Pequeño Instituto de Matemáticas
2024-2025

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

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.

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 $x \equiv 4 \pmod{5}$

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

Propiedades del signo "$\equiv$"

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 "$\equiv$", 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.

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.

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?

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

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. □

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.

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

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 $r_0 = 1$. □

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.

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

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

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.

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

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.

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.

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.

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

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.

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?

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

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.

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.

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.

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?

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.

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

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

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.

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?

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.

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.