Rightarrow x^2=2025=45^2$ y tenemos el par de soluciones $(\pm 45, 4)$.
Los casos $y \leq 3$ no generan soluciones, y por tanto las únicas soluciones al problema son $(\pm 45, 4)$.

Fuente: Olympiad Number Theory Through Challenging Problems (Justin Stevens), pág. 86

10.4.2

Supongamos que $3^m+3^n+1=x^2$ para cierto entero x.
En primer lugar vemos que 3^m+3^n+1 es impar, luego x es impar.
Si x es impar, $x^2 \equiv 1 \pmod 8$
En efecto: $x=2k+1 \Rightarrow x^2=(2k+1)^2=4k^2+4k+1=4k(k+1)+1$, y
$k \geq 1 \Rightarrow k+1 \geq 2 \Rightarrow 4k(k+1) \equiv 0 \pmod 8$
$k=0 \Rightarrow x=1 \Rightarrow x^2=1 \equiv 1 \pmod 8$
Pero, por otro lado, las potencias de 3 siempre son 1 o 3 módulo 8:
$3^0 \equiv 0,\ 3^1 \equiv 3,\ 3^2=9 \equiv 1,\ 3^3 \equiv 3 \ldots$
Luego todo número de la forma 3^m+3^n+1 será congruente con $1+1+1=3$, $1+3+1=5$ o $3+3+1=7$, en todo caso nunca será 1 módulo 8.

Observación: No era necesario especificar los impares: En general, todo cuadrado módulo 8 es 0, 1 o 4, y ninguno de los valores 3^m+3^n+1 es 0, 1 o 4.

10.4.3

La clave está en pasar a módulo 13:
Por un lado, $19 \equiv 6$, y por el PTF, $6^{13} \equiv 6$. Además,
$6^2=36 \equiv 10 \Rightarrow 6^3 \equiv 60 \equiv 8 \Rightarrow 6^6=(6^3)^2 \equiv 8^2=64 \equiv 12$
$19^{19} \equiv 6^{19}=6^{13} \cdot 6^6 \equiv 6 \cdot 12=72 \equiv 7$.
(Otra manera de verlo sería $19^{19} \equiv 6^{19}=6^{12} \cdot 6^7 \equiv 1 \cdot 6^7=6^6 \cdot 6 \equiv 12 \cdot 6 \equiv 7$)

Por otro lado, veamos las potencias $x^3 \pmod{13}$, $y^4 \pmod{13}$.
Por el Teorema de Euler, suponiendo $(x, 13)=1$, tenemos
$\phi(13)=12 \Rightarrow (x^3)^4=x^{12} \equiv 1 \pmod{13}$.
Luego $x^3=z \pmod{13} \Rightarrow 1 \equiv (x^3)^4=z^4 \pmod{13}$, y la ecuación $z^4 \equiv 1 \pmod{13}$ tiene las siguientes soluciones: $z \equiv 1, 5, 8, 12 \pmod{13}$, luego $x^3=0, 1, 5, 8, 12 \pmod{13}$.
De la misma forma, puesto que la ecuación $z^3 \equiv 1 \pmod{13}$ tiene las soluciones $z^3 \equiv 1, 3, 9 \pmod{13}$, los posibles valores $y^4 \pmod{13}$ son $x^3=0, 1, 3, 9 \pmod{13}$.

Finalmente, solo hay que comprobar que ninguna de las combinaciones posibles para x^3+y^4 nunca es 7.

Observación. Como es habitual, no queda claro cómo "adivinar" que debemos pasar a módulo 13. De hecho, mediante el uso del ordenador observamos que el módulo 13 (y 26 y siguientes...) es el único caso en el que se observa la "anomalía" de tener ningún valor

$x^3 + y^4 \equiv 7 \pmod{n}$. Basta buscar una combinación "bonita" de la forma $19^{19} \equiv 7$ para contruir un problema digamos "difícil".

10.4.4

Pasamos a módulo 11.

Sabemos que $x^{10} \equiv 1 \pmod{11}$ para todo x con $(x,11) = 1$.

Luego $x^5 \equiv z \pmod{11} \Rightarrow \left(x^5\right)^2 \equiv z^2 \pmod{11}$

Sabemos, aplicando el PTF o el Teorema de Euler, que $x^{10} \equiv 1 \pmod{11}$.

Por otro lado, vemos los cuadrados módulo 11:

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 9,\ 4^2 \equiv 5,\ 5^2 \equiv 3,$$
$$6^2 \equiv 3,\ 7^2 \equiv 5,\ 8^2 \equiv 9,\ 9^2 \equiv 4,\ 10^2 \equiv 1$$

Así pues, $y^2 \equiv z \pmod{11} \Rightarrow y^2 \in \{0, 1, 4, 5, 9\}$

y también se cumple $z^2 \equiv 1 \pmod{11} \Rightarrow z = \pm 1 \pmod{11}$

Por lo tanto $x^5 \equiv z \pmod{11} \Rightarrow \left(x^5\right)^2 \equiv z^2 \pmod{11} \Rightarrow x^5 = \pm 1 \pmod{11}$

Observamos se cumple $x^5 - y^2 \not\equiv 4 \pmod{11}$ para todo x, y, luego la ecuación no tiene solución.

10.4.5

Pasamos a módulo 9.

Los residuos cúbicos módulo 9 son -1, 0 y 1.

Los residuos de grado 6 módulo 9 son 0 y 1.

Luego tenemos

$$\begin{cases} a^5 b + 3 \equiv -1, -0, 1 \pmod{9} \\ ab^5 + 3 \equiv -1, -0, 1 \pmod{9} \end{cases} \Rightarrow \begin{cases} a^5 b \equiv 5, 6, 7 \pmod{9} \\ ab^5 \equiv 5, 6, 7 \pmod{9} \end{cases}$$

Pero $a^5 b \cdot ab^5 = a^6 b^6 = (ab)^6 \equiv 0, 1 \pmod{9}$

Comprobando todas las combinaciones posibles de 5, 6 y 7 :

$$5 \cdot 5 \equiv 7 \pmod{9},\ 5 \cdot 7 \equiv 8 \pmod{9},\ 7 \cdot 7 \equiv 4 \pmod{9}...$$

Vemos que la única posibilidad aceptable es

$$\begin{cases} a^5 b \equiv 6 \pmod{9} \\ ab^5 \equiv 6 \pmod{9} \end{cases}$$

Pero entonces $a^5 b \equiv 6 \pmod{9} \Leftrightarrow a^5 b = 9k + 6 = 3(3k + 2) \Rightarrow 3 \mid a^5 b$

Y por otro lado, $ab^5 \equiv 6 \pmod{9} \Leftrightarrow ab^5 = 9q + 6 = 3(3q + 2) \Rightarrow 3 \mid ab^5$

En todo caso, $3 \mid a \Rightarrow 9 \mid a^5 b \Rightarrow a^5 b \equiv 0 \pmod{9}$ o bien $3 \mid b \Rightarrow 9 \mid ab^5 \Rightarrow ab^5 \equiv 0 \pmod{9}$ llegando a contradicción.

Otra forma de justificarlo sería $a^5 b \equiv 6 \pmod{9}$ implica que tiene exactamente un factor de 3, y $ab^5 \equiv 6 \pmod{9}$ implica que tiene exactamente un factor de 3, pero entonces $a^5 b \cdot ab^5$ tendría exactamente dos factores de 3, lo que es imposible porque es una potencia sexta.

10.4.6

$$(x+1)^2+(x+2)^2+\ldots+(x+2001)^2=$$

$$=\sum_{k=1}^{k=2001}(x+k)^2=\sum_{k=1}^{k=2001}x^2+2kx+k^2=\sum_{k=1}^{k=2001}x^2+\sum_{k=1}^{k=2001}2kx+\sum_{k=1}^{k=2001}k^2=$$

$$=2001x^2+2x\frac{2001\cdot 2002}{2}+\frac{2001\cdot 2002\cdot 4003}{2}=$$

$$=2001x^2+2001\cdot 2002\,x+667\cdot 1001\cdot 4003\equiv 2 \pmod 3$$

Luego no puede ser ningún cuadrado perfecto (ver 7.3.9a)

10.4.7

Vemos que uno de los dos debe ser múltiple de 3.

Supongamos, por el contrario, que $p\equiv 1,2 \pmod 3$ y $q\equiv 1,2 \pmod 3$. Ninguna de las combinaciones posibles es aceptable:

$$p\equiv 1, q\equiv 1\Rightarrow\begin{cases}p^3-q^5\equiv 0\\(p+q)^2\equiv 2^2=4\equiv 1\end{cases}$$

$$p\equiv 1, q\equiv 2\equiv -1\Rightarrow\begin{cases}p^3-q^5\equiv 1-(-1)=2\\(p+q)^2\equiv 0\end{cases}$$

$$p\equiv 2\equiv -1, q\equiv 1\Rightarrow\begin{cases}p^3-q^5\equiv (-1)-1=-2=-1\\(p+q)^2\equiv 0\end{cases}$$

$$p\equiv 2\equiv -1, q\equiv 2\equiv -1\Rightarrow\begin{cases}p^3-q^5\equiv (-1)-(-1)\equiv 0\\(p+q)^2\equiv (-2)^2\equiv 1\end{cases}$$

Así pues, al menos uno de los dos debe ser múltiple de 3, y puesto que son primos, al menos uno de los dos debe ser igual a 3.

Supongamos que $p=3$. La ecuación queda de la forma:

$$p^3-q^5=(p+q)^2\Leftrightarrow 27-q^5=(3+q)^2>0\Rightarrow q^5<27 \text{ absurdo.}$$

Supongamos que $q=3$. La ecuación queda de la forma:

$p^3-q^5=(p+q)^2\Leftrightarrow p^3-3^5=(p+3)^2\Leftrightarrow p^3-243=(p+3)^2$, cuya única solución entera es $p=7$.

Así pues, la única solución con números primos es (7 , 3).

10.4.8

Sin pérdida de generalidad podemos suponer que $a\le b\le c$.

Está claro que $a=1, b=10, c=10$ es una solución para la ecuación. Vamos a ver que no hay ninguna más.

Vamos a resolver este problema trabajando en módulo 9, y nos basaremos en el siguiente lema:

Todo entero n^3 es de la forma $<9>+0$, $<9>+1$ o $<9>-1$, donde $<9>$ es cualquier número múltiplo de 9. En efecto, supongamos que n es un múltiplo de 3: $n=3k$. Entonces $n^3=(3k)^3=27k^3=9\cdot 3k^3=<9>+0$.
Por el contrario, si $n=3k\pm 1$, entonces $n^3=(3k\pm 1)^3=27k^3\pm 27k^2+9k\pm 1=<9>\pm 1$.

$2001=9\cdot 222+1=<9>+3$, luego forzosamente tendremos $a^3=<9>+1$, $b^3=<9>+1$ y $b^3=<9>+1$, luego, por el lema anterior, a, b y c son de la forma $<3>+1$.

Construimos la siguiente tabla:
$4^3=64$
$7^3=343$
$10^3=1000$
$13^3=2197$
$16^3=4096$
Puesto que $2001\div 3=667$, si $c<10$, $a^3+b^3+c^3<3\cdot 7^3=3\cdot 343=1029<2001$.
Pero si $c>10$, $c^3\geq 2197\Rightarrow a^3+b^3+c^3\geq 2197>2001$. Luego, forzosamente $c=10$.
Supongamos que $c=10\Rightarrow c^3=1000\Rightarrow a^3+b^3=2001-1000=1001$.
$1001\div 2=500.5$, al menos uno de los dos debe ser mayor de 500, necesariamente
$b=10\Rightarrow b^3=1000\Rightarrow a^3=1001-1000=1\Rightarrow a=1$.
Es decir, tenemos la solución encontrada inicialmente.

Las soluciones son $(a,b,c)=(1,10,10)$, $(10,1,10)$, $(10,10,1)$

10.5.1
$x^2+y^2=3z^2\Rightarrow x^2+y^2\equiv 0\ (\text{mod } 3)$.
Ahora aplicamos el resultado de que todo cuadrado es 0 o 1 módulo 3, luego

$$x^2\equiv 0\ (\text{mod } 3),\ y^2\equiv 0\ (\text{mod } 3)\Rightarrow x^2+y^2\equiv 0+0=0\ (\text{mod } 3)$$
$$x^2\equiv 1\ (\text{mod } 3),\ y^2\equiv 0\ (\text{mod } 3)\Rightarrow x^2+y^2\equiv 1+0=1\ (\text{mod } 3)$$
$$x^2\equiv 0\ (\text{mod } 3),\ y^2\equiv 1\ (\text{mod } 3)\Rightarrow x^2+y^2\equiv 0+1=1\ (\text{mod } 3)$$
$$x^2\equiv 1\ (\text{mod } 3),\ y^2\equiv 1\ (\text{mod } 3)\Rightarrow x^2+y^2\equiv 1+1=2\ (\text{mod } 3)$$

La única posibilidad válida es $x^2\equiv y^2\equiv 0\ (\text{mod } 3)\Rightarrow x\equiv y\equiv 0\ (\text{mod } 3)$

Luego

$$x=3x',y=3y'\Rightarrow x^2+y^2=(3x')^2+(3y')^2=9x'^2+9y'^2=9\left(x'^2+y'^2\right)=3z^2\Rightarrow$$
$$3\left(x'^2+y'^2\right)=z^2\Rightarrow 3\mid z^2\Rightarrow 3\mid z\Rightarrow z=3z'\Rightarrow z^2=(3z')^2=9z'^2$$

Luego:

$$3\left(x'^2+y'^2\right)=9z'^2\Rightarrow x'^2+y'^2=3z'^2$$

Llegando a la misma ecuación para valores $(x',y',z')=\left(\frac{x}{3},\frac{y}{3},\frac{z}{3}\right)$ estrictamente más pequeños que los primeros. Aquí aplicamos el Principio del Descenso Infinito para deducir que esta ecuación no tiene ninguna solución exceptuando la trivial $x=y=z=0$

10.5.2

$a^2+b^2+c^2=a^2b^2 \Leftrightarrow c^2=a^2b^2-a^2-b^2$

Puesto que todos los elementos involucrados son cuadrados, podemos reducir nuestro estudio a las soluciones positivas, y después duplicar las soluciones encontradas.

Vamos a utilizar que todo cuadrado es 0 o 1 módulo 4.

$$a^2=0 \pmod 4, b^2=0 \pmod 4 \Rightarrow a^2b^2-a^2-b^2=0\cdot 0-0-0=0 \pmod 4$$
$$a^2=1 \pmod 4, b^2=0 \pmod 4 \Rightarrow a^2b^2-a^2-b^2=1\cdot 0-1-0=-1=3 \pmod 4$$
$$a^2=0 \pmod 4, b^2=1 \pmod 4 \Rightarrow a^2b^2-a^2-b^2=0\cdot 1-0-1=-1=3 \pmod 4$$
$$a^2=1 \pmod 4, b^2=1 \pmod 4 \Rightarrow a^2b^2-a^2-b^2=1\cdot 1-1-1=-1=3 \pmod 4$$

Así pues, la única posibilidad aceptable es: $a^2=0 \pmod 4$ y $b^2=0 \pmod 4$.

Escribamos $a^2=4a'$ y $b^2=4b'$ para ciertos a',b'.

Luego $c^2=a^2b^2-a^2-b^2=4a'4b'-4a'-4b'=4\left(4a'b'-a'-b'\right)=2^2\left(4a'b'-a'-b'\right)$

y por tanto $4a'b'-a'-b'$ debe ser también un cuadrado, y por tanto 0 o 1 módulo 4.

Pero observamos que este proceso lo estamos repitiendo una y otra vez, obteniendo una cadena decreciente de divisores de 4, con lo que, aplicando la técnica del "descenso infinito de Fermat", llegamos a la conclusión de que la única solución aceptable es $a=b=0$, y por tanto también $c=0$.

10.5.3

Está claro que (0,0,0) es solución de la ecuación. Veamos que es la única solución posible aplicando la técnica del descenso infinito de Fermat.

Supongamos que (x,y,z) es solución de la ecuación.

$$x^3=2y^3+4z^3=2\left(y^3+2z^3\right)$$

Luego x^3 es par, y por tanto x es par: $x=2x_1 \Rightarrow x^3=\left(2x_1\right)=8x_1^3$, y por tanto

$$8x_1^3=2y^3+4z^3 \Rightarrow 4x_1^3=y^3+2z^3 \Rightarrow y^3=4x_1^3-2z^3=2\left(2x_1^3-z^3\right)$$

Luego y^3 es par, y por tanto y es par: $y=2y_1 \Rightarrow y^3=\left(2y_1\right)=8y_1^3$, y por tanto

$$8y_1^3=4x_1^3-2z^3 \Rightarrow 4y_1^3=2x_1^3-z^3 \Rightarrow z^3=2x_1^3-4y_1^3=2\left(x_1^3-2y_1^3\right)$$

Luego z^3 es par, y por tanto z es par $z=2z_1$

Así pues,

$$x^3=2y^3+4z^3 \Rightarrow \left(2x_1\right)^3=2\left(2y_1\right)^3+4\left(2z_1\right)^3 \Leftrightarrow 8x_1^3=2\cdot 8y_1^3+4\cdot 8z_1^3$$
$$\Leftrightarrow x_1^3=2y_1^3+4z_1^3$$

Así pues, tenemos otra solución (x_1,y_1,z_1) de la misma ecuación, con valores más pequeños en valor absoluto (dividiendo entre dos los respectivos números), cosa que nos lleva al absurdo pues estamos trabajando con números enteros.

10.6.1

$$(xy-7)^2 = x^2+y^2 \Leftrightarrow x^2y^2-14xy+49 = x^2+y^2 \Leftrightarrow$$
$$x^2y^2-14xy+49 = (x+y)^2-2xy \Leftrightarrow x^2y^2-12xy+49 = (x+y)^2 \Leftrightarrow$$
$$x^2y^2-2\cdot 6xy+6^2-6^2+49 = (x+y)^2 \Leftrightarrow (xy-6)^2+13 = (x+y)^2 \Leftrightarrow$$
$$13 = (x+y)^2-(xy-6)^2 = (x+y+xy-6)(x+y-xy+6)$$

Sumando y restando las ecuaciones observamos que el sistema

$$\begin{cases} x+y+xy-6 = a \\ x+y-xy+6 = b \end{cases}$$

es equivalente al sistema

$$\begin{cases} x+y = (a+b)/2 \\ xy-6 = (a-b)/2 \end{cases}$$

Veamos casos posibles:

$$a=1, b=13 \Rightarrow \begin{cases} x+y=7 \\ xy-6=-6 \end{cases} \Rightarrow \begin{cases} x=0,\ y=7 \\ x=7,\ y=0 \end{cases}$$
$$a=13, b=1 \Rightarrow \begin{cases} x+y=7 \\ xy-6=6 \end{cases} \Rightarrow \begin{cases} x=3,\ y=4 \\ x=4,\ y=3 \end{cases}$$
$$a=-1, b=-13 \Rightarrow \begin{cases} x+y=-7 \\ xy-6=6 \end{cases} \Rightarrow \begin{cases} x=-4,\ y=-3 \\ x=-3,\ y=-4 \end{cases}$$
$$a=-13, b=-1 \Rightarrow \begin{cases} x+y=-7 \\ xy-6=-6 \end{cases} \Rightarrow \begin{cases} x=-7,\ y=0 \\ x=0,\ y=-7 \end{cases}$$

Las soluciones con valores no negativos son los pares (0,7) , (7,0) , (3,4) , (4,3).

10.6.2

Primera versión.

$$x^2(y-1)+y^2(x-1)=1 \Leftrightarrow x^2y-x^2+xy^2-y^2=1 \Leftrightarrow$$
$$xy(x+y)-(x^2+y^2)=1 \Leftrightarrow xy(x+y)-((x+y)^2-2xy)=1$$

Realizando el cambio de variable $a=xy, b=x+y$, la ecuación se transforma en:

$$ab-(b^2-2a)=1 \Leftrightarrow ab-b^2+2a=1 \Leftrightarrow ab-b^2+2a+4=5 \Leftrightarrow$$
$$(a-b+2)(b+2)=5$$

Veamos las combinaciones posibles:

$$\begin{cases} a-b+2=1 \\ b+2=5 \end{cases} \Rightarrow b=3, a=2 \Rightarrow \begin{cases} xy=2 \\ x+y=3 \end{cases} \Rightarrow \begin{cases} x=1,\ y=2 \\ x=2,\ y=1 \end{cases}$$
$$\begin{cases} a-b+2=5 \\ b+2=1 \end{cases} \Rightarrow b=-1, a=2 \Rightarrow \begin{cases} xy=2 \\ x+y=-1 \end{cases}$$ no tiene soluciones reales.
$$\begin{cases} a-b+2=-1 \\ b+2=-5 \end{cases} \Rightarrow b=-7, a=-10 \Rightarrow \begin{cases} xy=-10 \\ x+y=-7 \end{cases}$$ no tiene soluciones enteras.

$$\begin{cases} a-b+2=-5 \\ b+2=-1 \end{cases} \Rightarrow b=-3 \Rightarrow \begin{cases} x=1, y=2 \\ x=2, y=1 \end{cases} \Rightarrow \begin{cases} x=-5, y=2 \\ x=2, y=-5 \end{cases}$$

Así pues, las soluciones son $x=1, y=2$; $x=2, y=1$; $x=-5, y=2$; $x=2, y=-5$.

Segunda versión.
Realizamos el cambio de variable $a=x-1$, $b=y-1$.

$$x=a+1 \Rightarrow x^2=(a+1)^2=a^2+2a+1$$
$$y=b+1 \Rightarrow y^2=(b+1)^2=b^2+2b+1$$
$$x^2(y-1)+y^2(x-1)=1 \Leftrightarrow (a^2+2a+1)b+(b^2+2b+1)a=1 \Leftrightarrow$$
$$a^2b+2ab+b+ab^2+2ab+a=1 \Leftrightarrow ab(a+b)+4ab+a+b=1 \Leftrightarrow$$
$$ab(a+b+4)+a+b=1 \Leftrightarrow ab(a+b+4)+a+b+4=5 \Leftrightarrow$$
$$(ab+1)(a+b+4)=5$$

y se continúa estudiando los casos posibles como en la primera versión.

Fuente de la segunda versión: An Introduction to Diophantine Equations A Problem-Based Approach (Andreescu, Cucurezeanu, Andrica), página 7.

10.6.3

$$xy^2+2y^2-x-107=0 \Leftrightarrow xy^2+2y^2-x=107 \Leftrightarrow (x+2)(y^2-1)+2=107 \Leftrightarrow$$
$$(x+2)(y^2-1)=105=3\cdot 5\cdot 7$$

Ahora estudiamos caso por caso:

$$\begin{cases} x+2=1 \\ y^2-1=3\cdot 5\cdot 7 \end{cases} \Rightarrow x=-1 \text{ imposible} \qquad \begin{cases} x+2=3 \\ y^2-1=5\cdot 7 \end{cases} \Rightarrow \begin{cases} x=1 \\ y^2=36 \Rightarrow y=6 \end{cases}$$

$$\begin{cases} x+2=5 \\ y^2-1=3\cdot 7 \end{cases} \Rightarrow y^2=22 \text{ imposible} \qquad \begin{cases} x+2=7 \\ y^2-1=3\cdot 5 \end{cases} \Rightarrow \begin{cases} x=5 \\ y^2=16 \Rightarrow y=4 \end{cases}$$

$$\begin{cases} x+2=3\cdot 5 \\ y^2-1=7 \end{cases} \Rightarrow y^2=8 \text{ imposible} \qquad \begin{cases} x+2=3\cdot 7 \\ y^2-1=5 \end{cases} \Rightarrow y^2=6 \text{ imposible}$$

$$\begin{cases} x+2=5\cdot 7 \\ y^2-1=3 \end{cases} \Rightarrow \begin{cases} x=33 \\ y^2=4 \Rightarrow y=2 \end{cases} \qquad \begin{cases} x+2=3\cdot 5\cdot 7 \\ y^2-1=1 \end{cases} \Rightarrow \begin{cases} x=105 \\ y^2=0 \end{cases} \text{ imposible}$$

Las soluciones son: (1,6), (5,4), (33,2)

Nota: Tal vez más elegante hubiera sido seguir con la descomposición:

$$(x+2)(y^2-1)=105 \Leftrightarrow (x+2)(y-1)(y+1)=105=3\cdot 5\cdot 7$$

10.6.4

Sea x el número de columnas, y sea y el número de filas de este teatro.
La ecuación diofántica que se nos plantea es

$$xy=12y+15x+7 \Leftrightarrow$$
$$xy-12y-15x=7 \Leftrightarrow$$
$$(x-12)(y-15)-12\cdot 15=7 \Leftrightarrow$$
$$(x-12)(y-15)=7+12\cdot 15=187=11\cdot 17$$

Estudiemos los casos:

$$1)\ \begin{cases} x-12=1 \\ y-15=187 \end{cases} \Rightarrow \begin{cases} x=13 \\ y=202 \end{cases} \Rightarrow xy=2626$$

$$2)\ \begin{cases} x-12=11 \\ y-15=17 \end{cases} \Rightarrow \begin{cases} x=23 \\ y=32 \end{cases} \Rightarrow xy=736$$

$$3)\ \begin{cases} x-12=17 \\ y-15=12 \end{cases} \Rightarrow \begin{cases} x=29 \\ y=27 \end{cases} \Rightarrow xy=783$$

$$4)\ \begin{cases} x-12=187 \\ y-15=1 \end{cases} \Rightarrow \begin{cases} x=199 \\ y=16 \end{cases} \Rightarrow xy=3184$$

Así pues, vemos que el mínimo número de butacas se obtiene para 736 (C).

10.6.5

Sea x el número de columnas, y sea y el número de filas de este teatro.
La ecuación diofántica que se nos plantea es

$$xy=11y+14x+17 \Leftrightarrow$$
$$xy-11y-14x=17 \Leftrightarrow$$
$$(x-11)(y-14)-11\cdot 14=17 \Leftrightarrow$$
$$(x-11)(y-14)=17+11\cdot 14=171=3^2\cdot 19$$

Estudiemos los casos:

$$1)\ \begin{cases} x-11=1 \\ y-14=171 \end{cases} \Rightarrow \begin{cases} x=12 \\ y=185 \end{cases} \Rightarrow xy=2220$$

$$2)\ \begin{cases} x-11=3 \\ y-14=3\cdot 19 \end{cases} \Rightarrow \begin{cases} x=14 \\ y=71 \end{cases} \Rightarrow xy=994$$

$$3)\ \begin{cases} x-11=3^2 \\ y-14=19 \end{cases} \Rightarrow \begin{cases} x=20 \\ y=33 \end{cases} \Rightarrow xy=660$$

$$4)\ \begin{cases} x-11=3\cdot 19 \\ y-14=3 \end{cases} \Rightarrow \begin{cases} x=68 \\ y=17 \end{cases} \Rightarrow xy=1156$$

$$5)\ \begin{cases} x-11=171 \\ y-14=1 \end{cases} \Rightarrow \begin{cases} x=182 \\ y=15 \end{cases} \Rightarrow xy=2730$$

Y vemos que el número mínimo de asientos es 660 (B).

10.6.6

Para resolver este problema utilizaremos la siguiente factorización:

$$2\left(x+y+z+2xyz\right)^2-\left(2xy+2yz+2zx+1\right)^2=\left(2x^2-1\right)\left(2y^2-1\right)\left(2z^2-1\right)$$

En Internet se pueden encontrar diversas formas más o menos largas de demostrar esta igualdad, pero todas ellas son significativamente farragosas y difíciles.

Con la identidad anterior el problema se resuelve fácilmente:

$$2(x+y+z+2xyz)^2=(2xy+2yz+2zx+1)^2+2023 \Leftrightarrow$$
$$2(x+y+z+2xyz)^2-(2xy+2yz+2zx+1)^2=2023$$
$$(2x^2-1)(2y^2-1)(2z^2-1)=2023=7\cdot 17^2$$

Los únicos divisores de $7\cdot 17^2$ que se pueden escribir de la forma $2x^2-1$ son
$x=2\Rightarrow 2x^2-1=7$
$x=3\Rightarrow 2x^2-1=17$

Así pues, las soluciones serán (2,2,3) y todas sus posibles permutaciones.

10.6.7

$x(x-y)=8y-7\Leftrightarrow x^2-xy-8y+7=0$

Interpretando esta ecuación como una ecuación de segundo grado en x, su discriminante será

$$\Delta=(-y)^2-4\cdot 1\cdot(-8y+7)=y^2+32y-28$$

Este discriminante tiene que ser un cuadrado perfecto.

$$y^2+32y-28=(y+16)^2-284=z^2\Leftrightarrow(y+16)^2-z^2=284=2^2\cdot 71\Leftrightarrow$$
$$\Leftrightarrow(y+16-z)(y+16+z)=2^2\cdot 71$$

Vamos probando opciones hasta encontrar las que tienen solución entera:

$\begin{cases} y+16-z=1 \\ y+16+z=2^2\cdot 71 \end{cases}$ no da soluciones enteras , $\begin{cases} y+16-z=2 \\ y+16+z=2\cdot 71 \end{cases}\Rightarrow y+16=72\Rightarrow y=56$

$\begin{cases} y+16-z=4 \\ y+16+z=71 \end{cases}$ no da soluciones enteras , $\begin{cases} y+16-z=2\cdot 71 \\ y+16+z=2 \end{cases}\Rightarrow y+16=72\Rightarrow y=56$

$\begin{cases} y+16-z=4\cdot 71 \\ y+16+z=1 \end{cases}$ no da soluciones enteras.

Así pues, la única solución posible es $y=56$ y por tanto $x(x-56)=8\cdot 56-7\Rightarrow x=-7,\ x=63$.
Descartamos la primera solución y por tanto la única solución posible es $x=63$, $y=56$.

10.7.1

En primer lugar vemos que esta ecuación se verifica para todas las parejas $(x,y)=(k,-k)$.
Supongamos que $y\neq -x$.

$x^3+y^3=(x+y)(x^2-xy+y^2)$, y por tanto

$$x^3+y^3=(x+y)^2\Leftrightarrow(x+y)(x^2-xy+y^2)=(x+y)^2$$

y puesto que estamos suponiendo que $y\neq -x\Leftrightarrow x+y\neq 0$, podemos cancelar este factor para llegar a:

$$x^2-xy+y^2=x+y$$

Y esta ecuación es equivalente a:

$$(x-y)^2+(x-1)^2+(y-1)^2=2$$

De aquí se deduce que

$$\begin{cases}(x-y)^2\le 2\\(x-1)^2\le 2\\(y-1)^2\le 2\end{cases}$$

$$(x-1)^2\le 2\Leftrightarrow\begin{cases}x-1=1\Leftrightarrow x=2\\x-1=0\Leftrightarrow x=1\\x-1=-1\Leftrightarrow x=0\end{cases}\qquad (y-1)^2\le 2\Leftrightarrow\begin{cases}y-1=1\Leftrightarrow y=2\\y-1=0\Leftrightarrow y=1\\y-1=-1\Leftrightarrow y=0\end{cases}$$

$$(x-y)^2\le 2\Leftrightarrow\begin{cases}x-y=1\\x-y=0\\x-y=-1\end{cases}$$

De los $3\times 3=9$ posibles candidatos (x,y), al final son válidas las parejas (0, 1), (1,0), (1,2), (2,1), (2,2), a los que debemos añadir todas las parejas posibles de la forma $(k,-k)$.

Fuente: An Introduction to Diophantine Equations A Problem-Based Approach (Andreescu, Cucurezeanu, Andrica) , página 13

10.7.2

Si $a,b,c\ge 2$,

$$\left.\begin{array}{l}\frac{1}{a+b}\le\frac{1}{4}\\\frac{1}{b+c}\le\frac{1}{4}\\\frac{1}{c+a}\le\frac{1}{4}\\a+b+c-2\ge 6-2=4\Rightarrow\frac{1}{a+b+c-2}\le\frac{1}{4}\end{array}\right\}\Rightarrow\frac{1}{a+b}+\frac{1}{b+c}+\frac{1}{c+a}+\frac{1}{a+b+c-2}\le 1$$

Y la igualdad solo puede darse si $a=b=c=2$, y se comprueba que este caso es solución de la ecuación.

Supongamos ahora que al menos una de las tres incógnitas es menor que 2. Podemos suponer, sin pérdida de generalidad, que $a=1$.

La ecuación nos queda

$$\frac{1}{b+1}+\frac{1}{b+c}+\frac{1}{c+1}+\frac{1}{b+c-1}=1$$

De nuevo, si $b,c\ge 3$,

$$\left.\begin{array}{l}\frac{1}{b+1}\le\frac{1}{4}\\\frac{1}{b+c}\le\frac{1}{6}<\frac{1}{4}\\\frac{1}{c+1}\le\frac{1}{4}\\\frac{1}{b+c-1}\le\frac{1}{5}<\frac{1}{4}\end{array}\right\}\Rightarrow\frac{1}{b+1}+\frac{1}{b+c}+\frac{1}{c+1}+\frac{1}{b+c-1}<1.$$ Luego $1\le b,c\le 2$

El caso $b=c=1$ no satisface la ecuación: $\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\frac{1}{1}=1$

El caso $b=1,\ c=2$ no satisface la ecuación: $\frac{1}{2}+\frac{1}{3}+\frac{1}{3}+\frac{1}{2}=1$

El caso $c=1,\ b=2$ tampoco por simetría.

Finalmente, el caso $b=c=2$ tampoco satisface la ecuación: $\frac{1}{3}+\frac{1}{4}+\frac{1}{3}+\frac{1}{3}=1$

Así pues, el único caso aceptable es $a=b=c=2$

10.7.3

Primera parte: Demostración de la desigualdad.

Supongamos que no es cierto, es decir, que existen a,b,n enteros positivos tales que $a>b$ y $ab-1=n^2$, pero $a-b<\sqrt{4n-3}$

$$(a+b)^2=(a-b)^2+4ab<4n-3+4ab=4n-3+4\left(n^2+1\right)=4n^2+4n+1=\left(2n+1\right)^2$$

Luego

$$a+b<2n+1\Rightarrow a+b\le 2n$$

Por otro lado, por la desigualdad AM-GM: $ab<\left(\frac{a+b}{2}\right)^2$

Y por tanto:

$$n^2+1=ab<\left(\frac{a+b}{2}\right)^2\le\left(\frac{2n}{2}\right)^2=n^2$$

llegando a contradicción.

Segunda parte. Resolución de la igualdad.

De nuevo utilizamos identidad $(a+b)^2=(a-b)^2+4ab$.

$$(a+b)^2=(a-b)^2+4ab=4n-3+4\left(n^2+1\right)=4n^2+4n+1=\left(2n+1\right)^2\Rightarrow a+b=2n+1.$$

La ecuación $a-b=\sqrt{4n-3}$ implica que $4n-3$ sea un cuadrado perfecto impar, es decir,

$4n-3=\left(2u+1\right)^2$ para cierto u entero no negativo, y $a-b=\sqrt{4n-3}=\sqrt{\left(2u+1\right)^2}=2u+1.$

$$4n-3=\left(2u+1\right)^2=4u^2+4u+1\Rightarrow 4n=4u^2+4u+4\Rightarrow n=u^2+u+1$$

$$\left.\begin{array}{l}a+b=2n+1\\a-b=2u+1\end{array}\right\}\Rightarrow 2b=2n+1-2u-1=2\left(n-u\right)\Rightarrow b=n-u=u^2+u+1-u=u^2+1$$

$$a-b=2u+1\Rightarrow a=2u+1+b=2u+1+u^2+1=u^2+2u+2$$

Luego el conjunto solución son todos los números a,b,n tales que

$$\left.\begin{aligned} a &= u^2+2u+2 \\ b &= u^2+1 \\ n &= u^2+u+1 \\ a-b &= 2u+1 \end{aligned}\right\}$$ para todo entero u positivo.

En efecto, se cumple:

$$ab=\left(u^2+2u+2\right)\left(u^2+1\right)=u^4+2u^3+2u^2+u^2+2u+2=u^4+2u^3+3u^2+2u+2=$$
$$=\left(u^2+u+1\right)^2+1=n^2+1$$

Fuente de esta solución: Soluciones oficiales OME.

10.7.4

$$\frac{x^4+y^3}{x^2+y}=x+y \Leftrightarrow x^4+y^3=\left(x^2+y\right)\left(x+y\right)=x^3+x^2y+xy+y^2$$

Vamos a ver que si $x\geq 2$ y $y\geq 4$, entonces

$$x^4+y^3>x^3+x^2y+xy+y^2$$

y por tanto no se puede dar la igualdad.

En efecto, aplicando la desigualdad AM-GM,

$$\frac{x^4+y^3}{2}\geq\sqrt{x^4y^3}=x^2y\sqrt{y}$$

Y puesto que $y\geq 4\Rightarrow\sqrt{y}\geq 2$, y por tanto

$$x^2y\sqrt{y}\geq 2x^2y=x^2y+x^2y>x^2y+xy \quad (1)$$

en donde hemos aplicado además que $x\geq 2\Rightarrow x^2>x$.

Por otro lado, $x\geq 2\Rightarrow x^4=x\cdot x^3\geq 2x^2$ y $y\geq 4\Rightarrow y^3=y\cdot y^2\geq 4y^2>2y^2$

$$\frac{x^4+y^3}{2}>\frac{2x^3+2y^2}{2}=x^3+y^2 \quad (2)$$

Con (1) y (2) llegamos a

$$x^4+y^3=\frac{x^4+y^3}{2}+\frac{x^4+y^3}{2}>x^3+x^2y+xy+y^2$$

tal y como queríamos ver.

Luego la ecuación solo puede tener solución cuando $x=1$ o bien $y\leq 3$.

Primer caso: $x=1$. Entonces:

$$1+y^3=1+y+y+y^2 \Leftrightarrow 0=y^3-y^2-2y=y\left(y^2-y-2\right)=y(y-2)(y+1) \Leftrightarrow \begin{cases} y=0 \\ y=2 \\ y=-1 \end{cases}$$

La única solución aceptable es $x=1, y=2$. En efecto:

$$\frac{1^4+2^3}{1^2+2}=\frac{9}{3}=3=1+2$$

Segundo caso: $y=1$. Entonces:

$$x^4+1^3=x^3+x^2+x+1^2 \Leftrightarrow 0=x^4-x^3-x^2-x=x\left(x^3-x^2-x-1\right)$$

La solución $x=0$ no es aceptable, luego $x^3-x^2-x-1=0$, cuyas soluciones enteras tienen que ser divisores de 1:

$$x=1 \Rightarrow 1^3-1^2-1-1=-2\neq 0$$

Luego no hay solución positiva.

Tercer caso: $y=2$. Entonces:

$$x^4+2^3=x^3+2x^2+2x+2^2 \Leftrightarrow x^4-x^3-2x^2-2x+4=0$$

Debemos buscar las soluciones enteras de esta ecuación entre los divisores de 4:

$$x=1 \Rightarrow 1^4-1^3-2\cdot 1^2-2\cdot 1+4=0$$
$$x=2 \Rightarrow 2^4-2^3-2\cdot 2^2-2\cdot 2+4=0$$
$$x=4 \Rightarrow 4^4-4^3-2\cdot 4^2-2\cdot 4+4=156\neq 0$$

Aquí aparece de nuevo la solución $x=1, y=2$ y encontramos otra solución: $x=2, y=2$. En efecto:

$$\frac{2^4+2^3}{2^2+2}=\frac{2^3(2+1)}{2(2+1)}=4=2+2$$

Cuarto caso: $y=3$. Entonces:

$$x^4+3^3=x^3+3x^2+3x+3^2 \Leftrightarrow x^4-x^3-3x^2-3x+18=0$$

Se verifica que ningún divisor positivo de 18 es solución de esta ecuación, por lo que las soluciones (x, y) enteras positivas de la ecuación del enunciado son $(1,2)$ y $(2,2)$.

Fuente de la solución: Soluciones oficiales (OMEC, pág. 424)

10.7.5

En primer lugar vemos que esta ecuación se cumple para $x=y=z=5$.

Por otro lado, está claro que

$$x, y, x>5 \Rightarrow \frac{1}{x}, \frac{1}{y}, \frac{1}{z}<\frac{1}{5} \Rightarrow \frac{1}{x}+\frac{1}{y}+\frac{1}{z}<\frac{1}{5}+\frac{1}{5}+\frac{1}{5}=\frac{3}{5}$$

por lo tanto, al menos una de las incógnitas debe estar entre 1 y 5. Podemos suponer, sin pérdida de generalidad que esa incógnita es la x. Veamos los casos:

a) $x=1$

$\frac{1}{1}+\frac{1}{y}+\frac{1}{z}=\frac{3}{5}\Leftrightarrow\frac{1}{y}+\frac{1}{z}=\frac{3}{5}-1=\frac{-2}{5}<0$ absurdo. No hay solución aceptable.

b) $x=2$

$$\frac{1}{2}+\frac{1}{y}+\frac{1}{z}=\frac{3}{5}\Leftrightarrow\frac{1}{y}+\frac{1}{z}=\frac{3}{5}-\frac{1}{2}=\frac{1}{10}\Leftrightarrow\frac{z+y}{zy}=\frac{1}{10}\Leftrightarrow 10y+10z=yz\Leftrightarrow$$

$$\Leftrightarrow 10y+10z-yz-100=-100\Leftrightarrow(y-10)(10-z)=-100$$

$$\left.\begin{matrix}y-10=1\\10-z=-100\end{matrix}\right\}\Rightarrow y=11\,,\ z=110\qquad \left.\begin{matrix}y-10=2\\10-z=-50\end{matrix}\right\}\Rightarrow y=12\,,\ z=60$$

$$\left.\begin{matrix}y-10=4\\10-z=-25\end{matrix}\right\}\Rightarrow y=14\,,\ z=35\qquad \left.\begin{matrix}y-10=5\\10-z=-20\end{matrix}\right\}\Rightarrow y=15\,,\ z=30$$

$$\left.\begin{matrix}y-10=10\\10-z=-10\end{matrix}\right\}\Rightarrow y=20\,,\ z=20\qquad \left.\begin{matrix}y-10=20\\10-z=-5\end{matrix}\right\}\Rightarrow y=30\,,\ z=15$$

$$\left.\begin{matrix}y-10=25\\10-z=-4\end{matrix}\right\}\Rightarrow y=35\,,\ z=14\qquad \left.\begin{matrix}y-10=50\\10-z=-2\end{matrix}\right\}\Rightarrow y=60\,,\ z=12$$

$$\left.\begin{matrix}y-10=100\\10-z=-1\end{matrix}\right\}\Rightarrow y=110\,,\ z=11$$

Otra manera de verlo es la siguiente:

$$\frac{1}{y}+\frac{1}{z}=\frac{1}{10}\Leftrightarrow\frac{1}{z}=\frac{1}{10}-\frac{1}{y}=\frac{y-10}{10y}\Leftrightarrow$$

$$z=\frac{10y}{y-10}=\frac{10y-100+100}{y-10}=\frac{10(y-10)+100}{y-10}=10+\frac{100}{y-10}$$

De lo que se deduce que $z>10$ y que $y-10\,|\,100$

c) $x=3$

$$\frac{1}{3}+\frac{1}{y}+\frac{1}{z}=\frac{3}{5}\Leftrightarrow\frac{1}{y}+\frac{1}{z}=\frac{3}{5}-\frac{1}{3}=\frac{4}{15}\Leftrightarrow\frac{y+z}{yz}=\frac{4}{15}\Leftrightarrow 15y+15z=4yz\Leftrightarrow$$

$$60y+60z-16yz=0\Leftrightarrow 60y+60z-16yz-225=-255\Leftrightarrow(4y-15)(15-4z)=-225$$

$$\Leftrightarrow(4y-15)(4z-15)=225=3^2\cdot 5^2$$

$$\left.\begin{matrix}4y-15=25\\4z-15=9\end{matrix}\right\}\Rightarrow y=10, z=6$$

Obtenemos las soluciones (3, 4, 60) , (3, 5, 15) , (3, 6, 10) , (3, 10, 6) , (3, 15, 5) , (3, 60, 4).

d) $x=4$

$$\frac{1}{4}+\frac{1}{y}+\frac{1}{z}=\frac{3}{5}\Leftrightarrow\frac{1}{y}+\frac{1}{z}=\frac{3}{5}-\frac{1}{4}=\frac{4}{15}\Leftrightarrow\frac{y+z}{yz}=\frac{4}{15}$$

y la única solución aceptable es (4, 4, 10) y sus permutaciones.

e) $x=5$

$$\frac{1}{5}+\frac{1}{y}+\frac{1}{z}=\frac{3}{5}\Leftrightarrow\frac{1}{y}+\frac{1}{z}=\frac{3}{5}-\frac{1}{5}=\frac{2}{5}$$

y la única solución aceptable es (5, 5, 5)

10.7.6

En primer lugar vemos que esta ecuación es perfectamente simétrica, por lo que podemos suponer que las incógnitas están ordenadas:

$$1\le a\le b\le c\Rightarrow 1\ge\frac{1}{a}\ge\frac{1}{b}\ge\frac{1}{c}\Rightarrow 2\ge 1+\frac{1}{a}\ge 1+\frac{1}{b}\ge 1+\frac{1}{c}\Rightarrow\left(1+\frac{1}{a}\right)\left(1+\frac{1}{b}\right)\left(1+\frac{1}{c}\right)\le\left(1+\frac{1}{a}\right)^3$$

Así pues, para cualquier terna $a\le b\le c$ de soluciones, se cumplirá la desigualdad

$$2\le\left(1+\frac{1}{a}\right)^3$$

La función $f(x)=\left(1+\frac{1}{x}\right)^3$ es estrictamente decreciente, pues $1+\frac{1}{x}$ es estrictamente decreciente y x^3 es estrictamente creciente.

Por otro lado, observamos que

$$f(3)=\left(\frac{4}{3}\right)^3=\frac{64}{27}>2\ \text{ y }\ f(4)=\left(\frac{5}{4}\right)^3=\frac{125}{64}<2$$

Luego el valor de a (que, recordemos, es el mínimo de la lista) debe cumplir $a\le 3$. Veamos los casos posibles.

Para $a=1$:

$$2=\left(1+\frac{1}{1}\right)\left(1+\frac{1}{b}\right)\left(1+\frac{1}{c}\right)=2\left(1+\frac{1}{b}\right)\left(1+\frac{1}{c}\right)\Rightarrow\left(1+\frac{1}{b}\right)\left(1+\frac{1}{c}\right)=1$$

es imposible puesto que $\frac{1}{b},\frac{1}{c}>0$

Para $a=2$:

$$2=\left(1+\frac{1}{2}\right)\left(1+\frac{1}{b}\right)\left(1+\frac{1}{c}\right)=\frac{3}{2}\left(1+\frac{1}{b}\right)\left(1+\frac{1}{c}\right)\Leftrightarrow 4=3\left(1+\frac{1}{b}\right)\left(1+\frac{1}{c}\right)=3\left(\frac{b+1}{b}\right)\left(\frac{c+1}{c}\right)\Leftrightarrow$$

$$4bc=3(b+1)(c+1)=3(bc+b+c+1)=3bc+3b+3c+3\Leftrightarrow$$

$$0=bc-3b-3c-3$$

Completamos esta última ecuación:

$$0=bc-3b-3c-3=bc-3b-3c+9-12=(b-3)(c-3)-12\Leftrightarrow$$

$$12=(b-3)(c-3)$$

Las posibilidades son (recordemos que estamos suponiendo $b\le c$):

$$\left.\begin{matrix}1=b-3\\12=c-3\end{matrix}\right\}\Rightarrow b=4,c=15\ ;\ \left.\begin{matrix}2=b-3\\6=c-3\end{matrix}\right\}\Rightarrow b=5,c=9$$

$$\left.\begin{aligned} 3 &= b-3 \\ 4 &= c-3 \end{aligned}\right\} \Rightarrow b=6,\ c=7$$

Para $a=3$:

$$2=\left(1+\frac{1}{3}\right)\left(1+\frac{1}{b}\right)\left(1+\frac{1}{c}\right)=\frac{4}{3}\left(1+\frac{1}{b}\right)\left(1+\frac{1}{c}\right)\Leftrightarrow 6=4\left(1+\frac{1}{b}\right)\left(1+\frac{1}{c}\right)$$

$$\Leftrightarrow 3=2\left(1+\frac{1}{b}\right)\left(1+\frac{1}{c}\right)=2\left(\frac{b+1}{b}\right)\left(\frac{c+1}{c}\right)\Leftrightarrow$$

$$3bc=2(b+1)(c+1)=2bc+2b+2c+2\Leftrightarrow 0=bc-2b-2c-2$$

De nuevo completamos cuadrados para resolver esta ecuación:

$$0=bc-2b-2c-2=(b-2)(c-2)-6\Leftrightarrow 6=(b-2)(c-2)$$

$$\left.\begin{aligned} 1 &= b-2 \\ 6 &= c-2 \end{aligned}\right\} \Rightarrow b=3,\ c=8$$

$$\left.\begin{aligned} 2 &= b-2 \\ 3 &= c-2 \end{aligned}\right\} \Rightarrow b=4,\ c=5$$

Llegamos así a la lista final de posibles soluciones ordenadas:

$a=2, b=4, c=15$; $a=2, b=5, c=9$; $a=2, b=6, c=7$; $a=3, b=3, c=8$; $a=3, b=4, c=5$

El conjunto total de soluciones son todas las permutaciones posibles que se pueden realizar con las ternas anteriores.

Fuente de esta solución: https://youtu.be/iYZFWq6sEsc

10.7.7

Ver DE , problema #10.18

10.8.1

Un número de la forma $n = \frac{p_1 + p_2 + p_3 + p_4 + p_5}{5}$ es entero si y solo si 5 divide a la suma de estos cinco primos.

Haciendo pruebas con los números primos más pequeños llegamos al resultado $2+3+5+7+13=30$ y la media aritmética de esos cinco primos es $\frac{30}{5}=6$ (A).

10.8.2

Factorizamos el producto:

$$10\cdot 20\cdot 30\cdot ...\cdot 90 = 2^{16}\cdot 3^4\cdot 5^{10}\cdot 7^1$$

Y necesitamos una factorización cuyos exponentes sean todos pares.

Está claro que debemos eliminar el 7, luego tachar el 70, con lo que nos queda:

$$2^{15}\cdot 3^4\cdot 5^9$$

Si tachamos además el 10 nos queda la factorización

$$2^{14}\cdot 3^4\cdot 5^8$$

Cuyos exponentes son todos pares, es decir, es un cuadrado perfecto.

Luego necesitamos eliminar 2 (B)

10.8.3

Supongamos que

$$\begin{cases} p+q=a^2 \\ p+7q=b^2 \end{cases}$$

Para ciertos a,b que podemos suponer positivos. Luego

$$6q = p+7q-(p+q) = b^2-a^2 = (b-a)(b+a)$$

Luego b^2-a^2 es par, y por tanto a y b tienen la misma paridad. Pero entonces $(b-a)(b+a)$ es el producto de dos números pares, luego es múltiplo de 4. De aquí se deduce que q también debe ser par, y el único par primo es 2. Así pues, $q=2$, y por tanto:

$$(b-a)(b+a)=12$$

De todas las soluciones posibles del sistema (ver Apartado 10.3)

$$\begin{cases} b-a=2^x3^y \\ b+a=2^{2-x}3^{1-y} \end{cases}$$

La única con soluciones positivas es $a=2, b=4$, y finalmente $p=a^2-q=2^2-2=2$.

10.8.4

Está claro que si $p=q$ entonces $p^2+7pq+q^2=9p^2=(3p)^2$ es siempre un cuadrado perfecto. Supongamos que $p\neq q$.

Supongamos que $p^2+7pq+q^2=r^2$ para cierto entero r. Luego

$r^2 = p^2+7pq+q^2 = (p+q)^2+5pq \Rightarrow$

$5pq = r^2-(p+q)^2 = (r+p+q)(r-p-q)$

Puesto que a la izquierda tenemos 3 números primos, está claro que uno de los dos factores de la derecha es igual a uno de ellos y el otro al producto de los otros dos.
El factor $r+p+q$ es mayor que 5, luego tendrá que ser el producto de dos de los primos de la izquierda, tal vez de los tres, mientras que el factor $r-p-q$ deberá ser igual a p, q, 5 o 1.

Veamos los casos:

Caso 1.
$r-p-q=p \Rightarrow r=2p+q$, y la ecuación original se convierte en
$p^2+7pq+q^2=(2p+q)^2=4p^2+4pq+q^2 \Leftrightarrow 0=3p^2-3pq=3p(p-q) \Leftrightarrow$
$\Leftrightarrow \begin{cases} p=0 \\ p-q=0 \end{cases}$
Ninguno de estos dos casos es aceptable.

Caso 2.
$r-p-q=5 \Rightarrow r=p+q+5$, y la ecuación
$5pq=(r+p+q)(r-p-q)$
Se convierte en:
$pq=p+q+5+p+q=2p+2q+5 \Leftrightarrow 5=-2p-2q+pq=(p-2)(q-2)-4 \Leftrightarrow$
$9=(p-2)(q-2)$
Las soluciones de esta última ecuación son $p=q=5$; $p=3, q=11$; $p=11, q=3$.

Caso 3.
$r-p-q=1 \Rightarrow r+p+q=5pq$, y restando ambas ecuaciones obtenemos
$2p+2q=5pq-1 \Leftrightarrow 2p+2q+1=5pq$

Lo cual es imposible porque el lado de la derecha es mayor que el lado de la izquierda (solo se podría cumplir para $p=q=1$, caso que está descartado.

Así pues, las soluciones son $p=q$; $p=3, q=11$; $p=11, q=3$

Fuente de esta solución: https://math.stackexchange.com/questions/478802/prime-numbers-and-perfect-squares

10.8.5

Supongamos que $\frac{p+1}{2}=a^2$ y $\frac{p^2+1}{2}=b^2$ para ciertos enteros a, b.

Entonces, restando ambas expresiones tenemos
$$p(p-1)=p^2-p=p^2+1-(p+1)=2b^2-2a^2=2(b^2-a^2)=2(b-a)(b+a) \quad (*)$$

Por ser p un número primo, se debe cumplir $p \mid b-a$ o $p \mid b+a$.

Pero
$$2b^2=p^2+1<p^2+p^2=2p^2 \Rightarrow b<p$$
$$2a^2=p+1<2p^2 \Rightarrow a<p$$

Luego $b-a<p$ y $b+a<2p$

De $b-a<p$ se deduce que no se puede cumplir $p\mid b-a$, por lo que, forzosamente, $p\mid b+a$. Pero teniendo en cuenta que $b+a<2p$ solo se puede cumplir $b+a=p$, y por tanto la ecuación (*) se convierte en el sistema

$$\begin{cases} a+b=p \\ 2(b-a)=p-1 \end{cases} \Rightarrow 2(b-a)=a+b-1 \Rightarrow 2b-2a=a+b-1 \Rightarrow b-3a=-1 \Rightarrow b=3a-1$$

Y por tanto:

$$a+b=p \Rightarrow a+3a-1=p \Rightarrow 4a-1=p$$

Luego:

$$\frac{p+1}{2}=a^2 \Rightarrow \frac{4a-1+1}{2}=a^2 \Rightarrow 2a=a^2 \Rightarrow a=2 \Rightarrow p=4\cdot 2-1=7$$

Así pues, $p=7$ es la única solución aceptable. En efecto, $\frac{7+1}{2}=2^2$ y $\frac{7^2+1}{2}=5^2$

Fuente de esta solución: Soluciones oficiales (OMEC, página 433)

10.8.6

Primera versión.

Supongamos que $2n^2=d\,k$ con $k\geq 1$.

Supongamos, por otro lado, que $n^2+d=m^2$ para cierto entero m.

Por un lado, $n^2+d=m^2 \Rightarrow m^2>n^2$

Pero por otro lado,

$$n^2+d=m^2 \Rightarrow k\left(n^2+d\right)=km^2 \Rightarrow kn^2+kd=km^2 \Rightarrow kn^2+2n^2=km^2 \Rightarrow$$

$$n^2\left(k+2\right)=km^2 \Rightarrow kn^2<(k+2)n^2=km^2 \Rightarrow kn^2<km^2 \Rightarrow n^2<m^2$$

Llegando a contradicción.

Segunda versión.

Supongamos que $2n^2=d\,k$ con $k\geq 1$.

Supongamos, por otro lado, que $n^2+d=m^2$ para cierto entero m.

Entonces $m^2=n^2+\frac{2n^2}{k} \Rightarrow \left(k\,m\right)^2=k^2\left(n^2+\frac{2n^2}{k}\right)=n^2\left(k^2+2k\right)$

Luego k^2+2k también debe ser un cuadrado perfecto, pero esto es imposible, pues este número está entre los cuadrados de dos enteros consecutivos. En efecto:

$$k^2<k^2+2k<k^2+2k+1=(k+1)^2$$

10.8.7

Para $p=2$, $2p^4-p^2+16=44$ y no es un cuadrado perfecto.

Para $p=3$, $2p^4-p^2+16=169=13^2$ y sí es un cuadrado perfecto.

Para todo primo $p>3$, está claro que no puede ser múltiple de tres, luego $p\equiv 1,2\pmod 3$

$$p \equiv 1 \pmod 3 \Rightarrow 2p^4 - p^2 + 16 \equiv 2 \cdot 1 - 1 + 1 = 2 \pmod 3$$
$$p \equiv 2 \pmod 3 \Rightarrow 2 \cdot 2^4 - 2^2 + 16 \equiv 2 \cdot 1 - 1 + 1 = 2 \pmod 3$$

Por otro lado,

$$0^2 \equiv 0 \pmod 3,\ 1^2 \equiv 1 \pmod 3,\ 2^2 = 4 \equiv 1 \pmod 3$$

Luego es imposible que $2p^4 - p^2 + 16 = k^2$.

Así pues, $p = 3$ es la única solución.

Fuente de esta solución: Mathematical Excalibur Volume 21, Number 4, 2018

10.8.8

La ecuación es equivalente a

$$(4x-1)(4y-1) = 4z^2 + 1$$

Sea p un factor primo de $4x-1$. Entonces $4z^2 \equiv -1 \pmod p$. En efecto:

$$p \mid 4x-1 \Rightarrow 0 \equiv (4x-1)(4y-1) = 4z^2 + 1 \pmod p \Rightarrow 4z^2 \equiv -1 \pmod p$$

Luego $(2z)^2 \equiv -1 \pmod p$

Por otro lado, aplicando el Pequeño Teorema de Fermat, $(2z)^{p-1} \equiv 1 \pmod p$, y por tanto:

$$1 \equiv (2z)^{p-1} \equiv \left((2z)^2\right)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod p$$

Y por tanto $p \equiv 1 \pmod 4$. Aquí hemos aplicado $1 \equiv (-1)^k \pmod p \Leftrightarrow k$ es par, y por tanto

$$\frac{p-1}{2} = 2a \Leftrightarrow p - 1 = 4a \Leftrightarrow p = 4a + 1 \Leftrightarrow p \equiv 1 \pmod 4$$

Así pues, todo factor p primo de $4x-1$ cumple $p \equiv 1 \pmod 4$, por lo tanto, el producto de todos estos factores, que es el propio $4x-1$ también lo será:

$$4x - 1 \equiv 1 \pmod 4$$

Lo cual nos lleva al absurdo $-1 \equiv 1 \pmod 4$.

10.8.9

Es de sobra conocido que $t_n = 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$, luego queremos determinar los números de la forma $\frac{n(n+1)}{2}$ que son cuadrados perfectos:

$$t_n = \frac{n(n+1)}{2} = m^2 \Leftrightarrow n(n+1) = 2m^2 \Leftrightarrow \frac{n}{2}(n+1) = m^2$$

para cierto entero positivo m.

Puesto que dos números consecutivos son coprimos, de la igualdad $n(n+1) = 2m^2$ podemos esperar que ambos números sean "casi" cuadrados perfectos, exceptuando un factor 2 "extra":

$a^2 = n$ es un cuadrado perfecto y $n-1 = 2b^2$ es otro cuadrado perfecto multiplicado por 2.

Puesto que n es par, n+1 será impar, y por tanto su cuadrado será impar. Esto nos evita chequear cuadrados de números pares.

$$a=3 \to n=a^2=3^2=9 \to n-1=8=2\cdot 4=2\cdot 2^2$$
$$a=5 \to n=a^2=5^2=25 \to n-1=24=2\cdot 12$$
$$a=7 \to n=a^2=7^2=49 \to n-1=48=2\cdot 24$$
$$a=9 \to n=a^2=9^2=81 \to n-1=80=2\cdot 40$$
$$a=11 \to n=a^2=11^2=121 \to n-1=120=2\cdot 60$$
$$a=13 \to n=a^2=13^2=169 \to n-1=168=2\cdot 84$$
$$a=15 \to n=a^2=15^2=225 \to n-1=224=2\cdot 112$$
$$a=17 \to n=a^2=17^2=289 \to n-1=288=2\cdot 144=2\cdot 12^2$$

Ya hemos encontrado un número que se adapta a nuestras condiciones:

$$2\cdot(12\cdot 17)^2 = 2\cdot 12^2\cdot 17^2 = 288\cdot 289$$

Y por tanto:

$$t_8 = \frac{288\cdot 289}{2} = 41616 \Rightarrow 4+1+6+1+6=18 \quad \text{(D)}$$

10.8.10

Pasando a módulo 8: $8m-7=n^2 \Rightarrow n^2=-7\equiv 1 \pmod 8$

Las soluciones de la congruencia $n^2 \equiv 1 \pmod 8$ son: $1, 3, 5, 7 \pmod 8$, es decir:

$$n=8k+1\ ,\ n=8k+3\ ,\ n=8k+5\ ,\ n=8k+7$$

Para cualquier entero k, y en todo caso n^2+7 será divisible entre 8 y por tanto: $m=\frac{n^2+7}{8}$

Segunda parte:

$$m=\frac{n^2+7}{8} \geq 1959 \Leftrightarrow n^2+7 \geq 1959\cdot 8 \Leftrightarrow n^2 \geq 1959\cdot 8-7=15665$$

El primer cuadrado superior a 15665 es $125^2=15625 \to 15625+7$, pero no sirve pues es impar y por tanto no es divisible entre 8.

El segundo cuadrado superior a 15665 es $126^2=15876 \to 15876+7$, pero no sirve pues es impar y por tanto no es divisible entre 8.

El tercer cuadrado superior a 15665 es $127^2=16129 \to 16129+7=16136=8\cdot 2017$, luego $m=2017$.

10.8.11

El valor y es solución si y solo si lo es $-y$, así que podemos suponer $y>0$.

Si $x=0$ entonces la ecuación es $y^2=1+2^0+2^{2\cdot 0+1}=1+1+2=4 \Rightarrow y=\pm 2$, llegando a las soluciones: $(0,\pm 2)$.

Supongamos que $x>0$.

$1+2^x+2^{2x+1}=y^2 \Leftrightarrow 2^x\left(1+2\cdot 2^x\right)=2^x+2\cdot 2^{2x}=2^x+2^{2x+1}=y^2-1=(y+1)(y-1)\Leftrightarrow$
$2^x\left(1+2\cdot 2^x\right)=(y+1)(y-1)$

De esta última igualdad deducimos que y tiene que ser impar, luego $y+1$, $y-1$ son pares. Pasando a módulo 4, tenemos

$y=4q+0$ descartado, pues es par.
$y=4q+1 \Rightarrow y-1$ es múltiple de 4, $y+1$ es múltiple de 2.
$y=4q+2$ descartado, pues es par.
$y=4q+3 \Rightarrow y+1$ es múltiple de 4, $y-1$ es múltiple de 2.

En todo caso, $(y+1)(y-1)$ es múltiplo de 8, pero $1+2\cdot 2^x$ es impar, luego $x\geq 3$.
$y=4q\pm 1\Rightarrow y^2-1=16q^2\pm 8q+1-1=16q^2\pm 8q=8q(2q\pm 1)$ y la ecuación queda

$2^x\left(1+2\cdot 2^x\right)=y^2-1\Leftrightarrow$
$2^x\left(1+2\cdot 2^x\right)=8q(2q\pm 1)=2^3q(2q\pm 1)\Leftrightarrow$
$2^{x-3}\left(1+2\cdot 2^x\right)=q(2q\pm 1)\Rightarrow q\mid 2^{x-3}\Rightarrow q=2^{x-3}k\Rightarrow y=4q\pm 1=2^2\cdot 2^{x-3}q-1=2^{x-1}k\pm 1$

Además, k debe ser impar, pues en caso contrario
$y=2^xt\pm 1\Rightarrow y^2=2^{2x}t^2+2^{x+1}t+1\Rightarrow y^2-1=2^{2x}t^2+2^{x+1}t=2^x(2^xt^2+2t)$
y la ecuación queda
$2^x\left(1+2\cdot 2^x\right)=y^2-1=2^x(2^xt^2+2t)\Rightarrow 1+2\cdot 2^x=2^xt^2+2t$, impar igual a par, absurdo.

Así pues, $y=2^{x-1}k+1$ o bien $y=2^{x-1}k-1$ para cierto $k\geq 1$ impar.

Primer caso: $y=2^{x-1}k+1$
Entonces $y^2-1=2^{2x-2}k^2+2^xk+1-1=2^x\left(2^{x-2}k^2+k\right)$ y la ecuación queda
$2^x\left(1+2^{x+1}\right)=2^x\left(2^{x-2}k^2+k\right)\Rightarrow 1+2^{x+1}=2^{x-2}k^2+k\Rightarrow$
$1-k=2^{x-2}k^2-2^{x+1}=2^{x-2}\left(k^2-2^3\right)\Leftrightarrow$
$1-k=2^{x-2}\left(k^2-8\right)$ (*)

Luego $k\geq 1\Rightarrow 2^{x-2}\left(k^2-8\right)\leq 0\Rightarrow k^2-8\leq 0\Rightarrow k^2\leq 8\Rightarrow k=1,2$

Hemos dicho anteriormente que k era impar, luego solo nos queda la posibilidad $k=1$.

Pero sustituyendo $k=1$ en (*) tenemos $1-1=2^{x-2}\left(1^2-8\right)\Leftrightarrow 0=2^{x-2}(-7)$ absurdo. No hay ninguna solución posible.

Segundo caso: $y=2^{x-1}k-1$
De la misma manera, Entonces $y^2-1=2^{2x-2}k^2-2^xk+1-1=2^x\left(2^{x-2}k^2-k\right)$ y la ecuación queda
$2^x\left(1+2^{x+1}\right)=2^x\left(2^{x-2}k^2-k\right)\Rightarrow 1+2^{x+1}=2^{x-2}k^2-k\Rightarrow$
$1+k=2^{x-2}k^2-2^{x+1}=2^{x-2}\left(k^2-2^3\right)\Leftrightarrow$
$1+k=2^{x-2}\left(k^2-8\right)$ (**)

Luego
$$1+k=2^{x-2}\left(k^2-8\right)\geq 2\left(k^2-8\right)\Leftrightarrow$$
$$2k^2-k-17\leq 0\Rightarrow k\leq 3\Rightarrow k=1,3$$

Sustituyendo en (**) vemos que $k=1$ no es aceptable:
$$2=1+1=2^{x-2}\left(1^2-8\right)=2^{x-2}\left(-7\right)$$

Así que la única opción aceptable es $k=3$, que sustituyendo en (**) nos determina el valor x:
$$1+3=2^{x-2}\left(3^2-8\right)\Leftrightarrow 4=2^{x-2}\left(1\right)\Leftrightarrow x=4$$

Y finalmente $y=2^{x-1}k-1=2^{4-1}\cdot 3-1=24-1=23$

Las soluciones son, por tanto, $x=4$, $y=\pm 23$.

Comprobemos que, efectivamente, los valores obtenidos satisfacen la ecuación:
$1+2^4+2^{2\cdot 4+1}=1+16+512=529=23^2$.

El problema tiene cuatro soluciones: $x=0, y=\pm 2$ y $x=4, y=\pm 23$.

Fuente de la solución: Soluciones oficiales (SE, página 880)

10.8.12
Vemos que la parte de la izquierda es una diferencia de dos impares, luego es un número par. Así pues, z^2 es par, y por tanto z es par, luego z^2 es divisible entre 4, y por tanto $3^x-5^y\equiv 0\pmod 4$.
$$0\equiv 3^x-5^y\equiv(-1)^x-1^y\equiv(-1)^x-1\pmod 4\Leftrightarrow x \text{ es par}\Leftrightarrow x=2a.$$
Sustituyendo en la ecuación tenemos
$$3^{2a}-5^y=z^2\Leftrightarrow 5^y=3^{2a}-z^2=\left(3^a\right)^k-z^2=\left(3^a-z\right)\left(3^a+z\right)$$
Luego
$$\begin{cases}3^a-z=5^b\\3^a+z=5^{y-b}\end{cases}\quad\text{para cierto } 0\leq b\leq y.$$
Sumando las dos ecuaciones anteriores llegamos a $2\cdot 3^a=5^b+5^{y-b}$.

Supongamos que $0<b<y$. Entonces la parte de la derecha de la ecuación será divisible entre 5, pero esto es absurdo, porque $2\cdot 3^a$ no puede ser divisible entre 5. Así es que solo se pueden dar dos casos: $b=0$ o $b=y$.
$$b=0\Rightarrow\begin{cases}3^a-z=1\\3^a+z=5^y\end{cases}\Rightarrow 2\cdot 3^a=5^y+1$$
$$b=y\Rightarrow\begin{cases}3^a-z=5^b\\3^a+z=5^0=1\end{cases}\Rightarrow 2\cdot 3^a=5^y+1$$
En ambos casos llegamos a la ecuación $2\cdot 3^a=5^y+1$.
Supongamos que $a\geq 2$. Entonces la parte izquierda es múltiplo de 9, y por tanto

$5^y+1\equiv 0\pmod 9\Leftrightarrow 5^y\equiv -1\pmod 9\Leftrightarrow y=6e+3$.

Pero en este caso $5^y+1=5^{6e+3}+1=5^3\cdot\left(5^6\right)^e+1$

y $5^3\equiv -1\pmod 7\Rightarrow 5^6\equiv (-1)^2\equiv 1\pmod 7\Rightarrow 5^3\cdot\left(5^6\right)^e+1\equiv (-1)\cdot 1^e+1\equiv -1+1\equiv 0\pmod 7$

pero $2\cdot 3^a$ no puede ser múltiplo de 7, llegando a contradicción.

Así pues, $a=1\Rightarrow 2\cdot 3=5^y+1\Rightarrow y=1\Rightarrow x=2\cdot 1=2\Rightarrow 3^x-5^y=9-5=4=2^2$, llegando a las únicas soluciones posibles $x=2, y=1, z=\pm 2$.

10.8.13

En primer lugar vemos que, puesto que el valor a_{n+1} solo depende de a_n, cada vez que se produzca una repetición de un valor: $A=a_n=a_{n+k}$ se generará una secuencia periódica $A=a_n=a_{n+k}=a_{n+2k}=a_{n+3k}=\ldots$. Así pues, estamos buscando los valores de a_0 para los que se genere una secuencia periódica.

Primer lema. Si $a_n\equiv 2\pmod 3$, entonces la sucesión es estrictamente creciente, y por tanto no periódica.

Demostración. Para todo $m>n$, a_m no es un cuadrado perfecto. En efecto, solo hace falta ver que $0^2\equiv 0\pmod 3$, $1^2\equiv 1\pmod 3$ y $2^2=4\equiv 1\pmod 3$. Por lo tanto, la sucesión será estrictamente creciente, y por tanto no periódica.

Segundo lema. Si $a_n\not\equiv 2\pmod 3$ y $a_n>9$, entonce exitirá un $m>n$ para el cual $a_m<a_n$.

Demostración. Sea t^2 el mayor cuadrado perfecto menor que 9. Puesto que suponemos $a_n>9$, se cumplirá

$$3^2\le t^2<a_n$$

Los siguientes cuadrados perfectos serán $(t+1)^2$, $(t+2)^2$ y $(t+3)^2$, cumpliendo

$$3^2\le t^2<a_n<(t+1)^2.$$

Estos tres números pertenecen a al menos dos clases modulares diferentes, luego podemos garantizar que en la sucesión $a_n, a_n+3, a_n+6, \ldots$ se alcanzará uno de estos tres números. Es decir, $a_{m-1}=(t+1)^2$ o bien $a_{m-1}=(t+2)^2$ o bien $a_{m-1}=(t+2)^2$, y por tanto $a_m=t+1$ o bien $a_m=t+2$ o bien $a_m=t+3$. En todo caso se cumplirá $a_m\le t+3<t^2<a_n$ tal y como queríamos demostrar.

Tercer lema. Si $a_n\equiv 0\pmod 3$, entonces existirá un índice $m>n$ tal que $a_m=3$.

En primer lugar, vemos que esto se cumple para $a_n=6$ y $a_n=9$. Supongamos que $a_n>9$. Sea $j>n$ tal que a_j es el valor mínimo del conjunto $\{a_{n+1}, a_{n+2}, a_{n+3}, \ldots\}$. Forzosamente se cumplirá $a_j\le 9$, pues de lo contrario podríamos aplicar el segundo lema para encontrar un elemento menor, lo que nos llevaría a contradicción. Así pues, $a_j\in\{3, 6, 9\}$, y en los tres casos la sucesión sigue hasta el valor 3.

Cuarto lema. Si $a_n\equiv 1\pmod 3$, entonces existirá un índice $m>n$ tal que $a_n\equiv 2\pmod 3$, y por lo tanto la sucesión continuará de forma creciente, y por tanto no periódica.

En el caso $a_n=4\to a_{n+1}=2$ está claro.

En el caso $a_n = 7$, la sucesión sigue 10, 13, 16, 4, 2 y también es cierto.
Supongamos $a_n \geq 10$. Como en el lema anterior, sea $j > n$ tal que a_j es el valor mínimo del conjunto $\{a_{n+1}, a_{n+2}, a_{n+3}, ...\}$. Ninguno de estos elementos son múltiples de 3. Supongamos que $a_j \equiv 1 \pmod 3$. Entonces por el segundo lema forzosamente $a_j \leq 9$ o llegaríamos a contradicción con la minimalidad de a_j. Así pues, $a_j \in \{4, 7\}$, y por tanto en todo caso se llega a $a_m = 2$, contradiciendo la minimalidad de a_j. Así pues, $a_j \equiv 2 \pmod 3$. Finalmente, aplicando el primer lema, la sucesión continuará con valores que no son cuadrados perfectos, luego será estrictamente decreciente, y por tanto no periódica.

Así pues, los únicos números que satisfacen la condición del enunciado son los múltiplos de 3.

Fuente de esta solución: Soluciones oficiales (Compendium IMO pág. 1708).

10.9.1
Denotando p a las personas, h a los caballos, s a las ovejas, c a las vacas y d a los patos, tenemos

$$\left.\begin{array}{l} p = 3h \\ s = 4c \\ d = 3p \end{array}\right\} \Rightarrow \left.\begin{array}{l} d = 9h \\ s = 4c \end{array}\right\} \Rightarrow T = p + h + s + c + d = 3h + h + 4c + c + 9h = 13h + 5c$$

Aplicando ahora el teorema "Chicken McNugget", el valor máximo no representable es $T = 13 \cdot 5 - 13 - 5 = 47$, luego la solución es (B).

10.9.2
El problema que se plantea es estudiar todas las combinaciones posibles

$$x \cdot 5 + y \cdot n + z \cdot (n+1)$$

con enteros $x, y, z \geq 0$

Y determinar aquellos enteros positivos n para los cuales 91 no se puede formar pero sí se pueden formar 92, 93, 94…

Está claro que, independientemente del valor n, se pueden formar todos los múltiplos de 5, pues basta ir dando valores a x, con $y = z = 0$.

Para un valor n cualquiera, está claro que podremos formar seguro todos los valores de la forma n, $n+5$, $n+10$, $n+15$,… También todos los valores de la forma $n+1$, $n+1+5 = n+6$, $n+1+10 = n+11$,…

Todo esto nos indica que la clave para resolver este problema es pasar a módulo 5:

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15

91	92	93	94	95
96	97	98	99	100

Aplicamos el Teorema "Chicken McNugget", a las combinaciones 5 y n:

$$91 = 5n - 5 - n \Rightarrow n = 24$$

Luego podemos garantizar que $n \geq 24$.

Primer caso: $n \equiv 1 \pmod 5$

Supongamos que n se encuentra en la primera columna, es decir, que $n \equiv 1 \pmod 5$.

Vemos que 91 también está en la primera columna, luego nos obliga a $n > 91$, es decir: $n = 96, 101, \ldots$

Pero entonces no podríamos obtener 92 (ni 93, 94…) con lo que dicho número no es aceptable.

Segundo caso: $n \equiv 2 \pmod 5$

Si n se encuentra en la segunda columna, $n+1$ se encontrará en la tercera, y por tanto $2n$ se encontrará en la cuarta. En efecto:

$$n = 5k + 2 \Rightarrow 2n = 2(5k + 2) = 10k + 4 \equiv 4 \pmod 5$$

También vemos que $2(n+1) = 2n + 2 \equiv 1 \pmod 5$ se puede obtener, y está en la primera columna.

Luego $2(n+1) \neq 91$, y el primer candidato interesante sería el siguiente: $2(n+1) = 96$

$$2(n+1) = 96 \Rightarrow n = 47$$

Comprobamos que, efectivamente, $n = 47$ satisface las condiciones del enunciado:

Están todos los múltiplos de 47, en particular $92 = 47 + 45 = 47 + 9 \cdot 5$, todos los múltiplos de 48, $2 \cdot 47 = 94$ y todos los múltiplos de 94, y observamos que 91 no se puede representar como combinación de 47, 48 y 5, pero sí podemos representar $96 = 2(47+1) = 2 \cdot 48$.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
	47	48		
91	92	93	94	95
96	97	98	99	100

Tercer caso: $n \equiv 3 \pmod 5$

$n \equiv 3 \pmod 5 \Rightarrow 2n \equiv 6 \equiv 1 \pmod 5$, y por tanto $2n$ se encontrará en la primera columna. Como en el caso anterior, deducimos que $2n \neq 91$ y el primer candidato interesante sería el siguiente: $2n = 96 \Rightarrow n = 48$

Pero con este valor nos encontramos con un problema en la segunda columna: No se puede representar 92, y por tanto no es válido.

En efecto, todo consiste en ir viendo las posibles combinaciones:

$$x=0, y=1, z=1 \Rightarrow x\cdot 5+y\cdot 48+z\cdot 49=97$$
$$x=1, y=1, z=1 \Rightarrow x\cdot 5+y\cdot 48+z\cdot 49=102$$
$$x=9, y=1, z=0 \Rightarrow x\cdot 5+y\cdot 48+z\cdot 49=93$$
$$\ldots$$

Cuarto caso: $n\equiv 4 \pmod 5$

En este caso $n+1\equiv 5 \pmod 5$ y es redundante, $2n\equiv 8\equiv 3 \pmod 5$, $3n\equiv 12\equiv 2 \pmod 5$ y $4n\equiv 1 \pmod 5$. Como en los casos anteriores, imponemos la condición

$$4n=96 \Rightarrow n=24$$

Y vemos que con este valor todas las cinco columnas están cubiertas, es decir, es una segunda solución al problema.

Quinto caso: $n\equiv 5\equiv 0 \pmod 5$

En este caso tendríamos $n+1\equiv 1 \pmod 5$, es decir, en la primera columna, y por tanto $n+1>91 \Rightarrow n\geq 92$. El primer candidato sería $n=95$, pero con este valor no podríamos formar 92 (ni 93…), luego no es aceptable.

Así pues, las soluciones de este problema son $n=24$ y $n=47$.

Fuente de esta solución: Vídeo "Momentum Learning" https://youtu.be/fTZP2e-_rjA

10.9.3

Si $(a,b)>1$ existirían infinitas puntuaciones no alcanzables, pues todas las puntuaciones posibles serían múltiples de (a,b). Así pues, $(a,b)=1$.

En este caso, podemos aplicar el teorema anterior que dice que existirán exactamente $\frac{(a-1)(b-1)}{2}$ puntuaciones no alcanzables:

$$\frac{(a-1)(b-1)}{2}=30 \Leftrightarrow (a-1)(b-1)=70=2\cdot 5\cdot 7.$$

Puesto que además sabemos que $a>b$ y $(a,b)=1$, las posibilidades son las siguientes:

$$a-1=10, b-1=7 \Rightarrow a=11, b=8$$
$$a-1=70, b-1=1 \Rightarrow a=71, b=2$$

Puesto que $58=0\cdot 71+29\cdot 2$, descartamos la segunda opción, y por tanto la única solución válida es $a=11, b=8$.

Fuente de esta solución: Number Theory for Mathematical Contests (David A. Santos) pág. 57

10.9.4

La columna más baja será de $4\cdot 94=376$, y la columna más alta será de $19\cdot 94=1786$.

Como nos piden determinar el número de alturas diferentes, podemos simplificar el problema con el siguiente argumento:

Cada ladrillo de 4×10×19 aportará un incremento de altura de 4, 10 o 19, o equivalentemente, un incremento de altura de 0, 6 y 15. Pero estos tres números son múltiples de 3, luego podemos reducir nuestro problema a determinar todos los incrementos de altura de 0, 2 y 5.

Así pues, tenemos una colección de incrementos entre $0\cdot 94=0$ y $5\cdot 94=470$.

Por un lado, no todas las combinaciones posibles de incrementos $n=2x+5y$ son posibles. Sabemos por el Teorema de Frobenius que se podrán dar todos los incrementos

$$n>2\cdot 5-2-5=3$$

Para valores menores de 3 determinamos los casos posibles uno a uno:

$$0=2\cdot 0+5\cdot 0$$
$$2=2\cdot 1+5\cdot 0$$

Luego no serán aceptables los incrementos 1 y 3.

Pero también debemos considerar que tenemos un tope de 470. Y vemos que es lo mismo subir 2 que bajar 3. Por ejemplo, los valores más altos son:

$$464=2\cdot 2+92\cdot 5=470-(2\cdot 3+0\cdot 5)$$
$$465=0\cdot 2+93\cdot 5=470-(0\cdot 3+1\cdot 5)$$
$$466=???$$
$$467=1\cdot 2+93\cdot 5=470-(1\cdot 3+0\cdot 5)$$
$$468=???$$
$$469=???$$
$$470=0\cdot 2+94\cdot 5=470-(0\cdot 3+0\cdot 5)$$

Es decir, tenemos que descartar las combinaciones imposibles de la forma $m=3x+5y$

De nuevo, aplicando el Teorema de Frobenius, garantizaremos todos los valores de

$$m>3\cdot 5-3-5=7.$$

Entre 0 y 7 se pueden alcanzar los valores siguientes:

$$0=5\cdot 0+3\cdot 0$$
$$3=5\cdot 0+3\cdot 1$$
$$5=5\cdot 1+3\cdot 0$$
$$6=5\cdot 0+3\cdot 2$$

No es posible encontrar soluciones para $m=1,2,4,7$.

Así pues, tenemos $470+1-2-4=465$ incrementos diferentes, que corresponderán a 465 alturas diferentes de la torre.

Fuente de esta solución: http://www.artofproblemsolving.com/

10.9.5

Estamos estudiando todas las combinaciones posibles $6a+10b+15c$ con $0\le a,b,c$ enteros. Sabemos que si n, m son coprimos, el "número de Frobenius" asociado, es decir, el mayor entero que no se puede representar de la forma $\alpha n+\beta m$, con $0\le \alpha,\beta$ es $nm-n-m$ (Ver Teoria de Números 20.10).

$6a+10b+15c=3(2a+5c)+10b$ y puesto que 3 y 10 son coprimos, podemos aplicar la fórmula anterior para garantizar que el máximo entero no representable es $3\cdot 10-3-10=17$.

Pero ahora tenemos que aplicar la fórmula del número de Frobenius a $2a+5c$, y su máximo entero no representable es $2\cdot 5-2-5=3$.

Luego también podemos tener problemas cuando $2a+5c=3$. En este caso los valores serán:

$$3(2a+5c)+10b=3\cdot 3+10b=9+10b$$

$b=2\rightarrow 9+10\cdot 2=29$, y observamos que este número no se puede escribir de ninguna otra forma $6a+10b+15c$, luego 29 tampoco es representable.

Sin embargo, si $b\geq 3$, entonces

$$9+10b=9+10(b-3+3)=9+10(b-3)+30=39+10(b-3)=3\cdot 13+10(b-3)$$

y 13 sí es representable $2a+5c=2\cdot 4+5\cdot 1$.

Así pues, el valor máximo no representable de la forma $6a+10b+15c$ es 29, y la respuesta correcta es 2+9=11 (D).

También podría haber problemas en los números de la forma $2a+5c=2$, pero entonces serían de la forma

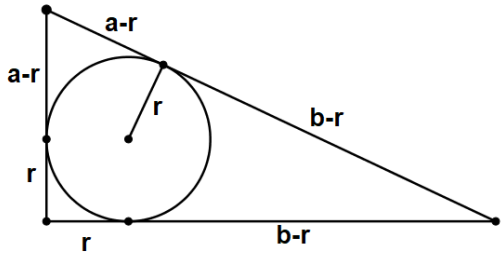
$3(2a+5c)+10b=3\cdot 2+10b=6\cdot 1+10b$, y estos números son perfectamente representables.

Finalmente, también podría haber problemas en los números de la forma $2a+5c=1$, pero entonces serían de la forma

$$3(2a+5c)+10b=3+10b, b\geq 3\Rightarrow 3+10b=3+10(b-3+3)=3+10(b-3)+30=$$
$$=33+10(b-3)=3\cdot 11+10(b-3)$$
,

10.10.1

En primer lugar consideremos los triángulos de catetos a, b y hipotenusa c, con una circunferencia inscrita de radio r. Sabemos que los segmentos tangentes a una circunferencia por un punto exterior son congruentes, luego deducimos que $c=a-r+b-r=a+b-2r$



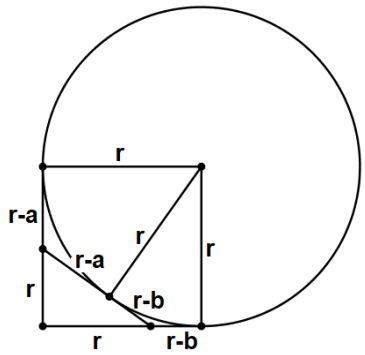
Por otro lado, aplicando Pitágoras, $c^2=a^2+b^2$, luego

$$\sqrt{a^2+b^2}=a+b-2r\Rightarrow a^2+b^2=(a+b-2r)^2=a^2+b^2+2ab-4ar-4br+4r^2$$
$$\Rightarrow 0=2ab-4ar-4br+4r^2\Rightarrow 0=ab-2ar-2br+2r^2$$
$$\Rightarrow 2ar+2br-ab=2r^2$$

Ahora factorizamos esta expresión mediante el llamado **Simon's Favorite Factoring Trick** (SFFT):

$$2r^2 = 2ar + 2br - ab \Leftrightarrow -2r^2 = ab - 2ar - 2br = (a-2r)(b-2r) - 4r^2 \Leftrightarrow$$
$$-2r^2 + 4r^2 = (a-2r)(b-2r) \Leftrightarrow 2r^2 = (a-2r)(b-2r)$$

Si ahora consideramos los triángulos de catetos a y b y hipotenusa c, con una circunferencia excrita de radio r:



y teniendo en cuenta de nuevo que segmentos tangentes son siempre congruentes, vemos que se cumple

$$c = r - a + r - b = 2r - a - b \Rightarrow \sqrt{a^2 + b^2} = 2r - a - b \Rightarrow a^2 + b^2 = (2r - a - b)^2$$

obteniendo la misma ecuación anterior.

Así pues, buscamos el valor mínimo de r para el cual existan 14 parejas (a_i, b_i) generando 14 segmentos distintos con las condiciones del enunciado, es decir, $2r^2 = (a-2r)(b-2r)$.

Es natural suponer un valor de r con muchos divisores, por lo que podemos especular que $r = 6$ es un buen candidato. Para este valor tendremos

$$(a-12)(b-12) = 2 \cdot 6^2 = 2^3 \cdot 3^2$$

Las posibles soluciones son:

(-60 , 11) , (-24 , 10) , (-12 , 9) , (-6 , 8) , (0 , 6) , (3 , 4) , (4 , 3)
(6 , 0) , (8 , -6) , (9 , -12) , (10 , -24) , (11 , -60) , (13 , 84) , (14 , 48)
(15 , 36) , (16 , 30) , (18 , 24) , (20 , 21) , (21 , 20) , (24 , 18)
(30 , 16) , (36 , 15) , (48 , 14) , (84 , 13)

Vemos claramente que el mayor valor de c posible será

$$a = 84 \Rightarrow b = 13 \Rightarrow c = \sqrt{84^2 + 13^2} = 85$$

Y el menor valor posible de c será

$$a = 3 \Rightarrow b = 4 \Rightarrow c = \sqrt{3^2 + 4^2} = 5$$

Y por lo tanto, finalmente, la razón pedida es $\frac{85}{5} = 17$ (E).

Se puede comprobar que para valores de r menores que 6 no aparecen tantas soluciones, y no se llega al mínimo de 14 exigidas en el enunciado.

Fuente de esta solución: https://artofproblemsolving.com/wiki/index.php?title=2022_AMC_12A_Problems/Problem_25

10.11.1

$2009 = 7^2 \cdot 41$ luego

$$\sqrt{a}+\sqrt{b}=\sqrt{2009}=7\sqrt{41}\Rightarrow\sqrt{a}=7\sqrt{41}-\sqrt{b}\Rightarrow$$
$$\Rightarrow a=\left(7\sqrt{41}-\sqrt{b}\right)^2=7^2\cdot 41+b-2\cdot 7\sqrt{41}\sqrt{b}=7^2\cdot 41+b-2\cdot 7\sqrt{41b}$$

Sabemos que a es un entero, y en la parte de la derecha de la igualdad, el único elemento susceptible de no ser entero es $\sqrt{41b}$. Luego $\sqrt{41b}$ también debe ser entero, y puesto que 41 es primo, deducimos que b es un múltiplo de 41 multiplicado por un cuadrado perfecto. De la misma forma deducimos que a debe ser un múltiplo de 41 multiplicado por un cuadrado perfecto:

$$\left.\begin{matrix}a=41x^2\\ b=41y^2\end{matrix}\right\}\Rightarrow\sqrt{a}+\sqrt{b}=\sqrt{41x^2}+\sqrt{41y^2}=\sqrt{41}x+\sqrt{41}y=7\sqrt{41}\Leftrightarrow x+y=7$$

Buscamos parejas $0\le x,y$ tales que $x+y=7$:

$$x=0,y=7\Rightarrow a=41\cdot 0^2,b=41\cdot 7^2$$
$$x=1,y=6\Rightarrow a=41\cdot 1^2,b=41\cdot 6^2$$
$$x=2,y=5\Rightarrow a=41\cdot 2^2,b=41\cdot 5^2$$
$$x=3,y=4\Rightarrow a=41\cdot 3^2,b=41\cdot 4^2$$

Y las tres que quedan, invirtiendo los valores de x e y. Son ocho soluciones en total:
(0 , 2009) , (41 , 1476) , (164 , 1025) , (369 , 656) , (656 , 369) , (1025 , 164) , (1476 , 41) , (2009 , 0)

Fuente: https://youtu.be/quECgYPNCXw

10.11.2

$$\frac{1}{x}+\frac{2}{y}-\frac{3}{z}=1\Leftrightarrow\frac{1}{x}+\frac{2}{y}=1+\frac{3}{z}$$

Si $x,y\ge 3\Rightarrow\frac{1}{x}+\frac{2}{y}\le\frac{1}{3}+\frac{2}{3}=1<1+\frac{3}{z}$ para todo $z\ge 1$, y la ecuación no tendrá solución.

Caso 1. $x=1$.

$1+\frac{2}{y}=1+\frac{3}{z}\Leftrightarrow\frac{2}{y}=\frac{3}{z}\Leftrightarrow 2z=3y$, cuyas soluciones son todas las ternas de la forma

$$\begin{cases}x=1\\ y=2k\quad,k>1\\ z=3k\end{cases}$$

En efecto, $\frac{1}{1}+\frac{2}{2k}-\frac{3}{3k}=1+\frac{1}{k}-\frac{1}{k}=1$

Caso 2: $y=1$

$$\frac{1}{x}+\frac{2}{1}=1+\frac{3}{z}\Leftrightarrow\frac{1}{x}+2=1+\frac{3}{z}\Leftrightarrow\frac{1}{x}+1=\frac{3}{z}\Leftrightarrow 1=\frac{3}{z}-\frac{1}{x}\Leftrightarrow 1=\frac{3x-z}{xz}$$
$$\Leftrightarrow xz-3x+z=0\Leftrightarrow(x+1)(z-3)+3=0\Leftrightarrow(x+1)(z-3)=-3$$

Puesto que $x>1\Rightarrow x+1>2$, la única solución posible es

$$\left.\begin{array}{l} x+1=3 \\ z-3=-1 \end{array}\right\} \Rightarrow \left.\begin{array}{l} x=2 \\ z=2 \end{array}\right\}$$

En efecto: $\frac{1}{2}+\frac{1}{1}-\frac{3}{2}=1$

A partir de aquí podemos suponer $x, y > 1$

Caso 3. $x = 2$.

$\frac{1}{2}+\frac{2}{y}=1+\frac{3}{z} \Leftrightarrow \frac{2}{y}=\frac{1}{2}+\frac{3}{z}=\frac{z+6}{2z} \Leftrightarrow 4z = y(z+6) = yz+6y \Leftrightarrow 4z - yz - 6y = 0 \Leftrightarrow$

$\Leftrightarrow (4-y)(z+6) - 24 = 0 \Leftrightarrow (4-y)(z+6) = 24$

$z+6$ es positivo, luego $4-y>0 \Rightarrow 1<y<4$

$y=2 \Rightarrow 2(z+6)=24 \Rightarrow z+6=12 \Rightarrow z=6$, obteniendo la solución $x=2, y=2, z=6$

$y=3 \Rightarrow z+6=24 \Rightarrow z=18$, obteniendo la solución $x=2, y=3, z=18$

Caso 4. $y = 2$

$\frac{1}{x}+\frac{2}{2}=1+\frac{3}{z} \Leftrightarrow \frac{1}{x}=\frac{3}{z} \Leftrightarrow \frac{1}{x}=\frac{3}{z} \Leftrightarrow z=3x$ dando lugar al conjunto de soluciones

$$\begin{cases} x = k \\ y = 1 \quad , k > 1 \\ z = 3k \end{cases}$$

En efecto: $\frac{1}{k}+\frac{2}{1}-\frac{3}{k}=\frac{1}{k}-\frac{3}{k}+2=\frac{k-3k}{k}+2=\frac{-2k}{k}+2=-2+2=0$

Así pues, las soluciones de esta ecuación son todas las ternas siguientes:

$(1, 2k, 3k), k \geq 1$; $(2, 1, 2)$; $(2, 3, 18)$; $(k, 2, 3k), k \geq 1$

10.11.3

$$\frac{1}{m}+\frac{4}{n}=\frac{1}{12} \Leftrightarrow \frac{n+4m}{mn}=\frac{1}{12} \Leftrightarrow 12(n+4m)=mn \Leftrightarrow 0=mn-12n-48m$$

Para resolver esta ecuación aplicamos el método de completar cuadrados:

$0 = mn - 12n - 48m = (n-48)(m-12) - 12 \cdot 48 \Leftrightarrow$

$12 \cdot 48 = (n-48)(m-12) \Leftrightarrow$

$2^6 \cdot 3^2 = (n-48)(m-12)$

Puesto que, además, n debe ser impar, el factor $n-48$ no puede ser divisible entre 2, y por tanto las únicas posibilidades aceptables son:

$$\left.\begin{array}{l} 1 = n-48 \\ 2^6 \cdot 3^2 = m-12 \end{array}\right\} \Rightarrow n = 49, m = 588$$

$$\left.\begin{array}{l} 3 = n - 48 \\ 2^6 \cdot 3 = m - 12 \end{array}\right\} \Rightarrow n = 51,\ m = 204$$

$$\left.\begin{array}{l} 3^2 = n - 48 \\ 2^6 = m - 12 \end{array}\right\} \Rightarrow n = 57,\ m = 76$$

10.11.4

$$\frac{1}{a} + \frac{1}{b} = \frac{3}{2018} \Leftrightarrow \frac{a+b}{ab} = \frac{3}{2018} \Leftrightarrow 2018(a+b) = 3ab \Leftrightarrow 0 = ab - \frac{2018}{3}a - \frac{2018}{3}b \Leftrightarrow$$

$$\Leftrightarrow 0 = \left(a - \frac{2018}{3}\right)\left(b - \frac{2018}{3}\right) - \frac{2018^2}{3^2} \Leftrightarrow$$

$$\frac{2018^2}{3^2} = \left(a - \frac{2018}{3}\right)\left(b - \frac{2018}{3}\right) \Leftrightarrow$$

$$2^2 \cdot 1009^2 = 2018^2 = (3a - 2018)(3b - 2018)$$

Estudiemos los posibles casos:

$$\left.\begin{array}{l} 1 = 3a - 2018 \\ 2^2 \cdot 1009^2 = 3b - 2018 \end{array}\right\} \Rightarrow \begin{cases} a = 673 \\ b = \left(2^2 \cdot 1009^2 + 2 \cdot 1009\right)/3 = 2 \cdot 1009 \cdot 673 = 1358114 \end{cases}$$

$$\left.\begin{array}{l} 2 = 3a - 2018 \\ 2 \cdot 1009^2 = 3b - 2018 \end{array}\right\} \Rightarrow a = 2020/3, \text{ no es entero.}$$

$$\left.\begin{array}{l} 2 \cdot 1009 = 3a - 2018 \\ 2 \cdot 1009^2 = 3b - 2018 \end{array}\right\} \Rightarrow a = 4036/3, \text{ no es entero}$$

Nota: Estos dos casos anteriores se podrían haber rechazado teniendo en cuenta que $3a - 2018 \equiv 1 \pmod 3$.

$$\left.\begin{array}{l} 2^2 = 3a - 2018 \\ 1009^2 = 3b - 2018 \end{array}\right\} \Rightarrow \begin{cases} a = 674 \\ b = 340033 \end{cases}$$

$$\left.\begin{array}{l} 2^2 \cdot 1009 = 3a - 2018 \\ 1009 = 3b - 2018 \end{array}\right\} \Rightarrow \begin{cases} a = 2018 \\ b = 1009 \end{cases}$$

El resto de soluciones se obtienen intercambiando los valores. Así pues, las soluciones son: $(673, 1358114), (674, 340033), (2018, 1009), (1009, 2018), (1358114, 673), (340033, 674)$.

10.11.5

$$2009 = x^2 - y^4 = \left(x - y^2\right)\left(x + y^2\right) = a \cdot b$$

Supongamos en primer lugar, que a y b no son primos entre sí. Entonces $mcd(a,b)^2$ es un divisor de $2009 = 7^2 \cdot 41$, y por tanto la única posibilidad es que $mcd(a,b) = 7$. Luego:

$\left.\begin{array}{l} a = x - y^2 = 7a' \\ b = x + y^2 = 7b' \end{array}\right\} \Rightarrow 2x = 7(a'+b') \Rightarrow 7$ es divisor de x, y puesto que es también divisor de a, será también divisor de y. Luego:

$\left.\begin{array}{l} x = 7x' \\ y = 7y' \end{array}\right\} (x-y^2)(x+y^2) = \left(7x'+7^2y'^2\right)\left(7x'-7^2y'^2\right) = 7^2\left(x'+7y'^2\right)\left(x'-7y'^2\right) = 7^2 \cdot 41 \Rightarrow$

$\left(x'+7y'^2\right)\left(x'-7y'^2\right) = 41$

La única posibilidad es

$x'+7y'^2 = 41$, $x'-7y'^2 = 1 \Rightarrow 2x' = 41+1 = 42 \Rightarrow x' = 21 \Rightarrow 7y'^2 = 41 - x' = 41 - 21 = 20$ absurdo.

Luego a y b son primos entre sí.

$\left.\begin{array}{l} x - y^2 = a \\ x + y^2 = b \end{array}\right\} \Rightarrow x = a + y^2 \Rightarrow a + y^2 + y^2 = b \Rightarrow 2y^2 = b - a$. Luego $b > a$, $b - a$ es positivo, par y $\dfrac{b-a}{2}$ es un cuadrado perfecto.

Veamos todas las posibilidades:

a)

$\left.\begin{array}{l} a = 7 \\ b = 7 \cdot 41 \end{array}\right\} \Rightarrow b - a = 287 - 7 = 280 \Rightarrow \dfrac{b-a}{2} = 140$ no es un cuadrado.

b)

$\left.\begin{array}{l} a = 41 \\ b = 7 \cdot 7 \end{array}\right\} \Rightarrow b - a = 49 - 41 = 8 \Rightarrow \dfrac{b-a}{2} = 4 = 2^2$, sí es un cuadrado.

En este caso: $\left.\begin{array}{l} x - y^2 = 41 \\ x + y^2 = 49 \end{array}\right\} \Rightarrow 2x = 41 + 49 = 90 \Rightarrow x = 45, y^2 = 49 - 45 = 4 \Rightarrow y = \pm 2$

En efecto, $\left(45 - 2^2\right)\left(45 + 2^2\right) = 41 \cdot 49 = 2009$

c)

$\left.\begin{array}{l} a = 1 \\ b = 7 \cdot 7 \cdot 41 = 2009 \end{array}\right\} \Rightarrow b - a = 2009 - 1 = 2008 \Rightarrow \dfrac{b-a}{2} = 1004$ no es un cuadrado.

Luego las soluciones son $x = \pm 45$, $y = \pm 2$.

Fuente de esta solución: Solución oficial de la OME.

10.11.6

Primera versión.

Vamos a resolver la ecuación diofántica $y^2 + 3x^2y^2 = 30x^2 + 517$

Sean $a = x^2$ y $b = y^2$. La ecuación anterior es equivalente a

$b + 3ab = 30a + 517 \Leftrightarrow b + 3ab - 30a = 517 \Leftrightarrow b(1+3a) - 30a - 10 = 517 - 10 \Leftrightarrow$

$b(1+3a) - 10(3a+1) = 507$ (*)

Sea $c = 1 + 3a$. Puesto que a y b son cuadrados, serán positivos, y también lo será c.

$(*) \Leftrightarrow bc - 10c = 507 \Leftrightarrow c(b-10) = 507 = 3 \cdot 13^2$

10.11.7
Realizamos la sustitución $a = p - q \Rightarrow p = a + q \Rightarrow p + q = a + q + q = a + 2q$
La ecuación se ha transformado en $a + 2q = a^3$
$a + 2q = a^3 \Rightarrow 2q = a^3 - a = a\left(a^2 - 1\right) = a(a-1)(a+1)$

Forzosamente uno de los tres factores deben ser 2.
$a = 2 \Rightarrow 2q = 2 \cdot 1 \cdot 3 = 6 = 2 \cdot 3 \Rightarrow q = 3 \Rightarrow p = a + q = 2 + 3 = 5$
Y en efecto, $8 = 5 + 3 = (5-3)^3$

Las otras opciones no son aceptables:
$a - 1 = 2 \Rightarrow a = 3 \Rightarrow 2q = 3 \cdot 2 \cdot 4 = 24 = 2 \cdot 12 \Rightarrow q = 12$ no es primo.
$a + 1 = 2 \Rightarrow a = 1 \Rightarrow 2q = 1 \cdot 0 \cdot 2 = 0 \Rightarrow q = 0$ no es primo.

La única solución es $p = 5$, $q = 3$.

De todas las soluciones posibles (tomando combinaciones de $3, 13, 13^2$), la única que genera como soluciones dos cuadrados es:
$b - 10 = 3 \cdot 13 \Rightarrow b = 49 = 7^2 \Rightarrow c = 13 = 1 + 3a \Rightarrow a = 4 = 2^2$
Y por tanto $3x^2y^2 = 3ab = 3 \cdot 4 \cdot 49 = 588$.

Segunda versión.
La ecuación original se puede escribir como $\left(y^2 - 10\right)\left(3x^2 + 1\right) = 3 \cdot 13^2$.
Observamos que, puesto que y es un entero y $3x^2 + 1$ es positivo, $y^2 - 10$ debe ser también positivo. Luego $y^2 - 10 \in \{1, 3, 13, 39, 169, 507\}$, y por tanto
$y^2 \in \{11, 13, 23, 49, 179, 517\}$. El único cuadrado perfecto de esta última lista es 49, luego
$y^2 - 10 = 39$, y por tanto $3x^2 + 1 = 12 \Rightarrow x^2 = 4 \Rightarrow 3x^2y^2 = 12 \cdot 49 = 588$.

Fuente de la segunda versión: The Contest Problem Book V (George Berzsenyi)

10.11.8
Primera versión.
En primer lugar, vemos que al menos uno de estos tres números tiene que ser 1.
Supongamos, por el contrario, que $a, b, c > 1$. Entonces podemos escribir
$a = x + 1$, $b = y + 1$, $c = z + 1$ con $x, y, z > 0$. Pero entonces:
$abc = a + b + c + 1 \Leftrightarrow (x+1)(y+1)(z+1) = x + 1 + y + 1 + z + 1 + 1 \Leftrightarrow$
$1 + x + y + z + xy + yz + xz + xyz = x + y + z + 4 \Leftrightarrow xy + yz + xz + xyz = 3$
Lo cual es imposible pues $x, y, z > 0 \Rightarrow xy + yz + xz + xyz \geq 4$

Así pues, podemos suponer que, por ejemplo, $b = 1$. Entonces la ecuación queda de la forma:
$ac = a + c + 2 \Leftrightarrow ac - a - c = 2 \Leftrightarrow ac - a - c + 1 = 3 \Leftrightarrow (a-1)(c-1) = 3$

Y los casos posibles son:

$$\left.\begin{matrix} a-1=1 \\ c-1=3 \end{matrix}\right\} \Rightarrow a=2, c=4 \qquad \left.\begin{matrix} a-1=3 \\ c-1=1 \end{matrix}\right\} \Rightarrow a=4, c=2$$

Así pues, la única solución es la terna $(1,2,4)$ y todas sus permutaciones, pues las incógnitas a,b,c de la ecuación del enunciado son perfectamente intercambiables.

Segunda versión.

$$abc=a+b+c+1 \Leftrightarrow abc-a=b+c+1 \Leftrightarrow a(bc-1)=b+c+1 \Rightarrow$$

$$bc-1 \mid b+c+1 \Rightarrow bc-1 \le b+c+1 \Leftrightarrow bc-b-c \le 2 \Leftrightarrow bc-b-c+1 \le 3$$

$$\Leftrightarrow (b-1)(c-1) \le 3$$

Veamos los casos posibles:

$$\left.\begin{matrix} b-1=1 \\ c-1=3 \end{matrix}\right\} \Rightarrow b=2, c=4 \Rightarrow a=1$$

$$\left.\begin{matrix} b-1=2 \\ c-1=1 \end{matrix}\right\} \Rightarrow b=3, c=2 \Rightarrow a=6/5$$, y esta solución no es aceptable, pues no es entera.

$$\left.\begin{matrix} b-1=1 \\ c-1=1 \end{matrix}\right\} \Rightarrow b=2, c=2 \Rightarrow a=5/3$$, y esta solución no es aceptable, pues no es entera.

Y un último caso: $b-1=0 \Rightarrow b=1$, que ya se consideró en la primera versión.

Tercera versión.

Supongamos que los tres son iguales. Entonces la ecuación queda de la forma $a^3=3a+1$, y entonces:

$$a^3=3a+1 \Leftrightarrow a^3-3a=1 \Leftrightarrow a\left(a^2-3\right)=1 \Rightarrow a \mid 1 \Rightarrow a=1$$

pero $1^3 \neq 3 \cdot 1+1$, por lo tanto los tres números son iguales.

Los ordenamos: $a \le b \le c$, y al no ser iguales, $a<c \Rightarrow a+1 \le c \Rightarrow a+b+1 \le b+c \le c+c=2c$.

Ahora volvemos a la ecuación del enunciado:

$$abc=a+b+c+1 \Leftrightarrow abc-c=a+b+1 \Leftrightarrow c\left(ab-1\right)=a+b+1 \Rightarrow c \mid a+b+1 \le 2c$$

Solo hay dos posibilidades:

$$c=a+b+1 \Rightarrow ab(a+b+1)=a+b+a+b+1+1 \Leftrightarrow$$

$$ab(a+b+1)=2a+2b+2=2(a+b+1) \Rightarrow ab=2 \Rightarrow a=1, b=2 \Rightarrow c=4$$

$$2c=a+b+1 \Rightarrow abc=2c+c=3c \Rightarrow ab=3 \Rightarrow a=1, b=3 \Rightarrow c=5.$$

Pero esta solución no es aceptable pues no se satisface la ecuación original:

$1 \cdot 3 \cdot 5 \neq 1+3+5+1$

La única solución es $a=1, b=2, c=4$ y todas sus permutaciones.

Fuente de las versiones 2 y 3: "Teoría de Números. Entrenamiento de Hidalgo para la Olimpiada Mexicana de matemáticas" pág. 23.

10.11.9

En primer lugar, vemos que $x=0, y=0$ es solución trivial de la ecuación. También vemos que la parte izquierda es positiva, y por tanto x, y deben tener el mismo signo. Si (x, y) es solución, también lo será $(-x,-y)$, así pues, podemos suponer que ambos son positivos.

Vamos a estudiar la presencia del factor 3 en la descomposición factorial de x, y.

Supongamos que $x = 3^m a$, $y = 3^n b$, con $m, n \geq 0$ y a, b no divisibles entre 3.
Podemos suponer, además, que $m \geq n$.

$$3^4 2^3 \left(x^2 + y^2\right) = x^3 y^3 \Leftrightarrow 3^4 2^3 \left(3^{2m} a^2 + 3^{2n} b^2\right) = 3^{3m} a^3 3^{3n} b^3 \Leftrightarrow 2^3 \left(3^{2m} a^2 + 3^{2n} b^2\right) = 3^{3m+3n-4} a^3 b^3$$
$$\Leftrightarrow 2^3 3^{2n} \left(3^{2m-2n} a^2 + b^2\right) = 3^{3m+3n-4} a^3 b^3 \Leftrightarrow 2^3 \left(3^{2m-2n} a^2 + b^2\right) = 3^{3m+n-4} a^3 b^3$$
$$\Leftrightarrow 8\left(\left(3^{m-n} a\right)^2 + b^2\right) = 3^{3m+n-4} a^3 b^3$$

Todo cuadrado es 0 o 1 módulo 3 (ver problema #3.16a), luego la suma de dos cuadrados será 0, 1 o 2 módulo 3, es decir, no será divisible entre 3, y por lo tanto, multiplicada por 8 tampoco será múltiplo de 3. Así pues, la parte de la izquierda no es múltiplo de 3, y por tanto, observando la parte de la derecha, necesariamente $3m + n - 4 = 0$, y esto solo pasa cuando $m = n = 1$.

Por lo tanto, la ecuación queda $8\left(a^2 + b^2\right) = a^3 b^3$.

Por simetría podemos suponer que $a \geq b$

$$a^3 b^3 = 8\left(a^2 + b^2\right) \leq 8\left(a^2 + a^2\right) = 16a^2 \Rightarrow ab^3 \leq 16$$

Las únicas opciones para b son $b = 1, 2$.

Si $b = 1 \Rightarrow a \leq 16$ y $8\left(a^2 + b^2\right) = a^3 b^3 \Rightarrow 8\left(a^2 + 1\right) = a^3$ ningún posible valor de a resuelve esta ecuación.

Si $b = 2 \Rightarrow a2^3 \leq 16 \Leftrightarrow a \cdot 8 \leq 16 \Rightarrow a \leq 2$. La pareja $b = 2, a = 1$ no soluciona $8\left(a^2 + b^2\right) = a^3 b^3$.
Finalmente, la pareja $b = 2, a = 2$ sí es solución de $8\left(a^2 + b^2\right) = a^3 b^3$:

$$8\left(2^2 + 2^2\right) = 64 = 4^3 = 2^3 2^3$$

Luego $x = 3^m a = 3 \cdot 2 = 6$, $y = 3^n b = 3 \cdot 2 = 6$, es la única solución posible (junto a $x = 0, y = 0$ y $x = -6, y = -6$).

Fuente de esta solución: Solución oficial.

10.11.10
Está claro que $xy + 61 > 0 \Rightarrow x^3 > y^3 \Rightarrow x > y$.
Aplicando la identidad $(x - y)^3 = x^3 - 3xy(x - y) - y^3 \Rightarrow x^3 - y^3 = (x - y)^3 + 3xy(x - y)$

Transformamos la ecuación anterior en

$$(x - y)^3 + 3xy(x - y) = xy + 61$$

Realizamos el cambio de variable

$$\begin{cases} a = x - y > 0 \\ b = xy > 0 \end{cases}$$

La ecuación se transforma en $a^3 + 3ab = b + 61 \Leftrightarrow a^3 + 3ab - b = 61 \Leftrightarrow a^3 + b(3a-1) = 61$
Vamos dando valores de a:

$a = 1 \Rightarrow 1^3 + b(3 \cdot 1 - 1) = 61 \Leftrightarrow b = 30$

$a = 2 \Rightarrow 2^3 + b(3 \cdot 2 - 1) = 61$ no tiene solución entera

$a = 3 \Rightarrow 3^3 + b(3 \cdot 3 - 1) = 61$ no tiene solución entera

$a \geq 4 \Rightarrow 4^3 \geq 62 > 61$ la ecuación $a^3 + b(3a-1) = 61$ no tiene solución.

Así pues, la única solución es $\begin{cases} a = x - y = 1 \\ b = xy = 30 \end{cases} \Rightarrow x = 6, y = 5$

Observación. Otro razonamiento alternativo es: Puesto que $x > y$
$x^3 - y^3 = (x-y)(x^2 + xy + y^2) = xy + 61 \Rightarrow x^2 + xy + y^2 \leq xy + 61 \Rightarrow x^2 + y^2 \leq 61 \Rightarrow$
$\Rightarrow 61 \geq x^2 + y^2 \geq 2y^2 \Rightarrow y \in \{1,2,3,4,5\}$
Y a partir de aquí vamos probando estos candidatos hasta dar con el único y aceptable.

10.11.11
$(x^2 + y)(x + y^2) = (x - y)^3 \Leftrightarrow$
$x^3 + y^3 + xy + x^2y^2 = x^3 - 3x^2y + 3xy^2 - y^3 \Leftrightarrow$
$2y^3 + xy + x^2y^2 + 3x^2y - 3xy^2 = 0 \Leftrightarrow$
$y(2y^2 + x + x^2y + 3x^2 - 3xy) = 0$

Puesto que estamos suponiendo $y \neq 0$ llegamos a

$$2y^2 + x + x^2y + 3x^2 - 3xy = 0$$

Esta ecuación la podemos interpretar como una ecuación de segundo grado en y:

$$2y^2 + (x^2 - 3x)y + 3x^2 + x = 0 \Rightarrow ay^2 + by + c = 0, \begin{cases} a = 2 \\ b = x^2 - 3x \\ c = 3x^2 + x \end{cases}$$

y por tanto $y = \dfrac{-b \pm \sqrt{\Delta}}{2a}$, $\Delta = b^2 - 4ac$

Estudiemos el discriminante Δ, que deberá ser un cuadrado perfecto:

$\Delta = b^2 - 4ac = (x^2 - 3x)^2 - 4 \cdot 2 \cdot (3x^2 + x) = x^2(x-3)^2 - 8x(3x+1) =$
$= x[x(x-3)^2 - 8(3x+1)]$
$x(x-3)^2 - 8(3x+1) = x^3 - 6x^2 - 15x - 8 = (x+1)^2(x-8)$
Luego $\Delta = x(x+1)^2(x-8)$
Y por tanto $\sqrt{\Delta} = \sqrt{x(x+1)^2(x-8)} = |x+1|\sqrt{x(x-8)}$

Así pues, $x(x-8)$ deberá ser un cuadrado perfecto. A partir de aquí podemos utilizar la técnica el problema 4.1.6:

$$x(x-8)=n^2 \Leftrightarrow x^2-8x-n^2=0 \Leftrightarrow x=\frac{8\pm\sqrt{64-4\left(-n^2\right)}}{2}=\frac{8\pm\sqrt{64+4n^2}}{2}=$$

$$=\frac{8\pm 2\sqrt{16+n^2}}{2}=4\pm\sqrt{16+n^2}=4\pm\sqrt{4^2+n^2}$$

Luego 4^2+n^2 debe ser un cuadrado perfecto:

$$4^2+n^2=m^2 \Leftrightarrow 4^2=m^2-n^2=\left(|m|+|n|\right)\left(|m|-|n|\right)$$

Puesto que $|m|+|n|\geq 0$, se tiene que cumplir $|m|-|n|>0 \Leftrightarrow |m|>|n|$

Veamos las diferentes posibilidades:

$$\left.\begin{matrix}|m|+|n|=1\\ |m|-|n|=16\end{matrix}\right\} \Leftrightarrow 2|m|=17 \Rightarrow |m|=17/2 \text{ no es entero}$$

$$\left.\begin{matrix}|m|+|n|=2\\ |m|-|n|=8\end{matrix}\right\} \Leftrightarrow 2|m|=10 \Rightarrow |m|=5\,,\ |n|=-3 \text{ absurdo}$$

$$\left.\begin{matrix}|m|+|n|=4\\ |m|-|n|=4\end{matrix}\right\} \Leftrightarrow 2|m|=8 \Rightarrow |m|=4\,,\ |n|=0 \Rightarrow m=\pm 4\,,\ n=0$$

$$\left.\begin{matrix}|m|+|n|=8\\ |m|-|n|=2\end{matrix}\right\} \Leftrightarrow 2|m|=10 \Rightarrow |m|=5\,,\ |n|=8-5=3$$

$$\left.\begin{matrix}|m|+|n|=16\\ |m|-|n|=1\end{matrix}\right\} \Leftrightarrow 2|m|=17 \Rightarrow |m|=17/2 \text{ no es entero}$$

Todas las combinaciones que generan el producto de dos negativos llevan al absurdo:

$$\left.\begin{matrix}|m|+|n|=-k_1\\ |m|-|n|=-k_2\end{matrix}\right\} \Leftrightarrow 2|m|=-k_1-k_2<0 \text{ absurdo}$$

Las únicas posibilidades aceptables son

a) $m=\pm 4\,,\ n=0$, y por tanto:

$$x=4\pm\sqrt{4^2+n^2}=4\pm\sqrt{4^2+0^2}=4\pm\sqrt{4^2}=4\pm 4=\begin{cases}8\\0\end{cases}$$

b) $|m|=5\,,\ |n|=3 \Rightarrow n=\pm 3$

$$x=4\pm\sqrt{4^2+n^2}=4\pm\sqrt{4^2+3^2}=4\pm\sqrt{25}=4\pm 5=\begin{cases}9\\-1\end{cases}$$

Así pues, llegamos a las posibles soluciones $x=-1\,,0\,,8\,,9$. Veamos caso a caso:

$$x=-1 \Rightarrow \Delta=x(x+1)^2(x-8)=0$$

$$b=x^2-3x=1+3=4$$

$$y=\frac{-b\pm\sqrt{\Delta}}{4}=\frac{-4}{4}=-1$$

$x=0\Rightarrow\Delta=x(x+1)^2(x-8)=0$ esta solución se descarta en el enunciado.

$x=8\Rightarrow\Delta=x(x+1)^2(x-8)=0$

$$b=x^2-3x=64-24=40$$

$$y=\frac{-b\pm\sqrt{\Delta}}{4}=\frac{-40}{4}=-10$$

$x=9\Rightarrow\Delta=x(x+1)^2(x-8)=9\cdot10^2\cdot1=900$

$$b=x^2-3x=81-27=54$$

$$y=\frac{-b\pm\sqrt{\Delta}}{4}=\frac{-54\pm\sqrt{900}}{4}=\frac{-54\pm30}{4}=\begin{cases}-21\\-6\end{cases}$$

Así pues, hemos llegado a las soluciones $(-1,-1)$, $(8,-10)$, $(9,-21)$, $(9,-6)$.

10.11.12

Multiplicamos la ecuación por 4, completamos cuadrados y aplicamos la fórmula "diferencia de cuadrados":

$$x^6+3x^3+1=y^4\Leftrightarrow4x^6+12x^3+4=4y^4\Leftrightarrow$$
$$(2x^3)^2+2\cdot2x^3\cdot3+3^2-9+4=4y^4\Leftrightarrow(2x^3+3)^2-5=4y^4\Leftrightarrow$$
$$(2x^3+3)^2-4y^4=5\Leftrightarrow(2x^3+3)^2-(2y^2)^2=5\Leftrightarrow$$
$$((2x^3+3)-(2y^2))((2x^3+3)+(2y^2))=5$$

Ahora solo queda ir viendo las diferentes posibilidades:

$$\left.\begin{matrix}2x^3+3-2y^2=1\\2x^3+3+2y^2=5\end{matrix}\right\}\Rightarrow-4y^2=-4\Leftrightarrow y^2=1\Leftrightarrow y=\pm1\Rightarrow2x^3+3+2\cdot1=5\Rightarrow x=0$$

$$\left.\begin{matrix}2x^3+3-2y^2=5\\2x^3+3+2y^2=1\end{matrix}\right\}\Rightarrow-4y^2=4\text{ absurdo}$$

$$\left.\begin{matrix}2x^3+3-2y^2=-1\\2x^3+3+2y^2=-5\end{matrix}\right\}\Rightarrow-4y^2=4\text{ absurdo}$$

$$\left.\begin{matrix}2x^3+3-2y^2=-5\\2x^3+3+2y^2=-1\end{matrix}\right\}\Rightarrow-4y^2=-4\Leftrightarrow y^2=1\Leftrightarrow y=\pm1$$ absurdo.

$$\Rightarrow2x^3+3-2\cdot1=-5\Rightarrow2x^3=-6\Rightarrow2x^3=-6\Rightarrow x^3=-3$$

La única solución aceptable es $x=0, y=\pm1$.

Efectivamente, estos valores satisfacen la ecuación:

$$x=0, y=1\Rightarrow0^6+3\cdot0^3+1=1=1^4$$
$$x=0, y=-1\Rightarrow0^6+3\cdot0^3+1=1=(-1)^4$$

Fuente de esta solución: https://youtu.be/C98xqJHMfvY (GG Maths)

10.11.13

Está claro que $x=0, y=0$ es solución trivial de la ecuación.

Si $x=0$ la ecuación se reduce a $py=0 \Rightarrow y=0$, con lo que llegamos a la solución trivial.

Si $y=0$ por el mismo razonamiento llegamos a la misma solución (la ecuación es simétrica).

$p(x+y)=xy \Rightarrow p \mid xy \Rightarrow p \mid x \; o \; p \mid y$

Supongamos que $p \mid x \Rightarrow x=px'$, y por tanto

$$p(x+y)=xy \Leftrightarrow p(px'+y)=px'y \Rightarrow px'+y=x'y \Rightarrow px'=x'y-y=(x'-1)y \Rightarrow p \mid (x'-1)y$$

Luego $p \mid (x'-1) \; o \; p \mid y$.

Si $p \mid y$, entonces $y=py'$ y por tanto la ecuación queda

$px'=(x'-1)y \Rightarrow px'=(x'-1)py' \Rightarrow x'=(x'-1)y'$

Esta última ecuación solo tiene soluciones $x'=0, y'=0$ y $x'=2, y'=2$, es decir, la solución trivial y $x=2p$, $y=2p$.

En efecto: $p(2p+2p)=4p^2=2p \cdot 2p=xy$.

Nos queda estudiar el caso $p \mid (x'-1)$, es decir $x'-1=pk$, y la ecuación queda

$$px'=(x'-1)y \Rightarrow p(pk+1)=pky \Rightarrow pk+1=ky \Rightarrow y=\frac{pk+1}{k}=p+\frac{1}{k}$$

La única posibilidad que y sea entero es $k=1$, luego $y=p+1$, $x'=p+1$, $x=p(p+1)$

En efecto:

$$p(p(p+1)+p+1)=p(p^2+p+p+1)=p(p^2+2p+1)=p(p+1)^2=p(p+1)(p+1)=xy$$

Luego las soluciones son tres:

$x=y=0$; $x=y=2p$; $x=p(p+1), y=p+1$

Observación.

En las soluciones oficiales (SE, pág. 849) se presenta un razonamiento parecido:

$$px'+y=x'y \Rightarrow 0=x'y-px'-y=x'(y-p)-y \Rightarrow p=x'(y-p)-y+p=$$

$$=x'(y-p)-(y-p)=(x'-1)(y-p) \Rightarrow \begin{cases} x'-1 \mid p \\ y-p \mid p \end{cases}$$

Y puesto que p es primo, tenemos que $x'-1 \mid p \Rightarrow \begin{cases} x'-1=p \\ x'-1=-p \\ x'-1=1 \\ x'-1=-1 \end{cases}$

10.11.14

En primer lugar pasamos la igualdad a módulo 3:

$$3^x + 4^y = 5^z \Rightarrow 3^x + 4^y = 5^z \pmod 3 \Leftrightarrow 0 + 1^y \equiv (-1)^z \pmod 3 \Leftrightarrow 1 \equiv (-1)^z \pmod 3$$

De aquí deducimos que z debe ser par: $z = 2k$ para cierto $k \in IN$.

$$3^x + 4^y = 5^{2k} \Leftrightarrow 3^x = 5^{2k} - 4^y = \left(5^k\right)^2 - \left(2^y\right)^2 = \left(5^k - 2^y\right)\left(5^k + 2^y\right)$$

Por lo tanto los dos factores de la parte derecha deben ser ambos potencias de 3.
Pero estos dos factores no pueden ser ambos múltiples de 3, pues aplicando el Algoritmo de Euclides:

$$(a,b) = (a,\ a+b)$$

En nuestro caso, sumando ambos factores:

$$\left(5^k - 2^y, 5^k + 2^y\right) = \left(5^k - 2^y, 2 \cdot 5^k\right)$$

Y claramente $2 \cdot 5^k$ no es múltiple de 3.

La única opción válida es que sean factores coprimos, y por tanto

$$\begin{cases} 5^k + 2^y = 3^x \\ 5^k - 2^y = 1 \end{cases}$$

Restamos las dos ecuaciones para llegar a

$$2 \cdot 2^y = 3^x - 1 \Leftrightarrow 2^{y+1} = 3^x - 1 \ (*)$$

Ahora observamos que si $y \geq 3$ entonces 2^{y+1} es un múltiplo de 16 y por tanto, pasando a módulo 16 llegamos a

$$0 \equiv 3^x - 1 \pmod{16} \Leftrightarrow 1 \equiv 3^x \pmod{16}$$

Estudiemos las potencias de 3 módulo 16:

$x = 0 \Rightarrow 3^0 \equiv 1 \pmod{16}$

$x = 1 \Rightarrow 3^1 \equiv 3 \pmod{16}$

$x = 2 \Rightarrow 3^2 \equiv 9 \pmod{16}$

$x = 3 \Rightarrow 3^3 \equiv 27 \pmod{16}$

$x = 4 \Rightarrow 3^4 = 81 = 5 \cdot 16 + 1 \equiv 1 \pmod{16}$

$x = 5 \Rightarrow 3^5 = 243 \equiv 3 \pmod{16}$

Vemos que generan un ciclo, es decir, que x ha de ser un múltiple de 4: $x = 4s$ para cierto $s \in IN$. Luego la ecuación se convierte en

$$2^{y+1} = 3^x - 1 = 3^{4s} - 1 = 81^s - 1 \Rightarrow 81^s = 2^{y+1} + 1$$

Pero ahora, pasando a módulo 5, tenemos

$$2^{y+1} + 1 \equiv 1^s = 1 \pmod 5 \Rightarrow 2^{y+1} \equiv 0 \pmod 5$$

Lo cual es imposible, pues ninguna potencia de 2 es múltiple de 5.

Con todo esto hemos demostrado que la hipótesis inicial $y \geq 3$ es inaceptable, y por tanto $y < 3$, y ahora podemos testear caso por caso en la ecuación (*):

$y=1\Rightarrow 2^{1+1}=4=3^x-1\Rightarrow 4+1=3^x\Rightarrow 5=3^x$ no tiene solución.

$y=2\Rightarrow 2^{2+1}=8=3^x-1\Rightarrow 8+1=3^x\Rightarrow 9=3^x\Rightarrow x=2$

Y resolvemos el sistema:

$$\begin{cases}5^k+2^y=3^x\\5^k-2^y=1\end{cases}\Leftrightarrow\begin{cases}5^k+4=9\\5^k-4=1\end{cases}\Leftrightarrow\begin{cases}5^k=9-4=5\\5^k=1+4=5\end{cases}\Rightarrow k=1\Rightarrow z=2k=2$$

Así pues, la única solución aceptable de este problema es la conocida terna pitagórica $3^2+4^2=5^2$.

10.11.15

$$\left.\begin{matrix}3^m-2^n=1\\2^n>0\end{matrix}\right\}\Rightarrow 3^m=1+2^n>1\Rightarrow m>0\Rightarrow 3^m\geq 3$$

Por otro lado, $3^m-2^n=1\Rightarrow 2^n=3^m-1\geq 3-1=2\Rightarrow n\geq 1$

Supongamos, en primer lugar, que $n=1$. Entonces $3^m=1+2^1=3\Rightarrow m=1$, y la solución es $m=1, n=1$.

Supongamos ahora que $n>1$, entonces 2^n es múltiplo de 4, y por tanto:
$2^n=3^m-1\equiv 0\pmod 4\Rightarrow 3^m\equiv(-1)^m\equiv 1\pmod 4\Rightarrow m=2k$, es decir, es un número par.

$$3^m-2^n=1\Leftrightarrow 2^n=3^m-1=3^{2k}-1^2=\left(3^k\right)^2-1^2=\left(3^k-1\right)\left(3^k+1\right)$$

Así pues, 3^k-1 y 3^k+1 son dos potencias de 2, y difieren en dos unidades, y esto solo puede ocurrir para

$$\left.\begin{matrix}3^k+1=4\\3^k-1=2\end{matrix}\right\}\Rightarrow k=1\Rightarrow m=2\Rightarrow n=3$$, que es la otra solución de esta ecuación.

Nota: Se debe justificar que solo 4 y 2 son las potencias de 2 que difieren en dos unidades:

$$2^a-2^b=2\Leftrightarrow 2^b\left(2^{a-b}-1\right)=2\Rightarrow\begin{cases}2^b=1\,,\,2^{a-b}-1=2\Rightarrow \textit{imposible}\\2^b=2\,,\,2^{a-b}-1=1\Rightarrow b=1\,,\,a=2\end{cases}$$

10.11.16

Empezamos como es habitual manipulando algébricamente la ecuación:

$$1+x^2y=x^2+2xy+2x+y\Leftrightarrow$$
$$x^2y-x^2-2xy-2x=y-1\Leftrightarrow$$
$$x\left(xy-x-2y-2\right)=y-1\Leftrightarrow$$
$$x\left[\left(x-2\right)\left(y-1\right)-4\right]=y-1$$

Si $x=0\Rightarrow y=1$, que es una solución de la ecuación. Supongamos que $x\neq 0$.

De aquí deducimos que x es un divisor de $y-1$, es decir, $y-1=a\,x$ para cierto entero a. Luego:

$$x\left[(x-2)ax-4\right]=ax$$

Como estamos suponiendo que $x\neq 0$ podemos cancelar dicho término y llegar a

$$(x-2)ax-4=a \Leftrightarrow$$
$$(x-2)ax-a=4 \Leftrightarrow$$
$$a\left[(x-2)x-1\right]=4 \Leftrightarrow$$
$$a\left[x^2-2x-1\right]=4$$

Ahora ya solo nos queda analizar todas las posibilidades:

$\begin{cases} a=1 \\ x^2-2x-1=4 \end{cases}$ La segunda ecuación tiene soluciones irracionales.

$\begin{cases} a=2 \\ x^2-2x-1=2 \Rightarrow \begin{cases} x=-1 \Rightarrow y-1=2(-1) \Rightarrow y=-1 \\ x=3 \Rightarrow y-1=2\cdot 3 \Rightarrow y=7 \end{cases} \end{cases}$

$\begin{cases} a=4 \\ x^2-2x-1=1 \end{cases}$ La segunda ecuación tiene soluciones irracionales.

$\begin{cases} a=-1 \\ x^2-2x-1=-4 \end{cases}$ La segunda ecuación tiene soluciones complejas.

$\begin{cases} a=-2 \\ x^2-2x-1=-2 \Rightarrow x=1 \Rightarrow y-1=(-2)\cdot 1 \Rightarrow y=-1 \end{cases}$

$\begin{cases} a=-4 \\ x^2-2x-1=-1 \Rightarrow \begin{cases} x=0 \text{ (descartada)} \\ x=2 \Rightarrow y-1=(-4)\cdot 2 \Rightarrow y=-7 \end{cases} \end{cases}$

Completando así todas las cinco soluciones posibles:

$$(0,1)\ ,\ (-1,-1)\ ,\ (3,7)\ ,\ (1,-1)\ ,\ (2,-7)$$

Fuente de esta solución: https://youtu.be/dzAWK-4Dv8c (GG Maths)

10.11.17

Dado un valor de n, sea T el número de casas que empiezan por "2".

Vamos a dividir el problema en casos diferentes en función del valor de n.

a) $100\leq n\leq 199$

Los únicos números que empiezan por el dígito "2" son el 2, y entre 21 y 29, once valores, luego

$$\frac{T}{n}=\frac{11}{n}=\frac{1}{k} \Leftrightarrow 11k=n \Leftrightarrow 11\,|\,n$$

Luego serán todos los múltiplos de 11: Del $11\cdot 10=110$ al $11\cdot 18=198$, nueve casos.

b) $300 \le n$

Los únicos números que empiezan por el dígito "2" son 2, del 21 al 29, diez valores, y los números entre 200 y 299, 100 valores, luego hay 111 casas que empiezan por "2" y por tanto

$$\frac{T}{n} = \frac{111}{n} = \frac{1}{k} \Leftrightarrow 111k = n \Leftrightarrow 111 \mid n$$

Luego serán todos los múltiplos de 111: 333, 444, 555,… 999, 7 casos en total.

c) $200 \le n \le 299$

En este caso T depende del valor de n: Hay 11 casos fijos (el 2 y del "21" al "29") y $n - 200 + 1$ casos entre "200" y n. Luego $T = 11 + n - 200 + 1 = n - 188$ y por tanto

$$\frac{T}{n} = \frac{n-188}{n} = \frac{1}{k} \Leftrightarrow k(n-188) = n$$

Para resolver esta ecuación diofántica completamos cuadrados:

$$\frac{T}{n} = \frac{n-188}{n} = \frac{1}{k} \Leftrightarrow k(n-188) = n \Leftrightarrow kn - 188k - n = 0$$

$$0 = kn - 188k - n = (k-1)(n-188) - 188 \Leftrightarrow (k-1)(n-188) = 188 = 2^2 \cdot 47$$

Vamos estudiando los casos uno a uno:

$k-1=1$, $n-188 = 2^2 \cdot 47$ absurdo.

$k-1=2$, $n-188 = 2 \cdot 47 = 94 \Rightarrow n = 188 + 94 = 282$, $k = 3$

$k-1=2^2$, $n-188 = 47 \Rightarrow n = 188 + 47 = 235$, $k = 5$

$k-1=47$, $n-188 = 2^2 \Rightarrow n = 188 + 4 = 192 < 200$ absurdo.

$k-1=2 \cdot 47$, $n-188 = 2 \Rightarrow n = 188 + 2 = 190 < 200$ absurdo.

$k-1=2^2 \cdot 47$, $n-188 = 1 \Rightarrow n = 188 + 1 = 189 < 200$ absurdo.

Luego las soluciones posibles son dos: $n = 282$, $k = 3$ y $n = 235$, $k = 5$

Finalmente, tenemos $9 + 7 + 2 = 18$ casos aceptables.

Observación.

Otra forma alternativa de resolver el apartado (c) es la siguiente:

Sea $200 \le n \le 299$

Sea $x = n - 199$

$$\frac{T}{n} = \frac{x+11}{x+199} = \frac{1}{k} \Leftrightarrow k = \frac{x+199}{x+11} = \frac{x+11+188}{x+11} = \frac{x+11}{x+11} + \frac{188}{x+11} = 1 + \frac{188}{x+11} \Leftrightarrow$$

$$k - 1 = \frac{188}{x+11}$$

Luego

$k-1 \mid 188 = 2^2 \cdot 47$, y los factores aceptables de 188 son 47 y 94.

13.1.5

Basta aplicar $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} \Rightarrow \tau(n) = (a_1+1)(a_2+1)\ldots(a_r+1)$

$\tau(n)$ es impar $\Leftrightarrow a_i + 1$ es impar $1 \le i \le r \Leftrightarrow a_i$ es par $1 \le i \le r \Leftrightarrow a_i = 2b_i$ $1 \le i \le r$

$$\Leftrightarrow n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} = p_1^{2b_1} p_2^{2b_2} \ldots p_r^{2b_r} = \left(p_1^{b_1} p_2^{b_2} \ldots p_r^{b_r}\right)^2$$

13.1.6

Está claro que si $n = p^{q-1}$ con p, q primos, entonces $\sigma(n) = q - 1 + 1 = q$ es primo.
Sea $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$ y supongamos que $\tau(n) = (a_1 + 1)(a_2 + 1)..(a_r + 1)$ es primo. Entonces está claro que $r = 1$. Luego
$n = p^a$ y $\tau(n) = a + 1$ primo, y podemos escribir $n = p^{\tau(n)-1}$ con $\tau(n)$ primo, como queríamos.

13.1.7
$10^{99} = (2 \cdot 5)^{99} = 2^{99} \cdot 5^{99}$
El número total de divisores es $(99 + 1)(99 + 1) = 100^2 = 10000$
De estos divisores, los múltiplos de 10^{88} serán aquellos de la forma $2^a 5^b$, con $88 \le a, b \le 99$, es decir, $12 \cdot 12 = 144$ números.
Luego la probabilidad es $\frac{144}{10000} = \frac{6}{625}$

13.1.8
Puesto que 6 solo se factoriza como $2 \cdot 3$ o $6 \cdot 1$, el número n solo puede constar de dos factores primos:
$n = p^a q^b \Rightarrow \left.\begin{matrix} a+1=2 \\ b+1=3 \end{matrix}\right\} \Rightarrow a = 1, b = 2 \Rightarrow n = p \cdot q^2$ con $p \neq q$.
O bien:
$n = p^a$, $\Rightarrow a + 1 = 6 \Rightarrow a = 5 \Rightarrow n = p^5$

13.1.9
$10^{10} = (2 \cdot 5)^{10} = 2^{10} 5^{10}$, y sus divisores son todas las combinaciones posibles de la forma $n = 2^a 5^b$ con $0 \le a, b \le 10$. Hay $11^2 = 121$ en total.

$15^7 = (3 \cdot 5)^7 = 3^7 5^7$, y sus divisores son todas las combinaciones posibles de la forma $n = 3^a 5^b$ con $0 \le a, b \le 7$. Hay $8^2 = 64$ divisores posibles.
Pero los divisores de la forma $n = 3^0 5^b = 5^b$ con $0 \le b \le 7$ ya aparecen como divisores del primer número, por lo tanto los restamos. En total hay $64 - 8 = 56$ divisores.

$18^{11} = (2 \cdot 3^2)^{11} = 2^{11} 3^{22}$, y sus divisores son todas las combinaciones posibles de la forma $n = 2^a 3^b$ con $0 \le a \le 11$ y $0 \le b \le 22$. Son $12 \cdot 23 = 276$

Pero de estos están repetidos aquellos de la forma
$n = 2^a 3^0$ con $0 \le a \le 10$: 11 divisores, y aquellos de la forma
$n = 2^0 3^b$ con $1 \le b \le 7$: 7 divisores. (¡Atención! No contemos el divisor 1 dos veces)
Luego hay $276 - 11 - 7 = 258$ nuevos.

Así pues, hay un total de $121 + 56 + 258 = 435$ divisores.

13.1.10
Para $n = 1$, $\tau(1) = 1$, $\tau(2) = 2$ y está claro que no cumple la condición. Luego $n \ge 2$, y por tanto $\tau(n)$, $\tau(n+1) \ge 2$ y en consecuencia $\tau(n) + \tau(n+1) = 7 \Rightarrow \tau(n)$, $\tau(n+1) \le 5$.

$\tau(n)=1 \Leftrightarrow n=1$ y ya hemos visto que no cumple la igualdad del enunciado.

Luego las posibilidades que quedan son:

a) $\tau(n)=2, \tau(n+1)=5$

b) $\tau(n)=3, \tau(n+1)=4$

c) $\tau(n)=4, \tau(n+1)=3$

d) $\tau(n)=5, \tau(n+1)=2$

Teniendo en cuenta que:

$\tau(n)=2 \Rightarrow n=p$

$\tau(n)=3 \Rightarrow n=p^2$

$\tau(n)=5 \Rightarrow n=p^4$

$\tau(n)=4=2\cdot 2 \Rightarrow \begin{cases} n=p\cdot q,\ p\neq q \\ n=p^3 \end{cases}$

Tenemos

a) $n=p\ ,\ n+1=p^4$

b) $n=p^2,\ n+1=pq$

$n=p^2,\ n+1=p^3$

c) $n=p^3\ ,\ n+1=q^2$

$n=pq\ ,\ n+1=q^2$

d) $n=p^4$ primo y $n+1=q$ primo.

Observamos que en todos los casos, uno de los dos números consecutivos es la potencia par de un número primo, y con esto vamos probando casos:

$2^2=4 \rightarrow \begin{cases} n=3\,,\ n+1=4 \rightarrow \tau(3)=2\,,\ \tau(4)=3 \\ n=4\,,\ n+1=5 \rightarrow \tau(4)=3\,,\ \tau(5)=2 \end{cases}$ ninguna cumple.

$3^2=9 \rightarrow \begin{cases} n=8\,,\ n+1=9 \rightarrow \tau(8)=4\,,\ \tau(9)=3 \\ n=9\,,\ n+1=10 \rightarrow \tau(9)=3\,,\ \tau(10)=4 \end{cases}$ ambas cumplen la condición del enunciado.

$2^4=16 \rightarrow \begin{cases} n=15\,,\ n+1=16 \rightarrow \tau(15)=4\,,\ \tau(16)=5 \\ n=16\,,\ n+1=17 \rightarrow \tau(16)=5\,,\ \tau(17)=2 \end{cases}$ cumple la segunda.

$5^2=25 \rightarrow \begin{cases} n=24\,,\ n+1=25 \rightarrow \tau(24)=8\,,\ \tau(25)=3 \\ n=25\,,\ n+1=26 \rightarrow \tau(25)=3\,,\ \tau(26)=4 \end{cases}$ cumple la segunda.

$7^2=49 \rightarrow \begin{cases} n=48\,,\ n+1=49 \rightarrow \tau(48)=10\,,\ \tau(49)=3 \\ n=49\,,\ n+1=50 \rightarrow \tau(49)=3\,,\ \tau(50)=6 \end{cases}$ ninguna cumple.

$3^4=81 \rightarrow \begin{cases} n=80\,,\ n+1=81 \rightarrow \tau(80)=10\,,\ \tau(81)=5 \\ n=81\,,\ n+1=82 \rightarrow \tau(81)=5\,,\ \tau(82)=4 \end{cases}$ ninguna cumple.

$11^2=121 \rightarrow \begin{cases} n=120\,,\ n+1=121 \rightarrow \tau(120)=16\,,\ \tau(121)=3 \\ n=121\,,\ n+1=122 \rightarrow \tau(121)=3\,,\ \tau(122)=4 \end{cases}$ cumple la segunda.

$13^2=169 \rightarrow \begin{cases} n=168\,,\ n+1=169 \rightarrow \tau(168)=16\,,\ \tau(169)=3 \\ n=169\,,\ n+1=170 \rightarrow \tau(169)=3\,,\ \tau(170)=8 \end{cases}$ ninguna cumple.

$17^2 = 289 \rightarrow \begin{cases} n = 288\ ,\ n+1 = 289 \rightarrow \tau(288) = 18\ ,\ \tau(289) = 3 \\ n = 289\ ,\ n+1 = 290 \rightarrow \tau(289) = 3\ ,\ \tau(290) = 8 \end{cases}$ ninguna cumple.

$19^2 = 361 \rightarrow \begin{cases} n = 360\ ,\ n+1 = 361 \rightarrow \tau(360) = 24\ ,\ \tau(361) = 3 \\ n = 361\ ,\ n+1 = 362 \rightarrow \tau(361) = 3\ ,\ \tau(362) = 4 \end{cases}$ cumple la segunda.

Y paramos porque hemos conseguido las seis soluciones pedidas. El resultado es 8+9+16+25+121+361=540

Fuente de esta solución: www.artofproblemsolving.com/wiki/index.php/2019_AIME_I_Problems/Problem_9

13.1.11

$2004 = 2^2 \cdot 3 \cdot 167 \Rightarrow 2004^{2004} = \left(2^2 \cdot 3 \cdot 167\right)^{2004} = 2^{4008} \cdot 3^{2004} \cdot 167^{2004}$.

Los divisores de 2004^{2004} son todos los números de la forma

$d = 2^a \cdot 3^b \cdot 167^c$, con $0 \le a \le 4008$, $0 \le b \le 2004$, $0 \le c \le 2004$.

Luego $\tau(d) = (a+1)(b+1)(c+1)$, y por tanto

$\tau(d) = 2004 \Leftrightarrow (a+1)(b+1)(c+1) = 2^2 \cdot 3 \cdot 167$

O equivalentemente, todas las posibilidades x, y, z con $x\,y\,z = 2^2 \cdot 3 \cdot 167$ y $1 \le x \le 4009$, $1 \le y \le 2005$, $1 \le z \le 2005$.

Colocamos primero los "2": Hay 6 formas diferentes.
2 – 2 - /
2 - / - 2
/ - 2 – 2
2^2 - / - /
/ - 2^2 - /
/ - / - 2^2

Ahora tenemos que colocar el 3 y el 167, en cualquiera de las tres posiciones, luego el total será $6 \cdot 3 \cdot 3 = 54$ formas diferentes.

13.1.12
Sean J, C y Z las edades respectivas de Joey, Chloe y Zoe.
Tenemos que $J = C+1$ y $Z = 1$
En cada aniversario tenemos la siguiente pauta:

Zoe	1	2	3	4	Z
Chloe	C	C+1	C+2	C+3	C+Z-1
Joey	C+1	C+2	C+3	C+4	C+Z

Está claro que C es múltiple de 1, y existirán ocho números más $Z_1, Z_2, \ldots, Z_8$ tales que

$Z_1 \mid C + Z_1 - 1,\ Z_2 \mid C + Z_2 - 1,\ ...,\ Z_8 \mid C + Z_8 - 1$

Puesto que $Z_i \mid Z_i$, entonces está claro que $Z_i \mid C - 1$, es decir, el número $C - 1$ tiene exactamente ocho divisores diferentes de 1. Luego $C - 1$ tiene nueve divisores contando el 1. Aplicando 13.4, tenemos que

$$C - 1 = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$$

entonces

$$9 = (a_1 + 1)(a_2 + 1)..(a_r + 1)$$

Con un solo factor primo sería imposible, pues como mínimo tendríamos el resultado $C - 1 = 2^8 = 256$, una edad absurda.

Con dos factores primos, la única posibilidad aceptable para una edad es

$$9 = (2 + 1)(2 + 1) \Rightarrow C - 1 = 2^2 3^2 = 36$$

Y por tanto $C = 36 + 1 = 37 \Rightarrow J = C + 1 = 38$

Zoe	1	2	3	4	5	Z
Chloe	37	38	39	40	41	...
Joey	38	39	40	41	42	$C = 37 + Z$

Nos piden determinar el siguiente Z tal que $Z \mid J \Leftrightarrow Z \mid 37 + Z \Rightarrow Z \mid 37$, pero puesto que 37 es primo, la única posibilidad es $Z = 37 \Rightarrow J = 37 + 37 = 74$, y la respuesta correcta es $7 + 4 = 11$ (E).

13.1.13

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{N} \Leftrightarrow \frac{y + x}{xy} = \frac{1}{N} \Leftrightarrow \frac{xy}{x + y} = N \Leftrightarrow xy = N(x + y) \Leftrightarrow$$

$$xy - Nx - Ny = 0 \Leftrightarrow (x - N)(y - N) - N^2 = 0 \Leftrightarrow (x - N)(y - N) = N^2$$

Que esta ecuación tenga exactamente 2005 soluciones es una forma de decir que existen exactamente 2005 formas diferentes de escribir N^2 como producto de dos enteros positivos, es decir, que N^2 tiene exactamente 2005 divisores, pues existe una biyección clara entre los divisores de un número y sus expresiones como producto:

$d \mapsto d \cdot (N / d)$

Ahora aplicaremos el problema 13.5: El número N es un cuadrado perfecto si y solo si $\tau(N)$ es impar.

Si la factorización canónica de N es $N = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_n^{a_n}$, la factorización canónica de N^2 es $N^2 = p_1^{2a_1} \cdot p_2^{2a_2} \cdot ... \cdot p_n^{2a_n}$, y por lo tanto $\tau(N^2) = (2a_1 + 1)(2a_2 + 1)...(2a_n + 1) = 2005$

Por otro lado, $2005 = 5 \cdot 401$, luego la única formas posibles son:

a) $a_1 = 2$ y $a_2 = 200$, y por tanto $\tau(N) = (a_1 + 1)(a_2 + 1) = 3 \cdot 201 = 603$, un número impar, y por tanto N es un cuadrado perfecto.

b) $a_1 = 1002 \Rightarrow N = p_1^{1002+1} \Rightarrow \tau(N) = 1003$ impar, luego es un cuadrado perfecto.

13.1.17

Por la teoría estudiada sabemos que si $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$ es la descomposición en factores primos de n, entonces

$$d(n) = (a_1 + 1)(a_2 + 1)...(a_r + 1)$$

Por otro lado, $\sqrt[3]{n} = p_1^{a_1/3} p_2^{a_2/3} ... p_r^{a_r/3}$,

Y por tanto:

$$f(n) = \frac{d(n)}{\sqrt[3]{n}} = \frac{(a_1 + 1)(a_2 + 1)...(a_r + 1)}{p_1^{a_1/3} p_2^{a_2/3} ... p_r^{a_r/3}} = \prod_{1 \le k \le r} \frac{a_k + 1}{p_k^{a_k/3}}$$

Puesto que en todo momento estamos trabajando con números positivos, y la función $\sqrt[3]{x}$ es estrictamente positiva, el n que determina el máximo de la función anterior será el n que determina el máximo de la función

$$f^3(n) = \prod_{1 \le k \le r} \frac{(a_k + 1)^3}{p_k^{a_k}}$$

Fijado un número primo p_k, la sucesión $\frac{(a_k + 1)^3}{p_k^{a_k/3}}$ es una sucesión con límite 0, pues es un cociente entre una potencial y una exponencial. Tenemos que estudiar el comportamiento para los diferentes valores de $p_k \in \{2, 3, 5, 7, 11, ...\}$

$p_k = 2, a_k = 1 \Rightarrow (a_k + 1)^3 / p_k^{a_k} = 4$
$p_k = 2, a_k = 2 \Rightarrow (a_k + 1)^3 / p_k^{a_k} = 27/4$
$p_k = 2, a_k = 3 \Rightarrow (a_k + 1)^3 / p_k^{a_k} = 8$ → Máximo
$p_k = 2, a_k = 4 \Rightarrow (a_k + 1)^3 / p_k^{a_k} = 125/16 \cong 7.81$

$p_k = 3, a_k = 1 \Rightarrow (a_k + 1)^3 / p_k^{a_k} = 8/3 \cong 2.67$
$p_k = 3, a_k = 2 \Rightarrow (a_k + 1)^3 / p_k^{a_k} = 3$ → Máximo
$p_k = 3, a_k = 3 \Rightarrow (a_k + 1)^3 / p_k^{a_k} = 64/27 \cong 2.37$

$p_k = 5, a_k = 1 \Rightarrow (a_k + 1)^3 / p_k^{a_k} = 8/5 \cong 1.6$ → Máximo
$p_k = 5, a_k = 2 \Rightarrow (a_k + 1)^3 / p_k^{a_k} = 27/25 \cong 1.08$

$p_k = 7, a_k = 1 \Rightarrow (a_k + 1)^3 / p_k^{a_k} = 8/7 \cong 1.14$ → Máximo
$p_k = 7, a_k = 2 \Rightarrow (a_k + 1)^3 / p_k^{a_k} = 27/49 \cong 0.55$

$p_k = 11, a_k = 1 \Rightarrow (a_k + 1)^3 / p_k^{a_k} = 8/11 < 1$

Vemos que, para todo $p_k \ge 11$ y para todo $a_i \ge 1$ el factor resultante es menor que 1 y por tanto disminuye el valor de la función. Así pues, el máximo de esta función lo encontraremos para $n = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 2520$

Y por tanto la respuesta correcta es $2 + 5 + 2 + 0 = 9$ (E)

Observación: Para no tener que calcular el producto final y ganar tiempo, se puede argumentar que el resultado será múltiplo de $3^2=9$, y por tanto la suma de sus cifras será también múltiplo de 9, y la respuesta (E) es la única con esta condición.

Fuente de esta solución: https://artofproblemsolving.com/wiki/index.php/2021_AMC_12A_Problems/Problem_25

13.2.5

$1815=3\cdot5\cdot11^2$

Sabemos que $n=2^a3^b$ para ciertos enteros positivos a,b. Sabemos que entonces

$$\sigma(n)=\frac{2^{a+1}-1}{2-1}\cdot\frac{3^{b+1}-1}{3-1}=\frac{1}{2}\left(2^{a+1}-1\right)\left(3^{b+1}-1\right)$$

A falta de algo mejor, vamos viendo los diferentes valores que se obtienen:

k	$2^{k+1}-1$	$3^{k+1}-1$
1	3	8
2	7	$26=2\cdot13$
3	$15=3\cdot5$	$80=2^4\cdot5$
4	31	$242=2\cdot11^2$
5	$63=3\cdot31$	$728=2^3\cdot7\cdot13$
…		

Vemos que la única combinación que se adapta a nuestro problema es $a=3$ y $b=4$: $\frac{1}{2}\left(2^{3+1}-1\right)\left(3^{4+1}-1\right)=\frac{1}{2}3\cdot5\cdot2\cdot11^2=1815$. Así pues, $n=2^33^4=8\cdot81=648$.