Matemática Discreta

HOJA 3 RESUELTA

---

1) Usando las reglas de la definición de la suma, los axiomas de Peano, la propiedad asociativa de la suma y una doble inducción, demostrar la propiedad conmutativa de la suma en $\mathbb{N}$:

$$\forall a,\, b \in \mathbb{N}, \qquad a + b = b + a.$$

Sea $A = \{a \in \mathbb{N} : \forall b \in \mathbb{N} \quad a + b = b + a\} \subseteq \mathbb{N}$.

Por el principio de inducción, para demostrar que $A = \mathbb{N}$ hace falta verificar que $1 \in A$ y que $n \in A$ implica $s(n) \in A$.

Base de inducción en la variable a: se trata de probar que $1 \in A$, o, de forma equivalente, que

$$\forall b \in \mathbb{N}, \qquad 1 + b = b + 1.$$

Vamos entonces a utilizar un razonamiento por inducción tomando como variable b y definimos el conjunto $B = \{b \in \mathbb{N} : 1 + b = b + 1\}$.

Base de inducción en la variable b: $1 \in B$, ya que $1 + 1 = 1 + 1$.

Paso de inducción en la variable b: sea $b \in B$. Tenemos que demostrar que $s(b) \in B$. Pero,

$$1 + s(b) \overset{\text{reglas de la suma}}{=} s(1 + b) \overset{b \in B}{=}$$

$$s(b + 1) \overset{\text{reglas de la suma}}{=} (b + 1) + 1 \overset{\text{reglas de la suma}}{=} s(b) + 1.$$

Entonces $B = \mathbb{N}$ y hemos verificado la base de inducción en la variable a.

Paso de inducción en la variable a: sea $a \in A$. Tenemos que demostrar que $s(a) \in A$, es decir que $\forall b \in \mathbb{N} \quad s(a) + b = b + s(a)$. Ahora,

$$s(a) + b \overset{\text{reglas de la suma}}{=} (a + 1) + b \overset{\text{prop.asoc.}}{=} a + (1 + b) \overset{a \in A}{=}$$

$$(1 + b) + a \overset{B \equiv \mathbb{N}}{=} (b + 1) + a \overset{\text{prop.asoc.}}{=} b + (1 + a) \overset{\text{reglas de la suma}}{=} b + s(a).$$

Entonces $A = \mathbb{N}$.

2) Aplicando el algoritmo de Euclides, encontrar el máximo común divisor, $mcd(n, m)$, de

a) $n = 7469$ y $m = 2464$,

b) $n = 1109$ y $m = 4999$.

a) Ya que $7469 = 2464 \times 3 + 77$, $mcd(7469, 2464) = mcd(2464, 77)$.

Ya que $2464 = 77 \times 32$, $mcd(7469, 2464) = 77$.

b) Ya que $4999 = 1109 \times 4 + 563$, $mcd(4999, 1109) = mcd(1109, 563)$.

Ya que

$$1109 = 563 \times 1 + 546, \quad 563 = 546 \times 1 + 17, \quad 546 = 17 \times 32 + 2,$$

$$17 = 2 \times 8 + 1, \quad 2 = 1 \times 2,$$

$mcd(4999, 1109) = 1$.

3) En los casos a) y b) del problema 2), expresar el máximo común divisor de n y m como combinación lineal entera de n y m.

a) $77 = 7469 - 3 \times 2464 = 1 \times n - 3 \times m$.

b)

$$1 = 17-2\times 8 = 17-(546-17\times 32)\times 8 = 17\times 257-546\times 8 = (563-546)\times 257-546\times 8 =$$
$$= 563\times 257-546\times 265 = 563\times 257-(1109-563)\times 265 = 563\times 522-1109\times 265 =$$
$$= (4999-1109\times 4)\times 522-1109\times 265 = 4999\times 522-1109\times 2353 = -2353\times n+522\times m.$$

4) Calcular la factorización de los siguientes números:

a) 1859 b) 2541

c) 1029 d) 1111.

a) $1859 = 11 \times 169 = 11 \times 13^2$.

b) $2541 = 3 \times 847 = 3 \times 7 \times 121 = 3 \times 7 \times 11^2$.

c) $1029 = 3 \times 343 = 3 \times 7 \times 49 = 3 \times 7^3$.

d) $1111 = 11 \times 101$ y $10 \leq \sqrt{101} \leq 11$. Por tanto si 101 no es primo, tiene un divisor primo menor o igual a 7. Como 2,3,5,7 no son divisores de 101, 101 es primo.

5) Demostrar por reducción al absurdo el teorema de Euclides: existen infinitos números primos.

(Sugerencia: Sea $P = \{p_1, p_2, \cdots, p_n\}$ un conjunto finito de números primos, entonces el número $k = 1 + p_1 p_2 \cdots p_n$ no es divisible por ningún elemento de P.)

Supongamos que el conjunto de todos los números primos, digamos P, sea finito. Entonces $P = \{p_1, p_2, \cdots, p_n\}$ para algún número natural n y podemos suponer que $p_1 < p_2 < \cdots < p_n$. El entero $k = 1 + p_1 p_2 \cdots p_n$ no es un elemento de P, pues $k > p_n$. Pero k es primo, ya que para todo $i = 1, \cdots, n, \quad k \quad mod p_i = 1$. Por tanto llegamos a una contradicción.

6) Verificar que para todo entero positivo k, los enteros

$$(k+1)!+2, \quad (k+1)!+3, \quad (k+1)!+4, \cdots, (k+1)!+k, \quad (k+1)!+(k+1)$$

son k enteros compuestos consecutivos y, por tanto, para todo número natural k, existen dos primos consecutivos p y q tales que $p - q > k$. (Si n es un número entero positivo, $n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$.)

Si k es un entero positivo y j un elemento del conjunto $\{2, 3, \cdots, k, k+1\}, \quad j$ divide a

$$(k+1)! + j = (k+1) \cdot k \cdots j \cdot (j-1) \cdots 2 \cdot 1 + j.$$

Se sigue que

$$(k+1)!+2, \quad (k+1)!+3, \quad (k+1)!+4, \cdots, (k+1)!+k, \quad (k+1)!+(k+1)$$

son k enteros compuestos consecutivos.

7) Realiza las siguientes operaciones módulo 5 y módulo 6:

$$2011 + 56, \qquad 36^{1532}, \qquad 130 - 51.$$

Módulo 5:

$$2011 + 56 \equiv 1 + 1 \equiv 2 \quad mod 5.$$
$$36 \equiv 1 \quad mod 5, \qquad 36^{1532} \equiv 1 \quad mod 5.$$

$$130 - 51 \equiv 0 - 1 \equiv 4 \quad mod5.$$

Módulo 6:

$$2011 + 56 \equiv 1 + 2 \equiv 3 \quad mod6.$$
$$36 \equiv 0 \quad mod6, \qquad 36^{1532} \equiv 0 \quad mod6.$$
$$130 - 51 \equiv 4 - 3 \equiv 1 \quad mod6.$$

8) Julio César solía usar congruencias para encriptar sus mensajes. Primero ordenaba alfabéticamente las 23 letras del alfabeto (latino romano) y asociaba a cada letra α su posición $p(\alpha)$, de 0 hasta 22. Así la letra a quedaba asociada al 0, la b al 1, la c al 2, $\cdots$. Luego, sumaba 3 módulo 23 a las posiciones de las letras. Al final, cada letra α quedaba asociada al entero $(p(\alpha) + 3) mod 23$.

Vamos a usar como alfabeto el conjunto ordenado de sólo 7 letras (B,C,E,H,I,N,O). Para aplicar el método de César tendremos que trabajar módulo 7. ¿Cuál sería, en este caso, el sentido del mensaje 3051 65462, enviado por César?.

En nuestro caso hay 7 letras del alfabeto. Para poder descifrar el mensaje 3051 65462 , tenemos que restar a cada cifra 3 módulo 7 (o sumar 4 módulo 7), obteniendo: 0425 32136.
Ya que (B,C,E,H,I,N,O) corresponde a (0,1,2,3,4,5,6), el mensaje es: BIEN HECHO.

9) Encuentra todos los enteros cuya división por 3,4,5 tenga resto igual a 1,2,3, respectivamente.

Se trata de resolver el sistema de congruencias

$$\begin{cases} x \equiv 1 \quad mod3 \\ x \equiv 2 \quad mod4 \\ x \equiv 3 \quad mod5. \end{cases}$$

Por el teorema chino del resto este sistema tiene solución, siendo 3,4 y 5 primos entre sí dos a dos. Sean

$$a_1 = 1,\ a_2 = 2,\ a_3 = 3, \quad p_1 = 3,\ p_2 = 4,\ p_3 = 5,$$
$$P = 3 \cdot 4 \cdot 5 = 60, \quad P_1 = 20,\ P_2 = 15,\ P_3 = 12.$$

Si q_1, q_2 y q_3 son tales que $q_i P_i \equiv 1 mod p_i, \quad i = 1, 2, 3,$ las soluciones son iguales, módulo 60, a

$$x_0 = a_1 P_1 q_1 + a_2 P_2 q_2 + a_3 P_3 q_3.$$

Ahora,

$$20q_1 \equiv 1 mod3, \quad \text{si} \quad q_1 = 2,$$
$$15q_2 \equiv 1 mod4, \quad \text{si} \quad q_2 = 3,$$
$$12q_3 \equiv 1 mod5, \quad \text{si} \quad q_3 = 3,$$
$$x_0 = 1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 238 \equiv 58 mod60.$$

Se sigue que las soluciones son del tipo $x = 58 + 60k, \qquad k \in \mathbb{Z}$.

10) Encuentra, si existen, las soluciones de los siguientes sistemas de congruencias:

a) $\begin{cases} x \equiv 3 \quad mod5 \\ x \equiv 4 \quad mod10, \end{cases}$ b) $\begin{cases} x \equiv 3 \quad mod5 \\ x \equiv 4 \quad mod11. \end{cases}$

a) En este caso no podemos aplicar el teorema chino del resto, ya que 5 y 10 no son primos entre sí. Las soluciones de la primera congruencia son $x = 3+5k, \quad k \in \mathbb{Z}$ y las soluciones de la segunda son $x = 4 + 10t, \quad t \in \mathbb{Z}$.

Se trata entonces de verificar si existen valores de k y de t tales que $3 + 5k = 4 + 10t$. Pero,

$$3 + 5k = 4 + 10t \Leftrightarrow 5k - 10t = 4 - 3 \Leftrightarrow 5(k - 2t) = 1.$$

Siendo $k-2t$ un número entero, la última identidad implicaría que 5 es un divisor de 1, que es falso. Por tanto el sistema de congruencia no tiene soluciones.

b) En este caso 5 y 11 son primos entre sí y podemos aplicar el teorema chino del resto, que afirma que existe una solución módulo 55. En este caso

$$a_1 = 3,\ a_2 = 4, \quad p_1 = 5,\ p_2 = 11,$$
$$P = 5 \cdot 11 = 55, \quad P_1 = 11,\ P_2 = 5.$$

Si q_1 y q_2 son tales que $q_i P_i \equiv 1\, mod p_i, \quad i = 1, 2,$ las soluciones son iguales, módulo 55, a

$$x_0 = a_1 P_1 q_1 + a_2 P_2 q_2.$$

Ahora,

$$11q_1 \equiv 1 mod 5, \quad \text{si} \quad q_1 = 1,$$
$$5q_2 \equiv 1 mod 11, \quad \text{si} \quad q_2 = 9,$$
$$x_0 = 3 \cdot 11 \cdot 1 + 4 \cdot 5 \cdot 9 \equiv 33 + 180 \equiv 33 + 15 \equiv 48 \quad mod 55.$$

Se sigue que las soluciones son del tipo $x = 48 + 55k, \qquad k \in \mathbb{Z}$.

11) Escribir 271 en base 2 y en base 3.

Base 2:

$$\begin{aligned} 271 &= 135 \cdot 2 + 1 \\ 135 &= 67 \cdot 2 + 1 \\ 67 &= 33 \cdot 2 + 1 \\ 33 &= 16 \cdot 2 + 1 \\ 16 &= 8 \cdot 2 + 0 \\ 8 &= 4 \cdot 2 + 0 \\ 4 &= 2 \cdot 2 + 0 \\ 2 &= 1 \cdot 2 + 0 \\ 1 &= 0 \cdot 2 + 1 \end{aligned}$$

$$271 = 100001111.$$

Base 3:

$$\begin{aligned} 271 &= 90 \cdot 3 + 1 \\ 90 &= 30 \cdot 3 + 0 \\ 30 &= 10 \cdot 3 + 0 \\ 10 &= 3 \cdot 3 + 1 \\ 3 &= 1 \cdot 3 + 0 \\ 1 &= 0 \cdot 3 + 1 \end{aligned}$$

$$271 = 101001.$$