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.

Problema 5. Demuestra que si $\text{mcd}(a, n) \neq 1$, entonces $ax \equiv 1$ (mód n) no tiene solución x.

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

Problema 6. Supón ahora que $\text{mcd}(a, n) = 1$.

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

b) Demuestra que si $ax \equiv ay$ (mód n), entonces $x \equiv y$ (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 $ax \equiv 1$ (mód n).

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 $a^2 \equiv 1$ (mód p). Entonces $a \equiv \pm 1$ (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 $b \equiv a$ (mód n). Por ejemplo, $[2]_5 = \{2, 7, -3, -8. - 10008, 127, \ldots\}$. Esta nueva notación evita escribir cada vez $\equiv$ (mód 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 4 (El pequeño teorema de Fermat)**.** *Sea p un número primo. Si a no es divisible por p, entonces* $a^{p-1} \equiv 1$ (mód 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 $(n+1)|(5n+17)$

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

Problema 12. Se sabe que

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

¿Qué cifra está sustituida por el asterisco?

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

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

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.

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:

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

Determina el valor de A, B y C.

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?

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

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.

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.

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.

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?

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

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?

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.

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]?

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

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?

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

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.

[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

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.