

Conjuntos y números 23/11

12. a) $x^n - 1 = (x-1) \sum_{j=0}^{n-1} x^j$ $n \in \mathbb{N}$. Por inducción:

$$\cdot n=1: x^1 - 1 = x - 1 \quad \checkmark$$

• Suponemos que es cierta para un $k \in \mathbb{N}$.

$$\cdot \text{Para } k+1: x(x^k - 1) \stackrel{\text{H.I.}}{=} x(x-1) \sum_{j=0}^{n-1} x^j$$

$$x^{k+1} - 1 - (x-1) = x(x-1) \sum_{j=0}^{n-1} x^j$$

$$x^{k+1} - 1 = (x-1) \left(\underbrace{1}_{\substack{\downarrow \\ \text{1}}} + x \sum_{j=0}^{n-1} x^j \right) = (x-1) \left(1 + \sum_{j=1}^n x^j \right) = (x-1) \sum_{j=0}^n x^j \quad \blacksquare$$

$2^n - 1$ es primo $\Rightarrow n$ es primo.

Supongamos que n no es primo, $n = a \cdot b$ $a, b > 1$

$$2^{ab} - 1 = (2^a)^b - 1 = \underbrace{(2^a - 1)}_{\substack{\downarrow \\ \text{1}}} \sum_{j=0}^{b-1} (2^a)^j \Rightarrow 2^a - 1 \mid 2^n - 1$$

Contradicción, $2^n - 1$ es primo. \blacksquare

b) Suponer que n no es potencia de 2, $n = 2^k \cdot m$ $m > 2$, $(m, 2) = 1$.

14. $\mathcal{U}(\mathbb{Z}_{/n})$ las unidades de $\mathbb{Z}_{/n}$. Demostrar:

$$\bar{a} \cdot \bar{b} \in \mathcal{U}(\mathbb{Z}_{/n}) \Leftrightarrow \bar{a} \in \mathcal{U}(\mathbb{Z}_{/n}) \text{ y } \bar{b} \in \mathcal{U}(\mathbb{Z}_{/n})$$

\Rightarrow Tenemos que $\exists x \in \mathbb{Z}_{/n}$ tq. $x \cdot (\bar{a} \cdot \bar{b}) = \bar{1}$. Entonces: $(x \cdot \bar{a}) \cdot \bar{b} = \bar{1}$

$\underbrace{}_{\text{inverso de } \bar{b}}$

También es verdad $(\bar{a} \cdot \bar{b}) x = \bar{1}$, luego $\bar{a} \underbrace{(\bar{b} x)}_{\text{inverso de } \bar{a}} = 1$

Es decir, $\bar{a} \in \mathcal{U}(\mathbb{Z}_{/n})$.

\Leftarrow Existen $\bar{a}^{-1}, \bar{b}^{-1} \in \mathbb{Z}_{/n}$ tq. $\bar{a} \bar{a}^{-1} = \bar{a}^{-1} \bar{a} = 1$ y $\bar{b} \bar{b}^{-1} = \bar{b}^{-1} \bar{b} = 1$

Entonces $(\bar{b}^{-1} \bar{a})(\bar{a} \cdot \bar{b}) = \bar{b}^{-1} \bar{b} = 1$, es decir $\bar{a} \cdot \bar{b} \in \mathcal{U}(\mathbb{Z}_{/n})$.

$\underbrace{}_{\text{inverso de } \bar{a} \cdot \bar{b}}$

15. $\mathcal{U}(\mathbb{Z}_{/2})$? En $\mathbb{Z}_{/n}$, un elemento m tiene inverso s.s.i (m, n)

$$(m \cdot l \equiv 1 \pmod{n} \Rightarrow m \cdot l = nk + 1 \quad k \in \mathbb{N})$$

Como 7 es primo, todas las clases que no son $\bar{0}$ tienen inverso.

$$U(\mathbb{Z}_7) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}.$$

$$\begin{aligned}\bar{1} \cdot \bar{1} &\equiv 1 \pmod{7} & \bar{6} \cdot \bar{6} &\equiv 1 \pmod{7} \\ \bar{3} \cdot \bar{5} &\equiv 1 \pmod{7} \\ \bar{2} \cdot \bar{4} &\equiv 1 \pmod{7}\end{aligned}$$

(16) a) p primo $\Rightarrow p \mid \binom{p}{k}$ para $1 \leq k \leq p-1$.

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdots (p-k+1)}{k!} \Rightarrow p(p-1) \cdots (p-k+1) = \binom{p}{k} \cdot k!$$

$\vdots p$

Luego $p \mid \binom{p}{k} \cdot k!$; pero $p \nmid k!$ Luego como p es primo $p \mid \binom{p}{k}$.

Para n no primo no es verdad: $\binom{4}{2} = \frac{4 \cdot 3}{2} = 6$, $4 \nmid 6$. ■

b) En \mathbb{Z}_{p^2} : $(\bar{a} + \bar{b})^p = \bar{a}^p + \bar{b}^p$.

$$(\bar{a} + \bar{b})^p = \sum_{j=0}^p \binom{p}{j} \bar{a}^j \bar{b}^{p-j} = \binom{p}{0} \bar{a}^0 \bar{b}^p + \binom{p}{1} \bar{a}^1 \bar{b}^{p-1} + \cdots + \binom{p}{p-1} \bar{a}^{p-1} \bar{b}^1 + \binom{p}{p} \bar{a}^p$$

$\vdots p \quad (\equiv 0 \pmod{p})$

$$= \bar{b}^p + \bar{a}^p.$$

■

(27) a) $\bar{13}^{-1}$ en \mathbb{Z}_{23} ?

• Aplicar algoritmo de Euclides con 23 y 13 :

$$\left\{ \begin{array}{l} 23 = 13 \cdot 1 + 10 \\ 13 = 10 \cdot 1 + 3 \\ 10 = 3 \cdot 3 + 1 \end{array} \right.$$

$$\begin{aligned}1 &= 10 - 3 \cdot 3 = 10 - 3(13 - 10) = 10 \cdot 4 + 13(-3) \\ &= (23 - 13) \cdot 4 + 13 \cdot (-3) = 4 \cdot 23 - 7 \cdot 13\end{aligned}$$

$$1 = 23 \cdot 4 + 13(-7) \Rightarrow 13 \cdot (-7) \equiv 1 \pmod{23}, -7 \equiv 16 \pmod{23}$$

Luego $\bar{13}^{-1} \equiv \bar{16} \pmod{23}$.

• $\bar{15}^{-1}$ en \mathbb{Z}_{23} ? $\bar{15} \equiv 8 \pmod{23}$. Repetir algoritmo de Euclides con 23 y 8 .

$$\text{Resultado: } 1 = 23(-1) + 8 \cdot 3 \Rightarrow \bar{8} \cdot \bar{3} \equiv 1 \pmod{23}, \quad \bar{-15}^{-1} \equiv 3 \pmod{23}.$$

b) Demostrar que $13x \equiv 2 \pmod{23}$ tiene sol. única en \mathbb{Z}_{23} .

$$13x \equiv 2 \pmod{23} \Rightarrow \bar{13}^{-1} \bar{13} \cdot x \equiv \bar{13}^{-1} \cdot 2 \pmod{23}$$

(\mathbb{Z}_{23} es un cuerpo)
[23 es primo] $\Rightarrow x \equiv \bar{16} \cdot \bar{2} \equiv \bar{9} \pmod{23}$. ■

18) Demostrar que existen infinitos naturales no representables como suma de 3 cuadrados.

Cuadrados mod. 8:

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

No puedo sumar $\bar{7}$ con 3 de estos restos, luego $l^2 + m^2 + n^2$ no puede ser $\equiv 7 \pmod{8}$. Luego los infinitos naturales de la forma $8k+7$ no pueden ser suma de 3 cuadrados.

19) $n > 1$, $(n-1)! + 1 \equiv 0 \pmod{n} \Rightarrow n$ es primo.

$$(n-1)! \equiv -1 \equiv n-1 \pmod{n}. \quad \text{mcd}(n, n-1) = 1, \text{ luego} \\ (n-1) \in U(\mathbb{Z}_n)$$

$$(n-1)(n-2) \dots 2 \cdot 1 \equiv n-1 \pmod{n}, \text{ multiplico por } (n-1)^{-1}:$$

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

$$(n-2) \left((n-3) \dots 2 \cdot 1 \right) \equiv 1 \pmod{n}, \text{ luego } (n-2) \in U(\mathbb{Z}_n)$$

$$\underbrace{\bar{a}}_{\bar{a}} \underbrace{\bar{b}}_{\bar{b}} \quad \text{Ej. 14: } \bar{abc} \in U(\mathbb{Z}_n) \Leftrightarrow \bar{a} \in U(\mathbb{Z}_n) \\ \bar{b} \in U(\mathbb{Z}_n) \quad \bar{c} \in U(\mathbb{Z}_n)$$

Luego $(n-3) \dots 2 \cdot 1 \in U(\mathbb{Z}_n)$. Repito el argumento:

$$(n-3) \left((n-4) \dots 2 \cdot 1 \right), \text{ luego } \frac{(n-3)}{(n-4) \dots 2 \cdot 1} \in U(\mathbb{Z}_n).$$

Repetiendo el argumento, todos los elem. del prod. son unidades.

Es decir $U(\mathbb{Z}_n) = \{\bar{1}, \bar{2}, \dots, \bar{n-2}, \bar{n-1}\}$, luego \mathbb{Z}_n es un cuerpo y n primo. ■

(20)

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 7 \end{cases}$$

3, 4 y 7 son coprimos 2 a 2, luego puedo utilizar el Tma. chino del resto.

$$a_1 = 1; n_1 = 4$$

$$N = 3 \cdot 4 \cdot 7 = 84$$

$$a_2 = 2; n_2 = 3$$

$$N_i = \frac{N}{n_i}, \quad N_1 = 21 \quad N_3 = 12$$

$$a_3 = 3; n_3 = 7$$

$$N_2 = 28$$

- Calcular $\bar{N}_i^{-1} \pmod{n_i}$.

$$\left\{ \begin{array}{l} N_1 = 21 \equiv 1 \pmod 4 \Rightarrow \bar{N}_1^{-1} \equiv 1 \pmod 4 \\ N_2 = 28 \equiv 1 \pmod 3 \Rightarrow \bar{N}_2^{-1} \equiv 1 \pmod 3 \\ N_3 = 12 \equiv 5 \pmod 7 \Rightarrow \bar{N}_3^{-1} \equiv 3 \pmod 7 \end{array} \right.$$

$$\bullet X = \sum_{i=1}^3 a_i \cdot N_i \cdot \bar{N}_i^{-1} \pmod{N} \Rightarrow X \equiv 21 + 56 + 108 \pmod{84}$$

$$\Rightarrow X \equiv 17 \pmod{84}$$

(21)

$$n^7 - n \text{ divisible por } 42 = 3 \cdot 7 \cdot 2$$

$$n \in \mathbb{N}$$

$$\Leftrightarrow \left\{ \begin{array}{l} n^7 - n \equiv 0 \pmod{2} \\ n^7 - n \equiv 0 \pmod{3} \\ n^7 - n \equiv 0 \pmod{7} \end{array} \right.$$

$$n^7 \equiv n \pmod{2} ? \quad Si: \frac{\bar{0}^7}{\bar{1}^7} = \bar{0} = 1$$

$$n^7 \equiv n \pmod{3} ? \quad Si: 2^7 = 128 \equiv 2 \pmod{3}$$

$$n^7 \equiv n \pmod{7} ? \quad Si, \text{ por el P.T. Fermat.}$$

■



22.

$$\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n \text{ es entero para todo } n.$$

$$\frac{\frac{1}{5}n^5 + \frac{1}{3}n^3 + 7n}{15} = \frac{3n^5 + 5n^3 + 7n}{15}, \text{ tengo que sacar } \frac{15}{15} \Big| \frac{3n^5 + 5n^3 + 7n}{15}$$

$$\text{Miramos } 3n^5 + 7n \pmod{5} \quad \xrightarrow{\text{P.T.F.}} \begin{aligned} n^5 &\equiv 1 \pmod{5} \Rightarrow n^5 \equiv n \pmod{5} \\ 3n^5 &\equiv 3n \pmod{5} \end{aligned}$$

$$3n + 2n \equiv 5n \equiv 0 \pmod{5}, \text{ luego } 5 \mid 3n^5 + 7n \text{ y por tanto} \\ 5 \mid 3n^5 + 5n^3 + 7n.$$

Miramos $5n^3 + 7n \pmod{3}$ $\xrightarrow{\text{PTF: }} n^2 \equiv 1 \pmod{3} \Rightarrow n^3 \equiv n \pmod{3}$

$$2n + n \equiv 3n \equiv 0 \pmod{3}, \text{ luego } 3 \mid 5n^3 + 7n \text{ y por tanto} \\ 3 \mid 3n^5 + 5n^3 + 7n.$$

$$(23) \quad 2222 \overset{5555}{+} 5555 \overset{2222}{=} ? \quad (\text{important: 7 is prime})$$

Hay que fijarse en las bases (2222 y 5555) mod 7 y en los exponentes mod. 6

$$2222 \equiv \begin{cases} 3 \pmod 7 \\ 2 \pmod 6 \end{cases} \quad 5555 = \begin{cases} 4 \pmod 7 \\ 5 \pmod 6 \end{cases}$$

$$\begin{array}{r} \overset{5}{\cancel{5}} \overset{5}{\cancel{5}} \overset{5}{\cancel{5}} \\ \overset{2}{\cancel{2}} \overset{2}{\cancel{2}} \overset{2}{\cancel{2}} \end{array} + \begin{array}{r} \overset{5}{\cancel{5}} \overset{5}{\cancel{5}} \overset{5}{\cancel{5}} \\ \overset{2}{\cancel{2}} \overset{2}{\cancel{2}} \overset{2}{\cancel{2}} \end{array} \equiv \begin{array}{r} \overset{5}{\cancel{5}} \overset{5}{\cancel{5}} \overset{5}{\cancel{5}} \\ 3 \end{array} + \begin{array}{r} \overset{2}{\cancel{2}} \overset{2}{\cancel{2}} \overset{2}{\cancel{2}} \\ 4 \end{array} \mod 7$$

"

$$3^{6k+5} + 4^{6k'+2} \pmod{7}$$

$$(3^6)^k \cdot 3^5 + (4^6)^{k'} \cdot 4^2 \mod 7$$

m P.T.F.

$$3^5 + 4^2 \equiv 5 + 2 \pmod{7}$$

$$0 \bmod 7$$

24.

$$3^{2011} \pmod{11}. \quad 2011 = 2 \cdot 10^3 + 1 \cdot 10 + 1 \equiv 1 \pmod{10}$$

$$3^{2011} = 3^{2010} \cdot 3 \leq (3^{20})^{201} \cdot 3 \equiv 3 \pmod{11}.$$

III P.T.F

$$1 \pmod{11}$$

(25) b) $\begin{cases} x \equiv 7 \pmod{8} \\ x \equiv 3 \pmod{12} \end{cases}$ 8 y 12 no son coprimos.

Si tiene sol.: $= \text{mcd}(8, 12) \mid (7 - 3) = 4$.

- Desarrollamos $a_1 \cdot 8 + b_1 \cdot 12 = 4 \Rightarrow a_1 = -1, b_1 = 1$.

- Multiplicamos la ecuación $\lambda = \frac{a_1 - a_2}{\text{mcd}(8, 12)} = 1$
por

$(-1) \cdot 8 + 12 \cdot 1 = 4$, entonces la solución:

$$x = a_1 - 8 \cdot a \cdot \lambda = 7 - 8(-1) = 15$$

$$\text{ " } a_2 + 12 \cdot b \cdot \lambda = 3 + 12 \cdot 1 = 15$$

$x = 15$ es la sol. inicial, todas las soluciones son:

$$x \equiv 15 \pmod{\text{lcm}(8, 12)} = 24$$

■