PEQUEÑO INSTITUTO DE MATEMATICAS

Hoja de Aritmética II

Fecha: 1, 8, 15 de Marzo de 2024 **Grupo: Júpiter, Urano, Venus**

Congruencias

Empezaremos con un pequeño repaso.

Teorema 1 (El algoritmo de la división)**.** *Sean a y b dos números enteros cualesquiera, con $b \neq 0$. Entonces, existen unos únicos enteros q (cociente) y r (resto) tales que*

$$\begin{cases} a = bq + r, \\ 0 \leq r \leq |b| - 1. \end{cases}$$

Una consecuencia del algoritmo de la división es el siguiente resultado.

Teorema 2 (Base a)**.** *Sean n y a dos números naturales, con $a \geq 2$. Entonces, existe una única manera de* expresar n en base a*, es decir, de escribir*

$$n = r_0 + r_1 a + r_2 a^2 + \dots,$$

donde r_i es un entero que satisface que $0 \leq r_i \leq a - 1$ para todo $i = 0, 1, 2, \dots$.

Igual que el número $2 + 2 \cdot 10 + 0 \cdot 10^2 + 2 \cdot 10^3$ lo escribimos como 2022 en base 10, el número $2 + 1 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3$ lo podemos escribir como 1012 en base 3. Cuando queremos que esté clara la base, la escribimos en subíndice, por ejemplo, escribimos $2022_{10} = 11111100110_2 = 2202220_3$.

La manera de obtener los valores de $r_0, r_1, r_2, \dots$ en la expresión anterior es aplicando el algoritmo de la división iterativamente, como explicamos a continuación:

$$\begin{aligned} n &= aq_0 + r_0 && \text{algoritmo de la división aplicado a } n \text{ y } a \\ q_0 &= aq_1 + r_1 && \text{algoritmo de la división aplicado a } q_0 \text{ y } a \\ q_1 &= aq_2 + r_2 && \text{algoritmo de la división aplicado a } q_1 \text{ y } a \\ &\vdots \end{aligned}$$

El proceso acaba cuando en el paso j ocurre que $q_j = 0$. Entonces, $n = r_0 + r_1 a + \dots + r_j a^j$.

Problema 1. Expresa el número 51 en base 2 y en base 3.

Problema 2. Explica por qué el proceso de obtención de los r_j descrito anteriormente funciona. Explica también usando el Teorema 1 por qué la expresión de n en base a es única, es decir, que si $n = r_0 + r_1 a + r_2 a^2 + \dots = \widetilde{r}_0 + \widetilde{r}_1 a + \widetilde{r}_2 a^2 + \dots$, donde $0 \leq r_i, \widetilde{r}_i \leq a - 1$ para todo $i = 0, 1, 2 \dots$, entonces $r_i = \widetilde{r}_i$ para todo $i = 0, 1, 2 \dots$.

Definición (Congruencia módulo n)**.** Sea n un número natural. Decimos que dos enteros a y b son *congruentes módulo n* si n divide a $a - b$. Lo escribiremos como

$$a \equiv b \ (\text{mód } n).$$

El siguiente ejercicio es **MUY IMPORTANTE**. Asegúrate de que sabes hacerlo antes de seguir adelante. Si lo entiendes, podrás aplicar las congruencias a la resolución de muchos problemas.

Problema 3. Justifica las siguientes afirmaciones usando la definición anterior.

(a) $a \equiv a \pmod{n}$

(b) Si $a \equiv b \pmod{n}$, entonces $b \equiv a \pmod{n}$.

(c) Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, entonces $a \equiv c \pmod{n}$. **Las propiedades (a), (b) y (c) son propiedades que también tiene el signo "=".**

(d) Si r es el resto que obtenemos al dividir a por n, entonces $a \equiv r \pmod{n}$. En otras palabras, cuando trabajamos con congruencias, **sólo nos importan los restos**.

(e) Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces

- $a + c \equiv b + d \pmod{n}$,
- $a - c \equiv b - d \pmod{n}$, y
- $a \cdot c \equiv b \cdot d \pmod{n}$.

En otras palabras, **podemos sumar, restar y multiplicar** con congruencias.

Las congruencias son algo que usamos en nuestro día a día, porque **las horas son congruencias módulo** 12. Si hacemos congruencias módulo 12, los únicos números que tenemos que tener en cuenta según la parte (d) del Problema 3 son los posibles restos al dividir por 12, es decir, $0, 1, 2, 3, 4, \ldots, 10, 11$. Como $0 \equiv 12 \pmod{12}$, estos restos representan todas las horas posibles (de la 1 a las 12). Además, estamos acostumbrados a sumar y restar módulo 12. Por ejemplo, si son las 11 y pasan cinco horas, serán las 4. Con el lenguaje de congruencias, eso es que $11 + 5 \equiv 4 \pmod{12}$.

El siguiente enunciado seguramente ya lo conoces, pero vamos a usar el ejercicio anterior para demostrarlo. Asegúrate de que entiendes la solución antes de seguir avanzando con la hoja.

Ejemplo resuelto (Criterio de divisibilidad por 3)**.** Demuestra que un número es divisible por 3 cuando la suma de sus cifras es divisible por 3.

Solución. Sea n un número natural. Lo expresamos en base 10 como $n = r_0 + r_1 \cdot 10 + r_2 \cdot 10^2 + \ldots$, es decir, r_0 es la cifra de las unidades, r_1 la de las decenas, r_2 la de las centenas, etc. Tenemos que $10 \equiv 1 \pmod{3}$. Por tanto, por la parte (e) del Problema 3 referente a la multiplicación, tenemos que $10^2 = 10 \cdot 10$ satisface que $10^2 \equiv 1 \pmod{3}$, y en general, $10^i \equiv 1 \pmod{3}$ para todo $i = 0, 1, 2, \ldots$.

Por la parte (e) del Problema 3, tenemos que

$$r_0 + r_1 \cdot 10 + r_2 \cdot 10^2 + \ldots \equiv r_0 + r_1 + r_2 + \ldots \pmod{3},$$

es decir, el número n es congruente a la suma de sus cifras módulo 3. Como "ser divisible por 3" es lo mismo que "ser congruente con 0 módulo 3", obtenemos que n es divisible por 3 cuando la suma de sus cifras es divisible por 3. □

Ejemplo resuelto. ¿Cuál es la última cifra de 12345^{6789} en base 7?

Solución: Si la expresión de 12345^{6789} en base 7 es $r_0 + r_1 \cdot 7 + r_2 \cdot 7^2 + \ldots$, estamos buscando el valor de r_0, que es el resto de dividir 12345^{6789} por 7, así que $12345^{6789} \equiv r_0 \pmod{7}$. Tenemos que $12345 = 7 \cdot 1763 + 4$, por lo que la parte (e) del Problema 3 referente a la multiplicación nos dice que $r_0 \equiv 4^{6789} \pmod{7}$. Calculamos las potencias de 4 módulo 7.

$$4^0 \equiv 1 \pmod{7}$$
$$4^1 \equiv 4 \pmod{7}$$
$$4^2 \equiv 2 \pmod{7}$$
$$4^3 \equiv 1 \pmod{7}$$
$$\vdots$$

Como $4^3 \equiv 1$, $4^{k+3} = 4^k 4^3 \equiv 4^k$ para todo k entero no negativo, es decir, la lista se repite cada 3 pasos. Por el criterio de divisibilidad por 3, $6789 \equiv 6+7+8+9 \equiv 0$ (mód 3), por lo que $3^{6789} \equiv 3^0 \equiv 1$ (mód 7). Por tanto, r_0 es un número entre 0 y 6 (incluidos) tal que $r_0 \equiv 1$ (mód 7), y la única posibilidad es que $r_0 = 1$.

División módulo n

En esta hoja utilizaremos un resultado básico de aritmética: el teorema fundamental de aritmética. Seguramente lo has visto antes. Debido a su naturaleza básica, podría parecer que es trivial y no requiere una demostración. Sin embargo, de hecho, para demostrarlo hace falta de un resultado que aún no has aprendido: el teorema de Bézout. Lo verás en la siguiente hoja de aritmética.

Teorema 3 (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.

Vamos a resolver las siguientes ecuaciones en congruencias:

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

a) $2x \equiv 4$ (mód 5)

b) $2x \equiv 2$ (mód 5)

c) $2x \equiv 5$ (mód 10)

d) $2x \equiv 6$ (mód 10)

e) $6x \equiv 2$ (mód 10)

f) $15x \equiv 0$ (mód 10)

Solución. a) $x \equiv 2$ (mód 5)

b) $x \equiv 1$ (mód 5)

c) No hay ninguna solución. .

d) $x \equiv 3, 8$ (mód 10)

e) $x \equiv 2, 7$ (mód 10)

f) $x \equiv 0$ (mód 2) $\equiv 0, 2, 4, 6, 8,$ (mód 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 $3/2 \equiv 4$ (mód 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 $3 \cdot 2 \equiv 1$ (mód 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 4. Demuestra que si para ciertos a y n la ecuación $ax \equiv 1$ (mód n) tiene solución, entonces sólo hay una solución módulo n.

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

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

$$x \overset{ax'\equiv 1}{\equiv} ax'x \overset{ax\equiv 1}{\equiv} x' \text{ (mód } n).$$

□

Problema 5. Demuestra que si $\text{mcd}(a, n) \neq 1$, entonces $ax \equiv 1 \text{ (mód } n)$ 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 6. Supón ahora que $\text{mcd}(a, n) = 1$.

a) Demuestra que si $ax \equiv 0 \text{ (mód } n)$, entonces $x \equiv 0 \text{ (mód } n)$.

b) Demuestra que si $ax \equiv ay \text{ (mód } n)$, entonces $x \equiv y \text{ (mód } n)$.

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 $ax \equiv 1 \text{ (mód } n)$.

Solución. a) Si $n|ax$, como n y a son primos entre sí, n tiene que dividir a x, porque todo primo en la factorización de n no está en la factorización de a, y por tanto está en la de x.

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

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 7. Sea p primo. Supongamos que $a^2 \equiv 1 \text{ (mód } p)$. Entonces $a \equiv \pm 1 \text{ (mód } p)$.

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

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

Luego, $a \equiv -1 \text{ (mód } p)$. □

Teorema 4 (Teorema de Wilson)**.** *Sea p un primo impar. Entonces* $(p-1)! \equiv -1 \text{ (mód } p)$.

Solución. Como hemos visto para cada número $a \in \{1, \ldots, p-1\}$ existe $b \in \{1, \ldots, p-1\}$ tal que $ab \equiv 1 \text{ (mód } p)$. 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 $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \text{ (mód } p)$. □

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 8. 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 9. 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 6(c). □

Teorema 5 (El pequeño teorema de Fermat)**.** *Sea p un número primo. Si a no es divisible por p, entonces $a^{p-1} \equiv 1 \pmod{p}$.*

Solución. 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 9, también tenemos que

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

Este producto es igual a

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

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

Problemas

Problema 10. Halla todos los positivos n tales que $(n+1)|(5n+17)$

Solución. Supongamos que $(n+1)|(5n+17)$. También sabemos que $(n+1)|5(n+1)$, por tanto, $(n+1)|(5n+17-5n-5)$, $(n+1)|12$, de modo que $n+1$ debe ser uno de los divisores de 12. Conclusión: $n \in \{1, 2, 3, 5, 11\}$

□

Problema 11. ¿Qué resto da 222...2111...1555...5 entre 6? En este número hay 301 doses, 300 unos y 300 cincos.

Solución. Si sumamos las cifras, la suma será $300 \cdot (5+2+1)+2$, por lo que es congruente con 2 módulo 3. Los números $3k+2$ pueden dar dos restos distintos módulo 6: 2 y 5. Como nuestro número es impar, hay que elegir la segunda opción.

□

Problema 12. Se sabe que

$$35! = 1 \cdot 2 \cdot 3 \cdot ... \cdot 35 = 10333147966386144929 * 66651337523200000000.$$

¿Qué cifra está sustituida por el asterisco?

Solución. Como 35! es múltiplo de 9, sus cifras deben sumar un múltiplo de 9. Por esto, la cifra escondida es el 6.

□

Problema 13. Busca todas las soluciones en números enteros de la ecuación $x^2 + y^2 = 10003$

Solución. Tanto x^2 como y^2 pueden dar restos 0 o 1 módulo 4, por lo que su suma módulo 4 no puede dar resto 3. Esta ecuación no tiene soluciones en enteros.

□

Problema 14. El número compuesto por 100 ceros, 100 unos y 100 doses, ¿puede ser cuadrado perfecto?

Solución. La suma de las cifras de nuestro número da 300. Es múltiplo de 3 pero no es múltiplo de 9. Sin embargo, si un cuadrado perfecto es múltiplo de 3, siempre es múltiplo de 9.

□

Problema 15. En la suma

$$\begin{array}{cccc} & B & M & C \\ + & & M & C \\ \hline X & Y & 7 & 0 \end{array}$$

cada letra representa una cifra distinta (del 0 al 9), y ni B ni M ni X pueden ser iguales a 0. Determina los valores de cada letra.

Solución. Mirando a la columna de las unidades observamos que la cifra de las unidades de $2C$ es 0, por lo que $C = 5$. Ahora, mirando la columna de las decenas, observamos que la cifra de las unidades de $2M+1$ es 7, y esto nos dice que $M = 3$ o $M = 8$.

Si $M = 3$, entonces mirando a la cifra de las centenas obtenemos que $B = Y$ y por tanto $X = 0$. Sabemos que $X \neq 0$, así que descartamos este caso.

Si $M = 8$, entonces $B + 1 = 10X + Y$, es decir, la cifra de las unidades de $B+1$ es Y y la de las decenas es X. Como $X \neq 0$ y $B + 1 \leq 9 + 1 = 10$, la única posibilidad es que $Y = 0$, $B = 9$ y $X = 1$.

Por tanto, la solución es $C = 5$, $M = 3$, $Y = 0$, $B = 9$ y $X = 1$.

□

Problema 16. Sea mcd el máximo común divisor de dos números enteros positivos y mcm su mínimo común múltiplo. Supongamos que A, B y C son tres números enteros positivos que satisfacen:

$$\begin{aligned} \text{mcd}(A,B) &= 2, \quad \text{mcm}(A,B) = 60, \\ \text{mcd}(A,C) &= 3, \quad \text{mcm}(A,C) = 42. \end{aligned}$$

Determina el valor de A, B y C.

Solución. $\mathrm{mcd}(A,B) = 2$ nos dice que existen dos números enteros positivos n y m tales que $A = 2n$, $B = 2m$ y $\mathrm{mcd}(n,m) = 1$. Además, $\mathrm{mcm}(A,B) = 2 \cdot n \cdot m = 60$, por lo que $n \cdot m = 30$.

$\mathrm{mcd}(A,C) = 3$ nos dice que existen dos números enteros positivos k y l tales que $n = 3k$, $C = 3l$, y $\mathrm{mcd}(2k,l) = 1$. Además, $\mathrm{mcm}(A,C) = 6 \cdot k \cdot l = 42$, por lo que $k \cdot l = 7$. Además, sabemos que $n = 3k$ es un divisor de 30, por lo que k no puede ser 7. Por tanto, la ecuación $k \cdot l = 7$ implica que $k = 1$ y $l = 7$. Por tanto, $C = 21$, $n = 3$, $m = 10$, $A = 6$ y $B = 20$.

□

Problema 17. Demuestra que a partir de determinado N los primos son menos de un tercio de todos los números. ¿Es verdad que a partir de un determinado número son menos de un cuarto?

Solución. Consideremos los números $6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5$. Entre ellos al menos 4 son compuestos si $k > 0$. Entre los primeros 5 hay solamente 1 compuesto, pero, como hemos visto antes, hay un sexteto de números seguidos que son todos compuestos.

Podemos hacer algo parecido para $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. En cada grupo de 2970 números habrá como mucho 720 coprimos con 2970, que es menos de un cuarto. Si te interesa el tema, puedes estudiar la demostración de Euler de que el porcentaje de primos tiende a cero.

□

Problema 18. Factoriza el número $2^{30} - 1$ completamente como producto de números primos.

Solución. Explicamos cómo hacerlo sin necesidad de usar calculadora. Tenemos que $2^{30} - 1 = (2^{15})^2 - 1^2 = (2^{15}+1)(2^{15}-1) = ((2^5)^3+1)((2^5)^3-1)$.

Para todo número real x tenemos que $x^3 - 1 = (x-1)(x^2+x+1)$, y $x^3+1 = (x+1)(x^2-x+1)$. Por tanto,

$$2^{30} - 1 = (2^5+1)(2^{10}-2^5+1)(2^5-1)(2^{10}+2^5+1) = 33 \cdot 993 \cdot 31 \cdot 1057.$$

Ahora, $33 = 3 \cdot 11$ (3 y 11) son primos, $993 = 3 \cdot 331$, y $1057 = 7 \cdot 151$. El número 31 es primo porque no es divisible por $2, 3$ ni 5, y $7^2 = 49 > 31$. El número 151 es primo porque no es divisible por $2, 3, 5, 7$ ni 11, y $13^2 = 169 > 151$. El número 331 no es divisible por $2, 3, 5$ claramente, tampoco es divisible por 7, no es divisible por 11 porque la suma alternada de sus cifras no lo es, se puede comprobar que no es divisible por 13 ni por 17, y $19^2 = 361 > 331$, por lo que 331 es primo. Por tanto,

$$2^{30} - 1 = 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331.$$

es la factorización de $2^{30} - 1$ en números primos.

También se puede hacer de manera relativamente rápida si en el paso inicial sólo llegamos a que $2^{30} - 1 = (2^{15}+1)(2^{15}-1)$, ya que tanto $2^{15}+1$ y $2^{15}-1$ son números de 5 cifras, y los podemos factorizar por fuerza bruta.

□

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. 1. Esta es la identidad de Sophie-Germain. Por desgracia, esta identidad es un simple truco que los profesores odian y que no quieren que conozcas. Por este motivo, parte está censurada (algunas partes de la identidad están ocultas). Encuentra qué esconde la censura:

$$a^4 + 4b^4 = (a^2 + 2b^2 + \text{🐙})(a^2 + \text{🐧🦒🐖})$$

2. Demuestra que $n^4 + 4^n$ nunca es un número primo para ningún natural n.

Solución. 1. En realidad, es una suma por diferencia:

$$((a^2 + 2b^2) + 2ab)((a^2 + 2b^2) - 2ab) = (a^2 + 2b^2)^2 - 4a^2b^2 = a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = a^4 + 4b^4.$$

2. Si n es par, n^4+4^n es un número par mayor que 32, así que n es impar, y podemos escribir $n = 2k+1$:

$$n^4 + 4^n = n^4 + 4 \cdot 4^{2k} = n^4 + 4 \cdot (2^k)^4 \overset{\text{Sophie-Germain}}{=} (n^2 + 2(2^k)^4 + 2n \cdot 2^k)(n^2 + 2(2^k)^4 - 2n \cdot 2^k).$$

Así que se factoriza. Te dejo que demuestres que ambos factores son mayores que 1.

□

Problema 21. 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 22. 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 23. Encuentra todas las soluciones de la ecuación $m^4 = n^3 + 137$ que sean números enteros positivos.

Solución. **Método 1:** Tomamos congruencias módulo 7, y calculamos los cubos y las potencias cuartas

	$x \equiv 0$	$x \equiv 1$	$x \equiv 2$	$x \equiv 3$	$x \equiv 4$	$x \equiv 5$	$x \equiv 6$
$x^4 \equiv$	0	1	2	4	4	2	1
$x^3 \equiv$	0	1	1	6	1	6	6
$x^3 + 137 \equiv$	4	5	5	3	5	3	3

Como ningún elemento de la tercera fila es igual a ningún elemento de la primera fila, esta ecuación no tiene ninguna solución en los números enteros, y por tanto ninguna solución en los enteros positivos.

Método 2: Hacer lo mismo con congruencias módulo 13. Las potencias cuartas módulo 13 son $0, 1, 3, 9$ y los cubos son $0, 1, 5, 8, 12$. Por tanto $m^4 - n^3 \equiv 7 \mod 13$ es imposible, y no hay ninguna solución.

□

Problema 24. 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 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[2]?

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.

[2]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 $r = 5$ 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.
- 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.

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

$1^2\cdot 1\cdot 1\cdot 1\cdot 1\cdot 6$	$=6$	$1^5\cdot 1\cdot 1\cdot 5$	$=5$	$1^6\cdot 1\cdot 1\cdot 4$	$=4$	$1^8\cdot 1\cdot 3$	$=3$	$1^{10}\cdot 2$	$=2$
$1^2\cdot 1\cdot 1\cdot 1\cdot 2\cdot 5$	$=10$	$1^5\cdot 1\cdot 2\cdot 4$	$=8$	$1^6\cdot 1\cdot 2\cdot 3$	$=6$	$1^8\cdot 2\cdot 2$	$=4$	1^{12}	$=1$
$1^2\cdot 1\cdot 1\cdot 1\cdot 3\cdot 4$	$=12$	$1^5\cdot 1\cdot 3\cdot 3$	$=5$	$1^6\cdot 2\cdot 2\cdot 2$	$=8$				
$1^2\cdot 1\cdot 1\cdot 2\cdot 2\cdot 4$	$=16$	$1^5\cdot 2\cdot 2\cdot 3$	12						
$1^2\cdot 1\cdot 1\cdot 2\cdot 3\cdot 3$	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								

(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. 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.

□