Pequeño Instituto de Matemáticas
2024-2025

Fechas: 31 de enero, 7 y 14 de febrero de 2025
Aritmética
Grupos: Júpiter, Urano y Venus **(Soluciones)**

Congruencias

Esta es la teoría que usamos el curso pasado. ¿La recuerdas? Te la puedes saltar, no herirás sus sentimientos. Si te la saltas y después descubres que no te acuerdas y quieres retroceder, ella estará aquí esperando. A no ser que pierdas las hojas. No pierdas las hojas.

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*

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

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

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 $r_0, r_1, r_2, \ldots$ en la expresión del Teorema 2 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, $n = r_0 + r_1 a + \ldots + r_j a^j$.

Problema 1. Expresa el número 62 en base 2 y en base 3.

Solución. $62_{10} = 111110_2 = 2022_3$. □

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

$$a \equiv b \pmod{n}.$$

Problema 2. ¿Cuáles de las siguientes afirmaciones son ciertas?

a) $7 \equiv 3 \pmod{2}$.

b) $7 \equiv 3 \pmod{3}$.

c) Si x es un número entero que satisface que $x \equiv 4 \pmod{5}$, entonces x es de la forma $x = 4+5k$ para algún entero número entero k.

d) Si k es un número entero y $x = 4+5k$, entonces $x \equiv 4 \pmod{5}$

Solución. a) Es cierta porque $7-3=4$ es divisible por 2.

b) Es falsa porque $7-3=4$ no es divisible por 3.

c) y d) Son ciertas: $x \equiv 4 \pmod{5}$ significa que $x-4$ es divisible por 5, que equivale a que existe un número entero k tal que $x-4=5k$, o lo que es lo mismo, tal que $x=4+5k$.

□

Trabajar con congruencias resulta sencillo porque satisfacen propiedades que nos resultan familiares. Más concretamente, el signo "≡" satisface las siguientes propiedades que también satisface el signo "=".

Propiedades del signo "≡"

Sea $n \geq 2$. Entonces:

1. Todo número es congruente a sí mismo módulo n, es decir

$$a \equiv a \pmod{n} \quad \text{para todo número entero } a.$$

2. Podemos intercambiar la parte de la izquierda y la de la derecha del signo "≡", es decir,

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

3. Se cumple la propiedad transitiva, es decir,

$$\text{Si } a \equiv b \pmod{n} \text{ y } b \equiv c \pmod{n}, \text{ entonces } a \equiv c \pmod{n}.$$

Problema 3. Justifica las tres propiedades del recuadro anterior usando la definición.

Solución. 1. $a \equiv a \pmod{n}$ significa que n divide a $a-a=0$, que es cierto.

2. Si $a \equiv b \pmod{n}$, entonces por definición tenemos que $a-b$ es divisible por n, por lo que $b-a = -(a-b)$ también será divisible por n, es decir, $b \equiv a \pmod{n}$.

3. Aplicando la definición, tenemos que demostrar lo siguiente: Si $a-b$ es divisible por n y $b-c$ es divisible por n, entonces $a-c$ es divisible por n. Esto es cierto porque la suma de enteros divisibles por n es divisible por n, y $a-c=(a-b)+(b-c)$.

□

Las congruencias módulo n están muy relacionadas con el algoritmo de la división (Teorema 1), más concretamente con los restos al dividir por n, como se muestra a continuación.

Trabajar con congruencias es lo mismo que trabajar con restos

Sean a, n dos números enteros, con $n \geq 2$, y sea r el resto obtenido al dividir a por n. Entonces,

$$a \equiv r \pmod{n}.$$

Problema 4. Usando el Teorema 1, justifica por qué es cierta la afirmación del recuadro anterior.

Solución. Por el Teorema 1 existe un entero q tal que $a = qn + r$, o equivalentemente, $a - r = qn$. Por tanto, $a - r$ es divisible por n, o equivalentemente, $a \equiv r \pmod{n}$. $\square$

Ahora ya sabemos que trabajar con congruencias es lo mismo que trabajar con restos, por lo que, si trabajamos módulo n, los únicos números que nos importarán serán los posibles restos al dividir por n, es decir, los enteros del 0 al $n - 1$. En efecto, la propiedad anterior nos dice que todo entero es congruente módulo n a alguno de estos n números.

Las congruencias (o trabajar con restos) 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 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 $11 + 5 \equiv 4 \pmod{12}$. Esto no es casualidad, siempre podemos operar con congruencias, como se muestra en el siguiente recuadro.

Operaciones con congruencias

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

- $a + c \equiv b + d \pmod{n}$.
- $a - c \equiv b - d \pmod{n}$.
- $ac \equiv bd \pmod{n}$.

En otras palabras, la suma, resta y multiplicación se comportan bien con respecto a las congruencias módulo n.

Antes de justificar por qué son ciertas las afirmaciones del recuadro anterior, vamos a ponerlas en práctica.

Problema 5. Halla el resto de dividir $23 \cdot 17$ de dos maneras:

- Multiplicando $23 \cdot 17$ y luego dividiendo por 3.
- Hallando los restos de dividir 23 y 17 por 3 y aplicando la propiedad de la multiplicación del recuadro anterior.

¿En cuál de las dos maneras has tenido que hacer cuentas más complicadas?

Solución.

- $23 \cdot 17 = 391 = 130 \cdot 3 + 1$, por lo que la respuesta es 1.

- $23 = 3 \cdot 7 + 2$ y $17 = 3 \cdot 5 + 2$. Como $2 \cdot 2 = 4 \equiv 1 \pmod 3$, la respuesta es 1.

Las cuentas son más complicadas de la primera manera. $\square$

Problema 6. Justifica las propiedades del recuadro anterior usando la definición de congruencia.

Solución. Aplicando la definición, tenemos que ver que si $a - b$ y $c - d$ son divisibles por n, entonces

- $(a + c) - (b + d) = (a - b) + (c - d)$ es divisible por n: Esto es cierto porque la suma de enteros divisibles por n es divisible por n.
- $(a - c) - (b - d) = (a - b) - (c - d)$ es divisible por n: Esto es cierto porque resta de dos enteros divisibles por n es divisible por n.
- $ac - bd = a(c - d) + d(a - b)$ es divisible por n. Esto es cierto porque la suma de dos enteros divisibles por n ($a(c - d)$ y $d(a - b)$) es divisible por n.

$\square$

Ahora que ya sabemos un montón de propiedades de las congruencias, podemos ponerlas en práctica para resolver problemas. El siguiente enunciado seguramente ya lo conoces, pero vamos a usar las propiedades de las congruencias para demostrarlo de manera sencilla. **Los ejemplos resueltos están allí por algo**, asegúrate de que entiendes la solución antes de seguir avanzando con la hoja.

Ejemplo resuelto (Criterio de divisibilidad por 3)**.** Demuestra que cualquier número natural n es congruente a la suma de todas sus cifras módulo 3. En particular, n 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 $10 \equiv 1 \pmod 3$. $10^2 \equiv 1^2 \equiv 1 \mod 3$, y en general, $10^i \equiv 1 \pmod 3$ para todo $i = 0, 1, 2, \ldots$.

Como sabemos operar con congruencias, 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. $\square$

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 6 referente a la multiplicación nos dice que $r_0 \equiv 4^{6789} \pmod 7$. Calculamos las potencias de 4 módulo 7.

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

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, $6789 \equiv 6 + 7 + 8 + 9 \equiv 0 \pmod 3$, por lo que $3^{6789} \equiv 3^0 \equiv 1 \pmod 7$. Por tanto, r_0 es un número entre 0 y 6 (incluidos) tal que $r_0 \equiv 1 \pmod 7$, y la única posibilidad es que $r_0 = 1$. $\square$

Problema 7. Sean a, b, c tres números impares. Demuestra que al menos uno de los números $ab-1$, $bc-1$ y $ca-1$ es divisible por 4.

Solución. a, b y c son congruentes con 1 o 3 módulo 4. Por el principio del palomar, existen dos de ellos son congruentes entre sí, por lo que su producto será congruente con 1 módulo 4, es decir, su producto menos 1 será divisible por 4.

□

Problema 8. Encuentra la última cifra del número $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots + 999 \cdot 1000$.

Solución. Agrupamos la suma en cien grupos de 10 sumandos, restándole el último término.

$$\begin{aligned}1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots 999 \cdot 1000 =& (1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots + 9 \cdot 10 + 10 \cdot 11) + \\ & (11 \cdot 12 + 12 \cdot 13 + \ldots + 19 \cdot 20 + 20 \cdot 21) + \\ & \vdots \\ & (981 \cdot 982 + 982 \cdot 983 + \ldots 989 \cdot 990 + 990 \cdot 991) + \\ & (991 \cdot 992 + 992 \cdot 993 + \ldots 999 \cdot 1000 + 1000 \cdot 1001) - 1000 \cdot 1001.\end{aligned}$$

Ahora, tomamos congruencias módulo 10. Cada uno de estos grupos de 10 sumandos coincide módulo 10, y el término que restamos es 0 módulo 10. Por tanto,

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots 999 \cdot 1000 \equiv 100 \cdot (1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots + 9 \cdot 10 + 10 \cdot 11) \equiv 0 \quad \text{módulo } 10,$$

por lo que la respuesta es 0.

□

Si te pidieran resolver la ecuación $2x = 4$, dividirías por 2 para obtener que la solución es $x = 2$. Si ahora te dieran una ecuación en congruencias podrías tener un problema, ya que hemos visto como sumar, restar y multiplicar en ese contexto, pero no dividir. Veamos un ejemplo de cómo salvar esta dificultad.

Ejemplo resuelto. Halla todas las soluciones de la ecuación $2x \equiv 4 \pmod{5}$.

Solución. La ecuación dada significa que $2x - 4 = 2 \cdot (x - 2)$ es divisible por 5. Como 2 y 5 no tienen factores primos en común, la ecuación equivale a decir que $x-2$ es divisible por 5. Por tanto, las soluciones a la ecuación son todos los enteros x que satisfacen que $x \equiv 2 \pmod{5}$, o equivalentemente, los números enteros cuyo resto al dividir por 5 es 2. □

Ahora, practicad vosotros:

Problema 9. 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) $x \equiv 0 \pmod{2} \equiv 0, 2, 4, 6, 8, \pmod{10}$

□

En este ejercicio hemos visto que algunas ecuaciones en congruencias tienen una solución, algunas ninguna y algunas tienen incluso varias soluciones (en el sentido de que corresponden a un resto de entre los posibles al dividir por n, a ninguno o a varios).

Problemas

Problema 10. Para cada uno de los siguientes casos, ¿es posible colocar los números $1, 2, \ldots, 60$ en un círculo de manera que se cumpla la siguiente condición?

a) La suma de todo par de números que tienen exactamente un número entre ellos dos es divisible por 2.

b) La suma de todo par de números que tienen exactamente dos números entre ellos dos es divisible por 3.

c) La suma de todo par de números que tienen exactamente seis números entre ellos dos es divisible por 7.

Solución. a) Sí se puede, hay el mismo número de números pares que impares entre 1 y 60, y basta colocarlos alternando par e impar, por ejemplo poniéndolos en orden del 1 al 60.

b) Sí se puede. Hay 20 números múltiplos de 3 entre 0 y 60, 20 congruentes con 1 módulo 3, y 20 congruentes con 2 módulo 3. Recorremos el círculo en el sentido de las agujas del reloj, numerando los lugares del 1 al 60. En los lugares congruentes con 0 módulo 3 colocamos los números congruentes con 0 módulo 3, en cualquier orden. En los lugares congruentes con 1 módulo 3 colocamos 10 números congruentes con 1 módulo 3 y 10 congruentes con 2 módulo 3, alternando. En los lugares congruentes con 2 módulo 3 también colocamos 10 números congruentes con 1 módulo 3 y 10 congruentes con 2 módulo 3, alternando. Esto satisface las condiciones del enunciado.

c) No se puede. Como $60/7$ son 8 y pico, hay 8 múltiplos de 7 entre 1 y 60. Argumentamos por reducción al absurdo. Supongamos que tenemos los números del 1 al 60 en círculo de manera que se satisfacen las condiciones del enunciado. Recorremos el círculo en el sentido de las agujas del reloj, de 7 en 7, empezando por el lugar que ocupa el número 7. La última de las condiciones nos dice que los lugares $1, 8, 15, 22, 29, 36, 43, 50, 57, 4, 11, 18, \ldots$ son todos múltiplos de 7. Esto son más de 8 múltiplos de 7, por lo que llegamos a una contradicción.

□

Problema 11. ¿Para cuántos pares de números x, y entre 1 y 100 es $x^2 + y^2$ divisible por 7?

Solución. Calculamos los cuadrados módulo 7:

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 2, \quad 4^2 \equiv 2, \quad 5^2 \equiv 4, \quad 6^2 \equiv 1,$$

Por tanto, $x^2 + y^2$ es divisible por 7 si y sólo si tanto x como y son divisibles por 7. Como 100 dividido por 7 son 14 y pico, hay 14 múltiplos de 7 entre 1 y 100. Por tanto, la respuesta es $\binom{14}{2} = 14 \cdot 13 = 182$.

□

Problema 12. Demuestra que para todo número natural n, siempre hay al menos un número en la lista $n, n+1, n+2, \ldots, n+9$ que no tiene ningún factor primo en común con ninguno de los otros números de la lista.

Solución. Si dos números de esa lista son divisibles por un primo p, entonces dicho primo divide a su resta. Por tanto, sólo nos tenemos que preocupar de los primos 2, 3, 5 y 7. En cualquier lista de 10 números consecutivos hay 5 pares y 5 impares. También hay 3 o 4 que son divisibles por 3 (según n no sea divisible por 3 o sí), pero como mucho dos son impares y divisibles por 3. Por tanto, hay tres impares que no son divisibles por 3. Uno de ellos es divisible por 5 y como mucho uno de ellos es divisible por 7. Por tanto, existe un número impar en esa lista que no es divisible ni por 3, ni por 5 ni por 7. Ese es el número que buscamos. □

Problema 13. Demuestra que para todo número entero positivo impar a existe un número entero positivo b tal que $2^b - 1$ es divisible por a.

Solución. Consideramos residuos módulo a. Como hay infinitos números de la forma $2^b - 1$, existirán dos números enteros $1 \leq n < m$ tal que

$$2^m - 1 \equiv 2^n - 1 \pmod{a},$$

o equivalentemente, $2^n(2^{m-n} - 1)$ es divisible por a. Como a es impar, no tiene ningún factor primo en común con 2^n, por lo que a divide a $2^{m-n} - 1$. Por tanto, el b que buscamos es $m - n$. □

Problema 14. Demuestra que si un número de 3 cifras, todas distintas, es múltiplo de 37, entonces hay una manera de reordenar las cifras para tener otro múltiplo de 37.

Solución. Llamemos a, b, c a las cifras, en orden, por lo que el número es $100a + 10b + c$. Tenemos que $100a + 10b + c \equiv 0 \pmod{37}$. Multiplicando por 10,

$$0 \equiv 1000a + 100b + 10c \equiv a + 100b + 10 \pmod{37},$$

es decir, bca también es múltiplo de 37.

□

Problema 15. Demuestra que la ecuación $x^2 + 6x - 1 = y^2$ no puede satisfacerse si x e y son ambos números enteros.

Solución. Consideramos congruencias módulo 4. El cuadrado de un número par es congruente con 0 módulo 4, y el de un número impar es congruente con 1 módulo 4.

Si x es impar, tenemos que $x^2 + 6x - 1$ es congruente con $2x$ módulo 4. Como x es impar, $x \equiv \pm 1$ módulo 4, por lo que $2x \equiv 2$. Por tanto, hemos visto que si x es impar, entonces $x^2 + 6x - 1 \equiv 2$, por lo que no puede ser el cuadrado de ningún número entero.

Si x es par, tenemos que $x^2 + 6x - 1 \equiv 3$ módulo 4, por lo que no puede ser el cuadrado de ningún número entero.

□

Problema 16. Sean a y b dos números enteros. Demuestra que si $a^3 - b^3$ es divisible por 3, entonces es divisible por 9.

Solución. Los restos módulo 9 que corresponden a números divisibles por 3 son 0, 3 y 6. Podemos calcular todos los cubos módulo 9:

$$\begin{array}{lll} 0^3 \equiv 0 & 1^3 \equiv 1 & 2^3 \equiv 8 \\ 3^3 \equiv 0 & 4^3 \equiv 1 & 5^3 \equiv 8 \\ 6^3 \equiv 0 & 7^3 \equiv 1 & 8^3 \equiv 8 \end{array}$$

Como $\pm(0-1) \equiv \mp 1$, $\pm(0-8) \equiv \pm 1$ y $\pm(1-8) \equiv \pm 2$, tenemos que si $a^3 - b^3 \equiv 0, 3, 6$ módulo 9, entonces $a^3 \equiv b^3$, o equivalentemente, $a^3 - b^3$ es divisible por 9.

□

Problema 17. ¿Puede existir un número natural tal que, dividido por la suma de todas sus cifras, da un cociente y un resto que son ambos iguales a 2023?

Solución. Supongamos que existe un tal número. Sea $n + 1$ el número de sus cifras, a las que llamamos a_0 (cifra de las unidades), a_1 (cifra de las decenas), así hasta a_n. Tenemos que

$$10^n a_n + 10^{n-1} a_{n-1} + \ldots 10^2 a_2 + 10 a_1 + a_0 = (a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0) \cdot 2023 + 2023.$$

Módulo 3, cualquier número natural es congruente a la suma de sus cifras. Además, $2023 \equiv 1$ módulo 3. Por tanto, la igualdad anterior módulo 3 se convierte en

$$\begin{aligned} a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0 &\equiv 10^n a_n + 10^{n-1} a_{n-1} + \ldots 10^2 a_2 + 10 a_1 + a_0 \\ &\equiv (a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0) \cdot 2023 + 2023 \\ &\equiv a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0 + 1, \end{aligned}$$

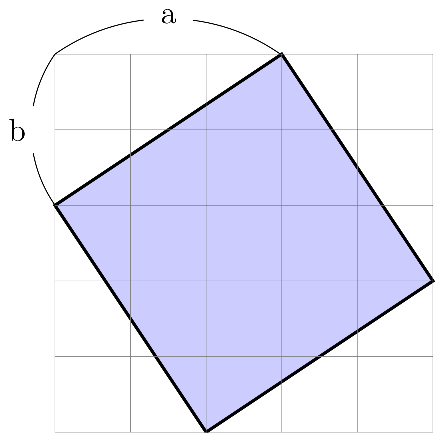
que implica que 1 es congruente con 0 módulo 3, lo que es una contradicción.

□

Problema 18. ¿Es posible encontrar un cuadrado con vértices en la cuadrícula cuya área sea igual a 40000003?

Solución. **Pistas:** Considera congruencias módulo 4

Un cuadrado con vértices en la cuadrícula se puede identificar con dos enteros a, b que determinan su posición como en el dibujo:



Su área es igual a $a^2 + b^2$ (por Pitágoras). Considerando la ecuación $a^2 + b^2 = 40000003 \equiv 3 \pmod 4$ y el hecho de que $\forall a\ a^2 \equiv 0, 1 \pmod 4$, es decir, los únicos restos posibles para un cuadrado perfecto módulo 4 son 0 o 1, llegamos a la conclusión de que la ecuación no tiene solución en enteros y, por consiguiente, no existe tal cuadrado.

□

Problema 19. Hay 10 números naturales escritos en una pizarra. Demuestra que siempre es posible escoger unos cuantos de ellos y escribir "+" o "−" entre ellos de manera que el resultado sea divisible por 1001.

Solución. Primero creamos todas las posibilidades de escoger unos cuantos números entre esos 10 y sumarlos: para cada uno de los 10 números tenemos 2 opciones, escogerlo o no. Como $1001 < 1023 = 2^{10} - 1$, el principio del palomar implica que hay dos maneras distintas de hacer este tipo de sumas (con al menos un sumando cada una) que dan el mismo resto al dividirlas por 1001. La resta de estas dos sumas es divisible por 1001 y puede obtenerse como una combinación de algunos de los 10 números con signos + y −.

□

Problema 20. Una caja fuerte tiene un candado con 27 botones, cada uno con una letra distinta del abecedario. Cuando instalaron el candado, a cada letra se le asignó un número natural, y sólo conoce esta asignación la dueña de la caja fuerte. Letras diferentes no tienen por qué tener números diferentes asignadas a ellas. Después de pulsar una combinación de letras distintas en la que cada letra aparece como mucho una vez, el candado lo interpreta como la suma de los números asignados a esas letras, y se abre si la suma es divisible por 27. Demuestra que existe una combinación de letras (en las que cada letra aparece como mucho una vez) que abre el candado.

Solución. Consideramos las 27 palabras $a, ab, abc, abcd, \ldots, abcde \cdots z$. Si una de ellas da lugar a un número divisible por 27, ya está. Si no, hay dos palabras que dan el mismo resto módulo 27. La palabra que empieza en la letra siguiente a la última letra de la primera de las palabras y acaba en la última letra de la segunda de las palabras corresponde a un número divisible por 27. □

Problema 21. $2n$ diplomáticos se sientan alrededor de una mesa redonda durante una reunión. Tras la pausa para el café, se vuelven a sentar en la misma mesa, pero quizá en otro orden diferente. Demuestra que siempre hay dos diplomáticos que tienen el mismo número de personas entre ellos antes y después del café.

Solución. Numeramos a los diplomáticos del 0 al $2n-1$ tal y como están sentados antes del café, siguiendo el sentido de las agujas del reloj. Para todo $j = 1 \ldots, 2n$, sea a_j un número del 0 al $2n-1$ que representa cuántas posiciones ha rotado el diplomático j en el sentido de las agujas del reloj después del café respecto de su posición inicial. Si existieran $i \neq j$ entre 0 y $2n-1$ tal que $a_i = a_j$, entonces los diplomáticos i y j tendrían el mismo número de personas entre ellos tanto antes como después del café, y en ese caso hemos acabado.

Supongamos por el contrario que $a_i \neq a_j$ para todo $i \neq j$. Tenemos que

$$a_0 + a_1 + \ldots + a_{2n-1} = 0 + 1 + 2 + \ldots + (2n-1) = (2n-1) \cdot n,$$

y que, como al volver del café están todos en posiciones distintas,

$$(0 + a_0) + (1 + a_1) + \ldots + (2n - 1 + a_{2n-1}) \equiv 0 + 1 + 2 + \ldots + (2n-1) \equiv (2n-1) \cdot n \pmod{2n}.$$

Por tanto,

$$0 \equiv 2n \cdot (2n-1) \equiv (2n-1) \cdot n + (2n-1) \cdot n \equiv (2n-1) \cdot n \pmod{2n}.$$

En otras palabras, $2n$ divide a $(2n-1) \cdot n$, que implica que 2 divide a $2n-1$, pero esto es imposible porque $2n-1$ es impar.

□

Problema 22. Hay dos ruedas dentadas con 14 dientes, idénticas, puestas una encima de otra. Desde arriba parecen una sóla rueda. Le pego un martillazo a 4 dientes, de manera que 4 parejas de dientes correspondientes se caen, 4 de cada rueda. ¿Es posible rotar una de las ruedas para que desde arriba parezca que no está ningún diente roto?

¿Y si tienen 13 dientes?

Solución. **Pistas:** Mira las distancias entre dientes rotos.

Con 14 dientes es posible siempre. Para cada par de dientes rotos, podemos medir su distancia, que estará entre 1 y 7. Como hay 4 dientes rotos, hay 6 pares de dientes, que pueden estar a 6 distancias distintas. Entonces, hay un número n entre 1 y 7 tal que no hay dos dientes a distancia n, y podemos rotar una rueda n pasos.

Con 13 dientes, si rompo los dientes 0, 2, 5 y 6 no se puede rotar la rueda de manera que no se solapen dos huecos.

□

Problema 23. Siete ladrones se están repartiendo una bolsa de monedas que contiene monedas de distintos tipos, todas ellas tienen como valor un número entero positivo. La suma total de dinero no se puede dividir a partes iguales entre ellos con las monedas que hay en la bolsa, pero si quitamos cualquiera de las monedas, la cantidad restante sí. Demuestra que la bolsa no puede tener 100 monedas.

Solución. Supongamos que hay n tipos de monedas. Sean $x_1, \ldots, x_n$ la cantidad de monedas de cada uno de los tipos, $a_1, \ldots, a_n$ sus valores. Como si quitamos cualquiera de las monedas obtenemos una cantidad que es divisible por 7 (y además divisible por 7 con las monedas dadas, pero eso no lo vamos a usar) tenemos que

$$\left(\sum_{i=1}^{n} a_i x_i \right) - a_j \quad \text{es divisible por 7 para todo } j = 1, \ldots, n.$$

En particular, restando dos de estas expresiones obtenemos que $a_j \equiv a_k$ módulo 7 para todo $j, k = 1, \ldots, n$.

Argumentamos por reducción al absurdo. Supongamos que hay 100 monedas en la bolsa, es decir, $x_1 + \ldots + x_n = 100$. Tenemos que la cantidad total de dinero es

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n \equiv 100 a_1 \equiv 2a_1 \text{ módulo 7.}$$

Como $(\sum_{i=1}^{n} a_i x_i) - a_1 \equiv 0$ módulo 7, obtenemos que a_1 es divisible por 7, y por tanto $a_1, \ldots, a_n$ son todos divisibles por 7. Ahora, nos damos cuenta de que las hipótesis del problema también se cumplen para 100 monedas de n tipos distintos tales que hay $x_1, \ldots, x_n$ monedas de cada uno de los tipos, y valen $\frac{a_1}{7}, \ldots, \frac{a_n}{7}$ respectivamente. Iterando este argumento, obtenemos que $a_1, \ldots, a_n$ son divisibles por cualquier potencia positiva de 7, por lo que llegamos a una contradicción.

□

Problema 24. ¿Se puede representar 2025^{2024} como suma de cubos de números naturales consecutivos?

Solución. **Pistas:** Considera los restos de división entre 7

No, no se puede.

Vamos a considerar los restos de división entre 7 para la $S_n = \sum_{k=1}^{n} k^3$.

$$S_1 = 1, S_2 = 1 + 2^3 \equiv 2, S_3 = 1 + 2^3 + 3^3 \equiv 1, S_4 = S_3 + 4^3 \equiv S_3 + (-3)^3 \equiv 2$$

Análogamente

$$S_5 \equiv 1, S_6 \equiv 0, S_7 \equiv 0$$

Entonces la suma de cubos de números consecutivos solamente puede dar $0, 1, 2, -1, -2$. Pero $2025 \equiv 2 mod\, 7, 2^{2024} = (2^3)^{674} \cdot 2^2 \equiv 1^{674} \cdot 4 = 4$. Contradicción.

□

Problema 25. Demuestra que en las cifras de π se puede encontrar un número múltiplo de 123456789.

Solución. Tomemos las primeras 123456789 cifras decimales, y formemos los 123456789 números posibles que terminan en la 123456789ª cifra. Por ejemplo, si tomáramos las primeras 6, como $\pi = 3,141592\ldots$, formaríamos los números 2, 92, 592, 1592, 41592 y 141592. Si uno de ellos diera resto 0 al dividir por 123456789, habríamos terminado. Si no, por el principio del palomar, hay dos que tienen el mismo resto. Entonces, su resta es un múltiplo de 123456789, que tiene este aspecto:

$$\overbrace{a_1a_2a_3\cdots a_n}^{\text{Cifras de } \pi}0\cdots 0 = (a_1\cdots a_n)\cdot 10^k$$

Es un múltiplo de 123456789, y como éste no es múltiplo de 2 ni 5, el número $a_1 \cdots a_n$ es múltiplo de 123456789 (estamos usando el teorema fundamental de la aritmética: todos los primos de la factorización de 123456789 están en la de $a_1 \cdots a_n$).

□

Problema 26. Si $a_0, a_1, \ldots, a_9$ son números entre 0 y 9, denotamos por $\overline{a_9a_8\ldots a_0}$ al número cuya cifra de las unidades es a_0, la de las decenas es a_1, etc. Es decir,

$$\overline{a_9a_8\ldots a_0} = a_9\cdot 10^9 + a_8\cdot 10^8 + a_7\cdot 10^7 + a_6\cdot 10^6 + a_5\cdot 10^5 + a_4\cdot 10^4 + a_3\cdot 10^3 + a_2\cdot 10^2 + a_1\cdot 10 + a_0.$$

Decimos que un número $\overline{a_9a_8\ldots a_0}$ de como mucho 10 cifras es *interesante* si es divisible por 11111 y las cifras $a_0, a_1, \ldots, a_9$ son todas distintas.

Responde a las siguientes preguntas.

a) Demuestra que $\overline{a_9a_8\ldots a_0}$ es divisible por 11111 exactamente cuando el número

$$(a_9 + a_4)\cdot 10^4 + (a_8 + a_3)\cdot 10^3 + (a_7 + a_2)\cdot 10^2 + (a_6 + a_1)\cdot 10 + (a_5 + a_0)$$

es divisible por 11111.

b) Demuestra que $\overline{a_9a_8a_7a_6a_5a_4a_3a_2a_1a_0}$ es interesante exactamente cuando $\overline{a_4a_8a_7a_6a_5a_9a_3a_2a_1a_0}$ es interesante (a_9 y a_4 han cambiado de posición).

c) Demuestra que $\overline{a_9a_8\ldots a_0}$ es interesante exactamente cuando $\overline{a_0a_9a_8\ldots a_1}$ es interesante.

d) ¿Cuántos números interesantes de exactamente 10 cifras existen? Justifica tu respuesta.

Solución. a) Sea $N = \overline{a_9a_8\ldots a_0} = a_9\cdot 10^9 + a_8\cdot 10^8 + \ldots + a_1\cdot 10 + a_0$. Tenemos que

$$\begin{aligned} N &= 10^5\cdot(a_9 10^4 + a_8 10^3 + a_7 10^2 + a_6 10 + a_5) + (a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10 + a_0) \\ &= (10^5 - 1)\cdot(a_9 10^4 + a_8 10^3 + a_7 10^2 + a_6 10 + a_5) + \\ &\quad \big((a_9 + a_4)\cdot 10^4 + (a_8 + a_3)\cdot 10^3 + (a_7 + a_2)\cdot 10^2 + (a_6 + a_1)\cdot 10 + (a_5 + a_0)\big). \end{aligned}$$

Como $10^5 - 1 = 99999 = 9\cdot 11111$ tenemos que, N es divisible por 11111 si y sólo si el número $(a_9 + a_4)\cdot 10^4 + (a_8 + a_3)\cdot 10^3 + (a_7 + a_2)\cdot 10^2 + (a_6 + a_1)\cdot 10 + (a_5 + a_0)$ es divisible por 11111.

b) Es consecuencia del apartado anterior. Intercambiar los roles de a_9 y a_4 no cambia la expresión $(a_9 + a_4) \cdot 10^4 + (a_8 + a_3) \cdot 10^3 + (a_7 + a_2) \cdot 10^2 + (a_6 + a_1) \cdot 10 + (a_5 + a_0)$.

c) Llamamos M al número $(a_9 + a_4) \cdot 10^4 + (a_8 + a_3) \cdot 10^3 + (a_7 + a_2) \cdot 10^2 + (a_6 + a_1) \cdot 10 + (a_5 + a_0)$. Tenemos que

$$M = 10\left((a_5 + a_0) \cdot 10^4 + (a_9 + a_4) \cdot 10^3 + (a_8 + a_3) \cdot 10^2 + (a_7 + a_2) \cdot 10 + (a_6 + a_1)\right) - (a_5 + a_0) \cdot (10^5 - 1).$$

Como $10^5 - 1$ es divisible por 11111 y el máximo común divisor de 11111 y 10 es 1, tenemos que M es divisible por 11111 si y sólo si $(a_5+a_0) \cdot 10^4 + (a_9+a_4) \cdot 10^3 + (a_8+a_3) \cdot 10^2 + (a_7+a_2) \cdot 10 + (a_6+a_1)$ es divisible por 11111. Por tanto, el apartado a) nos dice que $\overline{a_9a_8a_7a_6a_5a_4a_3a_2a_1a_0}$ es interesante si y sólo si $\overline{a_0a_9a_8a_7a_6a_5a_4a_3a_2a_1}$ es interesante.

d) Para encontrar todos los números interesantes $N = \overline{a_9a_8 \ldots a_0}$, usando el apartado c) basta encontrar aquellos números interesantes $N = \overline{a_9a_8 \ldots a_0}$ en los que $a_4 + a_9 \le a_8 + a_3, a_7 + a_2, a_6 + a_1, a_5 + a_0$. Supongamos que $a_4 + a_9 \le a_8 + a_3, a_7 + a_2, a_6 + a_1, a_5 + a_0$. El apartado a) nos dice que N es interesante si y sólo si $a_0, a_1, \ldots, a_9$ son todos distintos y el número

$$M = (a_9 + a_4) \cdot 10^4 + (a_8 + a_3) \cdot 10^3 + (a_7 + a_2) \cdot 10^2 + (a_6 + a_1) \cdot 10 + (a_5 + a_0)$$

es divisible por 11111. Sea $m_i = a_i + a_{5+i}$ para todo $i = 0, 1, 2, 3, 4$. Como $(a_9 + a_4) \cdot 11111 = (a_9 + a_4) \cdot (10^4 + 10^3 + 10^2 + 10 + 1)$ es divisible por 11111, tenemos que M es divisible por 11111 si y sólo si el número

$$M - (a_9 + a_4) \cdot 11111 = (m_3 - m_4) \cdot 10^3 + (m_2 - m_4) \cdot 10^2 + (m_1 - m_4) \cdot 10 + (m_0 - m_4)$$

es divisible por 11111. Llamamos a este último número M'. Como $0+1 = 1 \le m_4 \le m_i \le 8+9 = 17$, tenemos que $0 \le M' \le 16 \cdot 1111 = 17776$, por lo que M' es divisible por 11111 si y sólo si $M' = 0$ o $M' = 11111$. Hacemos los dos casos por separado.

- Caso $M' = 0$: Esto ocurre si y sólo si $m_0 = m_1 = m_2 = m_3 = m_4$, y como $m_0 + m_1 + m_2 + m_3 + m_4 = 0+1+2+3+4+5+6+7+8+9 = 45$, obtenemos que este caso es equivalente a $m_i = 9$ para todo $i = 0, 1, 2, 3, 4$. Veamos que hay exactamente $9 \cdot 8 \cdot 6 \cdot 4 \cdot 2 = 3456$ números interesantes de 10 cifras de esta forma: Hay 9 opciones para a_9 (que determinan el valor de a_4), ya que $a_9 \ne 0$. Para cada una de ellas, $10 - 2 = 8$ opciones para a_8 (que determinan el valor de a_3). Para cada una de ellas, 6 opciones para a_7 (que determinan el valor de a_2). Para cada una de ellas, 4 opciones para a_6 (que determinan el valor de a_1), Para cada una de ellas, 2 opciones para a_5 (que determinan el valor de a_0).
- Caso $M' = 11111$: Llamamos $\tilde{m}_i$ a $m_i - m_4$, para todo $i = 0, 1, 2, 3$. Tenemos que $\tilde{m}_i$ es un número entre 0 y 16, y $\tilde{m}_0$ acaba en 1. Por tanto, $\tilde{m}_0 = 1$ o $\tilde{m}_0 = 11$. Argumentando de esta manera, obtenemos que estas son todas las posibilidades para $(\tilde{m}_0, \tilde{m}_1, \tilde{m}_2, \tilde{m}_3)$:

  $$(1,1,1,11), (1,1,11,10), (1,11,0,11), (1,11,10,10),$$

  $$(11,0,1,11), (11,0,11,10), (11,10,0,11), (11,10,10,10).$$

  En cualquier caso, $\tilde{m}_0 + \tilde{m}_1 + \tilde{m}_2 + \tilde{m}_3 = m_0 + m_1 + m_2 + m_3 + m_4 - 5m_4 = 45 - 5m_4$ tendría que ser divisible por 5, y no lo es en ninguno de estos casos. Por tanto, no hay ningún número interesante que corresponda a este caso.

En conclusión, la respuesta es 3456.

No nos lo piden, pero de la demostración podemos obtener muchos ejemplos de números interesantes de 10 cifras, por ejemplo 9876501234.

$\square$

Problema 27. El creador de contenido FlinchPlays, tras el éxito de su vídeo viral REACCIONANDO A MI IMAGEN EN EL ESPEJO😱😱😱🔥🌐, quiere subir el listón inventando un nuevo reto. Quiere capturar los infinitos Pokémans (hay uno por cada número natural) en orden, de la siguiente manera: hay que capturar cada uno de los Pokémans una sola vez. Además, cuando haya capturado n Pokémans la suma de los PokéIDs de los Pokémans capturados debe ser múltiplo de n. ¿Es posible el sueño de FlinchPlays?

Solución. Es posible: construimos la sucesión por inducción, empezando por 1 (Pokéman Tulipán Pero Enfadado). Supongamos que llevamos $n-1$ números en la sucesión, y no se han repetido. Hay un número, llamémoslo k, que es el menor que aún no hemos incluido en la sucesión. Vamos a ver que lo podemos incluir en la sucesión, después de 2 números. Llamemos S a la suma de los n primeros términos, y p_n al siguiente. Tiene que cumplirse que $n|S+p_n$ y $n+1|S+p_n+k$, y que p_n sea un número no incluido en la sucesión hasta este momento.

Tomemos un p' cualquiera que cumpla que $S+p' \equiv 0 \pmod{n}$. Entonces, también nos serviría cualquier número de la forma $p'+qn$, para cualquier n, pues seguiremos teniendo un múltiplo de n. Ahora, tomando módulo $n+1$, tenemos que $n \equiv -1 \pmod{n+1}$. Queremos:

$$0 \equiv S + p' + qn + k \equiv S + p' - q + k \pmod{n+1}$$

Nos basta tomar $q \equiv qS + p' + k \pmod{n+1}$. Tomando q muy grande, con el mismo resto módulo $n+1$, podemos asegurarnos de que $p_n = p' + qn$ es un número nuevo en la sucesión. Hemos conseguido incluir el número k, y seguimos de la misma manera, por inducción.

Siguiendo esta construcción, la sucesión empezaría:

$$1, 3, 2, 10, 4, 52, 5, \ldots$$

□

Problemas para hacer en casa

7 de febrero

Problema 28. Demuestra que si $a-b$ y $c-d$ son divisibles por 2025, entonces $ac-bd$ y $ad-bc$ son ambos divisibles por 2025.

Solución. Tomamos congruencias módulo 2025. Por hipótesis, tenemos que $a \equiv b$ y $c \equiv d$. Por tanto, $ac - bd \equiv ac - ac \equiv 0$ y $ad - bc \equiv ac - ac \equiv 0$.

□

14 de febrero

Problema 29. Demuestra que hay una potencia de 3 (es decir, un número del tipo 3^n para un número entero $n \geq 1$) que acaba en 001.

Solución. Como hay infinitos números de la forma 3^n y sólo 1000 restos posibles al dividir por 1000, tendrán que existir dos números naturales $a > b$ tal que $3^a \equiv 3^b$ módulo 1000. Equivalentemente,

$$3^b \cdot (3^{a-b} - 1) \quad \text{es divisible por 1000.}$$

Como 1000 y 3^b no tienen factores primos en común, obtenemos que $3^{a-b} - 1$ es divisible por 1000, o equivalentemente,

$$3^{a-b} \equiv 1 \quad \text{módulo 1000.}$$

Por tanto, 3^{a-b} acaba en 001, y $a-b$ es un número entero mayor o igual que 1.

□