# Álgebra I Práctica 4 Resuelta

Por alumnos de Álgebra I Facultad de Ciencias Exactas y Naturales UBA

# Choose your destiny:

- Notas teóricas
- Ejercicios de la guía:

1.	<b>6.</b>	11.	<b>16.</b>	<b>21.</b>	<b>26.</b>	31.	<b>36.</b>
<b>2.</b>	<b>7.</b>	<b>12.</b>	<b>17.</b>	<b>22.</b>	<b>27</b> .	<b>32.</b>	<b>37.</b>
3.	8.	13.	18.	<b>23</b> .	<b>28.</b>	<b>33.</b>	38.
<b>4.</b>	9.	14.	19.	<b>24.</b>	<b>29</b> .	<b>34.</b>	39.
<b>5.</b>	10.	<b>15.</b>	20.	<b>25</b> .	<b>30.</b>	<b>35</b> .	<b>40.</b>

• Ejercicios Extras

<b>1</b> .	<b>3</b> .	<b>5</b> .	<b>७</b> 7.	<b>6</b> 9.
<b>2</b> .	<b>4</b> .	<b>♦</b> 6.	<b>♦8.</b>	

#### Notas teóricas:

- d divide a  $a \to d \mid a \iff \exists k \in \mathbb{Z} : a = k \cdot d$
- $\mathcal{D}(-a) = \{-|a|, \dots, -1, 1, \dots, |a|\}.$
- $d \mid 0$ , dado que  $0 = 0 \cdot d$ . Se desprende que  $\mathcal{D}(0) = \{\mathbb{Z} \{0\}\}\$
- $\bullet \left\{ \begin{array}{l} d \mid a \iff -d \mid a \text{ (pues } a = k \cdot d \iff a = (-k) \cdot (-d)) \\ d \mid a \iff d \mid -a \text{ (pues } a = k \cdot d \iff (-a) = (-k) \cdot d) \\ \Rightarrow d \mid a \iff |d| \mid |a| \end{array} \right.$
- $\bullet \ \begin{cases} d \mid a \neq d \mid b \Rightarrow d \mid a + b \\ d \mid a \neq d \mid b \Rightarrow d \mid a b \\ d \mid a \Rightarrow d \mid c \cdot a, \ \forall c \in \mathbb{Z} \\ d \mid a \Rightarrow d \mid c \cdot a \\ d \mid a \Rightarrow d^2 \mid a^2 \neq d^n \mid a^n \ \forall n \in \mathbb{N} \\ d \mid a \cdot b \text{ no implica } d \mid a \vee d \mid b. \text{ Por ejemplo } 6 \mid 3 \cdot 4 \end{cases}$
- $\begin{cases} a \text{ es congruente } a \text{ } b \text{ } m\'odulo \text{ } d \text{ si } d \mid a-b. \text{ Se nota } a \equiv b \text{ } (d) \\ a \equiv b \text{ } (d) \iff d \mid a-b \end{cases}$
- $\bullet \begin{cases}
  a_1 \equiv b_1 (d) \\
  \vdots \\
  a_n \equiv b_n (d)
  \end{cases} \Rightarrow a_1 + \dots + a_n \equiv a_b + \dots + b_n (d).$
- $\bullet \begin{cases}
  a_1 \equiv b_1 (d) \\
  \vdots \\
  a_n \equiv b_n (d)
  \end{cases} \Rightarrow a_1 \cdots a_n \equiv a_b \cdots b_n (d) \xrightarrow{a_i = a \wedge b_i = b \atop \forall i \in \{1, \dots, n\}} a^n \equiv b^n (d)$

### Algoritmo de división:

• Dados  $a, d \in \mathbb{Z}$  con  $d \neq 0$ , <u>existen</u> k (cociente),  $r(\text{resto}) \in \mathbb{Z}$  tales que:

$$\left\{ \begin{array}{l} a = k \cdot d + r, \\ \cos 0 \le r < |d|. \end{array} \right\}$$

Y además estos k y r son  $\underline{únicos}$ .

- Notación:  $r_d(a)$  es el resto de dividir a a entre d
- $0 \le r < |d| \Rightarrow r = r_d(r)$ . Un número que cumple condición de resto, es su resto.

cumple condición de resto

- $r_d(a) = 0 \iff d \mid a \iff a \equiv 0 \ (d)$
- $a \equiv r_d(a)$  (d). Tiene mucho sentido.
- $a \equiv r \ (d) \ \text{con} \ \underbrace{0 \le r < |d|}_{\text{cumple condición de resto}} \Rightarrow r = r_d(a)$
- $r_1 \equiv r_2$  (d) con  $0 \le r_1, r_2 < |d| \Rightarrow r_1 = r_2$

- $a \equiv b \ (d) \iff r_d(a) = r_d(b)$ . Dos números que son congruentes, tienen igual resto.
- $r_d(a+b) = r_d(r_d(a) + r_d(b))$  ya que si  $\left\{ \begin{array}{l} a \equiv r_d(a) \ (d) \\ b \equiv r_d(b) \ (d) \end{array} \right\} \to a+b \equiv r_d(a) + r_d(b) \ (d)$
- $r_d(a \cdot b) = r_d(r_d(a) \cdot r_d(b))$  ya que si  $\left\{ \begin{array}{l} a \equiv r_d(a) \ (d) \\ b \equiv r_d(b) \ (d) \end{array} \right\} \rightarrow a \cdot b \equiv r_d(a) \cdot r_d(b) \ (d)$

#### Sistema de numeración:

• Sea  $d \in \mathbb{N}, d \geq 2$ . Entonces  $\forall a \in \mathbb{N}_0$  se puede escribir en la forma

$$a = r_n d^n + r_{n-1} d^{n-1} + \dots + r_1 d^1 + r_0$$

con  $0 \le r_i < d$  para  $0 \le i \le n$  con  $r_n, \ldots, r_0$  son únicos en esas condiciones.

- Notación:  $a = (r_n r_{n-1} \cdots r_1 r_0)_d = \begin{cases} 2020 = (2020)_{10} \\ 2020 = (7E4)_{16} \\ 2020 = (31040)_5 \end{cases}$
- $\bullet \ d^n = (1 \underbrace{0 \cdots 0}_n)$
- ¿Cuál es el número más grande que puedo escribir usando n cifras en base d?

$$(\underline{d-1} \ \underline{d-1} \ \cdots \ \underline{d-1})_d = \sum_{i=0}^{n-1} (d-1)d^i = d^n - 1$$

- ¿Cuántos números hay con  $\leq n$  cifras? Hay del 0 hasta el  $d^n - 1$ , es decir  $d^n$ .
- ¿Cuál es la forma más rápida de calcular 2<sup>16</sup>

#### Máximo común divisor:

- Sean  $a, b \in \mathbb{Z}$ , no ambos nulos. El MCD entre a y b es el mayor de los divisores común entre a y b y se nota (a:b)
- $(a:b) \in \mathbb{N}$  (pues  $(a:b) \geq 1$ ) siempre existe.  $\mathcal{D}com_{+}(a,b) = \mathcal{D}_{+}(a) \cap \mathcal{D}_{+}(b) \neq \emptyset$  pues  $1 \in \mathcal{D}com_{+}(a,b)$ . Se ve también que está acotado por el menor entre a y b, pues si  $d \mid a \land d \mid b \Rightarrow d \leq |a| \land d \leq |b|$  y es <u>único</u>.
- Sean  $a y b \in \mathbb{Z}$ , no ambos nulos.

$$-(a:b) = (\pm a:\pm b)$$

$$-(a:b) = (b:a)$$

$$-(a:1) = 1$$

$$-(a:0) = |a|, \quad \forall a \in \mathbb{Z} - \{0\}$$

$$-\text{ si } b \mid a \Rightarrow (a:b) = |b| \text{ si } b \in \mathbb{Z} - \{0\}$$

$$-(a:b) = (a:b+na) \text{ con } n \in \mathbb{Z}$$

$$-(a:b) = (a:r_a(b)) \text{ con } n \in \mathbb{Z}$$

- Algoritmo de Euclides: Sean  $a, b \in \mathbb{Z}$  con  $b \neq 0$ , entonces,  $\forall k \in \mathbb{Z}$ , se tiene: (a : b) = (b : a kb). En particular, como  $r_b(a) = a - kb$ , con k el cociente (para  $b \neq 0$ ), se tiene  $(a : b) = (b : r_b(a))$
- 2 ¿Errores? Mandanos tu solución, prolija, así lo arreglamos.

- Combinación Entera: Sean  $a, b \in \mathbb{Z}$  no ambos nulos, entonces  $\exists s, t \in \mathbb{Z}$  tal que  $(a : b) = s \cdot a + t \cdot b$ .
  - Todos los divisores comunes entre a y b dividen al (a:b). Sean  $a,b\in\mathbb{Z}$  no ambos nulos,  $d\in\mathbb{Z}-\{0\}$ . Entonces:

$$d \mid a \le d \mid b \iff d \mid \underbrace{(a:b)}_{s \cdot a + t \cdot b}$$

- Sea  $c \in \mathbb{Z}$  entonces  $\exists s', t' \in \mathbb{Z}$  con  $c = s'a + t'b \iff (a:b) \mid c$ .

- Todos los números múltiplos del MCD se escriben como combinación entera de a y b.
- Si un número es una combinación entera de a y b entonces es un múltiplo del MCD.
- Sean  $a, b \in \mathbb{Z}$  no ambos nulos, y sea  $k \in \mathbb{N}$

$$(ka:kb) = k(a:b)$$

- Coprimos:
  - Dados  $a, b \in \mathbb{Z}$ , no ambos nulos, se dice que son coprimos si (a : b) = 1

$$\begin{array}{c} a \perp b \iff (a:b) = 1 \\ a \perp b \iff \exists \, s, \; t \in \mathbb{Z} \; \, \text{tal que} \; 1 = s \cdot a + t \cdot b \end{array}$$

- Sean  $a, b \in \mathbb{Z}$ , no ambos nulos. Entonces  $\frac{a}{(a:b)} \perp \frac{b}{(a:b)}$ .
- Coprimizar es :  $\left\{ \begin{array}{l} a = (a:b) \cdot a' \\ b = (a:b) \cdot b' \end{array} \right\} \rightarrow a' \ y \ b' \ \text{son coprimos}.$
- Sean  $a, c, d \in \mathbb{Z}$  con c, d no nulos. Entonces:

$$c \mid a \ y \ d \mid a \ y \ c \perp d \iff c \cdot d \mid a$$

- Sean  $a, b, d \in \mathbb{Z}$  con  $d \neq 0$ . Entonces:

$$d \mid a \cdot b \vee d \perp a \Rightarrow d \mid b$$

- Primos y Factorización:
  - Sea p primo y sean  $a, b \in \mathbb{Z}$ . Entonces:

$$p \mid a \cdot b \Rightarrow p \mid a \vee p \mid b$$

- Si p divide a algún producto de números, tiene que dividir a alguno de los factores  $\rightarrow$  Sean  $a_1, \ldots, a_n \in \mathbb{Z}$ :

$$\begin{cases} p \mid a_1 \cdot a_2 \cdots a_n \Rightarrow p \mid a_i \text{ para algún } i \text{ con } 1 \leq i \leq n. \\ p \mid a^n \Rightarrow p \mid a. \end{cases}$$

- Si  $a \in \mathbb{Z}$ , p primo:

$$\begin{cases} (a:p) = 1 \iff p \nmid a \\ (a:p) = p \iff p \mid a \end{cases}$$

– Sea  $n \in \mathbb{Z} - \{0\}$ ,  $n = \underbrace{s}_{\{-1,1\}} \cdot \prod_{i=1}^k p_i^{\alpha_i} = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  su factorización en primos. Entonces todo divisor m positivo de n se escribe como:

$$\begin{cases}
\operatorname{Si} m \mid n \to m = p_1^{\beta_1} \cdots p_k^{\beta_k} \operatorname{con} 0 \leq \beta_i \leq \alpha_i, & \forall i \ 1 \leq i \leq k \\ & \text{y hay} \end{cases}$$

$$(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_k + 1) = \prod_{i=1}^k \alpha_i + 1$$
divisores positivos de  $n$ .

- $\text{ Sean } a \text{ y } b \in \mathbb{Z} \text{ no nulos, con} \begin{cases} a = \pm p_1^{m_1} \cdots p_r^{m_r} \text{ con } m_1, \cdots, m_r \in \mathbb{Z}_0 \\ b = \pm p_1^{n_1} \cdots p_r^{n_r} \text{ con } n_1, \cdots, n_r \in \mathbb{Z}_0 \\ \begin{cases} \Rightarrow (a:b) = p_1^{\min\{m_1,n_1\}} \cdots p_r^{\min\{m_r,n_r\}} \\ \Rightarrow [a:b] = p_1^{\max\{m_1,n_1\}} \cdots p_r^{\max\{m_r,n_r\}} \end{cases}$
- Sean  $a, b, c \in \mathbb{Z}$  no nulos:
  - \*  $a \perp b \iff$  no tienen primos en común.
  - $* (a:b) = 1 \land (a:c) = 1 \iff (a:bc) = 1$
  - $* (a:b) = 1 \iff (a^m, b^n) = 1, \forall m, n \in \mathbb{Z}$
  - $* (a^n : a^m) = (a : b)^n$
- Si  $a \mid m \land b \mid m$ , entonces  $[a:b] \mid m$
- $-(a:b)\cdot [a:b] = |a\cdot b|$

### Ejercicios de la guía:

#### Divisibilidad

1. Decidir si las siguientes afirmaciones son verdaderas  $\forall a, b, c \in \mathbb{Z}$ : Calcular

i) 
$$a \cdot b \mid c \Rightarrow a \mid c \text{ y } b \mid c$$

$$\begin{cases} c = k \cdot a \cdot b = \underbrace{b}_{k \cdot b} \cdot a \Rightarrow a \mid c \quad \checkmark \\ c = k \cdot a \cdot b = \underbrace{i}_{k \cdot a} \cdot b \Rightarrow b \mid c \quad \checkmark \end{cases}$$

ii) 
$$4 \mid a^2 \Rightarrow 2 \mid a$$

$$a^2 = k \cdot 4 = \underbrace{h}_{k \cdot 2} \cdot 2 \Rightarrow a^2 \mid 2 \xrightarrow{\text{si } a \cdot b \mid c} a \mid 2 \quad \checkmark$$

iii) 
$$2 \mid a \cdot b \Rightarrow 2 \mid a \text{ o } 2 \mid b$$

Si 
$$2 \mid a \cdot b \Rightarrow \begin{cases} a \text{ tiene que ser } par \\ \lor \\ b \text{ tiene que ser } par \end{cases} \xrightarrow{\text{para que}} a \cdot b \text{ sea par. Por lo tanto si } 2 \mid a \cdot b \Rightarrow 2 \mid a \text{ o } 2 \mid b.$$

iv) 
$$9 \mid a \cdot b \Rightarrow 9 \mid a$$
 o  $9 \mid b$ 

Si  $a = 3 \land b = 3$ , se tiene que 9 | 9, sin embargo 9  $\not\mid$  3

v) 
$$a \mid b + c \Rightarrow a \mid b$$
 o  $a \mid c$ 

$$12 \mid 20 + 4 \Rightarrow 12 \not\mid 20 \text{ y } 12 \not\mid 4$$

### \* Falta hacerlo!

Si querés mandarlo: Telegram  $\to \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc$ .

### \* Falta hacerlo!

Si querés mandarlo: Telegram  $\to \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc$ .

# \* Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en LATEX  $\rightarrow \bigcirc$ .

ix)  $a \mid b + a^2 \Rightarrow a \mid b$ 

 $\begin{array}{l} a \mid b + a^2 \Rightarrow b + a^2 = k \cdot a \xrightarrow{\text{acomodo}} b = (k - a) \cdot a = h \cdot a \Rightarrow a \mid b \quad \checkmark \\ \xrightarrow{\text{también puedo}} \left\{ \begin{array}{l} a \mid a^2 \\ a \mid b - a^2 \end{array} \right\} \xrightarrow{\text{por propiedad}} a \mid (b - a^2) + (a^2) = b \Rightarrow a \mid b \quad \checkmark \end{array}$ 

 $(x) \ a \mid b \Rightarrow a^n \mid b^n, \ \forall n \in \mathbb{N}$ 

Pruebo por inducción.  $p(n) : a \mid b \Rightarrow a^n \mid b^n$ 

Caso base:  $n = 1 \Rightarrow a | b \Rightarrow a^1 | b^1 \checkmark$ Paso inductivo:  $\forall h \in \mathbb{N}, p(h) \ V \Rightarrow p(h+1) \ V$ ?
Si  $a | b \Rightarrow a^k | b^k \Rightarrow a^k \cdot c = b^k \xrightarrow{\text{multiplico por} \\ b \ \text{M.A.M}} b \cdot a^k \cdot c = b^{k+1} \xrightarrow{a | b} a \cdot d \cdot a^k \cdot c = a^{k+1} \cdot (cd) = b^{k+1} \xrightarrow{\text{concluyendo}} a^{k+1} | b^{k+1} \text{como quería mostrarse.}$ 

Como  $p(1) \wedge p(k) \wedge p(k+1)$  resultaron verdaderas, por el principio de inducción p(n) es verdadera  $\forall n \in \mathbb{N}$ 

Este resultado es importante y se va a ver en muchos ejercicios.  $a \mid b \Rightarrow a^n \mid b^n \iff b \equiv 0 \ (a) \Rightarrow b^n \equiv \underbrace{0}_{\stackrel{(a^n)}{\equiv} a^n} (a^n) \iff b^n \equiv a^n \ (a^n)$ 

- **2.** Hallar todos los  $n \in \mathbb{N}$  tales que:
  - i) 3n-1|n+7

Busco eliminar la *n* del *miembro* derecho.

$$\begin{cases}
3n - 1 \mid n + 7 \xrightarrow{a \mid c \Rightarrow} 3n - 1 \mid 3 \cdot (n + 7) = 3n + 21 \\
\frac{a \mid b \land a \mid c}{\Rightarrow a \mid b \pm c} 3n - 1 \mid 3n + 21 - (3n - 1) = 22
\end{cases} \rightarrow 3n - 1 \mid 22$$

$$\xrightarrow{\text{busco } n \text{ para que}} \xrightarrow{22 \atop \text{para que}} 22 \xrightarrow{3n - 1} \in \mathcal{D}(22) = \{1 \pm 1, \pm 2, \pm 11, \pm 22\} \xrightarrow{\text{probando}} n \in \{1, 4\} \quad \checkmark$$

- ii)
- iii)
- iv)  $n-2 | n^3 8$

 $\xrightarrow{a \mid b} n - 2 \mid \underbrace{(n-2) \cdot (n^2 + 2n + 4)}_{n^3 - 8}$  Esto va a dividir para todo  $n \neq 2$ 

- 3. Sean  $a, b \in \mathbb{Z}$ .
  - i) Probar que  $a b \mid a^n b^n$  para todo  $n \in \mathbb{N} \land a \neq b \in \mathbb{Z}$
  - ii) Probar que si n es un número natural par y  $a \neq -b$ , entonces  $a + b \mid a^n b^n$ .
  - iii) Probar que si n es un número natural impar y  $a \neq -b$ , entonces  $a + b \mid a^n + b^n$ .
- 2 ¿Errores? Mandanos tu solución, prolija, así lo arreglamos.

i) Si 
$$a - b \mid a^n - b^n \iff a^n \equiv b^n (a - b) \iff \begin{cases} a \equiv b (a - b) \\ a^2 \equiv \underbrace{a} \cdot b (a - b) \rightarrow a^2 \equiv b^2 (a - b) \\ \vdots \\ a^n \equiv b^n (a - b) \end{cases}$$

$$\Rightarrow a^n \equiv b^n (a - b) \iff a - b \mid a^n - b^n$$

ii) Sé que 
$$a \equiv -b$$
  $(a+b) \iff$ 

$$\begin{cases}
a^2 \equiv \underbrace{a} \cdot b \ (a+b) \xrightarrow{\text{propiedad}} a^2 \equiv (-1)^2 \cdot b^2 \ (a+b) \\
\vdots & \stackrel{(a-b)}{\equiv} -b \\
\vdots & \stackrel{(a-b)}{\rightleftharpoons} -b \\
\vdots & \stackrel{(a-b)}{\rightleftharpoons} -b
\end{cases}$$

$$\vdots & \stackrel{(a+b)}{\rightleftharpoons} \leftarrow$$

$$a^n \equiv (-1)^n \cdot b^n \ (a+b) \to \begin{cases}
a^n \equiv b^n \ (a+b) & \text{con n par} \\
a^n \equiv (-1)^n \cdot b^n \ (a+b) & \text{con n impar}
\end{cases}$$

$$\downarrow^2$$

$$\begin{cases}
\text{Con } n \text{ par: } a^n \equiv b^n \ (a+b) \Rightarrow a+b \ | \ a^n - b^n \ (a+b) \Rightarrow a+b \ | \ a^n + b^n
\end{cases}$$

Inducción:  $\begin{cases}
p(n) : \mathbf{a} \equiv -b \ (a+b) \Rightarrow a^n \equiv (-1)^n \cdot b^n \ (a+b) \ \forall n \in \mathbb{N} . \\
Caso base: \\
p(1) : \mathbf{a} \equiv -b \ (a+b) \Rightarrow a^1 \equiv (-1)^1 \cdot b^1 \ (a+b) \Rightarrow \mathbf{a} \equiv -b \ (a+b) \text{ Verdadero.} \\
Hipótesis inductiva: \\
p(k) \ V \Rightarrow p(k+1) \ V? \\
\mathbf{a} \equiv -b \ (a+b) \Rightarrow a^k \equiv (-1)^k \cdot b^k \ (a+b) \Rightarrow \mathbf{a} \equiv -b \ (a+b) \Rightarrow a^{k+1} \equiv (-1)^{k+1} \cdot b^{k+1} \ (a+b)
\end{cases}$ Parto de p(k):  $\begin{cases}
a^k \equiv (-1)^k \cdot b^k \ (a+b) \\
\frac{\text{multiplico}}{\text{por } a} \Rightarrow a \cdot a^k \equiv (-1)^k \cdot \underbrace{a} \cdot b^k \ (a+b) \\
\frac{\text{y acomodo}}{\text{por } a} \Rightarrow a^{k+1} \equiv (-1)^{k+1} \cdot b^{k+1} \ (a+b)
\end{cases}$ 

Como p(1), p(k), p(k+1) son verdaderas por principio de inducción lo es también p(n)  $\forall n \in \mathbb{N}$ 

- iii) hecho en el anterior.
- **4.** Sea  $a \in \mathbb{Z}$  impar. Probar que  $2^{n+2} | a^{2^n} 1$  para todo  $n \in \mathbb{N}$

Pruebo por inducción:  $p(n): 2^{n+2} \mid a^{2^n} - 1$   $\begin{cases}
Caso base: p(1): 2^3 \mid a^2 - 1 = (a-1) \cdot (a+1) \xrightarrow{a \text{ es impar} \atop a = 2m-1} (2m-2) \cdot (2m) = \\
4 \cdot \underbrace{m \cdot (m-1)}_{par} = 4 \cdot (2 \cdot h) = 8 * h \xrightarrow{\text{por lo} \atop \text{tanto}} 8 \mid 8 \cdot h \text{ con } h \text{ entero.} \quad \checkmark \\
Paso inductivo: p(k) V \Rightarrow p(k+1) V? \xrightarrow{\text{es} \atop \text{decir}} 2^{k+2} \mid a^{2^k} - 1 \Rightarrow 2^{k+3} \mid a^{2^{k+1}} - 1 \quad V? \\
\text{Hipótesis inductiva:} \\
\begin{cases}
2^{k+3} \mid a^{2^{k+1}} - 1 \xrightarrow{\text{acomodar} \atop \text{diferencia cuadrados}} 2 \cdot 2^k \mid (a^{2^k})^2 - 1 = \\
\underbrace{(a^{2^k} - 1) \cdot (a^{2^k} + 1)}_{\text{par}} \xrightarrow{\text{par}} \\
\underbrace{\begin{pmatrix} a \mid b & \Leftrightarrow & a \cdot k_1 = b \\ a \mid c \mid b \cdot d & \Leftrightarrow & a \cdot k_2 = d \\ a \cdot c \mid b \cdot d & \Leftrightarrow & a \cdot c \mid b \cdot d \end{pmatrix}}_{k_1 \cdot k_2} \xrightarrow{\text{Si } a \mid b \text{ y } c \mid d} \underbrace{2^{k+2} \cdot 2}_{a \mid c \mid b \cdot d} \mid \underbrace{(a^{2^k} - 1) \cdot (a^{2^k} + 1)}_{d} \Rightarrow 2^{k+3} \mid a^{2^{k+1}} - 1 \quad V \quad \checkmark \end{cases}}_{s \mid a \mid b \mid b \mid c \mid b \mid d}$ 

Como  $p(1) \land p(k) \land p(k+1)$  resultaron verdaderas, por el principio de inducción p(n) es verdadera  $\forall n \in \mathbb{N}$ 

# 5. \*\* Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

### 6. \*\* Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en LATEX $\rightarrow \bigcirc$ .

7.

i) 
$$99 \mid 10^{2n} + 197$$

ii) 
$$9 \mid 7 \cdot 5^{2n} + 2^{4n+1}$$

iii) 
$$56 \mid 13^{2n} + 28n^2 - 84n - 1$$

iv) 
$$256 \mid 7^{2n} + 208n - 1$$

i) 
$$99 \mid 10^{2n} + 197 \stackrel{\text{def}}{\Longleftrightarrow} 10^{2n} + 197 \equiv 0 \ (99) \rightarrow 10^{2n} + 198 \equiv 1 \ (99) \rightarrow 10^{2n} + \underbrace{198}_{\stackrel{(99)}{\equiv} 0} \equiv 1 \ (99) \rightarrow 100^n \equiv 1 \ (99) \rightarrow 100 \equiv 1 \ (99) \iff 100^2 \equiv \underbrace{100}_{\stackrel{(99)}{\equiv} 1} \ (99) \rightarrow 100^2 \equiv 1 \ (99) \iff \dots \iff 100^n \equiv 1 \ (99)$$

$$\begin{array}{c} \stackrel{\text{sé}}{\rightleftharpoons} 100 \equiv 1 \ (99) \iff 100^2 \equiv \underbrace{100}_{\stackrel{(99)}{\equiv} 1} \ (99) \rightarrow 100^2 \equiv 1 \ (99) \iff \dots \iff 100^n \equiv 1 \ (99) \\ \hline Tengoquedemostrareserenglnporinduccinocon" propiedad de congruencia" funciona? \\ \text{Se concluye que } 99 \mid 10^{2n} + 197 \iff 99 \mid \underbrace{100 - 1}_{99} \ (99) \rightarrow 100^{2n} = 1 \ (99) \Rightarrow \dots \iff 100^n \equiv 1 \ (99) \Rightarrow \dots \implies 10$$

ii) 
$$9 \mid 7 \cdot 5^{2n} + 2^{4n+1} \iff 7 \cdot 5^{2n} + 2^{4n+1} \equiv 0 \ (9) \xrightarrow{\text{sumo } 2 \cdot 5^{2n} \atop \text{M.A.M}} \underbrace{9 \cdot 5^{2n}}_{\text{M.A.M}} + 2 \cdot 2^{4n} \equiv 2 \cdot 5^{2n} \ (9)$$

$$\xrightarrow{\text{simplifico} \atop \text{y acomodo}} 2^{4n} \equiv 5^{2n} \ (9) \rightarrow 16^n \equiv 25^n \ (9) \xrightarrow{\text{congruencia}} 25^n \equiv 16^n \ (9) \xrightarrow{25 \stackrel{\text{(9)}}{\equiv} 16} 25 \equiv 16 \ (9) = 9 \equiv 0 \ (9)$$
Se concluye que  $9 \mid 7 \cdot 5^{2n} + 2^{4n+1} \iff 9 \mid 9 \leftarrow \text{¿Se concluye esto...?}$ 

### iii) **\*** Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX$ 

# iv) \* Falta hacerlo!

Si querés mandarlo: Telegram  $\to \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc$ .

#### Algoritmo de División:

- Calcular el cociente y el resto de la división de a por b en los casos:
  - i) a = 133, b = -14.

iv)  $a = b^2 - 6$ ,  $b \neq 0$ 

ii) a = 13, b = 111.

v)  $a = n^2 + 5$ ,  $b = n + 2 \ (n \in \mathbb{N})$ . vi) a = n + 3,  $= n^2 + 1 \ (n \in \mathbb{N})$ .

iii)  $a = 3b + 7, b \neq 0.$ 

- i)  $133: (-14) \Rightarrow 133 = (-9) \cdot (-14) + 7$
- ii)

iii) 
$$a = 3b + 7 \rightarrow \text{me interesa:} \rightarrow \left\{ \begin{array}{l} |b| \le |a| \checkmark \\ 0 \le r < |b| \checkmark \end{array} \right\} \rightarrow$$

$$\rightarrow \begin{cases} \text{Si: } |b| > 7 \to (q, r) = (3, 7) \\ \text{Si: } |b| \le 7 \to (q, r) = (3, 7) \\ \hline (a, b) \mid (-14, -7) \mid (-11, -6) \mid (-8, -5) \mid (-5, -4) \mid (4, -1) \mid \dots \\ \hline (q, r) \mid (2, 0) \mid (2, 1) \mid (2, 2) \mid (2, 3) \mid (4, 0) \mid \dots \end{cases}$$

- iv)  $a = b^2 6$ ,  $b \neq 0$ .
- Sabiendo que el resto de la división de un entero a por 18 es 5, calcular el resto de:
  - i) la división de  $a^2 3a + 11$  por 18.
  - ii) la división de a por 3.
  - iii) la división de 4a + 1 por 9.
  - iv) la división de  $7a^2 + 12$  por 28.
  - i)  $r_{18}(a) = r_{18} \underbrace{(r_{18}(a)^2)}_{52} \underbrace{r_{18}(3)}_{3} \cdot \underbrace{r_{18}(a)}_{5} + \underbrace{r_{18}(11)}_{11} = r_{18}(21) = 3$
  - ii)  $\left\{ \begin{array}{l} a = 3 \cdot q + r_3(a) \\ 6 \cdot a = 18 \cdot q + \underbrace{6 \cdot r_3(a)}_{r_{18}(6a)} \end{array} \right\} \rightarrow r_{18}(6a) = r_{18}(r_{18}(6) \cdot r_{18}(a)) = r_{18}(30) = 12$
  - iii)  $r_9(4a+1) = \underbrace{r_9(4 \cdot r_9(a)+1)}_{*1} \rightarrow a = 18 \cdot q + 5 = 9 \cdot \underbrace{(9 \cdot q)}_{s'} + \underbrace{5}_{r_9(a)} \xrightarrow{*_1} r_9(a) = r_9(21) = 3$
- 🌎 ¡Aportá! Correcciones, subiendo ejercicios, 🗡 al repo, críticas, todo sirve.

iv) 
$$r_{28}(7a^2 + 12) = r_{28}(7 \cdot r_{28}(a)^2 + 12) \xrightarrow{\text{iqué es}} r_{28}(a)$$

$$\begin{cases}
a = 18 \cdot q + 5 \xrightarrow{\text{busco algo}} \\
14 \cdot a = \underbrace{252 \cdot q}_{28 \cdot 9 \cdot q} + 70 \xrightarrow{\text{corrijo según}} 28 \cdot 9 \cdot q + \underbrace{2 \cdot 28 + 14}_{70} = 28 \cdot (9 \cdot q + 2) + 14 \quad \checkmark \\
\xrightarrow{\text{por lo}} 14a = 28 \cdot q' + 14 \Rightarrow 14 \cdot a \equiv 14 \ (28) \iff a \equiv 1 \ (28)
\end{cases}$$
Ahora que sé que  $r_{28}(a) = 1$  sale que  $r_{28}(7a^2 + 12) = r_{28}(7 \cdot r_{28}(a)^2 + 12) = r_{28}(19) = 19 \quad \checkmark$ 

10.

- i) Si  $a \equiv 22$  (14), hallar el resto de dividir a a por 14, por 2 y por 7.
- ii) Si  $a \equiv 13$  (5), hallar el resto de dividir a  $33a^3 + 3a^2 197a + 2$  por 5.
- iii) Hallar, para cada  $n\in\mathbb{N},$ el resto de la división de  $\sum\limits_{i=1}^n (-1)^i\cdot i!$  por 12

$$\begin{cases} a \equiv 22 \ (14) \rightarrow a = 14 \cdot q + \underbrace{22}_{14+8} = 14 \cdot (q+1) + 8 \xrightarrow{\text{el resto}} r_{14}(a) = 8 \quad \checkmark \\ a \equiv 22 \ (14) \rightarrow a = \underbrace{14 \cdot q}_{2 \cdot (7 \cdot q)} + \underbrace{22}_{2 \cdot 11} = 2 \cdot (7q+11) + 0 \xrightarrow{\text{el resto}} r_{2}(a) = 0 \quad \checkmark \\ a \equiv 22 \ (14) \rightarrow a = \underbrace{14 \cdot q}_{7 \cdot (2 \cdot q)} + \underbrace{22}_{1+7 \cdot 3} = 7 \cdot (2q+3) + 1 \xrightarrow{\text{el resto}} r_{7}(a) = 1 \quad \checkmark \end{cases}$$

- ii) Dos números congruentes tienen el mismo resto.  $a \equiv 13 \ (5) \iff a \equiv 3 \ (5) \ r_5(33a^3 + 3a^2 197a + 2) = r_5(3 \cdot r_5(a)^3 + 3 \cdot r_5(a)^2 2 \cdot r_5(a) + 2) = \frac{\text{como } a \equiv 13 \ (5)}{r_5(a) = 3} r_5(33a^3 + 3a^2 197a + 2) = 4$
- iii) \* Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

11.

- i) Probar que  $a^2 \equiv -1$  (5)  $\iff a \equiv 2$  (5)  $\forall a \equiv 3$  (5)
- ii) Probar que no existe ningún entero a tal que  $a^3 \equiv -3$  (7)
- iii) Probar que  $a^7 \equiv a$  (7)  $\forall a \in \mathbb{Z}$
- iv) Probar que  $7 \mid a^2 + b^2 \iff 7 \mid a \land 7 \mid b$ .
- v) Probar que  $5 \mid a^2 + b^2 + 1 \iff 5 \mid a \vee 5 \mid b$ . ¿Vale la recíproca?
- i) Me piden que pruebe una congruencia es válida solo para ciertos  $a \in \mathbb{Z}$ . Pensado en términos de restos quiero que el resto al poner los a en cuestión cumplan la congruencia.

$$\begin{cases}
a^{2} \equiv -1 & (5) \iff a^{2} \equiv 4 & (5) \iff a^{2} - 4 \equiv 0 & (5) \iff (a-2) \cdot (a+2) \equiv 0 & (5) \\
\frac{\text{quiero que el}}{\text{resto sea } 0} r_{5}(a^{2}+1) = r_{5}(a^{2}-4) = r_{5}(r_{5}(a-2) \cdot r_{5}(a+2)) = \underbrace{r_{5}((r_{5}(a)-2) \cdot (r_{5}(a)+2))}_{\bigstar^{1}} = 0
\end{cases}$$

$$\xrightarrow{\text{el resto ser\'{a}}} r_{5}(a^{2}+1) = 0$$

$$\Rightarrow r_{5}((r_{5}(a)-2) \cdot (r_{5}(a)+2)) = 0$$

$$\begin{cases}
r_{5}(a) = 2 \Leftrightarrow a \equiv 2 & (5) \\
r_{5}(a) = -2 \Leftrightarrow a \equiv 3 \\
\end{cases} (5)$$

$$\Rightarrow r_{5}(a) = -2 \Leftrightarrow a \equiv 3 \\
\end{cases} (5)$$

Más aún:

Para una congruencia módulo 5 habrá solo 5 posibles restos, por lo tanto se pueden ver todos los casos haciendo una table de restos.

a	0	1	2	3	4	
$r_5(a)$	0	1	2	3	4	$\rightarrow$ La tabla muestra que para un dado $a$
$r_5(a^2)$						
$\rightarrow r_5(a)$	=	$\left\{\begin{array}{c} 2\\ 3\\ 3\end{array}\right.$	2 ¢	$\Rightarrow$	$a \\ a$	$\equiv 2 (5) \iff a^2 \equiv 4 (5) \iff a^2 \equiv -1 (5)$ $\equiv 3 (5) \iff a^2 \equiv 4 (5) \iff a^2 \equiv -1 (5)$

### ii) 😭 Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

iii) Me piden que exista una dada congruencia para todo  $a \in \mathbb{Z}$ . Eso equivale a probar a que al dividir el lado izquierdo entre el divisor, el resto sea lo que está en el lado derecho de la congruencia.

$$a^7 - a \equiv 0 \ (7) \iff a \cdot (a^6 - 1) \equiv 0 \ (7) \iff a \cdot (a^3 - 1) \cdot (a^3 + 1) \equiv 0 \ (7) \xrightarrow{\text{tabla de restos con} \atop \text{sus propiedades lineales}}$$

a	0	1	2	3	4	5	6	
$r_7(a)$	0	1	2	3	4	5	6	$\rightarrow$ Cómo para todos los $a$ , alguno de los factores del resto siempre
$r_7(a^3-1)$	6	0	0	5	0	5	5	7 Como para todos los a, alguno de los factores del resto siempre
$r_7(a^3+1)$	1	2	2	0	2	0	0	

se anula, es decir:

$$r_7(a^7 - a) = r_7(r_7(a) \cdot r_7(a^3 - 1) \cdot r_7(a^3 + 1)) = 0 \ \forall a \in \mathbb{Z}$$

iv)

 $\mathbf{v})$ 

### 12. 🛣 Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

**13.** Se define por recurrencia la sucesión  $(a_n)_{n\in\mathbb{N}}$ :

$$a_1 = 3, \ a_2 = -5 \ \mathrm{y} \ a_{n+2} = a_{n+1} - 6^{2n} \cdot a_n + 21^n \cdot n^{21}, \ \mathrm{para \ todo} \ n \in \mathbb{N} \, .$$

Probar que  $a_n \equiv 3^n \pmod{7}$  para todo  $n \in \mathbb{N}$ .

La infumabilidad de esos números me obliga a atacar a esto con el resto e inducción.

$$\xrightarrow{\text{acomodo} \atop \text{enunciado feo}} r_7(a_{n+2}) = r_7(r_7(a_{n+1}) - \underbrace{r_7(36)^n}_{\stackrel{(7)}{=}1} \cdot r_7(a_n) + \underbrace{r_7(21)^n}_{\stackrel{(7)}{=}0} \cdot r_7(n)^{21}) = \underbrace{r_7(a_{n+2}) = r_7(a_{n+1}) - r_7(a_n)}_{\stackrel{(7)}{=}1} \quad \checkmark$$

Puesto de otra forma 
$$a_{n+2} \equiv a_{n+1} - a_n$$
 (7)  $\rightarrow$  
$$\begin{cases} a_1 \equiv 3^1 \ (7) \iff a_1 \equiv 3 \ (7) \\ a_2 \equiv 3^2 \ (7) \iff a_2 \equiv 2 \ (7) \\ a_3 \equiv 3^3 \ (7) \iff a_3 \equiv 6 \ (7) \end{cases}$$

Quiero probar que  $a_n \equiv 3^n \pmod{7} \rightarrow \text{inducción completa}$ :

$$\begin{cases} \text{Casos base:} & \begin{cases} p(n=1) : a_1 \equiv 3^1 \text{ (7)Verdadera} \\ p(n=2) : a_2 \equiv 3^2 \text{ (7)} \stackrel{\text{(7)}}{\equiv} 2 \stackrel{\text{(7)}}{\equiv} -5 \text{Verdadera} \\ p(k) : a_k \equiv 3^k \text{ (mod 7) Verdadera} \end{cases} \\ \begin{cases} p(k+1) : a_{k+1} \equiv 3^{k+1} \text{ (mod 7) Verdadera} \\ \Rightarrow p(k+1) : a_{k+2} \equiv 3^{k+2} \text{ (mod 7) Verdadera} \end{cases} \\ \begin{cases} a_k \equiv 3^k \text{ (mod 7)} \\ a_{k+1} \equiv 3^{k+1} \text{ (mod 7)} \\ \hline a$$

Concluyendo como  $p(1), p(2), p(k), p(k+1) \wedge p(k+2)$  resultaron verdaderas por el principio de inducción p(n) es verdadera  $\forall n \in \mathbb{N}$ .

#### 14.

- i) Hallar el desarrollo en base 2 de
  - (a) 1365
  - (b) 2800
  - (c)  $3 \cdot 2^{12}$
  - (d)  $13 \cdot 2^n + 5 \cdot 2^{n-1}$

#### Hacer!

### 15. \*\* Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc 3$ .

### 16. \*\* Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc 3$ .

### 17. \*\* Falta hacerlo!

Si querés mandarlo: Telegram  $\to \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc$ .  $Máximo\ común\ divisor:$ 

- 18. En cada uno de los siguientes casos calcular el máximo común divisor entre a y b y escribirlo como combinación lineal entera de a y b:
  - i) a = 2532, b = 63.
- 🖸 ¿Errores? Mandanos tu solución, prolija, así lo arreglamos.

- ii) a = 131, b = 23.
- iii)  $a = n^4 3$ ,  $b = n^2 + 2$   $(n \in \mathbb{N})$ .

### Hacer!

### 19. \*\* Falta hacerlo!

Si querés mandarlo: Telegram  $\to \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc 3$ .

- Sea  $a \in \mathbb{Z}$ . 20.
  - a) Probar que (5a + 8 : 7a + 3) = 1 o 41. Exhibir un valor de a para el cual da 1, y verificar que efectivamente para a = 23 da 41.
  - b) Probar que  $(2a^2 + 3a : 5a + 6) = 1$  o 43. Exhibir un valor de a para el cual da 1, y verificar que efectivamente para a = 16 da 43
  - c) Probar que  $(a^2 3a + 2 : 3a^3 5a^2) = 2$  o 4, y exhibir un valor de a para cada caso. (Para este item es **indispensable** mostrar que el máximo común divisor nunca puede ser 1).

### i) **\*** Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

# ii) **\*** Falta hacerlo!

Si querés mandarlo: Telegram o extstyle extstyle o, o mejor aún si querés subirlo en LATFextstyle o

iii) 
$$(a^2 - 3a + 2 : 3a^3 - 5a^2) \xrightarrow{\text{Euclides}} (\underbrace{a^2 - 3a + 2}_{par} : \underbrace{6a - 8}_{par})$$

iii) 
$$(a^2 - 3a + 2 : 3a^3 - 5a^2) \xrightarrow{\text{Euclides}} (\underbrace{a^2 - 3a + 2}_{par} : \underbrace{6a - 8}_{par})$$

$$\xrightarrow{\text{busco}} \left\{ \begin{array}{c} d \mid a^2 - 3a + 2 \\ d \mid 6a - 8 \end{array} \right\} \xrightarrow{\times 6} \left\{ \begin{array}{c} d \mid 10a - 12 \\ d \mid 6a - 8 \end{array} \right\} \xrightarrow{\times 6} \left\{ \begin{array}{c} d \mid 10a - 12 \\ d \mid 6a - 8 \end{array} \right\} \xrightarrow{\times 6} \left\{ \begin{array}{c} d \mid 10a - 12 \\ d \mid 6a - 8 \end{array} \right\} \xrightarrow{\times 6} \left\{ \begin{array}{c} d \mid 8 \end{array} \right\} \rightarrow \mathcal{D}_{+}(8) = \{1, 2, 4, 8\} \stackrel{\bigstar}{\bigstar}^{1} = \{2, 4, 8\}$$

$$\begin{cases} a = 1 \quad (0 : -2) = 2 \\ a = 2 \quad (0 : 4) = 4 \end{cases}$$
Paracido al backs on alace

Parecido al hecho en clase.

¿Qué onda el 8? Hice mal cuentas? Si no, cómo lo descarto?

Sean  $a, b \in \mathbb{Z}$  coprimes. Probar que 7a - 3b y 2a - b son coprimes.

$$\left\{ \begin{array}{l} d \mid 7a - 3b \stackrel{\cdot 2}{\longrightarrow} d \mid b \longrightarrow d \mid b \\ d \mid 2a - b \stackrel{\cdot 7}{\longrightarrow} d \mid 2a - b \longrightarrow d \mid a \end{array} \right\} \xrightarrow{\text{propiedad}} d \mid (a:b) \xrightarrow{(a:b)} d \mid 1$$
 Por lo tanto  $(7a - 3b:2a - b) = 1$  son coprimos como se quería mostrar.

### Falta hacerlo!

Si querés mandarlo: Telegram  $\to \odot$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc$ .

23.

- i) Determinar todos los  $a, b \in \mathbb{Z}$  coprimos tales que  $\frac{b+4}{a} + \frac{5}{b} \in \mathbb{Z}$ .
- ii) Determinar todos los  $a, b \in \mathbb{Z}$  coprimos tales que  $\frac{9a}{b} + \frac{7a^2}{b^2} \in \mathbb{Z}$ .
- iii) Determinar todos los  $a, b \in \mathbb{Z}$  tales que  $\frac{2a+3}{a+1} + \frac{a+2}{4} \in \mathbb{Z}$ .
- i)  $\frac{b+4}{a} + \frac{5}{b} = \frac{b^2 + 4b + 5a}{ab} \xrightarrow{\text{quiero que}} ab \mid b^2 + 4b + 5a$   $\xrightarrow{\text{coprimitusibilidad}} \begin{cases} a \mid b^2 + 4b + 5a \\ b \mid b^2 + 4b + 5a \end{cases} \rightarrow \begin{cases} a \mid b^2 + 4b \\ b \mid 5a \end{cases} \xrightarrow{\text{debe dividr a 5}} \begin{cases} a \mid b \cdot (b+4) \\ b \mid 5 \end{cases}$ Seguro tengo que  $b \in \{\pm 1, \pm 5\} \rightarrow \text{pruebo valores de } b \text{ y veo que valor de } a \text{ queda:}$   $\begin{cases} b = 1 \rightarrow (a \mid 5, 1) \rightarrow \{(\pm 1, 1).(\pm 5, 1)\} \\ b = -1 \rightarrow (a \mid -3, 1) \rightarrow \{(\pm 1, -1).(\pm 3, 1)\} \end{cases}$   $b = 5 \rightarrow (a \mid 45, 5) \xrightarrow{\text{atención que}} \{(\pm 1, 5), (\pm 3, 5).(\pm 9, 5)\}$   $b = -5 \rightarrow (a \mid 5, -5) \xrightarrow{\text{atención que}} \{(\pm 1, -5)\}$
- ii) Hacer!
- iii) **\*** Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX$ 

Primos y factorización:

24.

- **25.** Sea p primo positivo.
  - i) Probar que si  $0 < k < p \mid \binom{p}{k}$ .
  - ii) Probar que si  $a, b \in \mathbb{Z}$ , entonces  $(a+b)^p \equiv a^p + b^p$  (p).

### **26.** Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc 3$ .

### 27. 🚼 Falta hacerlo!

Si querés mandarlo: Telegram  $\to \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc$ .

### 28. 🚼 Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en LATEX  $\rightarrow \bigcirc$ .

### 29. 🚼 Falta hacerlo!

Si querés mandarlo: Telegram  $\to \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc$ .

# 30. 🚼 Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

② ¿Errores? Mandanos tu solución, prolija, así lo arreglamos.

31. \*\* Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

32. \*\* Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc 3$ .

33. 😭 Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

34. \*\* Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

35. \*\* Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

**36.** Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

37. **\frac{1}{2}** Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc 3$ .

38. 🏖 Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc 3$ .

39. 😭 Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc 3$ .

40. Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc 3$ .



### Ejercicios extras:

4400 ¿Cuántos divisores distintos tiene? ¿Cuánto vale la suma de sus divisores.

$$4400 \xrightarrow{\text{factorizo}} 4400 = 2^4 \cdot 5^2 \cdot 11 \xrightarrow{\text{los divisores } m \mid 4400} m = \pm 2^{\alpha} \cdot 2^{\beta} \cdot 2^{\gamma}, \text{ con } \left\{ \begin{array}{l} 0 \leq \alpha \leq 4 \\ 0 \leq \beta \leq 2 \\ 0 \leq \gamma \leq 1 \end{array} \right\}$$

Hay entonces un total de  $5 \cdot 3 \cdot 2 = 30$  divisores positivos y 60 enteros.

Ahora busco la suma de esos divisores: 
$$\sum_{i=0}^{4} \sum_{j=0}^{2} \sum_{k=0}^{1} 2^{i} \cdot 5^{j} \cdot 11^{k} = \left(\sum_{i=0}^{4} 2^{i}\right) \cdot \left(\sum_{j=0}^{2} 5^{j}\right) \cdot \left(\sum_{k=0}^{1} 11^{k}\right)$$

$$\frac{\text{sumas}}{\text{geométricas}} \underbrace{\frac{2^{4+1}-1}{2-1}}_{31} \cdot \underbrace{\frac{5^{2+1}-1}{5-1}}_{31} \cdot \underbrace{\frac{11^{1+1}-1}{11-1}}_{12} = 11532.$$

- Hallar el menor  $n \in \mathbb{N}$  tal que:
  - i) (n:2528)=316
  - ii) n tiene exáctamente 48 divisores positivos
  - iii) 27 ∦ n

$$\begin{cases} \frac{\text{factorizo}}{2528} 2528 = 2^5 \cdot 79 & \checkmark \\ \frac{\text{factorizo}}{316} 316 = 2^2 \cdot 79 & \checkmark \\ \frac{\text{reescribo}}{\text{condición}} & (n:2^5 \cdot 79) = 2^2 \cdot 79 \\ \frac{\text{quiero}}{\text{encontrar}} & n = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdot 5^{\alpha_5} \cdot 7^{\alpha_7} \cdots 79^{\alpha_7 9} \cdots \end{cases}$$

encontrar

encontrar

$$n = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 4 \cdot 4 \cdot 19^{3} \cdot \dots \cdot 19^{3$$

sería  $n = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 79$ 

Sabiendo que (a:b) = 5. Probar que  $(3ab:a^2+b^2) = 25$ 

Coprimizar: 
$$\begin{cases} c = \frac{a}{5} \\ d = \frac{b}{5} \end{cases} \rightarrow (a:b) = 5 \cdot \underbrace{(c:d)}_{1} = 5$$
$$\rightarrow \begin{cases} \frac{\text{según}}{\text{enunciado}} \ 25 = (3ab:a^2 + b^2) \xrightarrow{\text{reemplazo}} 25 = 25 \cdot \underbrace{(3cd:c^2 + d^2)}_{1} \end{cases}$$

② ¿Errores? Mandanos tu solución, prolija, así lo arreglamos.

$$\xrightarrow{\text{Ovy a probar}} (3cd : c^2 + d) = 1.$$

### **△**4.

- i) Calcular los posibles valores de:  $(7^{n-1} + 5^{n+2} : 5 \cdot 7^n 5^{n+1})$ .
- ii) Encontrar n tales que el mcd para ese n tome 3 valores distintos.

Busco independencia de 
$$n$$
 en algún lado del  $(a:b)$ . Si  $d = (7^{n-1} + 5^{n+2} : 5 \cdot 7^n - 5^{n+1}) \rightarrow \begin{cases} d \mid 7^{n-1} + 5^{n+2} \\ d \mid 5 \cdot 7^n - 5^{n+1} \end{cases} \rightarrow \begin{cases} d \mid 7^{n-1} + 5^{n+2} \\ \frac{(5)}{2} : 2^n \end{cases} \xrightarrow{p \nmid d \land d \mid p \cdot k} \begin{cases} d \mid 7^{n-1} + 5^{n+2} \\ d \mid 7^n - 5^n \end{cases} \xrightarrow{p \nmid d \land d \mid p \cdot k} \begin{cases} d \mid 176 \\ d \mid 7^n - 5^n \end{cases} \rightarrow d = (176 : 7^n - 5^n) \checkmark$ 
Factorizo:  $176 = 2^4 \cdot 11 \rightarrow \mathcal{D}_+(176) = \{1, 2, 4, 8, 11, 16, 22, 44, 88, 176\}.$ 
Descarto  $\rightarrow \begin{cases} 1 \rightarrow 7^n - 5^n \equiv 2^n (5) \rightarrow d \text{ tiene que ser par } y \ge 1 \\ 11 \rightarrow 7^n - 5^n \equiv 2^n (5) \rightarrow d \text{ tiene que ser par } y \ge 1 \end{cases}$ 
Estudio congruencia de los pares e impares: 
$$\begin{cases} 7^{2k} - 5^{2k} \equiv 1^k - 25^k (8) \rightarrow 1 - \underbrace{1}_{\stackrel{(8)}{=}25} \equiv 0 (8) \end{cases}$$
Puedo descartar a los múltiplos de 4 que no sean múltiplos de 8.  $\rightarrow \mathcal{D}_+(d) = \{2, 8, 16, 22, 88, 16, 22, 16, 22, 88, 16, 22, 16, 22, 16, 22, 88, 16, 22, 16$ 

$$\rightarrow \left\{ \begin{array}{l} d \mid 176 \cdot 5^n \\ d \mid 7^n - 5^n \end{array} \xrightarrow{p \not\mid d \wedge d \mid p \cdot k} \left\{ \begin{array}{l} d \mid 176 \\ d \mid 7^n - 5^n \end{array} \right. \rightarrow d = (176 : 7^n - 5^n) \quad \checkmark \right.$$

$$\begin{cases} 7^{2k} - 5^{2k} \equiv 1^k - 25^k \ (8) \to 1 - \underbrace{1}_{\stackrel{(8)}{\equiv} 25} \equiv 0 \ (8) \end{cases}$$

$$7^{2k+1} - 5^{2k+1} \equiv 3 - 1 \ (4) \stackrel{(4)}{\equiv} 2$$

Puedo descartar a los múltiplos de 4 que no sean múltiplos de 8.  $\rightarrow \mathcal{D}_{+}(d) = \{2, 8, 16, 22, 88, 176\}$ No lo terminé, no entiendo bien este paso y como descartar algún otro.

Estudiar los valores parar todos los  $a \in \mathbb{Z}$  de  $(a^3 + 1 : a^2 - a + 1)$ .

Primero hay que notar que el lado  $a^2 - a + 1$  es siempre impar ya que:

$$\left\{ \begin{array}{l} (2k-1)^2 - (2k-1) + 1 \stackrel{(2)}{\equiv} (-1)^2 - 1 + 1 \stackrel{(2)}{\equiv} 1 \\ (2k)^2 - (2k) + 1 \stackrel{(2)}{\equiv} (0)^2 - 0 + 1 \stackrel{(2)}{\equiv} 1. \\ \text{expresiones y si } 2 \not\mid A \Rightarrow 2 \cdot k \not\mid A \text{ tampoco.} \end{array} \right\} \text{ Por lo tanto 2 no puede ser un divisor de ambas}$$

Se ve fácil contrarecíproco:  $2k \choose par | A \Rightarrow 2 | A$ . Porque existe un k tal que  $2 \cdot c \cdot k = A \Rightarrow 2 \cdot (c \cdot k) = A$ . Ahora cuentas para simplificar la expresión y encontrar número del lado derecho.

$$\begin{cases} d \mid a^3 + 1 \\ d \mid a^2 - a + 1 \end{cases} \rightarrow d \mid 30 \rightarrow \mathcal{D}_+(d) = \{1, 2, 3, 5, 6, 10, 15, 30\} \xrightarrow{\text{por lo de antes}} \mathcal{D}_+(d) = \{1, 3, 5, 15\}$$

$$\xrightarrow{\text{hacer tabla de restos}} \left\{ \begin{array}{l} r_3(a^3+1) = 0 \quad \text{si} \quad a \equiv 2 \ (3) \\ \wedge \\ r_3(a^2-a+1) = 0 \quad \text{si} \quad a \equiv 2 \ (3) \end{array} \right\} \rightarrow \left\{ \begin{array}{l} r_5(a^3+1) \neq 0 \quad \forall a \in \mathbb{Z} \end{array} \right\}.$$
 Luego si 5 //  $(a^3+1:a^2-a+1) \Rightarrow \underbrace{15}_{5\cdot 3}$  //  $(a^3+1:a^2-a+1) \xrightarrow{\text{se achica el} \\ \text{conjunto de divisores}} \mathcal{D}_+(d) = \{1,3\}$  
$$d = \left\{ \begin{array}{l} 3 \quad \text{si} \quad a \equiv 2 \ (3) \\ 1 \quad \text{si} \quad a \equiv 1 \lor 2 \ (3) \end{array} \right.$$

**♦6.** Sean  $a, b \in \mathbb{Z}$  tal que (a : b) = 6. Hallar todos los d = (2a + b : 3a - 2b) y dar un ejemplo en cada caso.

Conviene coprimizar: 
$$(a:b) = 6 \iff \begin{cases} a = 6A \\ b = 6B \end{cases}$$
 con  $(A:B)^{\bigstar 1} = 1$ 

$$d = (2 \cdot 6A + 6B : 3 \cdot 6A - 2 \cdot 6B) = (6 \cdot (2 \cdot A + B) : 6 \cdot (3 \cdot A - 2 \cdot B)) = 6 \cdot \underbrace{(2A + B : 3A - 2B)}_{D}$$

$$\rightarrow d^{\bigstar 2} = 6D \xrightarrow{\text{busco divisores}}_{\text{comunes}} \begin{cases} D \mid 2A + B \\ D \mid 3A - 2B \end{cases} \xrightarrow{\text{operaciones}}_{\dots} \begin{cases} D \mid 7B \\ D \mid 7A \end{cases} \Rightarrow D = (7A : 7B) = 7 \cdot (A : B)^{\bigstar 1} = 7$$
Por lo tanto  $D \in \mathcal{D}_{+}(7) = \{1, 7\}$ , pero yo quiero encontrar ejemplos de  $a$  y  $b$ :
$$\begin{cases} \text{Si: } A = 2 \rightarrow a = 12 \\ B = 3 \rightarrow b = 18 \\ (7 : 0) \Rightarrow D = 7 \rightarrow d = (42 : 0) = \underbrace{42}_{6 \cdot D} \end{cases}$$

$$\bigstar^{2} \rightarrow \begin{cases} \text{Si: } A = 0 \rightarrow a = 0 \\ B = 1 \rightarrow b = 6 \\ (1 : -2) \Rightarrow D = 1 \rightarrow d = (6 : -12) = \underbrace{6}_{6 \cdot D} \end{cases}$$

**♦**7. Sea  $a \in \mathbb{Z}$  tal que  $32a \equiv 17$  (9). Calcular  $(a^3 + 4a + 1 : a^2 + 2)$ 

$$32a \equiv 17 \ (9) \to 5a \equiv 8 \ (9) \xrightarrow{\text{multiplico}} a \equiv 7 \ (9) \quad \checkmark$$

$$d = (a^3 + 4a + 1 : a^2 + 2) \xrightarrow{\text{Euclides}} \left\{ \begin{array}{c} a^3 + 4a + 1 & | \ a^2 + 2 \\ -a^3 - 2a & | \ a \end{array} \right\} \to d = (a^2 + 2 : 2a + 1) \quad \checkmark$$

$$\xrightarrow{\text{buscar}} \left\{ \begin{array}{c} d \mid a^2 + 2 & | \ 2F_1 - aF_2 \rangle \\ d \mid 2a + 1 & | \ \end{array} \right\} \left\{ \begin{array}{c} d \mid -a + 4 \\ d \mid 2a + 1 & | \ \end{array} \right\} \left\{ \begin{array}{c} d \mid -a + 4 \\ d \mid 9 & | \ \end{array} \right\}$$

$$\to d = (-a + 4 : 9) \xrightarrow{\text{divisores}} \left\{ \begin{array}{c} 1, 3, 9 \right\} \quad \checkmark$$

Hago tabla de restos 9 y 3, para ver si las expresiones  $(a^2 + 2 : 2a + 1)$  son divisibles por mis potenciales MCDs.

$r_9(a)$	0	1	2	3	4	5	6	7	8	$\rightarrow a \equiv 4$ (9), valores de a candidatos para obtener MCD.	
$r_9(-a+4)$	4	3	2	1	0	-1	-2	-3	-4	$\rightarrow u \equiv 4$ (9), valores de <i>u</i> candidatos para obtener MCD.	
$r_3(a)$ 0 1 2 $\rightarrow a \equiv 1$ (3), valores de $a$ candidatos para obtener MCD.											
$r_3(-a+4)$	2	0	2	]	u =	= 1 (	), va	10168	ue a	Candidatos para obtener MCD.	

La condición  $a \equiv 7$  (9) no es compatible con el resultado de la tabla de  $r_9$ , pero sí con  $r_3$ . Notar que

$$a = 9k + 7 \stackrel{\text{(3)}}{\equiv} 1.$$

El MCD 
$$(a^3 + 4a + 1 : a^2 + 2) = \begin{cases} 3 & \text{si } a \equiv 7 \ (9) \\ 1 & \text{si } a \not\equiv 7 \ (9) \end{cases}$$

- **38.** Sea  $(a_n)_{n \in \mathbb{N}_0}$  con  $\begin{cases} a_0 = 1 \\ a_1 = 3 \\ a_n = a_{n-1} a_{n-2} & \forall n \ge 2 \end{cases}$ 
  - a) Probar que  $a_{n+6} = a_n$

- b) Calcular  $\sum_{k=0}^{255} a_k$
- (a) Por inducción:  $p(n): a_{n+6} = a_n \ \forall n \geq \mathbb{N}_0$  Verdadero?

Por inducción: 
$$p(n): a_{n+6} = a_n \ \forall n \geq \mathbb{N}_0 \ \text{Verdadero?}$$

$$\begin{cases}
Caso \ Base: \text{Primero notar que,} \\
a_0 = 1 \\
a_1 = 3 \\
a_2 \stackrel{\text{def}}{=} 2 \\
a_3 \stackrel{\text{def}}{=} -1 \\
a_4 \stackrel{\text{def}}{=} -3 \\
a_5 \stackrel{\text{def}}{=} -2
\end{cases} \rightarrow \begin{cases}
a_6 \stackrel{\text{def}}{=} 1 \\
a_7 \stackrel{\text{def}}{=} 3 \\
a_8 \stackrel{\text{def}}{=} 2 \\
a_9 \stackrel{\text{def}}{=} -1 \\
a_{10} \stackrel{\text{def}}{=} -3 \\
a_{11} \stackrel{\text{def}}{=} -2
\end{cases} \rightarrow \cdots \text{ Se ve que tiene un período de 6 elementos.}$$

p(n=2) Verdadero? ?  $\rightarrow a_8 \stackrel{?}{=} a_2$   $\checkmark$  Paso inductivo: Supongo p(k) Verdadero?  $\Rightarrow p(k+1)$  Verdadero? ?

Hipótesis inductiva: Supongo 
$$a_{k+6} = a_k \ \forall k \in \mathbb{N}_0$$
 Verdadero? , quiero ver que  $a_{k+7} = a_{k+1}$  
$$\underbrace{a_{k+7}}_{\text{def}} = a_{k+6} - a_{k+5} \stackrel{\text{HI}}{=} a_k - a_{k+5} \stackrel{\text{def}}{=} a_k - (\underbrace{a_k + a_{k+4}}_{a_{k+5}}) = -a_{k+4}$$

$$\rightarrow a_{k+7} = -a_{k+4} \stackrel{\text{def}}{=} -(a_{k+3} - a_{k+2}) \stackrel{\text{def}}{=} -(a_{k+2} - a_{k+1} - a_{k+2}) = a_{k+1} \quad \checkmark$$

Como  $p(0) \wedge p(1) \wedge \cdots p(5)$  son verdaderas y p(k) es verdadera así como p(k+1) también lo es, por el principio de inducción p(n) es verdadera  $\forall n \in \mathbb{N}_0$ 

(b) 
$$\sum_{k=0}^{255} a_k = \underbrace{a_0 + a_1 + a_2 + a_3 + a_4 + a_5}_{=0} + \underbrace{a_6 + a_7 + a_8 + a_9 + a_{10} + a_{11}}_{=0} + \cdots + a_{252} + a_{253} + a_{254} + a_{255}$$
  
En la sumatoria hay 256 términos. 
$$256 = 42 \cdot 6 + 4 \text{ por lo tanto van a haber 42 bloques que}$$

dan 0 y sobreviven los últimos 4 términos.  $\sum_{k=0}^{255} a_k = \underbrace{0 + 0 + \dots + 0}_{42 \text{ ceros}} + a_{252} + a_{253} + a_{254} + a_{255} =$ 

$$a_{252} + a_{253} + a_{254} + a_{255} = a_{253} + a_{254} = 5$$

Donde usé que: 
$$a_n = \begin{cases} 1 & \text{si} & n \mod 6 = 0 \\ 3 & \text{si} & n \mod 6 = 1 \\ 2 & \text{si} & n \mod 6 = 2 \\ -1 & \text{si} & n \mod 6 = 3 \\ -3 & \text{si} & n \mod 6 = 4 \\ -2 & \text{si} & n \mod 6 = 5 \end{cases} \longrightarrow \underbrace{\sum_{k=0}^{255} a_k = 5}_{k=0}$$

**9**. Determinar todos los  $a \in \mathbb{Z}$  que cumplen que

$$\frac{2a-1}{5} - \frac{a-1}{2a-3} \in \mathbb{Z}.$$

Busco una fracción. Para que esa fracción  $en \mathbb{Z}$  es necesario que el denominador divida al numerador. Fin.

$$\frac{2a-1}{5} - \frac{a-1}{2a-3} = \frac{4a^2 - 13a + 8}{10a - 15} \quad \checkmark$$

$$10a - 15 \mid -25 \iff 10a - 25 \in \{\pm 1, \pm 5, \pm 25\} \stackrel{\bigstar}{\bigstar}$$
 para algún  $a \in \mathbb{Z}$ .  $\checkmark$ 

De paso observo que |10a - 25| < 25. Busco a:

Caso: 
$$d = 10a - 15 = 1$$
  $\iff$   $a = \frac{8}{5}$    
Caso:  $d = 10a - 15 = -1$   $\iff$   $a = \frac{8}{5}$    
Caso:  $d = 10a - 15 = 5$   $\iff$   $a = 2$   $\checkmark$    
Caso:  $d = 10a - 15 = -5$   $\iff$   $a = 1$   $\checkmark$    
Caso:  $d = 10a - 15 = 25$   $\iff$   $a = 4$   $\checkmark$    
Caso:  $d = 10a - 15 = -25$   $\iff$   $a = -1$   $\checkmark$ 

Los valores de  $a \in \mathbb{Z}$  que cumplen  $\bigstar^2$  son  $\{-1, 1, 2, 4\}$ . Voy a evaluar y así encontrar para cual de ellos se cumple  $\bigstar^1$ , es decir que el númerador sea un múltiplo del denominador para el valor de a usado.

$$\begin{cases} d = 5 & a = 2 \\ d = -5 & a = 1 \end{cases} \Rightarrow 4 \cdot 2^2 - 13 \cdot 2 + 8 = -2 \qquad \rightarrow 5 \not \mid -2 \not \mid 2 \\ d = -5 & a = 1 \Rightarrow 4 \cdot 1^2 - 13 \cdot 1 + 8 = 1 \qquad \rightarrow -5 \not \mid 1 \not \mid 2 \\ d = 25 & a = 4 \Rightarrow 4 \cdot 4^2 - 13 \cdot 4 + 8 = 4 \qquad \rightarrow 25 \not \mid 4 \not \mid 2 \\ d = -25 & a = -1 \Rightarrow 4 \cdot (-1)^2 - 13 \cdot (-1) + 8 = 25 \rightarrow -25 \mid 25 \end{cases} \checkmark$$

El único valor de  $a \in \mathbb{Z}$  que cumple lo pedido es a = -1

Notas extras sobre el ejercicio:

Para a = -1 se obtiene  $\frac{2a-1}{5} - \frac{a-1}{2a-3} = -1$ . Más aún, si hubiese encarado el ejercicio con tablas de restos para ver si lo de arriba es divisible por los divisores en  $\star^3$ , calcularía:

$$r_5(4a^2 - 13a + 8)$$
 y  $r_{25}(4a^2 - 13a + 8)$ 

$$r_5(4a^2 - 13a + 8) = 0 \Leftrightarrow \begin{cases} a \equiv 3 \ (5) \\ a \equiv 4 \equiv -1 \ (5) \end{cases} \quad \text{y} \quad r_{25}(4a^2 - 13a + 8) = 0 \Leftrightarrow \begin{cases} a \equiv 23 \ (25) \\ a \equiv 24 \equiv -1 \ (25) \end{cases}$$

Se puede ver también así que el único valor de  $a \in \mathbb{Z}$ , que cumple  $\bigstar^{\perp}$  es a = -1