PEQUEÑO INSTITUTO DE MATEMATICAS

Hoja de Aritmética III

Fecha: 1, 8, 15 de Marzo de 2024 **Grupo: Mercurio**

El teorema de Bezout

Consideremos el problema de verter una cantidad específica de líquido utilizando dos (a veces tres) recipientes vacíos. Solo se permiten dos operaciones: vaciar un recipiente y llenar otro hasta el borde.

Una persona tiene un barril con 12 pintas de vino y quiere regalar la mitad del vino, pero no tiene un recipiente de 6 pintas. Sin embargo, tiene dos recipientes vacíos de 8 pintas y 5 pintas. ¿Cómo se puede verter exactamente 6 pintas de vino utilizando estos recipientes?

Este es el problema más conocido de este tipo; se llama el problema de Poisson. El famoso matemático, y físico francés Siméon Denis Poisson (1781-1840) lo resolvió en su juventud y posteriormente dijo que este problema fue lo que lo inspiró a convertirse en matemático.

La solución al problema se puede escribir de la siguiente manera:

Recipiente de 8 pintas	0	8	3	3	0	8	6	6
Recipiente de 5 pintas	0	0	5	0	3	3	5	0

Debes entenderlo de la siguiente manera. Al principio, ambos recipientes están vacíos (primera columna). Llenamos el recipiente de 8 pintas (segunda columna), luego llenamos el recipiente de 5 pintas desde el primero (tercera columna), luego vertemos esas 5 pintas del recipiente más pequeño al barril que contenía 12 pintas (cuarta columna), luego transferimos 3 pintas de vino del recipiente de 8 pintas al recipiente de 5 pintas (quinta columna) y así sucesivamente hasta que el recipiente más grande tenga 6 pintas de vino.

Intenta resolver el problema de otra manera, llenando primero el recipiente de 5 pintas. ¿No será la solución más corta?

Resuelve los siguiente problemas

Problema 1. ¿Cómo se puede obtener exactamente 1 litro de agua de un río utilizando dos bidones vacíos, uno de tres litros y otro de cinco litros?

Solución.

Recipiente de 3 litros	0	0	3	0	2	2	3	0	3
Recipiente de 5 litros	0	5	2	2	0	5	4	4	1

□

Problema 2. ¿Es posible recoger exactamente 4 litros de agua del río utilizando dos cubos vacíos, uno de 12 litros y otro de 9 litros?

Solución. Dado que las capacidades iniciales de los cubos son divisibles por 3, en cualquier trasvase de uno a otro y al recoger agua del río, en cada uno de ellos habrá una cantidad de agua con un volumen divisible por 3. Pero dado que 4 no es divisible por 3, entonces no se puede obtener 4 litros de agua. □

Pensemos en la generalización del apartado anterior. Supongamos que tenemos dos recipientes vacíos con capacidades de a litros y b litros, y se necesita recoger exactamente c litros de agua del río, donde a, b y c son números naturales, y c no supera el número más grande entre a y b. Si el número c no es divisible por el máximo común divisor de los números a y b, entonces, de manera similar a lo anterior, no es posible lograrlo.

(*Recordatorio*: d es el máximo común divisor de a y b si d divide a ambos y es el más grande con esta propiedad.)

Problema 3. ¿Qué sucede si c es divisible por el máximo común divisor de los números a y b? Demuestra que en este caso, el problema siempre tiene una solución. En particular, esto siempre es posible si los números a y b son coprimos.

(Ayuda 1: usa la identidad de Bezout: si el máximo común divisor de a y b divide a c entonces c se puede expresar como $c = a \cdot x + b \cdot y$, donde x, y son enteros.

Ayuda 2: si te resulta difícil trabajar con letras, piensa que $a = 8$ y $b = 11$.)

Solución. El caso $a = b$ es obvio y por eso consideramos el caso cuando son distintos.

Suponemos que el primer recipiente contiene a litros y el segundo b y ademas $a > b$.

Vamos a ver que si tenemos en uno de los recipientes z litros y $0 \leq z \leq b$ entonces podemos obtener $z + a - b$ litros:

Recipiente de a litros	0	a	$a - (b - z) = z + a - b$
Recipiente de b litros	z	z	b

Ahora suponemos que $c = x \cdot a - y \cdot b$ con $x, y > 0$. Entonces podemos obtener c en y pasos. En el primer paso obtenemos $c_1 = a - b$. Supongamos que después de k pasos tenemos c_k. Entonces en el siguiente paso hacemos lo siguiente:

(i) si $c_k \leq b$ obtenemos $c_{k+1} = c_k + (a - b)$ de forma como hemos explicado antes;

(ii) si $c_k > b$, ponemos c_k en el primer recipiente y le quitamos b: $c_{k+1} = c_k - b$.

Por último suponemos que $c = y \cdot b - x \cdot a$ con $x, y > 0$. Existe m tal que $x \leq m \cdot b$. Entonces

$$c = (m \cdot b - x) \cdot a - (m \cdot a - x) \cdot b$$

y podemos obtener c como antes. □

Teorema 1 (La identidad de Bezout)**.** *Si el máximo común divisor de a y b divide a c entonces c se puede expresar como $c = a \cdot x + b \cdot y$, donde x, y son enteros.*

Demostración. Tomemos el conjunto

$$S = \{ax + by > 0 : x, y \in \mathbb{Z}\}.$$

Sin pérdida de generalidad, supongamos que $a < b$. Entonces, $b - a > 0$ está en S, por lo que S es un conjunto no vacío de números naturales positivos. Entonces existe un elemento mínimo $d \in S$, que sabemos que tiene la forma $ax' + by'$. Existen q y r con $0 \leq r < d$ tal que $a = qd + r$.

Pero entonces $r = a - qd$ es un número no negativo de la forma $ax + by$, pero más pequeño que d, por lo que debe ser necesariamente cero. Esto significa que d divide a a. Por un argumento completamente análogo, se sigue que d divide a b. Entonces, d es un divisor común de a y b. Pero si e es cualquier divisor común de a y b, debe dividir a $d = ax' + by'$. Según la definición del máximo común divisor, acabamos de demostrar que $d = ax' + by'$ es el máximo común divisor de a y b.

Si d divide a c, entonces está claro que c también se puede expresar como $c = a \cdot x + b \cdot y$. □

Observamos que la demostración anterior proporciona una propiedad adicional del máximo común divisor d de a y b: si e divide a a y a b, entonces e divide a d.

Ahora planteamos la siguiente pregunta. Dados $a, b \in \mathbb{Z}$, ¿cómo encontrar $x, y \in \mathbb{Z}$ tales que $\text{mcd}(a, b) = x \cdot a + y \cdot b$? Antes de contestar a esta pregunta, resolvemos primero el siguiente ejercicio.

Problema 4. Sean $a, b, q, r \in \mathbb{Z}$, tales que $a = q \cdot b + r$. Demuestra que $\text{mcd}(a, b) = \text{mcd}(b, r)$.

Proof. Esta claro que un elemento entero e divide a a y b si y sólo si e divide a b y r. Por lo tanto, $\text{mcd}(a, b) = \text{mcd}(b, r)$. □

Este ejercicio nos proporciona una forma muy rápida de calcular $\mathrm{mcd}(a, b)$. En vez de formular el algoritmo de manera formal veamos un ejemplo. Este algoritmo se llama el **algoritmo de Euclides**.

Ejemplo resuelto. Calcula $\mathrm{mcd}(1026, 873)$ sin factorizar los números.

Solución. El algoritmo de Euclides consiste en sucesivas divisiones entre los números dados hasta llegar a un cociente de cero. El último divisor no nulo es el máximo común divisor de los números originales.

Dividimos 1026 por 873: $1026 = 1 \cdot 873 + 153$. El Ejercicio **??** nos dice que $\mathrm{mcd}(1026, 873) = \mathrm{mcd}(873, 153)$.

Ahora, dividimos 873 por 153: $873 = 5 \cdot 153 + 18$. Entonces $\mathrm{mcd}(873, 153) = \mathrm{mcd}(153, 18)$.

Luego, dividimos 153 por 18: $153 = 8 \cdot 18 + 9$. Tenemos $\mathrm{mcd}(153, 18) = \mathrm{mcd}(18, 9)$.

Finalmente, como $18 = 2 \cdot 9$, obtenemos que

$$\mathrm{mcd}(1026, 873) = \mathrm{mcd}(873, 153) = \mathrm{mcd}(153, 18) = \mathrm{mcd}(18, 9) = 9. \quad \square$$

Ahora podemos explicar como obtener los coeficientes en la identidad de Bezout. Otra vez en vez de explicar el procedimiento formalmente presentaremos un ejemplo. El algoritmo que usamos se llama el **algoritmo inverso de Euclides**.

Ejemplo resuelto. Encuentra algunos eneros x e y que cumplen $\mathrm{mcd}(1026, 873) = 1026 \cdot x + 873 \cdot y$.

Solución. Recuperamos las igualdades aparecidas cuando aplicamos el algoritmo de Euclides para calcular $\mathrm{mcd}(1026, 873)$, escribiendo las de esta forma

$$\begin{aligned} 153 &= 1026 - 1 \cdot 873 \\ 18 &= 873 - 5 \cdot 153 \\ 9 &= 153 - 8 \cdot 18 \end{aligned}$$

El proceso es ir sustituyendo desde abajo hacia arriba. En la última ecuación sustituimos 18 y agrupamos los terminos:

$$9 = 153 - 8 \cdot 18 = 153 - 8 \cdot (873 - 5 \cdot 153) = 41 \cdot 153 - 8 \cdot 873.$$

Ahora sustituimos 153 y agrupamos:

$$9 = 41 \cdot 153 - 8 \cdot 873 = 41 \cdot (1026 - 1 \cdot 873) - 8 \cdot 873 = 41 \cdot 1026 - 49 \cdot 873.$$

Por lo tanto $x = 41$ e $y = -49$ son soluciones buscadas. $\square$

Problema 5. Encuentra algunos eneros x e y que cumplen

1. $\mathrm{mcd}(1067, 893) = 1067 \cdot x + 893 \cdot y$.
2. $\mathrm{mcd}(2037, 1512) = 2037 \cdot x + 1512 \cdot y$.

División módulo n

Uno de los propósitos de esta sección es demostrar el Teorema fundamental de Aritmética.

Teorema 2 (El teorema fundamental de Aritmética)**.** *Todo entero positivo $n > 1$ puede ser representado exactamente de una única manera como un producto de potencias de números primos:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i},$$

donde $p_1 < p_2 < \ldots < p_k$ son primos y α_i son enteros positivos.

Seguramente lo has visto antes y te parece tan evidente que piensas que no requiere demostración. Sin embargo, su demostración rigurosa no es tam sencilla y requiere el teorema de Bezout que acabamos de ver.

Vamos a resolver las siguientes ecuaciones en congruencias:

Ejemplo resuelto. Encuentra **todas** las soluciones de estas ecuaciones.

a) $2x \equiv 4 \pmod 5$

b) $2x \equiv 2 \pmod 5$

c) $2x \equiv 5 \pmod{10}$

d) $2x \equiv 6 \pmod{10}$

e) $6x \equiv 2 \pmod{10}$

f) $15x \equiv 0 \pmod{10}$

Solución. a) $x \equiv 2 \pmod 5$

b) $x \equiv 1 \pmod 5$

c) No hay ninguna solución. .

d) $x \equiv 3, 8 \pmod{10}$

e) $x \equiv 2, 7 \pmod{10}$

f) $x \equiv \pmod 2 \equiv 0, 2, 4, 6, 8, \pmod{10}$

□

Vemos que algunas ecuaciones en congruencias tienen una solución, algunas ninguna y algunas tienen incluso varias soluciones. Vamos a intentar a explicarlo. Si queremos resolver la ecuación $2x = 4$ lo que vamos a hacer es dividir 4 por 2. ¿Podemos hacer algo parecido con las congruencias?

Ya sabemos "multiplicar" módulo n. Tómate un momento para hacer analepsis[1] a tu más tierna infancia y piensa qué significaría "dividir" módulo n. ¿Qué significaría decir que $3/2 \equiv 4 \pmod 5$? ¿Qué era el "inverso"? ¿Qué tienen que ver dividir con el inverso? ¿Qué significaría decir que un número es el inverso de 2 módulo 5? ¿Puede ser que todos los números tengan inverso módulo n?

Que yo recuerde, decir que $3/2 = 4$ es decir que $2 \cdot 4 = 3$ (y también que 4 es el único número que cumple esto). El inverso de n es el (único) número x que cumple que $xn = 1$. Dividir es lo mismo que multiplicar por el inverso. Decir que 3 es el inverso de 2 módulo 5 es decir que $3 \cdot 2 \equiv 1 \pmod 5$. No todos los números tienen inverso: el 0 no tiene inverso. 2 tampoco tiene inverso módulo 10, porque $2x$ siempre es par y no puede ser 1.

Problema 6. Demuestra que si para ciertos a y n la ecuación $ax \equiv 1 \pmod n$ tiene solución, entonces sólo hay una solución módulo n.

Solución. Si x, x' son ambas soluciones, entonces

$$x \overset{ax' \equiv 1}{\equiv} ax'x \overset{ax \equiv 1}{\equiv} x' \pmod n.$$

□

Problema 7. Demuestra que si $\mcd(a, n) \neq 1$, entonces $ax \equiv 1 \pmod n$ no tiene solución x.

Solución. Supongamos que algún primo p divide a a y a n. No puede ser que $n|ax - 1$, porque entonces $p|ax - 1$, y como $p|a$, tiene que ser que $p|x$. □

Problema 8. Supón ahora que $\mcd(a, n) = 1$.

a) Demuestra que si $ax \equiv 0 \pmod n$, entonces $x \equiv 0 \pmod n$ (ayuda: usa el teorema de Bezout).

b) Demuestra que si $ax \equiv ay \pmod n$, entonces $x \equiv y \pmod n$.

c) Demuestra que los números $0, a, 2a, 3a, \ldots, (n-1)a$ son todos distintos módulo n.

d) Demuestra que existe un único x tal que $ax \equiv 1 \pmod n$.

Solución. a) Por el teorema de Bezout existen $b, c \in \mathbb{Z}$, tales que $ba + cn = 1$. Por lo tanto $ba \equiv 1 \pmod n$. Entonces $bax \equiv x \pmod n$. Como $ax \equiv 0 \pmod n$, concluimos que $x \equiv 0 \pmod n$.

b) $ax \equiv ay \Rightarrow a(x - y) \equiv 0 \overset{\text{Parte a)}}{\Rightarrow} x - y \equiv 0 \Rightarrow x \equiv y$

[1] *Analepsis*: Pasaje de una obra literaria que trae una escena del pasado rompiendo la secuencia cronológica. Sin.: flashback.

c) Como $0, 1, 2, \ldots, n-1$ son todos distintos módulo n, por la parte b) concluimos que multiplicados por a siguen siendo todos distintos.

d) Si tomamos los restos de dividir $0, a, 2a, \ldots, (n-1)a$ por n, tenemos n restos distintos (por la parte (c)) entre 0 y $n-1$, así que tienen que aparecer todos los restos, en particular, $xa = 1$ para algún x. Para ver que es único, lo hemos hecho hace dos ejercicios.

□

Teorema de *inserte su nombre aquí*

Módulo n, a tiene inverso si y sólo si a y n cumplen que...

Entonces, módulo n se puede dividir por a, haciendo...

Problema 9. Sea p un número primo y $a, b \in \mathbb{Z}$. Demuestra que si p divide a ab entonces p divide a a o p divide a b. (Queremos usar este ejercicio para demostrar el teorema fundamental de Aritmética. Por eso no usa el teorema fundamental de Aritmética para resolver este ejercicio).

Solución. Queremos ver que si $ab \equiv 0 \pmod{p}$, entonces $a \equiv 0 \pmod{p}$, o $b \equiv 0 \pmod{p}$.

Si $a \not\equiv 0 \pmod{p}$, entonces existe $c \in \mathbb{Z}_n$ tal que $ca \equiv 1 \pmod{p}$. Por lo tanto

$$b \equiv (c \cdot a) \cdot b \equiv c \cdot (a \cdot b) \equiv 0 \pmod{p}. \quad \square$$

Ahora podemos demostrar el Teorema fundamental de Aritmética.

Demostración del Teorema fundamental de Aritmética. La existencia de una factorización es evidente, porque cualquier descomposición en factores tiene que terminar en algún momento.

Para demostrar la unicidad supón que hay dos factorizaciones diferentes y usando el Problema **??** obtén una contradicción. □

Problema 10. Sea p primo. Supongamos que $a^2 \equiv 1 \pmod{p}$. Demuestra que $a \equiv \pm 1 \pmod{p}$.

Solución. Si $a^2 \equiv 1 \pmod{p}$, entonces, $(a-1)(a+1) \equiv 0 \pmod{p}$. Si $a - 1 \not\equiv 0 \pmod{p}$, existe $b \in \mathbb{Z}$ tal que $b(a-1) \equiv 1 \pmod{p}$. Por lo tanto,

$$0 \equiv b \cdot 0 \equiv b \cdot (a-1)(a+1) \equiv (a+1) \pmod{p}.$$

Luego, $a \equiv -1 \pmod{p}$. □

Teorema 3 (Teorema de Wilson)**.** *Sea p un primo impar. Entonces* $(p-1)! \equiv -1 \pmod{p}$.

Demostración. Como hemos visto para cada número $a \in \{1, \ldots, p-1\}$ existe $b \in \{1, \ldots, p-1\}$ tal que $ab \equiv 1 \pmod{p}$. Además, $a = b$ sólo en los casos $a = 1$ y $a = p-1$. Por lo tanto, si agrupamos el producto $1 \cdot 2 \cdot \ldots (p-1)$ en parejas de invertibles, obtenemos que en el producto se quedan sólo 1 y $p-1$. Así que concluimos que $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$. □

Vamos a dar un paso más en nuestra forma de trabajar con congruencias. Dado un número n natural y a un número entero entenderemos por $[a]_n$ todos los enteros $b \in \mathbb{Z}$ que cumplen $b \equiv a \pmod{n}$. Por ejemplo, $[2]_5 = \{2, 7, -3, -8. - 10008, 127, \ldots\}$. Esta nueva notación evita escribir cada vez $\equiv \pmod{n}$.

Con esta notación tenemos que $[a]_n + [b]_n = [a+b]_n$ y $[a]_n[b]_n = [ab]_n$. En total hay n congruencias (mód n) y el conjunto de todas las congruencias se denota $\mathbb{Z}_n$. Por ejemplo, $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$. La tablas de la suma y la multiplicación de $\mathbb{Z}_5$ son las siguientes.

+	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$

X	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0_5$
$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

Las tablas hay que entender de la siguiente forma: el resultado de operación de a y b está en la intersección de la fila de a y la columna de b.

Problema 11. Construye la tabla de multiplicación de $\mathbb{Z}_6$.

El teorema de Wilson se puede interpretar de la siguiente forma. Si p es primo, entonces

$$\prod_{[0]_p \neq [b]_p \in \mathbb{Z}_p} [b]_p = [-1]_p.$$

Problema 12. Sea n un número natural. Demuestra que si n es coprimo con $a \in \mathbb{Z}$. Entonces cuando $[b]_n$ recorre todas las congruencias modulo n, $[a]_n[b]_n$ también las recorre y además cada congruencia aparece exactamente una vez. (En la tabla de multiplicación de $\mathbb{Z}_n$, $[a]_n[b]_n$ son los elementos que están en la fila que corresponde a $[a]_n$).

Solución. Es el Problema **??**(c). □

Teorema 4 (El pequeño teorema de Fermat)**.** *Sea p un número primo. Si a no es divisible por p, entonces* $a^{p-1} \equiv 1 \pmod{p}$.

Demostración. Queremos ver que $[a^{p-1}]_p = [1]_p$. Por el Teorema de Wilson el producto de todas las congruencias coprimas con p nos dan $[-1]_p$. Por lo tanto, por el Problema **??**, también tenemos que

$$\prod_{[0]_p \neq [b]_p \in \mathbb{Z}_p} [a]_p[b]_p = [-1]_p.$$

Este producto es igual a

$$\prod_{[0]_p \neq [b]_p \in \mathbb{Z}_p} [a]_p[b]_p = ([a]_p)^{p-1} \prod_{[0]_p \neq [b]_p \in \mathbb{Z}_p} [b]_p = [a^{p-1}]_p \cdot [-1]_p.$$

Es decir, $[a^{p-1}]_p \cdot [-1]_p = [-1]_p$. Por lo tanto, $[a^{p-1}]_p = [1]_p$. □

El teorema chino del resto

Se llama el teorema chino del resto por este problema del siglo V, del libro Sunzi Suanjing (El Manual Matemático de Sunzi).

Problema 13. Tenemos un número indeterminado de cosas. Si las contamos de tres en tres, sobran dos; de cinco en cinco, sobran tres; y de siete en siete, sobran dos. ¿Cuántas hay?

Notemos que podemos escribir el problema de Sunzi como un sistema de ecuaciones.

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

Teorema chino del resto

Si n, m son primos entre sí, entonces el sistema de ecuaciones

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

tiene una solución, que es única módulo nm.

Problema 14. Demuestra el teorema chino del resto. Aquí tienes unas posibles pistas.

a) Demuestra que los restos de un número x módulo n y módulo m sólo dependen de su resto módulo nm. Concluye que para cada resto posible módulo nm, obtenemos una pareja de restos, al dividir por n y por m.

b) Cuenta cuántos posibles restos módulo nm hay, y cuántas posibles parejas de restos módulo n y módulo m hay. Por ejemplo, si $n = 2$ y $m = 3$, hay 6 posibles parejas:

$$(0 \text{ (mód 2) y } 0 \text{ (mód 3)}), (1 \text{ y } 0), (0 \text{ y } 1), (1 \text{ y } 1), (0 \text{ y } 2), (1 \text{ y } 2).$$

c) Si tomamos todos los restos posibles, demuestra que todas las parejas de restos (módulo n y módulo m) son distintas. (Recuerda que n y m son primos entre sí). Por ejemplo, para $n = 2$ y $m = 3$, obtenemos parejas distintas:

(mód 6)	(mód 2)	(mód 3)
0	0	0
1	1	1
2	0	2
3	1	0
4	0	1
5	1	2

d) Demuestra que cada pareja de restos (a, b) se obtiene exactamente para un x.

Solución. a) Esto consiste en decir que si $x \equiv y$ (mód nm), entonces también ocurre que $x \equiv y$ (mód n) (o módulo m, pero es el mismo razonamiento). Es decir, que si $mn|y - x$, entonces $n|y - x$.

b) Hay nm restos módulo nm (desde 0 hasta $nm - 1$). Como hay n restos módulo n y m restos módulo m, por la regla del producto, hay nm posibles parejas.

c) Si x, x' (mód nm) nos dieran parejas iguales, esto significa que $x - x' \equiv 0$ (mód n) y también $x - x' \equiv 0$ (mód m). Es decir, $n|x - x'$ y $m|x - x'$. **Como** $\text{mcd}(n, m) = 1$, esto quiere decir que $nm|x - x'$: cada primo de la factorización de nm aparece sólo en la factorización de n o sólo en la de m. Por tanto, $x \equiv x'$ (mód nm), es decir, eran el mismo resto.

d) Como las parejas que obtenemos son todas distintas, hay nm parejas que obtenemos, es decir, obtenemos todas. Al ser distintas, las obtenemos todas una sóla vez.

□

Si n, m son primos entre sí, vamos a describir un método general para resolver el sistema.

$$\begin{cases} x \equiv a \text{ (mód } n) \\ x \equiv b \text{ (mód } m) \end{cases}$$

Observemos que $x = a + t \cdot n = b + s \cdot m$ para algunos números enteros t y s. Por lo tanto, $b - a = t \cdot n - s \cdot m$. Como n, m son primos entre sí, el algoritmo inverso de Euclides nos proporciona números enteros t_0 y s_0 tales que $1 = t_0 \cdot n - s_0 \cdot m$. Por lo tanto, podemos poner $t = (b - a)t_0$ y concluir que $x = a + (b - a)t_0 \cdot n$ es una solución del sistema.

Problema 15. Resuelve estos sistemas de ecuaciones (es decir, encuentra todas las soluciones).

a) $\begin{cases} x \equiv 0 \text{ (mód } 3) \\ x \equiv 0 \text{ (mód } 5) \\ x \equiv 0 \text{ (mód } 7) \end{cases}$ b) $\begin{cases} x \equiv 2 \text{ (mód } 3) \\ x \equiv 2 \text{ (mód } 5) \\ x \equiv 2 \text{ (mód } 7) \end{cases}$ c) $\begin{cases} x \equiv 2 \text{ (mód } 3) \\ x \equiv 3 \text{ (mód } 5) \\ x \equiv 1 \text{ (mód } 7) \end{cases}$

d) $\begin{cases} x \equiv 8 \text{ (mód 3)} \\ x \equiv 8 \text{ (mód 5)} \\ x \equiv 8 \text{ (mód 7)} \end{cases}$ e) $\begin{cases} x \equiv 1 \text{ (mód 3)} \\ x \equiv 1 \text{ (mód 5)} \\ x \equiv 2 \text{ (mód 10)} \end{cases}$ f) $\begin{cases} x \equiv 1 \text{ (mód 3)} \\ x \equiv 1 \text{ (mód 5)} \\ x \equiv 6 \text{ (mód 10)} \end{cases}$

Solución. a) $x \equiv 0 \text{ (mód 105)}$.

b) $x \equiv 2 \text{ (mód 105)}$.

c) $x \equiv 8 \text{ (mód 105)}$.

d) $x \equiv 8 \text{ (mód 105)}$.

e) No tiene solución, porque si $x \equiv 2 \text{ (mód 10)}$, entonces $x \equiv 2 \text{ (mód 5)}$.

f) $x \equiv 16 \text{ (mód 30)}$

□

Problema 16. Describe un método para resolver

$$\begin{cases} x \equiv a \text{ (mód } n) \\ x \equiv b \text{ (mód } m) \end{cases}$$

sin suponer que n y m son coprimos.

Problema 17. Si no hubiera años bisiestos, calcula cada cuántos años empezaría el año en lunes.

Solución. Cada 7, porque 7 y 365 son primos entre sí: el año empezaría en todos los días posibles una vez cada 7 años. □

Problema 18. Dice Wikipedia que el año santo de Santiago de Compostela ocurre los años en los que el 25 de julio es domingo. Esto sucede con una cadencia regular de 6-5-6-11 años[2]. También dice que las cigarras del género *Magicicada* que salen del subsuelo a reproducirse cada 13 años y otras cada 17. En 2024, coincidirán las 2 en Illinois (de las poblaciones XIX y XIII, me podéis verificar la información).

- Explica qué es eso de la cadencia regular de 6-5-6-11 años.
- Los último cuatro años santos fueron 1999, 2004, 2010 y 2021. ¿Cuándo será la próxima vez que coincida el año santo con la salida de las poblaciones XIX y XIII)?

Solución. Un ciclo de 4 años son $365 \cdot 3 + 366 \equiv 1 \cdot 3 + 2 \equiv 5 \text{ (mód 7)}$ días. Esto significa que si un 25 de julio de domingo, cuatro años después será martes, 4 años después será jueves, sábado, lunes, etc hasta que pasen 28 años y vuelva a ser domingo. Dentro del ciclo de 28 años, hay qué ver en qué días es domingo. Después de un año normal, el 25 de julio retrocede un día, y después de un año bisiesto avanza un día. Podemos hacer una tabla pues. Voy a poner los años en columnas para ahorrar espacio, y numerar los días de la semana, con el domingo en el 0.

	Años 0-4	4- 8	8- 12	12-16	16-20	20-24	24-28
Año 0 (mód 4)	0	2	4	6	1	3	5
Año 1 (mód 4)	6	1	3	5	0	2	4
Año 2 (mód 4)	5	0	2	4	6	1	3
Año 3 (mód 4)	4	6	1	3	5	0	2

Efectivamente, se repite cada 6-5-6-11 años.

Si llamamos x al año que buscamos, para que sea año santo tiene que ser congruente con 1999, 2004, 2010 ó 2021 módulo 28, es decir, con 11, 16, 22 ó 5. Las cigarras salen cada $\text{mcm}(13, 17) = 13 \cdot 17 = 221$ años, con lo que salen cuando el año es congruente con 2024 módulo 221, es decir, con 35. El próximo año de coincidencia será la solución del sistema de ecuaciones:

$$\begin{cases} x \equiv 5, 11, 16, 22 & \text{(mód 28)} \\ x \equiv 35 & \text{(mód 221)} \end{cases}$$

[2]Estoy ignorando lo que pasa cuando el año es divisible por 100, que no siempre es bisiesto, como bien sabes

Vamos a escribir $x = 221y + 35$, con lo que tenemos que

$$221y + 35 \equiv -3y + 7 \equiv 5, 11, 16, 22 \text{ (mód 28)} \Leftrightarrow -3y \equiv -2, 4, 9, 15 \text{ (mód 28)}$$

El inverso de -3 módulo 28 es 9, con lo que tenemos que

$$y \equiv -18, 36, 81, 135 \equiv 10, 8, -3, -5 \text{ (mód 28)}$$

Así que podemos escribir $y = 28z + \{-10, -5, -3, 8\}$, y sustituyendo,

$$x = 6188y + \left\{ \begin{array}{c} -2210 \\ -1105 \\ -663 \\ 1768 \end{array} \right\}$$

El próximo año es 3978. □

Problemas

Problema 19. Un grupo de m amigos tiene n magdalenas iguales. Quieren dividir las magdalenas entre todos de manera que cada amigo reciba la misma cantidad, y lo quieren hacer dividiendo cada magdalena en algún número de partes (que no tienen por qué ser iguales, ni cada magdalena estar dividida de la misma forma), y luego asignando una o varias de esas partes a cada persona.

1. Si $m = 3$ y $n = 5$, demuestra que pueden dividir las magdalenas de manera que todas las piezas sean estrictamente más grandes que $\frac{1}{3}$ de magdalena.

2. Si $m = 5$ y $n = 3$, demuestra que pueden dividir las magdalenas de manera que todas las piezas sean estrictamente más grandes que $\frac{1}{5}$ de magdalena.

Solución. 1. Cada persona tiene que recibir $\frac{5}{3} = \frac{20}{12}$ magdalenas. Tenemos que $\frac{7}{12} > \frac{1}{2} > \frac{5}{12} > \frac{1}{3}$. Si dividimos 4 de las magdalenas en una parte de $\frac{7}{12}$ de magdalena y otra de $\frac{5}{12}$, y la última magdalena en 2 partes iguales, tenemos que $\frac{5}{12} + \frac{5}{12} + \frac{5}{12} + \frac{5}{12} = \frac{7}{12} + \frac{7}{12} + \frac{1}{2} = \frac{20}{12}$. Por tanto, podemos asignar a una persona las cuatro partes de tamaño $\frac{5}{12}$, y a cada una de las otras dos personas dos partes de tamaño $\frac{7}{12}$ y una parte de tamaño $\frac{1}{2}$.

2. Cada persona tiene que recibir $\frac{3}{5} = \frac{12}{20}$ magdalenas. Tenemos que $\frac{7}{20} > \frac{6}{20} > \frac{1}{4} > \frac{1}{5}$. Si dividimos dos de las magdalenas en dos partes de $\frac{7}{20}$ de magdalena y otra de $\frac{6}{20}$, y la última magdalena en 4 partes iguales, tenemos que $\frac{1}{4} + \frac{7}{20} = \frac{6}{20} + \frac{6}{20} = \frac{12}{20}$. Por tanto, podemos asignar a una persona las dos partes de tamaño $\frac{6}{20}$, y a cada una de las otras cuatro personas una parte de tamaño $\frac{7}{20}$ y una parte de tamaño $\frac{1}{4}$.

□

Problema 20. Un número de 2025 cifras es múltiplo de 27. Lo escribimos en círculo y lo rotamos varias posiciones. Demuestra que este nuevo número de 2025 cifras también es múltiplo de 27.

Solución. Basta demostrar que si colocamos la última cifra al principio el nuevo número será también múltiplo de 27 (para el caso general aplicaremos este procedimiento las veces que haga falta).

Sea el número original $N = a_0 + 10a_1 + 10^2a_2 + ... + 10^{2024}a_{2024}$. Sea $M = a_1 + 10^1a_2 + ... + 10^{2023}a_{2024}$, entonces $27|N = a_0 + 10M$. Queremos demostrar que $27|M + 10^{2024}a_0$. Restemos estos dos números, si la resta es múltiplo de 27, lo hemos conseguido:

$$R = (M + 10^{2024}a_0) - (a_0 + 10M) = a_0(10^{2024} - 1) - 9M$$

$$10R = a_0(10^{2025} - 10) - 90M = a_0(10^{2025} - 1) - 9(a_0 + 10M) = a_0(10^{2025} - 1) - 9N$$

Ahora bien, en esta última resta $27|10^{2025} - 1$ (porque son 2025 nueves) y $27|9N$.

□

Problema 21. En el número A han cambiado las cifras de orden y han llamado el número resultante B. La resta $A - B = 11...1$ está compuesta por n unos. ¿Cuál es el mínimo n posible?

Solución. Los números A, B son congruentes módulo 9 ya que el resto de división entre 9 coincide con el resto de división de la suma de sus cifras, que es la misma. Por tanto, el mínimo n posible debe ser 9. Ejemplo:

$$9012345678 - 8901234567 = 111111111$$

□

Problema 22. Amancio tiene una fábrica donde se embotella zumo de naranja. Está preparando un envío de 1.000.000 de botellas de zumo de naranja cuando se entera de que un error en la fábrica ha provocado que una de las botellas esté envenenada. Nadie sabe qué botella es, pero Amancio tiene sólo 20 tests de detección de veneno. Cada test se puede usar sólo una vez, pero puede llevarlo a cabo con cualquier cantidad de zumo de naranja que desee, y detectará si la muestra contiene veneno sea cual sea la concentración de veneno en la muestra. ¿Cómo puede determinar Amancio qué botella está envenenada?

Solución. Numeramos las botellas del 1 al 1.000.000 en binario. El número 1.000.000 escrito en binario es

$$11.110.100.001.001.000.000,$$

que tiene 20 dígitos.

En el test número i (donde i va del 1 al 20) echamos un poquito de cada zumo que tiene un 1 en el dígito en binario correspondiente a la potencia 2^{i-1}. Por ejemplo, echaremos un poco del zumo de la botella número 1.000.000 en los tests número $20, 19, 18, 17, 15, 10$ y 7. Sea $a_i = 0$ si el test i no detecta veneno, y $a_i = 1$ si el test i detecta veneno. La botella envenenada será la número

$$a_1 + a_2 \cdot 2 + a_3 \cdot 2^2 + \ldots + a_{20} \cdot 2^{19}.$$

□

Problema 23. Pensamos en una permutación de $\{1, 2, \ldots, n\}$ como una función f, que lleva cada número x a uno distinto $f(x)$. Llamamos $P(n)$ al número de permutaciones de $\{1, 2, \ldots, n\}$ que cumplen que $xf(x)$ es un cuadrado perfecto para todo x. Encuentra el mínimo n tal que $P(n)$ es múltiplo de 2024.

Solución. Cualquier número natural x se puede escribir como $x = ly^2$, donde l no tiene ningún primo repetido en su factorización (es su parte **libre de cuadrados**). Si $xf(x)$ es un cuadrado, signifca que x y $f(x)$ tienen la misma parte libre de cuadrados. Es decir, que los cuadrados se tienen que permutar entre ellos, y lo mismo ocurre con los números de la forma $2y^2, 3y^2, 5y^2, 6y^2, \ldots$ (para todas las posibles partes l, es decir, para todos los números libres de cuadrados). Por ejemplo, una permutación con $n = 20$ tiene que preservar cada uno de estos conjuntos:

$$\{1, 4, 9, 16\}, \{2, 8, 18\}, \{3, 12\}, \{5, 20\}, \{6\}, \{7\}, \{10\}, \{11\}, \{13\}, \{14\}, \{15\}, \{17\}, \{19\}.$$

Es decir, consiste en elegir una permutación de cada conjunto: las maneras de elegir una permutación para cada conjunto son el producto de las maneras de elegir cada permutación, es decir,

$$P(20) = 4! \cdot 3! \cdot 2! \cdot 2! \cdot 1! \cdot 1! \cdots = 576.$$

En general, tenemos que contar cuántos elementos hay en cada subconjunto: convéncete de que el número de cuadrados menores que n es $\lfloor \sqrt{n} \rfloor$ (el mayor entero menor o igual que $\sqrt{n}$). El segundo conjunto contiene el doble de los cuadradados: estos son $\left\lfloor \sqrt{\frac{n}{2}} \right\rfloor$. Y así sucesivamente, con lo que en total,

$$P(n) = \lfloor \sqrt{n} \rfloor ! \cdot \left\lfloor \sqrt{\frac{n}{2}} \right\rfloor ! \cdot \left\lfloor \sqrt{\frac{n}{3}} \right\rfloor ! \cdot \left\lfloor \sqrt{\frac{n}{5}} \right\rfloor ! \cdot \left\lfloor \sqrt{\frac{n}{6}} \right\rfloor ! \cdots$$

Como $2024 = 2^3 \cdot 11 \cdot 23$, este número tiene que ser múltiplo de 23, con lo que $\sqrt{n} \geq 23$ (es el factorial más grande que aparece). Si $n = 23^2 = 529$, vemos que $P(n)$ es múltiplo de 23!, que contiene 2^3, 11 y 23 en su factorización, así que $n = 529$.

□

Problema 24. Para todo número entero positivo n, definimos $f(n)$ como $\frac{n}{2}$ si n es par, y como $5n+1$ si n es impar. Denotamos por $f^1(n) = f(n)$, $f^2(n) = f(f(n))$, $f^3(n) = f(f(f(n)))$, etc. Encuentra el menor número entero positivo n para el cual $f^m(n) \neq 1$ para todo entero positivo m.

Solución. Empezamos haciendo un ejemplo: $f(1) = 6$, $f(6) = 3$, $f(3) = 16$, $f(16) = 8$, $f(8) = 4$, $f(4) = 2$, $f(2) = 1$. Por tanto, $f^7(1) = f^1(2) = f^5(3) = f^2(4) = 1$, y el número que buscamos es mayor o igual que 5.

$f(5) = 26$, $f(26) = 13$, $f(13) = 66$, $f(66) = 33$, $f(33) = 166$. Vamos a demostrar el siguiente enunciado: Para todo entero positivo m, la última cifra de $f^{2m-1}(5)$ es 6. Si m es par, y la última cifra de $f^{2m}(5)$ es 3. Demostramos este enunciado por inducción. El caso base es $m = 1$, y ya hemos calculado tanto $f(5) = 26$ como $f^2(5) = 13$, por lo que sabemos que el resultado es cierto. Para el paso de inducción, asumimos que el resultado es cierto para un cierto $m \geq 3$, y tenemos que ver que es cierto para $m+1$. Tenemos que $f^{2(m+1)-1}(5) = f(f^{2m}(5))$. Por hipótesis de inducción, $f^{2m}(5)$ es impar (porque acaba en 3). Por tanto, $f^{2(m+1)-1}(5) = 5 \cdot f^{2m}(5) + 1$, y la última cifra de esto es 6. También tenemos que $f^{2(m+1)}(5) = f(f^{2(m+1)-1}(5))$. Acabamos de demostrar que $f^{2(m+1)-1}(5)$ acaba en 6, luego es un número par tal que su mitad acaba en 3. Por tanto, $f^{2(m+1)}(5) = \frac{f^{2(m+1)-1}(5)}{2}$ acaba en 3, y esto termina nuestra demostración del paso de inducción.

En resumen, acabamos de demostrar que, para todo entero positivo k, $f^k(5)$ acaba en 6 si k es impar, y en 3 si k es par, para todo entero positivo k. En particular, $f^m(5) \neq 1$ para todo entero positivo m, por lo que la respuesta a este ejercicio es 5.

□

Problema 25. Demuestra que si n es un número entero positivo para el cual $2+2\sqrt{1+12n^2}$ es un número entero, entonces $2+2\sqrt{1+12n^2}$ es un cuadrado perfecto.

Solución. Sea $m = 2+2\sqrt{1+12n^2}$. Tenemos que $1+12n^2 = \left(\frac{m}{2}-1\right)^2$, por lo que

$$12n^2 = \frac{m^2}{4} - m$$

y por tanto

$$2^4 \cdot 3 \cdot n^2 = m(m-4).$$

Si m fuese impar, $m \cdot (m-4)$ sería impar, así que esto es imposible. Si m fuera par pero del tipo $4k+2$ para algún entero k, entonces la mayor potencia de 2 que dividiría a $m(m-4)$ sería 4, por lo que esto es imposible. Por tanto, m es múltiplo de 4, es decir, existe un entero positivo k tal que $m = 4k$, por lo que

$$3n^2 = k(k-1).$$

Como 4 es un cuadrado perfecto, basta demostrar que k es un cuadrado perfecto. $k = 1$ es un cuadrado perfecto, y la ecuación anterior nos dice que k no puede ser 2, por loque podemos asumir que $k \geq 3$. En ese caso, notemos que k y $k-1$ son enteros positivos mayores que 1 que no tienen ningún factor primo en común, y por tanto se pueden escribir como producto de números primos tales que los primos de la factorización de $k-1$ no aparecen en la de k y viceversa. Teniendo esto en cuenta, la ecuación $3n^2 = k(k-1)$ nos dice que, salvo el 3, los números primos de las factorizaciones de k y $k-1$ aparecen al cuadrado, por lo que tenemos dos opciones:

- Existen dos números enteros $x \geq 1$ e $y \geq 2$ tales que $xy = n$, $k = 3x^2$, $k-1 = y^2$.
- Existen dos números enteros $x \geq 1$ e $y \geq 2$ tales que $xy = n$, $k = y^2$, $k-1 = 3x^2$.

Para acabar el ejercicio basta descartar la primera de estas dos opciones. Si la primera opción fuera cierta, $3x^2 - 1 = y^2$. Módulo 3, tendríamos que $y^2 \equiv 2 \mod 3$, y como los cuadrados módulo 3 son 0 y 1, esto es imposible. Por tanto, la primera opción no puede ocurrir, y esto concluye nuestra demostración de que k (y por tanto m) es un cuadrado perfecto.

□

Problema 26. Juan Carlos y Cris están jugando a un juego con n monedas en una mesa. Se turnan quitando 2, 5 o 6 monedas en cada turno. Pierde la persona que en su turno no puede quitar 2, 5 o 6 monedas. Si Juan Carlos es el primero en jugar, ¿para qué valores de n tendrá una estrategia ganadora[3]?

Solución. Veamos que Cris tiene estrategia ganadora si el resto de dividir n entre 11 es 0, 1, 4 u 8, y que Juan Carlos tiene estrategia ganadora en caso contrario, es decir, si el resto de dividir n entre 11 es 2, 3, 5, 6, 7, 9, o 10.

Sea $n = 11q + r$, con q el cociente y el resto de n al dividir por 11. Lo demostramos por inducción sobre q. El caso base es $q = 0$:

- Cris tiene estrategia ganadora si hay 0, 1, 4, u 8 monedas en la mesa. Si hay 0 o 1 gana automáticamente. Si hay 4, Juan Carlos quitará 2 monedas, Cris otras 2 y ganará. Si hay 8, si Juan Carlos quita 6, Cris quitará 2 y gana; si Juan Carlos quita 5 Cris quitará 2 y gana, y si Juan Carlos quita 2, Cris quitará 6 y gana.

- Juan Carlos tiene estrategia ganadora si hay $2, 3, 5, 6, 7, 9, 10$. En los dos primeros casos Juan Carlos quitará 2 monedas; en el caso de 5 monedas quitará 5; en los dos siguientes 6; en el caso de 9 quitará 5, luego Cris 2 y Juan Carlos 2; y en el caso de 10 quitará 6, luego Cris 2 y Juan Carlos 2.

Por tanto queda demostrado el caso base.

Supongamos que el resultado está demostrado para k monedas siempre que el cociente de dividir k entre 11 sea menor o igual que m, con $m \geq 0$. Supongamos que hay $n = 11q + r$ monedas, con $q = m + 1$.

- Veamos que Cris tiene estrategia ganadora si $r = 0$, 1, 4, u 8. Si Juan Carlos quita 5 o 6 monedas de la mesa, Cris quitará 6 o 5 respectivamente y así a Juan Carlos le quedarán $11(q-1)$ monedas en la mesa, por lo que Cris gana por hipótesis de inducción. Por tanto, sólo tenemos que comprobar qué pasa si Juan Carlos quita 2 monedas de la mesa

  - Si $r = 0$: Si Juan Carlos quita 2 monedas de la mesa, Cris quitará 5 y así a Juan Carlos le quedarán $11(q-1)+4$ monedas en la mesa, por lo que gana Cris por hipótesis de inducción.
  - Si $r = 1$: Si Juan Carlos quita 2 monedas de la mesa, Cris quitará 6 y así a Juan Carlos le quedarán $11(q-1)+4$ monedas en la mesa, por lo que gana Cris por hipótesis de inducción.
  - Si $r = 4$: Si Juan Carlos quita 2 monedas de la mesa, Cris quitará 2 y así a Juan Carlos le quedarán $11q$ monedas en la mesa. Este es el caso $r = 0$, que ya lo hemos analizado, y Cris puede asegurarse ganar.
  - Si $r = 8$: Si Juan Carlos quita 2 monedas de la mesa, Cris quitará 6 y así a Juan Carlos le quedarán $11q$ monedas en la mesa. Este es el caso $r = 0$, que ya lo hemos analizado, y Cris puede asegurarse ganar.

- Veamos que Juan Carlos tiene estrategia ganadora si $r = 2, 3, 5, 6, 7, 9, 10$.

  - En los dos primeros casos Juan Carlos quitará 2 monedas, dejando $11q$ u $11q+1$ monedas en la mesa en un juego donde él juega segundo. Este caso ya lo hemos analizado, y ganará Juan Carlos.
  - En el caso $r = 5$ Juan carlos quitará 5 monedas, dejando $11q$ monedas en la mesa en un juego donde él juega segundo. Este caso ya lo hemos analizado, y ganará Juan Carlos.
  - En los casos $r = 6$ o $r = 7$ Juan Carlos quitará 6 monedas, dejando $11q$ u $11q+1$ monedas en la mesa en un juego donde él juega segundo. Este caso ya lo hemos analizado, y ganará Juan Carlos.
  - En el caso $r = 9$ Juan carlos quitará 5 monedas, dejando $11q+4$ monedas en la mesa en un juego donde él juega segundo. Este caso ya lo hemos analizado, y ganará Juan Carlos.

[3]Juan Carlos tiene una estrategia ganadora si, juegue Cris de la manera que juegue, Juan Carlos siempre puede contrarrestar los movimientos de Cris de manera que se asegure que acabará ganando

– En el caso $r = 10$ Juan carlos quitará 6 monedas, dejando $11q + 4$ monedas en la mesa en un juego donde él juega segundo. Este caso ya lo hemos analizado, y ganará Juan Carlos.

Esto concluye la demostración del paso de inducción, y por tanto también la solución a este ejercicio

□

Problema 27. Los dígitos de N están en orden estrictamente creciente. ¿Cuánto suman las cifras de $9N$?

Solución. La respuesta es 9. Llamemos $a_m \cdots a_1 a_0$ a los dígitos de N. Multipliquemos:

$$\begin{array}{rr} & a_m \cdots a_1 a_0 \\ \times & \qquad 9 \\ \hline \end{array}$$

Vamos en orden:

1. Cuando multiplico $9 \times a_0$, la última cifra es $10 - a_0$, y me llevo $a_0 - 1$. (Si ya he terminado, las cifras suman 9)

2. Como $a_1 < a_0$,
$$9a_1 + a_0 - 1 = 10a_1 + \underbrace{(a_0 - a_1 - 1)}_{\text{Entre 0 y 9}},$$
así que al multiplicar $9 \times a_1$ y sumar $a_0 - 1$ que me llevo, la última cifra es $a_0 - a_1 - 1$, y me llevo a_1.

3. Vamos a ver por inducción que para $i \geq 2$, el dígito correspondiente es $a_{i-1} - a_i$, excepto para $i = 1$, que nos da $a_0 - a_1 - 1$, y para $i \geq 1$ siempre me llevo a_i: ya hemos visto que se cumple para $i = 1$. Suponiendo que se cumple para $i - 1$, entonces $a_{i-1} < a_i$, y tenemos que
$$9a_i + a_{i-1} = 10a_i + \underbrace{(a_{i-1} - a_i)}_{\text{Entre 0 y 9}},$$
por lo que se cumple lo que hemos prometido.

Total, que $9N$ tiene cifras:

$$a_m, a_{m-1} - a_m, a_{m-2} - a_{m-1}, \ldots, a_1 - a_2, a_1 - a_0 - 1, 10 - a_0,$$

que suman 9.

□

Problema 28. MAX ESTRELLA: ¡Don Latino de Hispalis, grotesco personaje, te inmortalizaré en una novela! ¿Sabías que tu número favorito es la suma de las edades de mis tortugas, y que tu número favorito es su producto?
LATINO: Una tragedia. No lo sabía, porque no conozco tu número favorito. Si me dijeras tu número favorito y cuántas tortugas tienes, sabría las edades de tus tortugas?
MAX: No. ¡Me estoy helando!
LATINO: Levántate. Vamos a caminar. Ahora ya sé que tu número favorito es...
¿Cuál es?

Solución. La suma es 12. Tiene que ocurrir que para esa sumar, haya algún producto que se obtenga de dos maneras distintas con el mismo número de factores. Esto no ocurre para sumas menores que 12, pero para la suma 12 sí. Estas son todas las maneras de sumar 12 (excepto con un sumando), y el producto

correspondiente. Las maneras de sumar un número menor que 11 están aquí incluidas.

$$\begin{array}{ll}1\cdot 11 & =11\\ 2\cdot 10 & =20\\ 3\cdot 9 & =27\\ 4\cdot 8 & =32\\ 5\cdot 7 & =35\\ 6\cdot 6 & =36\end{array}\quad\Vert\quad\begin{array}{ll}1\cdot 1\cdot 10 & =10\\ 1\cdot 2\cdot 9 & =18\\ 1\cdot 3\cdot 8 & =24\\ 1\cdot 4\cdot 7 & =28\\ 1\cdot 5\cdot 6 & =30\\ 2\cdot 2\cdot 8 & =32\\ 2\cdot 3\cdot 7 & =42\\ 2\cdot 4\cdot 6 & =48\\ 3\cdot 3\cdot 6 & =54\\ 3\cdot 4\cdot 5 & =60\\ 4\cdot 4\cdot 4 & =64\end{array}\quad\Vert\quad\begin{array}{ll}1\cdot 1\cdot 1\cdot 9 & =9\\ 1\cdot 1\cdot 2\cdot 8 & =16\\ 1\cdot 1\cdot 3\cdot 7 & =21\\ 1\cdot 1\cdot 4\cdot 6 & =24\\ 1\cdot 1\cdot 5\cdot 5 & =25\\ 1\cdot 2\cdot 2\cdot 7 & =28\\ 1\cdot 2\cdot 3\cdot 6 & =36\\ 1\cdot 2\cdot 4\cdot 5 & =40\\ 1\cdot 3\cdot 3\cdot 5 & =45\\ 1\cdot 3\cdot 4\cdot 4 & =48\\ 2\cdot 2\cdot 2\cdot 6 & =48\\ 2\cdot 2\cdot 3\cdot 5 & =60\\ 2\cdot 3\cdot 3\cdot 4 & 72\\ 3\cdot 3\cdot 3\cdot 3 & 81\end{array}\quad\Vert\quad\begin{array}{ll}1\cdot 1\cdot 1\cdot 1\cdot 8 & =8\\ 1\cdot 1\cdot 1\cdot 2\cdot 7 & =14\\ 1\cdot 1\cdot 1\cdot 3\cdot 6 & =36\\ 1\cdot 1\cdot 1\cdot 5\cdot 4 & =20\\ 1\cdot 1\cdot 2\cdot 2\cdot 6 & =24\\ 1\cdot 1\cdot 2\cdot 3\cdot 5 & =30\\ 1\cdot 1\cdot 2\cdot 4\cdot 4 & =32\\ 1\cdot 1\cdot 3\cdot 3\cdot 4 & =36\\ 1\cdot 2\cdot 2\cdot 2\cdot 5 & =40\\ 1\cdot 2\cdot 2\cdot 3\cdot 4 & =48\\ 2\cdot 2\cdot 2\cdot 2\cdot 4 & 64\\ 2\cdot 2\cdot 2\cdot 3\cdot 3 & 72\end{array}\quad\Vert\quad\begin{array}{ll}1\cdot 1\cdot 1\cdot 1\cdot 1\cdot 7 & =7\\ 1\cdot 1\cdot 1\cdot 1\cdot 2\cdot 6 & =12\\ 1\cdot 1\cdot 1\cdot 1\cdot 3\cdot 5 & =15\\ 1\cdot 1\cdot 1\cdot 1\cdot 4\cdot 4 & =16\\ 1\cdot 1\cdot 1\cdot 2\cdot 2\cdot 5 & =20\\ 1\cdot 1\cdot 1\cdot 2\cdot 3\cdot 4 & =24\\ 1\cdot 1\cdot 2\cdot 2\cdot 2\cdot 4 & =32\\ 1\cdot 1\cdot 2\cdot 2\cdot 3\cdot 3 & =36\\ 1\cdot 2\cdot 2\cdot 2\cdot 2\cdot 3 & =48\\ 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2 & =64\end{array}$$

$$\begin{array}{ll}1^2\cdot 1\cdot 1\cdot 1\cdot 1\cdot 6 & =6\\ 1^2\cdot 1\cdot 1\cdot 1\cdot 2\cdot 5 & =10\\ 1^2\cdot 1\cdot 1\cdot 1\cdot 3\cdot 4 & =12\\ 1^2\cdot 1\cdot 1\cdot 2\cdot 2\cdot 4 & =16\\ 1^2\cdot 1\cdot 1\cdot 2\cdot 3\cdot 3 & 18\\ 1^2\cdot 1\cdot 2\cdot 2\cdot 2\cdot 3 & 24\\ 1^2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2 & 32\end{array}\quad\Vert\quad\begin{array}{ll}1^5\cdot 1\cdot 1\cdot 5 & =5\\ 1^5\cdot 1\cdot 2\cdot 4 & =8\\ 1^5\cdot 1\cdot 3\cdot 3 & =5\\ 1^5\cdot 2\cdot 2\cdot 3 & 12\end{array}\quad\Vert\quad\begin{array}{ll}1^6\cdot 1\cdot 1\cdot 4 & =4\\ 1^6\cdot 1\cdot 2\cdot 3 & =6\\ 1^6\cdot 2\cdot 2\cdot 2 & =8\end{array}\quad\Vert\quad\begin{array}{ll}1^8\cdot 1\cdot 3 & =3\\ 1^8\cdot 2\cdot 2 & =4\end{array}\quad\Vert\quad\begin{array}{ll}1^{10}\cdot 2 & =2\\ 1^{12} & =1\end{array}$$

(Una posible solución para) el número favorito de Latino de Hispalis es el 12, y el de Max es el 48: Latino, sabiendo que con la información del número 48 no tendría suficiente, sabe que el producto de las edades es 48.

Ahora bien, no es posible que la suma sea mayor que 12: si la suma fuera un número $N \geq 13$, entonces siempre hay al menos dos posibles products para los que no puede saber las edades:

$$2\cdot 2\cdots 2\cdot 6\cdot (S-12) = 2\cdot 2\cdot 3\cdot 4\cdot (S-12) = 48(S-12)$$
$$2\cdot 2\cdot 9\cdot (S-13) = 1\cdot 6\cdot 6\cdot (S-13) = 36(S-13)$$

□

Problema 29. ¿Existen números enteros a y b para los cuales $a^2 = b^{15} + 1004$?

Solución. La respuesta es no. Podemos intentar tomar congruencias con distintos módulos para ver si esto es posible. La parte más difícil de calcular va a ser b^{15}, por lo que idealmente querríamos un módulo para el que calcular b^{15} fuese sencillo. Recordamos el pequeño teorema de Fermat, que nos dice que si p es primo, enconces $b^p \equiv b \mod p$ para todo entero b. Eligiendo $p = 31 = 15\cdot 2 + 1$, tenemos que

$$b^{31} = (b^{15})^2 b \equiv b \mod 31$$

y por tanto, 31 divide a $b((b^{15})^2 - 1)$. En particular, como 31 es primo, si b no es congruente con 0 módulo 31 entonces $(b^{15})^2 \equiv 1 \mod 31$. La ecuación $x^2 \equiv 1 \mod 31$ tiene como soluciones $x \equiv \pm 1$. Esto se puede ver calculando todas los cuadrados módulo 31. De esto concluimos que si b es un número entero, entonces $b^{15} \equiv -1, 0, 1 \mod 31$. Por tanto, si b es un número entero, entonces $b^{15} + 1004 \equiv b^{15} + 12 \equiv 11, 12, 13 \mod 31$.

Por otra parte, si a es un entero, entonces $a^2 \equiv 0, 1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8 \mod 31$. Ninguno de estos números es 11, 12 o 13, por lo que la ecuación no tiene soluciones enteras.

□

Problema 30. En una pizarra está escrito el número 0. Cada minuto que pasa, Juan Carlos reemplaza simultáneamente cada 0 de la pizarra por un 1 y cada 1 por un 10. Por ejemplo, si el número que estuviera

escrito en la pizarra fuera 1100, al minuto siguiente sería 101011. En un momento dado Juan Carlos se cansa y se va, dejando un número N en la pizarra. Si N es divisible por 9, demuestra que N es divisible por 99.

Solución. Como $99 = 9 \cdot 11$ y 9 y 11 no tienen factores primos en común, esto es equivalente a demostrar que si N es divisible por 9 entonces es también divisible por 11.

La sucesión de números en la pizarra después del primer cambio de Juan Carlos es

$$1, 10, 101, 10110, 10110101, 1011010110110, \ldots$$

- El número de cifras de los elementos de esta sucesión es $1, 2, 3, 5, 8, 13, \ldots$.
- El número de 1's en la pizarra es $1, 1, 2, 3, 5, 8, \ldots$

Esto nos recuerda a la sucesión de Fibonacci: esta es la sucesión f_1, f_2, f_3, ... construida recurrentemente de esta manera: $f_1 = 1$, $f_2 = 1$, y para todo $n \geq 3$, $f_n = f_{n-1} + f_{n-2}$. Observamos que con esta definición,

$$f_1 = 1, f_2 = 1, f_3 = 2, f_4 = 3, f_5 = 5, f_6 = 8, f_7 = 13, \ldots$$

Con esto en mente, podemos hacer las siguientes conjeturas. Si decimos que en el minuto n el número que hay en la pizarra es a_n, con $a_1 = 1$, $a_2 = 10$, $a_3 = 101$, etc,

- **Conjetura 1:** El número de cifras del número en la pizarra en el minuto n es f_{n+1} para todo $n \geq 1$.
- **Conjetura 2:** El número de 1's del número en la pizarra en el minuto n es f_n para todo $n \geq 1$.
- **Conjetura 3:** a_n se obtiene concatenando a_{n-1} y a_{n-2} para todo $n \geq 3$.

Demostremos las conjeturas 1 y 2 a la vez por inducción. El caso base ($n = 1$) es inmediato. Supongamos que las dos conjeturas son ciertas para el minuto n, es decir, hay f_n 1's y $(f_{n+1} - f_n)$ 0's. Como Juan Carlos cambia los 1's por 10's y los 0's por 1's, el número de cifras en el minuto $n + 1$ es $2 \cdot f_n + (f_{n+1} - f_n) = f_n + f_{n+1} = f_{n+2}$, y el número de 1's en el minuto $n + 1$ es $f_n + (f_{n+1} - f_n) = f_{n+1}$. Esto demuestra que si la conjetura es cierta para el minuto n, también lo es para el minuto $n + 1$, por lo que queda demostrado el paso de inducción. Hemos demostrado que nuestras primeras dos conjeturas son ciertas.

Como la Conjetura 1 es cierta, podemos reescribir la Conjetura 3 como

$$\text{Conjetura 3: } a_n = a_{n-1} \cdot 10^{f_{n-1}} + a_{n-2} \quad \text{para todo } n \geq 2,$$

donde $a_0 = 0$ (el número que había originalmente en la pizarra). Demostremos la Conjetura 3 por inducción. El caso base ($n = 2$) es cierto. Supongamos que la Conjetura 3 es cierta para el minuto n, es decir $a_n = a_{n-1} \cdot 10^{f_{n-1}} + a_{n-2}$. Como a_n es el resultado de concatenar a_{n-1} y a_{n-2}, después de los cambios que hace Juan Carlos obtendremos un número que es el resultado de concatenar a_n y a_{n-1}. Esto demuestra que si la conjetura es cierta para el minuto n, también lo es para el minuto $n + 1$, por lo que queda demostrado el paso de inducción. Hemos demostrado que la Conjetura 3 es cierta.

Observamos que f_n es par si y solo si n es divisible por 3, ya que, como los dos primeros términos de la sucesión son 1 (impar) y los siguientes términos se obtienen como suma de los dos anteriores, la sucesión es de la forma impar, impar, par, impar, impar, par,.... Por tanto, tenemos que

$$10^{f_n} \equiv \begin{cases} 1 \mod 11 & \text{si } n \text{ es divisible por 3} \\ -1 \mod 11 & \text{si } n \text{ no es divisible por 3} \end{cases}$$

Recordamos que un número es divisible por 9 si la suma de todas sus cifras es divisible por 9. Por la Conjetura 2, esto nos dice que a_n es divisible por 9 si y solo si f_n es divisible por 9. Módulo 9, la sucesión de Fibonacci es $1, 1, 2, 3, 5, 8, 4, 3, 7, 1, 8, 0, 8, 8, 7, 6, 4, 1, 5, 6, 2, 8, 1, 0, 1, 1, 2, \ldots$. Así, vemos que módulo 9, la sucesión de Fibonacci tiene periodo 24, y que f_n es divisible por 9 si y sólo si $n \equiv 0, 12 \mod 24$. Por tanto, hemos demostrado que a_n es divisible por 9 si y solo si $n \equiv 0, 12 \mod 24$.

Con esto en mente, el problema nos pide demostrar que si $n \equiv 0, 12 \mod 24$, entonces a_n es divisible por 11. Usando la fórmula recursiva $a_n = a_{n-1} \cdot 10^{f_{n-1}} + a_{n-2}$ de la Conjetura 3, calculemos a_n módulo 11: $1, 10, 2, 1, 1, 0, 1, 10, 2, 1, \ldots$. La manera de obtener la sucesión es $a_n \equiv a_{n-2} + a_{n-1} \mod 11$ si $n \equiv 1$ módulo 3 y $a_n \equiv a_{n-2} - a_{n-1}$ en caso contrario. Por tanto, esta sucesión tiene periodo 6, y a_n es divisible por 11 si y solo si n es divisible por 6. Como los números congruentes con 0 o 12 módulo 24 son todos divisibles por 6, esto nos dice que si a_n es divisible por 9, entonces es divisible por 11, concluyendo nuestra demostración.

□

Problema 31. Una sucesión infinita de números reales $a_1, a_2, a_3, \ldots$ satisface que

$$\text{mín}(a_m, a_n) = a_{\text{mcd}(m,n)}$$

para todo par de enteros positivos m, n.

a) Para todo número real k tal que $k \leq \text{máx}(a_1, a_2, \ldots, a_{26})$, llamamos n_k al número entero mínimo tal que $a_{n_k} \geq k$. Demuestra que, para todo número entero positivo m,

$$a_m \geq k \quad \text{ si y sólo si } \quad n_k \mid m.$$

b) Usa la parte anterior para demostrar que

$$a_1 + a_2 + \ldots + a_{26} \leq a_{2023} + a_{2024} + \ldots + a_{2048}.$$

Solución. a) Tenemos que si $a_m \geq k$, entonces $k \leq \text{mín}(a_m, a_{n_k}) = a_{\text{mcd}(m,n_k)}$, por lo que $\text{mcd}(m, n_k) \geq n_k$ y esto es equivalente a que $n_k \mid m$. Recíprocamente, si $n_k \mid m$, entonces $a_m \geq \text{mín}(a_m, a_{n_k}) = a_{\text{mcd}(m,n_k)} = a_{n_k} \geq k$. En resumen, hemos justificado que

$$a_m \geq k \quad \text{ si y sólo si } \quad n_k \mid m.$$

b) Empezamos notando que hay tantos números del 1 al 26 (ambos incluidos) como del 2023 al 2048 (ambos incluidos).

Para todo número real $k \leq \text{máx}(a_1, a_2, \ldots, a_{26})$, la parte anterior implica que el número de elementos de $\{a_1, a_2, \ldots, a_{26}\}$ que son mayores o iguales que k coincide con el número de múltiplos de n_k entre 1 y 26 (ambos incluidos), y esta cantidad es $\lfloor \frac{26}{n_k} \rfloor$ (es decir, el número entero más grande de entre los que son menores o iguales que $\frac{26}{n_k}$). Por otra parte, el número de elementos de $\{a_{2023}, a_{2024}, \ldots, a_{2048}\}$ que son mayores o iguales que k coincide con el número de múltiplos de n_k entre 2023 y 2048 (ambos incluidos), y esta cantidad puede ser $\lfloor \frac{26}{n_k} \rfloor$ o $\lfloor \frac{26}{n_k} \rfloor + 1$. En resumen, hemos justificado que

> para todo número real $k \leq \text{máx}(a_1, a_2, \ldots, a_{26})$,
> el número de elementos de $\{a_1, a_2, \ldots, a_{26}\}$ que son $\geq k$
> es menor o igual que el número de elementos de $\{a_{2023}, a_{2024}, \ldots, a_{2048}\}$ que son $\geq k$.

Sea $\{b_1, b_2, \ldots, b_{26}\}$ el mismo conjunto de números que $\{a_1, a_2, \ldots, a_{26}\}$, pero ordenado de menor a mayor. Sea $\{b_{2023}, b_{2024}, \ldots, b_{2048}\}$ el mismo conjunto de números que $\{a_{2023}, a_{2024}, \ldots, a_{2048}\}$, pero ordenado de menor a mayor. Haciendo $k = b_j$ en el párrafo anterior, tenemos que, para todo $j = 1, \ldots, 26$,

$$\begin{aligned} 27 - j \leq & \text{ (el número de de elementos de } \{b_1, b_2, \ldots, b_{26}\} \text{ que son } \geq b_j) \\ \leq & \text{ (el número de de elementos de } \{b_{2023}, b_{2024}, \ldots, b_{2048}\} \text{ que son } \geq b_j) \end{aligned}$$

por lo que, como los $27-j$ valores más grandes de $\{b_{2023}, b_{2024}, \ldots, b_{2048}\}$ son $b_{2022+j}, b_{2023+j}, \ldots, b_{2048}$, concluimos que

$$b_j \leq b_{2022+j} \quad \text{ para todo } j = 1, 2, \ldots, 26.$$

Sumando todas estas desigualdades para $j = 1, 2, \ldots, 26$ obtenemos el resultado deseado.

□

Problema 32. Seis matemáticas se colocan formando un corro. Se les pone a cada uno de ellas un gorro que está pintado de manera aleatoria de rojo o de azul. Ninguna de las matemáticas puede ver el color de su gorro, pero sí puede ver el color del gorro de las otras cinco matemáticas. Si las matemáticas pueden elegir una estrategia conjuntamente de antemano, describe una estrategia que pueden seguir para maximizar la probabilidad de que todas ellas adivinen correctamente el color de su gorro en silencio, y calcula esa probabilidad.

Por ejemplo, si siguieran la estrategia de adivinar aleatoriamente, tendrían una probabilidad de $\frac{1}{2^6}$ de acertar todas. Sin embargo, si siguieran la estrategia de decir el mismo color del gorro de la matemática que está dos puestos a la derecha, acertarían si todas tuvieran el gorro rojo, todas azules, o los gorros fueran alternando entre azul y rojo en el círculo, es decir, acertarían en 4 ocasiones de 2^6 posibles. Por tanto, la probabilidad de acertar todas con esta estrategia es $\frac{4}{2^6} = \frac{1}{16}$, y esto es mejor que adivinar aleatoriamente.

Solución. Empezamos viendo que la probabilidad buscada no puede ser mayor que $\frac{1}{2}$. Una persona concreta puede tener un gorro de color rojo o azul. Si el resto de personas tiene una configuración de colores en los gorros concreta, la estrategia le hará adivinar azul o rojo, pero sólo adivinará en la mitad de ocasiones. Por tanto la probabilidad de que todas las matemáticas acierten no puede ser mayor que esto.

Veamos que la probabilidad $\frac{1}{2}$ se puede alcanzar. Identificamos el color azul con el número 1 y el color rojo con el número 0. Cada matemática dirá que lleva un gorro azul si la suma de los números correspondientes a los gorros del resto de matemáticas es congruente con 1 módulo 2, y dirá que lleva un gorro rojo si esa suma es congruente con 0 módulo 2. Todas las matemáticas acertarán si y sólo si la suma de los números correspondientes a los gorros de las seis matemáticas es congruente con 0 módulo 2, y eso ocurre en la mitad de ocasiones.

□

Problema 33. Seis matemáticas se colocan formando un corro alrededor de un árbol. Se les pone a cada uno de ellas un gorro que está pintado de manera aleatoria de rojo o de azul. Ninguna de las matemáticas puede ver el color de su gorro ni el de la persona que está enfrente de ella en el corro (se la tapa el árbol), pero sí puede ver el color del gorro de las otras cuatro matemáticas. Si las matemáticas pueden elegir una estrategia conjuntamente de antemano, describe una estrategia que pueden seguir para maximizar la probabilidad de que todas ellas adivinen correctamente el color de su gorro en silencio, y calcula esa probabilidad.

Por ejemplo, si siguieran la estrategia de adivinar aleatoriamente, tendrían una probabilidad de $\frac{1}{2^6}$ de acertar todas. Sin embargo, si siguieran la estrategia de decir el mismo color del gorro de la matemática que está dos puestos a la derecha, acertarían si todas tuvieran el gorro rojo, todas azules, o los gorros fueran alternando entre azul y rojo en el círculo, es decir, acertarían en 4 ocasiones de 2^6 posibles. Por tanto, la probabilidad de acertar todas con esta estrategia es $\frac{4}{2^6} = \frac{1}{16}$, y esto es mejor que adivinar aleatoriamente.

Solución. Empezamos viendo que la probabilidad buscada no puede ser mayor que $\frac{1}{4}$. Cada pareja de personas opuestas (que están enfrente la una de la otra) ve la misma información. Con la información que ven, la estrategia que sigan les tiene que decir qué tienen que responder. Sin embargo, hay 4 posibilidades para los colores de los gorros de esta pareja de personas opuestas (2 posibilidades por persona), por lo que como mucho estas dos sólo podrán asegurarse que aciertan una de cada 4 veces, y por tanto la probabilidad de que todas las matemáticas acierten no puede ser mayor que esto.

Veamos que la probabilidad $\frac{1}{4}$ se puede alcanzar. Cada matemática dirá que lleva un gorro azul si las matemáticas que están dos puestos a su derecha y dos puestos a su izquierda llevan gorros del mismo color, y si no dirá que lleva un gorro rojo. Fijamos una matemática como inicio del círculo, y recorriendo el círculo en el sentido de las agujas del reloj, especificamos las posiciones en las que las matemáticas ganan siguiendo esta estrategia. Aquí, 0 denota el color azul, y 1 el rojo:

$(0,0,0,0,0,0)$	$(0,1,0,0,0,1)$	$(1,0,0,0,1,0)$	$(1,1,0,0,1,1)$
$(0,0,0,1,0,1)$	$(0,1,0,1,0,0)$	$(1,0,0,1,1,1)$	$(1,1,0,1,1,0)$
$(0,0,1,0,1,0)$	$(0,1,1,0,1,1)$	$(1,0,1,0,0,0)$	$(1,1,1,0,0,1)$
$(0,0,1,1,1,1)$	$(0,1,1,1,1,0)$	$(1,0,1,1,0,1)$	$(1,1,1,1,0,0)$

Estas son las posiciones en la que la suma de las coordenadas impares es congruente con 0 módulo 2, y lo mismo para la suma de las coordenadas pares. Hay 16 de estas, y como $\frac{16}{2^4} = \frac{1}{4}$, esta estrategia da la probabilidad óptima.

□

Problema 34. Demuestra que no pueden existir tres números primos p, q, r tales que $2 < p < q < r$ y tales que $\frac{r-q}{p}$ y $\frac{r-p}{q}$ son números enteros que son cuadrados perfectos.

Solución. Supongamos que p, q, r son tres números primos tales que $2 < p < q < r$ y tales que $\frac{r-q}{p}$ y $\frac{r-p}{q}$ son números enteros que son cuadrados perfectos. Entonces, multiplicando $\frac{r-q}{p}$ por p^2 y $\frac{r-p}{q}$ por q^2 obtenemos que $p(r-q)$ y $q(r-p)$ son cuadrados perfectos.

Sea $m = \sqrt{p(r-q)}$ y $n = \sqrt{q(r-p)}$. Tenemos que

$$(n+m)(n-m) = n^2 - m^2 = qr - pq - pr + pq = r(q-p)$$

Como r es primo y $q - p < r$, tenemos que o r divide a $n+m$ o r divide a $n-m$, pero no puede dividir a los dos. Además, como la parte derecha de la igualdad anterior es positiva, tenemos que $m < n$. Además, como $q - p$ es par, tenemos que n y m tienen que tener la misma paridad, y en particular $n + m$ es par.

Como $p < q < r$, tenemos que $n, m < r$, por lo que r no puede dividir a $m - n$. Por tanto r divide a $n + m$. Como $n + m < 2r$, la única posibilidad es que $n + m = r$. Esto contradice que $n + m$ sea par.

□

Problema 35. Érase una vez un rey indio que había nacido el día 5 del séptimo mes. Cuando se coronó, mandó retirar todas las monedas antiguas y sustituirlas por dos tipos de monedas nuevas, uno de 5 rupias y el otro, de 7 rupias. Decretó también que prohibía todos los precios que no se pudieran pagar con monedas de 5 y 7 (tampoco permitía dar el cambio), de modo que nada en su reino podía costar 1, 2, 3, 4, 6, 8 rupias pero sí permitía que la mercancía costase 5, 7, 10 o 12 rupias. ¿Había más precios permitidos o prohibidos durante su reinado? ¿Serías capaz de nombrar 15 precios prohibidos y 15 permitidos?

Segunda parte: supongamos que el rey nació el día 30. ¿En qué mes pudo haber nacido para que en su reinado hubiera una cantidad infinita de precios prohibidos?

Solución. Escribamos los primeros números naturales en 5 columnas:

0	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
...				

y marquemos los múltiplos de 7 de cada columna. Está claro que tanto el precio rojo, como cualquier precio debajo suyo puede ser pagado con monedas de 5 y 7 (piensa que en cada columna los números van de 5 en 5, por eso si uno se puede pagar, todos los que están debajo también). Solamente hay 12 precios prohibidos, los que están encima de los números en rojo.

Si el día D y el mes M tienen un divisor común $d > 1$, cualquier combinación de $aD + bM$ será múltiplo de d, por lo que habrá infinitos precios prohibidos. □

Problema 36. Demuestra que existe un conjunto S de números enteros tales que todo número entero n se puede expresar de una manera única como $n = 20x + 23y$ para un par de números x, y en S.

Solución. Por la identidad de Bézout, existen enteros x, y tal que $1 = 20x + 23y$. Nosotros escogemos $x = -8$, $y = 7$. Ordenamos los números enteros así, $a_0 = 0$, $a_1 = 1, a_2 = -1, a_3 = 2, a_4 = -2, a_5 = 3, a_6 = -3, \ldots$. Para cada $n \geq 1$ tenemos que

$$a_n = 20 \cdot (-8 \cdot a_n + 23N) + 23 \cdot (7 \cdot a_n - 20N) \tag{1}$$

para todo entero N.

Vamos a describir un algoritmo para hallar un conjunto S. Empezamos definiendo el conjunto $T_0 = \{0\}$. Nuestro algoritmo va a ser el siguiente: en el paso i, si a_i se puede escribir como $a_i = 20x + 23y$ para x, y en T_{i-1} entonces definimos $T_i = T_{i-1}$. Si por el contrario a_i no se puede escribir como $a_i = 20x + 23y$ para x, y en T_{i-1}, entonces elegimos un entero N_i lo suficientemente grande (luego especificamos qué significa "suficientemente grande"), llamamos $x_i = -8 \cdot a_i + 23N_i$ e $y_i = 7 \cdot a_i - 20N_i$, y definimos T_i como la unión de T_{i-1} con $\{x_i, y_i\}$. La idea es que si hemos elegido N_i bien en cada paso, el conjunto S formado por la unión de todos los T_i's para $i \geq 0$ es una solución al problema, y por tanto existe la solución.

Veamos unas condiciones que describan que N_i sea lo "suficientemente grande". Estas condiciones van a parecer muy arbitrarias, pero no lo son: nosotros las hemos obtenido a posteriori porque son las condiciones que aparecen de manera natural en la demostración por inducción que hacemos después. Elegimos N_i como un entero positivo lo suficientemente grande como para que se cumplan todas estas condiciones (hay un número finito de ellas):

1. Los números $|x_i|$ y $|y_i|$ son estrictamente mayores que los siguientes números:
   (a) $|a_j - 23x|$ para todo j tal que $0 \leq j \leq i$, y para todo x en T_{i-1}.
   (b) $|a_j - 20x|$ para todo j tal que $0 \leq j \leq i$, y para todo x en T_{i-1}.
   (c) $|20x + 23(y - y')|$ para todo x, y, y' en T_{i-1}.
   (d) $|20(x - x') + 23y|$ para todo x, x', y en T_{i-1}.

2. Sea $b_i = 20y_i + 23x_i = (20x_i + 23y_i) + 3(x_i - y_i) = a_i + 3(-15a_i + 43N_i) = -44a_i + 129N_i$. Imponemos que N_i sea lo suficientemente grande como para que $|b_i|$ sea un número estrictamente mayor que $|20x + 23y|$ para todo x, y en T_{i-1}.

3. Se puede comprobar que los números $|20x_i + 23y_i|$, $43|x_i|$, $43|y_i|$ y $b_i = |20y_i + 23x_i|$ tienen todos expresiones distintas en función de a_i y de N_i. Por tanto, se puede escoger N_i lo suficientemente grande como para que $|20x_i + 23y_i|$, $43|x_i|$, $43|y_i|$ y $b_i = |20y_i + 23x_i|$ sean cuatro números distintos.

4. Consideramos todos los números que se pueden obtener como $|20(x-x')+23y|$ para x, x', y' en $\{x_i, y_i\}$. Se puede comprobar que todos estos números dependen de N_i de manera no trivial. Elegimos N_i lo suficientemente grande como para que los números $|20(x - x') + 23y|$ sean estrictamente mayores que $|23y'|$ para todo x, x', y en $\{x_i, y_i\}$ y y' en T_{i-1}.

5. Consideramos todos los números que se pueden obtener como $|20x+23(y-y')|$ para x, y, y' en $\{x_i, y_i\}$. Se puede comprobar que todos estos números dependen de N_i de manera no trivial. Elegimos N_i lo suficientemente grande como para que los números $|20x + 23(y - y')|$ sean estrictamente mayores que $|20x'|$ para todo x, y, y' en $\{x_i, y_i\}$ y x' en T_{i-1}.

6. Se puede comprobar que el número $|x_i - y_i|$ depende no trivialmente de N_i. Elegimos N_i lo suficientemente grande como para que $|x_i - y_i|$ es estrictamente mayor que $23|x - y|$ para todo x, y en T_{i-1}.

7. Consideramos todos los números que se pueden obtener como $|20x - 23y|$ para x, y en $\{x_i, y_i\}$. Se puede comprobar que todos estos números dependen de N_i de manera no trivial. Elegimos N_i lo suficientemente grande como para que los números $|20x - 23y|$ son todos estrictamente mayores que todos los números de la forma $|20x' - 23y'|$ para x', y' en T_{i-1}.

Para que este proceso que hemos descrito nos de una solución S al ejercicio, tenemos que asegurarnos que este proceso que hemos descrito cumple que a_j se puede representar de manera única como $a_j = 20x + 23y$ con x, y en T_n para todo $n = 0, 1, 2, \ldots$ y para todo $0 \leq j \leq n$. Si podemos asegurar esto, la solución S será la unión de todos los T_i para $i \geq 0$.

Demostramos esto por inducción sobre n. Si $n = 0$, a_0 se puede representar de manera única como $a_0 = 20x + 23y$ con x, y en $T_0 = \{0\}$, por lo que queda demostrado el paso base.

Supongamos que $k \geq 0$, y que a_j se puede representar de manera única como $a_j = 20x + 23y$ con x, y en T_k para todo $0 \leq j \leq k$. Queremos demostrar que nuestra manera de definir T_{k+1} tal que para todo $0 \leq j \leq k+1$, a_j se puede representar de manera única como $a_j = 20x + 23y$ con x, y en T_{k+1}. Tenemos dos casos:

- El caso en el que a_{k+1} no se puede expresar como $20x + 23y$ con x, y en T_k. En este caso tenemos que demostrar que, para todo $0 \leq j \leq k+1$, a_j no se puede expresar como $a_j = 20x + 23y$ con x en $\{x_{k+1}, y_{k+1}\}$ e y en T_k o viceversa. Supongamos que sí se puede para llegar a una contradicción. Veamos cada uno de estos casos por separado:
  - x está en $\{x_{k+1}, y_{k+1}\}$ e y está en T_k: En ese caso, tenemos que $20x = a_j - 23y$. Por la condición 1(a), $|x|$ es estrictamente mayor que $|a_j - 23y|$, así que esto es imposible.
  - El caso en el que x está en T_k e y está en $\{x_{k+1}, y_{k+1}\}$ se argumenta de manera análoga usando la condición 1(b).

- El caso en el que a_{k+1} se puede expresar como $20x + 23y$ con x, y en T_k. En este caso tenemos que ver que a_{k+1} no se puede expresar de otra manera como $20x' + 23y'$ con x', y' en T_k. Supongamos que sí se puede para llegar a una contradicción. Ponemos la convención de que T_{-1} es el conjunto vacío. Tenemos que existen $0 \leq j_1, j_2, j_3, j_4 \leq k$ tal que x está en T_{j_1} pero no en T_{j_1-1}, y está en T_{j_2} pero no en T_{j_2-1}, x' está en T_{j_3} pero no en T_{j_3-1}, y' está en T_{j_4} pero no en T_{j_4-1}. Sin pérdida de generalidad, podemos asumir que el máximo de j_1 y j_2 es mayor o igual que el máximo de j_3 y j_4. Tenemos los siguientes casos:
  - El máximo de j_1 y j_2 es estrictamente mayor que el máximo de j_3 y j_4. Las condiciones 1(c) y 1(d) nos dicen que esto sólo es posible si $j_1 = j_2$. En ese caso, $a_{k+1} = b_{j_1} = b_{j_2}$, y la condición 2 nos dice que esto es imposible.
  - El máximo de j_1 y j_2 es igual al máximo de j_3 y j_4. En ese caso no pueden ser todos los j_i iguales por la condición 3. Por tanto, existe un j_i distinto del resto, que sin pérdida de generalidad podemos asumir que es j_3 o j_4. Además, las condiciones 4 y 5 nos dicen que no puede haber exactamente tres números iguales de entre los j_i's. Por tanto, tenemos cuatro casos posibles.
    - $j_1 = j_3$, $j_1 > j_2$ y $j_3 > j_4$: En ese caso, $|x - x'| = 0$ o $|x - x'| = |x_{j_1} - y_{j_1}|$. El primero de los casos implica que $x = x'$ e $y = y'$, que contradice que hubiera dos maneras distintas de expresar a_{k+1}. El segundo de los casos implica que $20|x_{j_1} - y_{j_1}| = 23|y' - y|$, y esto es imposible por la condición 6.
    - $j_1 = j_4$, $j_1 > j_2$ y $j_4 > j_3$: En este caso, $20x - 23y' = 20x' - 23y$, y la condición 7 nos dice que esto es imposible.
    - $j_2 = j_3$, $j_2 > j_1$ y $j_3 > j_4$: En este caso, $20x - 23y' = 20x' - 23y$, y la condición 7 nos dice que esto es imposible.
    - $j_2 = j_4$, $j_2 > j_1$ y $j_4 > j_3$: En ese caso, $|y - y'| = 0$ o $|y - y'| = |x_{j_2} - y_{j_2}|$. El primero de los casos implica que $y = y'$ e $x = x'$, que contradice que hubiera dos maneras distintas de expresar a_{k+1}. El segundo de los casos implica que $23|x_{j_2} - y_{j_2}| = 20|x' - x|$, y esto es imposible por la condición 6 ($23|x_{j_2} - y_{j_2}| > |x_{j_2} - y_{j_2}| > 23|x' - x| > 20|x' - x|$).

Esto concluye nuestra demostración del paso de inducción, y por tanto la solución a este ejercicio.

□