

# Apunte único: Álgebra I - Práctica 4

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

*Choose your destiny:*

*(doubleclick en los ejercicio para saltar)*

- Notas teóricas

- Ejercicios de la guía:

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

- Ejercicios de Parciales

 1.	 4.	 7.	 10.	 13.	 16.
 2.	 5.	 8.	 11.	 14.	 17.
 3.	 6.	 9.	 12.	 15.	

### Disclaimer:

Dirigido para aquél que esté listo para leerlo, o no tanto. Va con onda.

## ¡Recomendación para sacarle jugo al apunte!

Estudiar con resueltos puede ser un arma de doble filo. Si estás trabado, antes de saltar a la solución que hizo otra persona:

- 📖<sub>1</sub> Mirar la solución ni bien te trabás, te *condicionas pavlovianamente* a **no** pensar. Necesitás darle tiempo al cerebro para llegar a la solución.
- 📖<sub>2</sub> Intentá un ejercicio similar, pero **más fácil**.
- 📖<sub>3</sub> ¿No sale el fácil? Intentá uno **aún más fácil**.
- 📖<sub>4</sub> Fijate si tenés un ejercicio similar hecho en clase. Y mirá ese, así no quemás el ejercicio de la guía.
- 📖<sub>5</sub> Tomate 2 minutos para formular una pregunta que realmente sea lo que **no** entendés. Decir '*no me sale*'  $\neq$  +. Escribí esa pregunta, vas a dormir mejor.

Ahora sí mirá la solución.

*Si no te salen los ejercicios fáciles sin ayuda*, no te van a salir los ejercicios más difíciles: **Sentido común**.

¡Los más fáciles van a salir! Son el alimento de nuestra confianza.


Si mirás miles de soluciones a parciales en el afán de tener un ejemplo hecho de todas las variantes, estás apelando demasiado a la suerte de que te toque uno igual, *pero no estás aprendiendo nada*. Hacer un parcial bien lleva entre 3 y 4 horas. Así que si vos en 4 horas "hiciste" 3 o 4 parciales, *algo raro debe haber*. A los parciales se va a **pensar** y eso hay que practicarlo desde el primer día.

Mirá los videos de las teóricas **de Teresa que son buenísimos** 📺.

Videos de prácticas de pandemia, complemento extra: **Prácticas Pandemia** 📺.

Los ejercicios que se dan en clase suelen ser similares a los parciales, a veces más difíciles, repasalos siempre **Just Do IT** 🙌🙌🙌!

Eh, loco, fatalista, distópico, **relajá un toque te vas a quedar (más) pelado...** 🙌🙌🙌 *va a salir todo bien!*

El repo en [github](#)  para descargar las guías con los últimos updates.



<https://github.com/nad-garraz/algebraUno>

La Guía 4 se actualizó por última vez: 12/12/24 @ 22:06

#### Guía 4



<https://github.com/nad-garraz/algebraUno/blob/main/4-guia/4-sol.pdf>

Si querés mandar un ejercicio o avisar de algún error, lo más fácil es por

[Telegram](#) .



<https://t.me/+1znt2GV1i8cwMTNh>

**Notas teóricas:***Divisibilidad:*

- Definición divisibilidad y notación:

$$d \text{ divide a } a \xLeftrightarrow[\text{que decir}]{\text{es lo mismo}} a \text{ es un múltiplo entero de } d$$

$$d \mid a \iff \exists k \in \mathbb{Z} \text{ tal que } a = k \cdot d$$

- Conjunto de divisores de  $a$ :

$$\mathcal{D}(a) = \{-|a|, \dots, -1, 1, \dots, |a|\}.$$

- $d \mid 0$ , dado que  $0 = 0 \cdot d$ . Se desprende que  $\mathcal{D}(0) = \{\mathbb{Z} - \{0\}\}$
- A la hora de laburar con la divisibilidad “*los signos no importan*”:

$$\begin{cases} d \mid a \iff -d \mid a \text{ (pues } a = k \cdot d \iff a = (-k) \cdot (-d)) \\ d \mid a \iff d \mid -a \text{ (pues } a = k \cdot d \iff (-a) = (-k) \cdot d) \end{cases} \xRightarrow{\text{corta}} \boxed{d \mid a \iff |d| \mid |a|}$$

- Propiedades súper útiles para justificar los cálculos en los ejercicios:

$$\begin{cases} d \mid a \text{ y } d \mid b \Rightarrow d \mid a \pm b \\ d \mid a \Rightarrow d \mid c \cdot a, \forall c \in \mathbb{Z} \\ d \mid a \xLeftrightarrow{!!} d^n \mid a^n \forall n \in \mathbb{N} \end{cases}$$

**Error recurrente:**  $d \mid a \cdot b \not\Rightarrow \begin{cases} d \mid a \\ \text{o} \\ d \mid b \end{cases}$ . Por ejemplo  $6 \mid 3 \cdot 4$  pero  $\begin{cases} 6 \not\mid 3 \\ \text{ni} \\ 6 \not\mid 4 \end{cases}$

*Definición congruencia:*

- Definición congruencia:**

$$\begin{cases} 'a' \text{ es congruente a } 'b' \text{ módulo } 'd' \text{ si } d \mid a - b. & \text{Notación } \boxed{a \equiv b (d)} \\ a \equiv b (d) \iff d \mid a - b \end{cases}$$

- Sumar ecuaciones de congruencia *de mismo módulo*, conserva la congruencia:

$$\begin{cases} a_1 \equiv b_1 (d) \\ \vdots \\ a_n \equiv b_n (d) \end{cases} \Rightarrow a_1 + \dots + a_n \equiv b_1 + \dots + b_n (d)$$

- Multiplicar ecuaciones de congruencia *de mismo módulo*, conserva la congruencia:

$$\begin{cases} a_1 \equiv b_1 (d) \\ \vdots \\ a_n \equiv b_n (d) \end{cases} \Rightarrow a_1 \cdot \dots \cdot a_n \equiv b_1 \cdot \dots \cdot b_n (d)$$

Un caso particular con un simpático resultado:

$$n \text{ ecuaciones } \begin{cases} a \equiv b (d) \\ \vdots \\ a \equiv b (d) \end{cases} \Rightarrow \boxed{a^n \equiv b^n (d)}$$

Algoritmo de división:

- Dados  $a, d \in \mathbb{Z}$  con  $d \neq 0$ , existen únicos  $q$  (cociente),  $r$  (resto)  $\in \mathbb{Z}$  tales que:

$$\begin{cases} a = q \cdot d + r, \\ \text{con } 0 \leq r < |d|. \end{cases}$$

- Notación:**  $\boxed{r_d(a)}$  es el resto de dividir  $a$  entre  $d$
- $\underbrace{0 \leq r < |d|}_{\text{cumple condición de resto}} \Rightarrow r = r_d(r)$ . Un número que cumple condición de resto, es su resto.

- Así es como me gusta pensar a la congruencia. La derecha es el resto de dividir  $a$  entre  $d$ :

$$a \equiv r_d(a) \ (d).$$

- Si  $d$  divide al número  $a$ , entonces el resto de la división es 0:

$$r_d(a) = 0 \iff d \mid a \iff a \equiv 0 \ (d)$$

- El resto es único:

$$a \equiv r \ (d) \text{ con } \underbrace{0 \leq r < |d|}_{\text{cumple condición de resto}} \Rightarrow r = r_d(a)$$

$$r_1 \equiv r_2 \ (d) \text{ con } \underbrace{0 \leq r_1, r_2 < |d|}_{\text{cumple condición de resto}} \Rightarrow r_1 = r_2$$

- Dos números que son congruentes módulo  $d$  entre sí, tienen igual resto al dividirse por  $d$ :

$$a \equiv b \ (d) \iff r_d(a) = r_d(b).$$

- Propiedades útiles para los ejercicios de calcular restos:

$$r_d(a + b) = r_d(r_d(a) + r_d(b)) \quad \text{y} \quad r_d(a \cdot b) = r_d(r_d(a) \cdot r_d(b))$$

ya que si,

$$\begin{cases} a \equiv r_d(a) \ (d) \\ b \equiv r_d(b) \ (d) \end{cases} \xrightarrow[\text{ecuaciones}]{\text{sumo}} a + b \equiv r_d(a) + r_d(b) \ (d)$$

y,

$$\begin{cases} a \equiv r_d(a) \ (d) \\ b \equiv r_d(b) \ (d) \end{cases} \xrightarrow[\text{ecuaciones}]{\text{multiplico}} a \cdot b \equiv r_d(a) \cdot r_d(b) \ (d)$$

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:

$$\boxed{\text{máximo común divisor: } \text{MCD} = (a : b)}$$

- $(a : b) \in \mathbb{N}$  (pues  $(a : b) \geq 1$ ) *siempre existe* y es *único*.
- Propiedades del  $(a : b)$ , con  $a$  y  $b \in \mathbb{Z}$ , no ambos nulos.

- ✳ Los signos no importan:  $(a : b) = (\pm a : \pm b)$
- ✳ Es simétrico:  $(a : b) = (b : a)$
- ✳ Entre 1 y  $a \in \mathbb{Z}$  siempre  $(a : 1) = 1$
- ✳ Entre 0 y  $a$  siempre  $(a : 0) = |a|$ ,  $\forall a \in \mathbb{Z} - \{0\}$
- ✳ si  $b \mid a \Rightarrow (a : b) = |b|$  con  $b \in \mathbb{Z} - \{0\}$
- ✳ Útil para ejercicios:  $(a : b) = (a : b + na)$  con  $n \in \mathbb{Z}$
- ✳ Útil para ejercicios:  $(a : b) = (a : r_a(b))$  con  $n \in \mathbb{Z}$
- ✳ Útil para ejercicios: Sean  $a, b \in \mathbb{Z}$  no ambos nulos, y sea  $k \in \mathbb{N}$

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

- *Algoritmo de Euclides*: Para encontrar el  $(a : b)$  con números o expresiones feas. Hay que saber hacer esto. Fin. ¡Se usa de acá hasta el final de la materia!.
- *Combinación Entera*: Otra herramienta gloriosa que sale de hacer *Euclides*. Por ejemplo se usa cuando no se ve a ojo una solución en ecuaciones diofánticas. ¡Se usa de acá hasta el final de la materia!.

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:

$$d \mid a \quad \text{y} \quad d \mid b \iff d \mid \underbrace{(a : b)}_{s \cdot a + t \cdot b}.$$

- ✳ 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.

*Coprimos*:

- Definición coprimos:

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

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

- Sean  $a, b \in \mathbb{Z}$  no ambos nulos. *coprimizar* los números es dividirlos por su máximo común divisor, para obtener un nuevo par que sea coprimo:

$$(a : b) \neq 1 \xrightarrow{\text{coprimizar}} a' = \frac{a}{(a : b)}, b' = \frac{b}{(a : b)}, \Rightarrow \boxed{(a' : b') = 1} \quad \checkmark$$

- ¡Causa de muchos errores! Sean  $a, c, d \in \mathbb{Z}$  con  $c, d$  no nulos. Entonces:

$$c \mid a \quad \text{y} \quad d \mid a \quad \text{y} \quad c \perp d \iff c \cdot d \mid a$$

Al ser  $c$  y  $d$  coprimos, pienso a  $a$  como un número cuya factorización tiene a  $c, d$  y la coprimicidad hace que en la factorización aparezca  $c \cdot d$ . (no sé, así lo piensa mi 🍷).

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

$$d \mid a \cdot b \quad \text{y} \quad d \perp a \Rightarrow d \mid b$$

- *Primos y Factorización:*

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

$$p \mid a \cdot b \Rightarrow p \mid a \quad \text{o} \quad p \mid b$$

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

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

- 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:

$$\begin{cases} \text{Si } m \mid n \rightarrow m = p_1^{\beta_1} \cdots p_k^{\beta_k} \text{ con } 0 \leq \beta_i \leq \alpha_i, \quad \forall i \ 1 \leq i \leq k \\ \text{y hay} \\ (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_k + 1) = \prod_{i=1}^k \alpha_i + 1 \\ \text{divisores positivos de } n. \end{cases}$$

- Sean  $a$  y  $b \in \mathbb{Z}$  no nulos, con

$$\begin{cases} a = \pm p_1^{m_1} \cdots p_r^{m_r} \text{ con } m_1, \dots, m_r \in \mathbb{Z}_0 \\ b = \pm p_1^{n_1} \cdots p_r^{n_r} \text{ con } n_1, \dots, n_r \in \mathbb{Z}_0 \\ \begin{cases} \Rightarrow (a : b) = p_1^{\min\{m_1, n_1\}} \cdots p_r^{\min\{m_r, n_r\}} \\ \Rightarrow [a : b] = p_1^{\max\{m_1, n_1\}} \cdots p_r^{\max\{m_r, n_r\}} \end{cases} \end{cases}$$

- Sean  $a, d \in \mathbb{Z}$  con  $d \neq 0$  y sea  $n \in \mathbb{N}$ . Entonces

$$d \mid a \iff d^n \mid a^n.$$

- Sean  $a, b, c \in \mathbb{Z}$  no nulos:

- \*  $a \perp b \iff$  no tienen primos en común.
- \*  $(a : b) = 1 \quad \text{y} \quad (a : c) = 1 \iff (a : bc) = 1$
- \*  $(a : b) = 1 \iff (a^m : b^n) = 1, \quad \forall m, n \in \mathbb{N}$
- \*  $(a^n : b^n) = (a : b)^n \quad \forall n \in \mathbb{N}$

- Si  $a \mid m \wedge b \mid m$ , 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  $\forall a, b, c \in \mathbb{Z}$

- |  |  |
|--|--|
| a) $a \cdot b \mid c \Rightarrow a \mid c \text{ y } b \mid c$ | f) $a \mid c \text{ y } b \mid c \Rightarrow a \cdot b \mid c$   |
| b) $4 \mid a^2 \Rightarrow 2 \mid a$                           | g) $a \mid b \Rightarrow a \leq b$                               |
| c) $2 \mid a \cdot b \Rightarrow 2 \mid a \text{ o } 2 \mid b$ | h) $a \mid b \Rightarrow  a  \leq  b $                           |
| d) $9 \mid a \cdot b \Rightarrow 9 \mid a \text{ o } 9 \mid b$ | i) $a \mid b + a^2 \Rightarrow a \mid b$                         |
| e) $a \mid b + c \Rightarrow a \mid b \text{ o } a \mid c$     | j) $a \mid b \Rightarrow a^n \mid b^n, \forall n \in \mathbb{N}$ |

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

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

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

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

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

$$\text{Si } 2 \mid a \cdot b \Rightarrow \left\{ \begin{array}{c} a \text{ tiene que ser par} \\ \vee \\ b \text{ tiene que ser par} \end{array} \right\} \xrightarrow{\text{para que}} a \cdot b \text{ sea par. Por lo tanto si } 2 \mid a \cdot b \Rightarrow 2 \mid a \text{ o } 2 \mid b.$$

d)  $9 \mid a \cdot b \Rightarrow 9 \mid a \text{ o } 9 \mid b$

Si  $a = 3 \wedge b = 3$ , se tiene que  $9 \mid 9$ , sin embargo  $9 \nmid 3$

e)  $a \mid b + c \Rightarrow a \mid b \text{ o } a \mid c$

$$12 \mid 20 + 4 \Rightarrow 12 \nmid 20 \text{ y } 12 \nmid 4$$

f) \_\_\_\_\_

🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram  $\rightarrow$  , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X  $\rightarrow$  .

g) \_\_\_\_\_

🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram  $\rightarrow$  , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X  $\rightarrow$  .

h) \_\_\_\_\_

🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram  $\rightarrow$  , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X  $\rightarrow$  .



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

$$a \mid b + a^2 \Rightarrow b + a^2 = k \cdot a \xrightarrow{\text{acomodo}} b = (k - a) \cdot a = h \cdot a \Rightarrow a \mid b \quad \checkmark$$

$$\xrightarrow[\text{decir si:}]{\text{también puedo}} \left\{ \begin{array}{l} a \mid a^2 \\ a \mid b - a^2 \end{array} \right\} \xrightarrow[\text{propiedad}]{\text{por}} a \mid (b - a^2) + (a^2) = b \Rightarrow a \mid b \quad \checkmark$$

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

Pruebo por inducción.

$$p(n) : a \mid b \Rightarrow a^n \mid b^n$$

Caso base:

$$n = 1 \Rightarrow a \mid b \Rightarrow a^1 \mid b^1 \quad \checkmark$$

$p(1)$  resulta verdadera.

Paso inductivo:

Asumo  $\underbrace{p(h) : a \mid b \Rightarrow a^h \mid b^h}_{\text{hipótesis inductiva}}$  verdadera  $\Rightarrow$  quiero ver que  $p(h+1) : a \mid b \Rightarrow a^{h+1} \mid b^{h+1}$

Parto de la **hipótesis inductiva** y voy llegar a  $p(k+1)$ . Si:


$$a \mid b \xrightarrow{\text{HI}} a^k \mid b^k \Leftrightarrow a^k \cdot c = b^k \xLeftrightarrow{\times b} b \cdot a^k \cdot c = b^{k+1} \xLeftrightarrow[a \cdot d = b]{a \mid b} a \cdot d \cdot a^k \cdot c = a^{k+1} \cdot (cd) = b^{k+1} \Leftrightarrow a^{k+1} \mid b^{k+1}.$$

Como  $p(1)$ ,  $p(k)$  y  $p(k+1)$  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:

$$a \mid b \Rightarrow a^n \mid b^n \iff b \equiv 0 \pmod{a} \Rightarrow b^n \equiv 0 \pmod{a^n} \xLeftrightarrow[0 \equiv a^n]{a^n} b^n \equiv a^n \pmod{a^n}$$

$$\boxed{a \mid b \Rightarrow b^n \equiv a^n \pmod{a^n}}$$

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

2. Hallar todos los  $n \in \mathbb{N}$  tales que:

a)  $3n - 1 \mid n + 7$

c)  $2n + 1 \mid n^2 + 5$

b)  $3n - 2 \mid 5n - 8$

d)  $n - 2 \mid n^3 - 8$

a)  $3n - 1 \mid n + 7$

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

$$\left\{ \begin{array}{l} 3n - 1 \mid n + 7 \xrightarrow[a \mid k \cdot c]{a \mid c \Rightarrow} 3n - 1 \mid 3 \cdot (n + 7) = 3n + 21 \\ \frac{a \mid b \text{ y } a \mid c}{\Rightarrow a \mid b \pm c} \rightarrow 3n - 1 \mid 3n + 21 - (3n - 1) = 22 \end{array} \right\} \rightarrow 3n - 1 \mid 22$$

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

b)

c)

d)  $n - 2 \mid n^3 - 8$ 

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

**3.** Sean  $a, b \in \mathbb{Z}$ .a) Probar que  $a - b \mid a^n - b^n$  para todo  $n \in \mathbb{N}$  y  $a \neq b \in \mathbb{Z}$ b) Probar que si  $n$  es un número natural par y  $a \neq -b$ , entonces  $a + b \mid a^n - b^n$ .c) Probar que si  $n$  es un número natural impar y  $a \neq -b$ , entonces  $a + b \mid a^n + b^n$ .a) *Inducción:**Proposición:*

$$p(n) : a - b \mid a^n - b^n \quad \forall n \in \mathbb{N} \quad \text{y} \quad a \neq b \in \mathbb{Z}$$

*Caso Base:*

$$p(1) : a - b \mid a^1 - b^1,$$

 $p(1)$  es verdadera. ✓*Paso inductivo:*

Asumo que  $p(k) : a - b \mid a^k - b^k$  es verdadera  $\Rightarrow$  quiero probar que  $p(k+1) : a - b \mid a^{k+1} - b^{k+1}$  también lo sea.

$$\left\{ \begin{array}{l} a - b \mid a^k - b^k \\ a - b \mid a^k - b^k \end{array} \right\} \xrightarrow[\times b]{\times a} \left\{ \begin{array}{l} a - b \mid a^{k+1} - ab^k \\ a - b \mid ba^k - b^{k+1} \end{array} \right\} \xrightarrow{+} \{ a - b \mid a^{k+1} - b^{k+1} \}. \quad \checkmark$$

Como  $p(1)$ ,  $p(k)$  y  $p(k+1)$  resultaron verdaderas por el principio de inducción  $p(n)$  también lo es.

b) Sé que

$$a + b \mid a + b \stackrel{\text{def}}{\iff} a \equiv -b \pmod{a+b}$$

Multiplicando la ecuación de congruencia por  $a$  sucesivas veces me formo:

$$\left\{ \begin{array}{l} a \cdot a = a^2 \stackrel{(a+b)}{\equiv} a \cdot (-b) \stackrel{(a+b)}{\equiv} (-1)^2 b \\ \vdots \quad \leftarrow \star^1 \\ a^n \stackrel{(a+b)}{\equiv} (-1)^n \cdot b^n \rightarrow \begin{cases} a^n \equiv b^n \pmod{a+b} & \text{con } n \text{ par} \\ a^n \equiv (-1)^n \cdot b^n \pmod{a+b} & \text{con } n \text{ impar} \end{cases} \end{array} \right.$$

$$\left\{ \begin{array}{ll} \text{Con } n \text{ par:} & a^n \equiv b^n \pmod{a+b} \Rightarrow a + b \mid a^n - b^n \\ \text{Con } n \text{ impar:} & a^n \equiv -b^n \pmod{a+b} \Rightarrow a + b \mid a^n + b^n \end{array} \right.$$

 $\star^1$  *Inducción:*

$$p(n) : a \equiv -b \pmod{a+b} \Rightarrow a^n \equiv (-1)^n \cdot b^n \pmod{a+b} \quad \forall n \in \mathbb{N}.$$

Caso base:

$$p(1) : a \equiv -b (a+b) \Rightarrow a^1 \equiv (-1)^1 \cdot b^1 (a+b)$$

$p(1)$  es verdadera.

Paso inductivo:

$p(k) : a \equiv -b (a+b) \Rightarrow a^k \equiv (-1)^k \cdot b^k (a+b)$  asumo verdadera para algún  $k \in \mathbb{Z}$   
 $\Rightarrow$  quiero probar que

$$\text{Partiendo de } p(k) : \begin{cases} p(k+1) : a \equiv -b (a+b) \Rightarrow a^{k+1} \equiv (-1)^{k+1} \cdot b^{k+1} (a+b) \\ a \equiv -b (a+b) \Rightarrow a^k \equiv (-1)^k \cdot b^k (a+b) \\ \xrightarrow[\text{por } a]{\text{multiplico}} \\ a \cdot a^k = a^{k+1} \equiv (-1)^k \cdot \underbrace{a}_{(a+b)_b} \cdot b^k (a+b) \\ \Rightarrow \\ a^{k+1} \equiv (-1)^{k+1} \cdot b^{k+1} (a+b) \iff a+b \mid a^{k+1} - (-1)^{k+1} b^{k+1} \quad \checkmark \end{cases}$$

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

c) Hecho en el anterior 🙌.

4. Sea  $a \in \mathbb{Z}$  impar. Probar que  $2^{n+2} \mid a^{2^n} - 1$  para todo  $n \in \mathbb{N}$

Pruebo por inducción:

$$p(n) : 2^{n+2} \mid a^{2^n} - 1, \text{ con } a \in \mathbb{Z} \text{ e impar. } \forall n \in \mathbb{N}.$$

Caso base:

$$\begin{aligned} p(1) : 2^3 = 8 \mid a^2 - 1 &= (a-1) \cdot (a+1) \\ &\xrightarrow[a = 2m-1]{a \text{ es impar, si } m \in \mathbb{Z}} \\ (a-1) \cdot (a+1) &\stackrel{\star^1}{=} (2m-2) \cdot (2m) \stackrel{!}{=} 4 \cdot \underbrace{m \cdot (m-1)}_{\text{par: } 2h, h \in \mathbb{Z}} = 4 \cdot 2h = 8 * h \\ &\xrightarrow[\text{tanto}]{\text{por lo}} \\ 8 \mid 8h &= (a-1) \cdot (a+1) \text{ para algún } h \in \mathbb{Z} \quad \checkmark \end{aligned}$$

Por lo tanto  $p(1)$  es verdadera.

Paso inductivo:


Asumo que:  $p(k) : 2^{k+2} \mid a^{2^k} - 1$ , es verdadera  $\Rightarrow$  Quiero ver que  $p(k+1) : 2^{k+3} \mid a^{2^{k+1}} - 1$ , también lo sea.

$$\begin{aligned} 2^{k+3} \mid a^{2^{k+1}} - 1 &\stackrel{!}{\iff} 2^{k+2} \cdot 2 \mid (a^{2^k} - 1) \cdot \overbrace{(a^{2^k} + 1)}^{\text{par !}} \\ &\xleftrightarrow[\text{hipótesis inductiva}]{\text{Si } a \mid b \text{ y } c \mid d \Rightarrow ac \mid bd} \\ &2^{k+2} \cdot 2 \mid (a^{2^k} - 1) \cdot \underbrace{(a^{2^k} + 1)}_{\text{par}}. \end{aligned}$$

El ! es todo tuyo, *hints*: diferencia de cuadrados, propiedades de exponentes... 🙌

En el último paso se comprueba que  $p(k+1)$  es verdadera.

Como  $p(1)$ ,  $p(k)$  y  $p(k+1)$  resultaron verdaderas, por el principio de inducción también lo será  $p(n) \forall n \in \mathbb{N}$ .

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

## 5. ... hay que hacerlo!

Si querés mandarlo: Telegram  $\rightarrow$  , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X $\rightarrow$  .

## 6.

- Probar que el producto de  $n$  enteros consecutivos es divisible por  $n!$
- Probar que  $\binom{2n}{n}$  es divisible por 2.

## ... hay que hacerlo!

Si querés mandarlo: Telegram  $\rightarrow$  , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X $\rightarrow$  .

## 7. Proba que las siguientes afirmaciones son verdaderas para todo $n \in \mathbb{N}$ .

- $99 \mid 10^{2n} + 197$
- $9 \mid 7 \cdot 5^{2n} + 2^{4n+1}$
- $56 \mid 13^{2n} + 28n^2 - 84n - 1$
- $256 \mid 7^{2n} + 208n - 1$

$$a) \quad 99 \mid 10^{2n} + 197 \stackrel{\text{def}}{\iff} 10^{2n} + 197 \equiv 0 \pmod{99} \rightarrow 10^{2n} + 198 \equiv 1 \pmod{99} \rightarrow 10^{2n} + \underbrace{198}_{\substack{(99) \\ \equiv 0}} \equiv 1 \pmod{99} \rightarrow 100^n \equiv$$

$$1 \pmod{99} \rightarrow \left\{ \begin{array}{l} \xrightarrow[\text{que}]{\text{sé}} 100 \equiv 1 \pmod{99} \iff 100^2 \equiv \underbrace{100}_{\substack{(99) \\ \equiv 1}} \pmod{99} \rightarrow 100^2 \equiv 1 \pmod{99} \iff \dots \iff 100^n \equiv 1 \pmod{99} \end{array} \right.$$

$$\text{Se concluye que } 99 \mid 10^{2n} + 197 \iff 99 \mid \underbrace{100 - 1}_{99}$$

$$b) \quad 9 \mid 7 \cdot 5^{2n} + 2^{4n+1} \stackrel{\text{def}}{\iff} 7 \cdot 5^{2n} + 2^{4n+1} \equiv 0 \pmod{9} \xrightarrow[\text{M.A.M}]{\text{sumo } 2 \cdot 5^{2n}} \underbrace{9 \cdot 5^{2n}}_{\substack{(9) \\ \equiv 0}} + 2 \cdot 2^{4n} \equiv 2 \cdot 5^{2n} \pmod{9}$$

$$\xrightarrow[\text{y acomodo}]{\text{simplifico}} 2^{4n} \equiv 5^{2n} \pmod{9} \rightarrow 16^n \equiv 25^n \pmod{9} \xrightarrow[\text{congruencia}]{\text{simetría}} 25^n \equiv 16^n \pmod{9} \xrightarrow{25 \equiv 16} 25 \equiv 16 \pmod{9} = 9 \equiv 0 \pmod{9}$$

$$\text{Se concluye que } 9 \mid 7 \cdot 5^{2n} + 2^{4n+1} \iff 9 \mid 9 \leftarrow \text{¿Se concluye esto...?}$$

## c) ... hay que hacerlo!

Si querés mandarlo: Telegram  $\rightarrow$  , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X $\rightarrow$  .

## d) Hermoso ejercicio en el que sin fe en el todo poderoso Gauss sencillamente uno tira la toalla.

Sale por inducción:

Quiero ver que:

$$p(n) : 256 \mid 49^n + 208n - 1$$

O en notación de congruencia:

$$p(n) : 49^n + 208n - 1 \equiv 0 \pmod{256}$$

Caso base:

$$p(1) : 256 \mid 49^1 + 208 \cdot 1 - 1 \quad \checkmark$$

Por lo tanto  $p(1)$  resulta verdadera.

Paso inductivo:

Uso la notación de congruencia de acá en adelante, porque es mucho más cómodo. Supongo que:

$$p(k) : \underbrace{49^k + 208 \cdot k - 1 \equiv 0 \pmod{256}}_{\text{hipótesis inductiva}} \quad \forall k \in \mathbb{Z}$$

es una proposición verdadera. Entonces quiere probar que:

$$p(k+1) : 49^{k+1} + 208 \cdot (k+1) - 1 \equiv 0 \pmod{256},$$


también sea verdadera. Arranco del paso  $(k+1)$  y haciendo un poco de *matemagia*:

$$\begin{aligned} 49^{k+1} + 208 \cdot (k+1) - 1 &= 49 \cdot 49^k + 208k + 208 - 1 \stackrel{(256)}{\equiv} 49 \cdot (-208k + 1) + 208k + 208 - 1 \\ &\stackrel{(256)}{\equiv} 49 \cdot (48k + 1) - 48k - 48 - 1 = 2352k + 49 - 48k - 49 \\ &\stackrel{(256)}{\equiv} 48k + 49 - 48k - 49 = 0 \quad \checkmark \\ &\quad !! \end{aligned}$$

En !! y gracias a Gauss  $2352 \equiv 48 \pmod{256}$  ¿Casualidad? No sé y no me importa.

Dado que  $49^{k+1} + 208 \cdot (k+1) - 1 \equiv 0 \pmod{256}$ , la proposición  $p(k+1)$  resultó verdadera.

Dado que  $p(1), p(k)$  y  $p(k+1)$  resultaron verdaderas, por principio de inducción  $p(n)$  también lo es para todo  $n \in \mathbb{N}$ .

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

Algoritmo de División:

8. Calcular el cociente y el resto de la división de  $a$  por  $b$  en los casos:

a)  $a = 133, \quad b = -14.$

d)  $a = b^2 - 6, \quad b \neq 0.$

b)  $a = 13, \quad b = 111.$

e)  $a = n^2 + 5, \quad b = n + 2 \quad (n \in \mathbb{N}).$

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

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

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

b)

$$c) a = 3b + 7 \rightarrow \text{me interesa: } \rightarrow \left\{ \begin{array}{cc} |b| \leq |a| & \checkmark \\ 0 \leq r < |b| & \checkmark \end{array} \right\} \rightarrow$$

$$\rightarrow \left\{ \begin{array}{l} \text{Si: } |b| > 7 \rightarrow (q, r) = (3, 7) \\ \text{Si: } |b| \leq 7 \rightarrow (q, r) = (3, 7) \end{array} \right.$$

$(a, b)$	$(-14, -7)$	$(-11, -6)$	$(-8, -5)$	$(-5, -4)$	$(4, -1)$	$\dots$
$(q, r)$	$(2, 0)$	$(2, 1)$	$(2, 2)$	$(2, 3)$	$(4, 0)$	$\dots$

$$d) a = b^2 - 6, \quad b \neq 0. \quad \text{😬... hay que hacerlo! 🤖}$$

Si querés mandarlo: Telegram  $\rightarrow$  , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X  $\rightarrow$  .

9. Sabiendo que el resto de la división de un entero  $a$  por 18 es 5, calcular el resto de:

a) la división de  $a^2 - 3a + 11$  por 18.

b) la división de  $a$  por 3.

c) la división de  $4a + 1$  por 9.

d) la división de  $7a^2 + 12$  por 28.

$$a) r_{18}(a) = r_{18}(\underbrace{r_{18}(a)^2}_{5^2} - \underbrace{r_{18}(3)}_3 \cdot \underbrace{r_{18}(a)}_5 + \underbrace{r_{18}(11)}_{11}) = r_{18}(21) = 3$$

$$b) \left\{ \begin{array}{l} a = 3 \cdot q + r_3(a) \\ 6 \cdot a = 18 \cdot q + \underbrace{6 \cdot r_3(a)}_{r_{18}(6a)} \end{array} \right\} \rightarrow r_{18}(6a) = r_{18}(r_{18}(6) \cdot r_{18}(a)) = r_{18}(30) = 12$$

$$\Rightarrow 6 \cdot r_3(a) = r_{18}(6a) \rightarrow r_3(a) = 2$$

$$c) r_9(4a + 1) = \underbrace{r_9(4 \cdot r_9(a) + 1)}_{*1} \rightarrow$$

$$a = 18 \cdot q + 5 = 9 \cdot \underbrace{(9 \cdot q)}_{q'} + \underbrace{5}_{r_9(a)} \xrightarrow{*1} r_9(a) = r_9(21) = 3$$

$$d) r_{28}(7a^2 + 12) = r_{28}(7 \cdot r_{28}(a)^2 + 12) \xrightarrow{\text{¿qué es}} r_{28}(a)$$

$$\left\{ \begin{array}{l} a = 18 \cdot q + 5 \xrightarrow[\text{para el 28}]{\text{busco algo}} \\ 14 \cdot a = \underbrace{252 \cdot q}_{28 \cdot 9 \cdot q} + 70 \xrightarrow[\text{condición resto}]{\text{corrijo según}} 28 \cdot 9 \cdot q + \underbrace{2 \cdot 28 + 14}_{70} = 28 \cdot (9 \cdot q + 2) + 14 \quad \checkmark \\ \xrightarrow[\text{tanto}]{\text{por lo}} 14a = 28 \cdot q' + 14 \Rightarrow 14 \cdot a \equiv 14 \pmod{28} \iff a \equiv 1 \pmod{28} \end{array} \right.$$

$$\text{Ahora que sé que } r_{28}(a) = 1 \text{ sale que } r_{28}(7a^2 + 12) = r_{28}(7 \cdot \underbrace{r_{28}(a)^2}_1 + 12) = r_{28}(19) = 19 \quad \checkmark$$

## 10.

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

$$a) \begin{cases} a \equiv 22 \pmod{14} \rightarrow a = 14 \cdot q + \underbrace{22}_{14+8} = 14 \cdot (q+1) + 8 \xrightarrow[\text{es}]{\text{el resto}} r_{14}(a) = 8 \quad \checkmark \\ a \equiv 22 \pmod{14} \rightarrow a = \underbrace{14 \cdot q}_{2 \cdot (7 \cdot q)} + \underbrace{22}_{2 \cdot 11} = 2 \cdot (7q+11) + 0 \xrightarrow[\text{es}]{\text{el resto}} r_2(a) = 0 \quad \checkmark \\ a \equiv 22 \pmod{14} \rightarrow a = \underbrace{14 \cdot q}_{7 \cdot (2 \cdot q)} + \underbrace{22}_{1+7 \cdot 3} = 7 \cdot (2q+3) + 1 \xrightarrow[\text{es}]{\text{el resto}} r_7(a) = 1 \quad \checkmark \end{cases}$$

- b) Dos números congruentes tienen el mismo resto.  $a \equiv 13 \pmod{5} \iff a \equiv 3 \pmod{5}$   $r_5(33a^3 + 3a^2 - 197a + 2) = r_5(3 \cdot r_5(a)^3 + 3 \cdot r_5(a)^2 - 2 \cdot r_5(a) + 2)$   
 $\xrightarrow[r_5(a)=3]{\text{como } a \equiv 13 \pmod{5}} r_5(33a^3 + 3a^2 - 197a + 2) = 4$

- c) 🤔... hay que hacerlo! 🧐

Si querés mandarlo: Telegram  $\rightarrow$  📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X  $\rightarrow$  📄.

## 11.

- a) Probar que  $a^2 \equiv -1 \pmod{5} \iff a \equiv 2 \pmod{5} \vee a \equiv 3 \pmod{5}$
- b) Probar que no existe ningún entero  $a$  tal que  $a^3 \equiv -3 \pmod{7}$
- c) Probar que  $a^7 \equiv a \pmod{7} \quad \forall a \in \mathbb{Z}$
- d) Probar que  $7 \mid a^2 + b^2 \iff 7 \mid a \wedge 7 \mid b$ .
- e) Probar que  $5 \mid a^2 + b^2 + 1 \Rightarrow 5 \mid a \quad \text{o} \quad 5 \mid b$ . ¿Vale la implicación recíproca?

- a) 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.

$$\begin{cases} a^2 \equiv -1 \pmod{5} \Leftrightarrow a^2 \equiv 4 \pmod{5} \Leftrightarrow a^2 - 4 \equiv 0 \pmod{5} \Leftrightarrow (a-2) \cdot (a+2) \equiv 0 \pmod{5} \\ \xrightarrow[\text{resto } 0]{\text{quiero}} r_5(a^2 + 1) = r_5(a^2 - 4) = r_5(r_5(a-2) \cdot r_5(a+2)) = \underbrace{r_5((r_5(a)-2) \cdot (r_5(a)+2))}_{\star^1} = 0 \\ r_5(a^2 + 1) = 0 \xLeftrightarrow{\star^1} r_5((r_5(a)-2) \cdot (r_5(a)+2)) = 0 \begin{cases} r_5(a) = 2 \Leftrightarrow a \equiv 2 \pmod{5} \quad \checkmark \\ r_5(a) = -2 \Leftrightarrow a \equiv 3 \pmod{5} \quad \checkmark \end{cases} \end{cases}$$

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
$r_5(a^2)$	0	1	4	4	1

→ La tabla muestra que para un dado  $a$

$$\rightarrow r_5(a) = \left\{ \begin{array}{l} 2 \iff a \equiv 2 \pmod{5} \iff a^2 \equiv 4 \pmod{5} \iff a^2 \equiv -1 \pmod{5} \\ 3 \iff a \equiv 3 \pmod{5} \iff a^2 \equiv 4 \pmod{5} \iff a^2 \equiv -1 \pmod{5} \end{array} \right\}$$

b) 🙄... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 🐙.

c) 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.

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

$a$	0	1	2	3	4	5	6
$r_7(a)$	0	1	2	3	4	5	6
$r_7(a^3 - 1)$	6	0	0	5	0	5	5
$r_7(a^3 + 1)$	1	2	2	0	2	0	0

se anula, es decir:

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

d)

e)

12. 🙄... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 🐙.

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

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

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.

$$r_7(a_{n+2}) = r_7(r_7(a_{n+1}) - \underbrace{r_7(36)^n}_{\equiv 1 \pmod{7}} \cdot r_7(a_n) + \underbrace{r_7(21)^n}_{\equiv 0 \pmod{7}} \cdot r_7(n)^{21}) = \underbrace{r_7(a_{n+2})}_{\star^1} = r_7(a_{n+1}) - r_7(a_n) \quad \checkmark$$

$$\text{Puesto de otra forma } a_{n+2} \equiv a_{n+1} - a_n \pmod{7} \rightarrow \left\{ \begin{array}{l} a_1 \equiv 3^1 \pmod{7} \iff a_1 \equiv 3 \pmod{7} \\ a_2 \equiv 3^2 \pmod{7} \iff a_2 \equiv 2 \pmod{7} \\ a_3 \equiv 3^3 \pmod{7} \iff a_3 \equiv 6 \pmod{7} \end{array} \right.$$

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

$$p(n) : a_n \equiv 3^n \pmod{7} \quad \forall n \in \mathbb{N}$$



$$\begin{array}{ll}
\text{Casos base:} & \left\{ \begin{array}{l} p(1) : a_1 \equiv 3^1 \pmod{7} \quad \checkmark, \quad p(1) \text{ es verdadera} \\ p(2) : a_2 \equiv 3^2 \pmod{7} \equiv 2 \equiv -5 \pmod{7} \quad \checkmark, \quad p(2) \text{ es verdadera} \\ p(k) : a_k \equiv 3^k \pmod{7} \quad \checkmark, \quad p(k) \text{ la asumo verdadera} \end{array} \right. \\
\text{Paso Inductivo:} & \left\{ \begin{array}{l} \text{y} \\ p(k+1) : a_{k+1} \equiv 3^{k+1} \pmod{7} \quad \checkmark, \quad p(k+1) \text{ también asumo verdadera} \\ \Rightarrow p(k+2) : a_{k+2} \equiv 3^{k+2} \pmod{7} \text{ quiero probar que es verdadera} \end{array} \right. \\
\text{Hipótesis inductiva:} & \left\{ \begin{array}{l} a_k \equiv 3^k \pmod{7} \\ a_{k+1} \equiv 3^{k+1} \pmod{7} \\ \xrightarrow{\text{suma}} a_{k+2} = a_{k+1} - a_k \equiv 3^{k+1} - 3^k = 2 \cdot 3^k \equiv 9 \cdot 3^k = 3^{k+2} \pmod{7} \quad \checkmark \\ \star^1 \\ p(k+2) \text{ resultó ser verdadera.} \end{array} \right.
\end{array}$$

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

14.

(a) Hallar el desarrollo en base 2 de

i. 1365

ii. 2800

iii.  $3 \cdot 2^{12}$

iv.  $13 \cdot 2^n + 5 \cdot 2^{n-1}$

(b) Hallar el desarrollo en base 16 de 2800.

🙄... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

15. 🙄... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

16. 🙄... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

17. 🙄... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

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)  $a = 2532$ ,  $b = 63$ .

ii)  $a = 131$ ,  $b = 23$ .

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

Hacer!

19. 🙄... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

 ¿Errores? Avisá así se corrige y ganamos todos.

Ir a índice ↑  
12/12/24 © 22:06

20. Sea  $a \in \mathbb{Z}$ .

- 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 ítem es **indispensable** mostrar que el máximo común divisor nunca puede ser 1).

i) 😞... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

ii) 😞... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

$$\text{iii) } (a^2 - 3a + 2 : 3a^3 - 5a^2) \xrightarrow{\text{Euclides}} (\underbrace{a^2 - 3a + 2}_{\star^1_{\text{par}}} : \underbrace{6a - 8}_{\star^1_{\text{par}}})$$

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

$$\left\{ \begin{array}{l} a = 1 \quad (0 : -2) = 2 \\ a = 2 \quad (0 : 4) = 4 \end{array} \right.$$

Parecido al hecho en clase.

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

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

$$\left\{ \begin{array}{l} d \mid 7a - 3b \xrightarrow{\cdot 2} d \mid b \rightarrow d \mid b \\ d \mid 2a - b \xrightarrow{\cdot 7} d \mid 2a - b \rightarrow d \mid a \end{array} \right\} \xrightarrow[\text{divisor y (a:b)}]{\text{propiedad}} d \mid (a : b) \xrightarrow[\text{coprimos}]{(a : b)} d \mid 1$$

Por lo tanto  $(7a - 3b : 2a - b) = 1$  son coprimos como se quería mostrar.

22. 😞... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

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  $\frac{2a+3}{a+1} + \frac{a+2}{4} \in \mathbb{Z}$ .

$$\text{i) } \frac{b+4}{a} + \frac{5}{b} = \frac{b^2+4b+5a}{ab} \xrightarrow{\text{quiero que}} ab \mid b^2 + 4b + 5a$$

$$\xrightarrow[\text{coprimitusibilidad}]{\text{por}} \left\{ \begin{array}{l} a \mid b^2 + 4b + 5a \\ b \mid b^2 + 4b + 5a \end{array} \right\} \rightarrow \left\{ \begin{array}{l} a \mid b^2 + 4b \\ b \mid 5a \end{array} \right\} \xrightarrow[\text{debe dividir a 5}]{\text{es seguro que } b \nmid a} \left\{ \begin{array}{l} a \mid b \cdot (b + 4) \\ b \mid 5 \end{array} \right.$$

Seguro tengo que  $b \in \{\pm 1, \pm 5\} \rightarrow$  pruebo valores de  $b$  y veo que valor de  $a$  queda:

$$\begin{cases} b = 1 \rightarrow (a \mid 5, 1) \rightarrow \{(\pm 1, 1).(\pm 5, 1)\} \\ b = -1 \rightarrow (a \mid -3, 1) \rightarrow \{(\pm 1, -1).(\pm 3, 1)\} \\ b = 5 \rightarrow (a \mid 45, 5) \xrightarrow[\substack{\text{atención que} \\ (a:b)=1}]{\text{atención que}} \{(\pm 1, 5), (\pm 3, 5).(\pm 9, 5)\} \\ b = -5 \rightarrow (a \mid 5, -5) \xrightarrow[\substack{\text{atención que} \\ (a:b)=1}]{\text{atención que}} \{(\pm 1, -5)\} \end{cases}$$

ii) **Hacer!**

iii)

$$\frac{2a+3}{a+1} + \frac{a+2}{4} = \frac{a^2+11a+14}{4a+4} \star^1$$

Para que  $\frac{a^2+11a+14}{4a+4} \in \mathbb{Z}$  debe ocurrir que

$$4a+4 \mid a^2+11a+14$$

Busco eliminar la  $a$  del lado derecho:

$$\begin{cases} 4a+4 \mid a^2+11a+14 \\ 4a+4 \mid 4a+4 \end{cases} \xrightarrow{!} \begin{cases} 4a+4 \mid 16 \\ 4a+4 \mid 4a+4 \end{cases}$$


Las cuentas del **!** te las dejo a vos.



$4a+4$  tiene que dividir a 16, por lo tanto mis posibles valores serán  $\{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}$ .

Teniendo en cuenta que  $4a+4 \in \mathbb{Z}$  y también que  $a \in \mathbb{Z}$ , quedan como únicos posibles valores:

$$\begin{aligned} 4(-5) + 4 &= -16 \quad \checkmark \\ 4(-2) + 4 &= -4 \quad \checkmark \end{aligned}$$

reemplazando esos valores de  $a$  en  $\star^1$  se obtiene tiene valor  $-1 \in \mathbb{Z}$ .

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz   
Primos y factorización:

**24.** ... hay que hacerlo! 

Si querés mandarlo: Telegram  $\rightarrow$  , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X  $\rightarrow$  .

**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  $(a+b)^p \equiv a^p + b^p \pmod{p}$ .

**26.** 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 📄.

**27.** Sea  $n \in \mathbb{N}, n \geq 2$ . Probar que si  $p$  es un número primo positivo entonces  $\sqrt[n]{p} \notin \mathbb{Q}$ .

Supongamos que  $\sqrt[n]{p} \in \mathbb{Q}$  y lleguemos a una contradicción:

$$\sqrt[n]{p} \in \mathbb{Q} \Rightarrow \sqrt[n]{p} = \frac{a}{b}, \quad a, b \in \mathbb{Z} \quad \text{y} \quad b \neq 0 \Rightarrow b \cdot \sqrt[n]{p} = a \Rightarrow b^n \cdot p = a^n$$

Por otro lado, por TFA, tenemos que

$$\begin{cases} a = (P_1)^{m_1} \dots (P_r)^{m_r}, & m_1, \dots, m_r \in \mathbb{N}_0 \\ b = (P_1)^{l_1} \dots (P_r)^{l_r}, & l_1, \dots, l_r \in \mathbb{N}_0 \end{cases} \Rightarrow \begin{cases} a^n = (P_1)^{n \cdot m_1} \dots (P_r)^{n \cdot m_r} \\ b^n = (P_1)^{n \cdot l_1} \dots (P_r)^{n \cdot l_r} \end{cases}$$

Luego

$$b^n \cdot p = a^n \iff (P_1)^{n \cdot l_1} \dots (P_r)^{n \cdot l_r} \cdot p^1 = (P_1)^{n \cdot m_1} \dots (P_r)^{n \cdot m_r}$$

En el lado izquierdo de la igualdad, el primo  $p$  aparece con el exponente  $n \cdot l_p + 1$ , mientras que en el lado izquierdo aparece con el exponente  $n \cdot m_p$

Entonces, por la unicidad de la factorización, tenemos que

$$\begin{aligned} n \cdot l_p + 1 &= n \cdot m_p \\ 1 &= n \cdot m_p - n \cdot l_p \\ \frac{1}{n} &= m_p - l_p \end{aligned}$$

Lo cual es absurdo, pues  $m_p - l_p \in \mathbb{Z}$  pero claramente  $\frac{1}{n} \notin \mathbb{Z}$  para  $n \geq 2$ . La contradicción proviene de la única suposición que hicimos, que  $\sqrt[n]{p} \in \mathbb{Q}$ . Luego,  $\sqrt[n]{p} \notin \mathbb{Q}$ , tal como queríamos probar.

Dale las gracias y un poco de amor 🧡 a los que contribuyeron! Gracias por tu aporte:

👉 Nunezca 📄

**28.** 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 📄.

**29.** 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 📄.

**30.** 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 📄.

**31.** 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 📄.

**32.** 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 📄.

**33.** 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 🐙.

**34.** Hallar el menor número natural  $n$  tal que  $(n : 3150) = 45$  y  $n$  tenga exactamente 12 divisores positivos.

Trabajemos con la primera condición:

$$(n : 3150) = 45 \iff (n : 2 \cdot 3^2 \cdot 5^2 \cdot 7) = 3^2 \cdot 5$$

Utilizando que el MCD se calcula como primos en común a la menor potencia, concluimos que  $n$  no tiene en su factorización al 2 ni al 7 y que si tiene en su factorización un 5 y un  $3^i$ , con  $i \geq 2$ . Es decir:

$$n = 3^i \cdot 5 \cdot (P_1)^{m_1} \dots (P_k)^{m_k}, \quad i \geq 2 \text{ y } m_j \geq 0$$

De la segunda condición tenemos que

$$12 = 2(i+1)(m_1+1)\dots(m_k+1) \iff 6 = (i+1)(m_1+1)\dots(m_k+1)$$

Como  $i \geq 2 \Rightarrow i+1 \geq 3$  y como queremos que el producto nos de 6, esto nos deja dos opciones:

- $(i+1) = 6$  y  $(m_1+1)\dots(m_k+1) = 1$
- $(i+1) = 3$  y  $(m_1+1)\dots(m_k+1) = 2$

De la primera tenemos que  $i = 5$  y que no hay otro primo en la factorización. De modo que  $n = 3^5 \cdot 5 = 1215$

De la segunda tenemos que  $i = 2$  y que solo puede haber otro primo en la factorización con  $m_1 = 1$ . Como nos piden el menor  $n$ , elegimos el menor primo que le sigue a 5 que no sea el 7, es decir, el 11. Entonces,  $n = 3^2 \cdot 5 \cdot 11 = 495$

Luego, eligiendo el menor entre los dos, la respuesta es  $n = 495$

Dale las gracias y un poco de amor ❤️ a los que contribuyeron! Gracias por tu aporte:

👉 Nunezca 🐙

**35.** 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 🐙.

**36.** 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 🐙.

**37.** 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 🐙.

**38.** 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 🐙.

**39.** 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 🐙.

40. 😬... hay que hacerlo! 🏠

Si querés mandarlo: Telegram → 📩, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 🐙.

## 🔥 Ejercicios de parciales:

🔥1. 4400 ¿Cuántos divisores distintos tiene? ¿Cuánto vale la suma de sus divisores?

Factorizo el número a estudiar:

$$4400 = 2^4 \cdot 5^2 \cdot 11$$

Quiero encontrar los divisores  $m$  de 4400, por lo tanto:

$$m \mid 4400 \Leftrightarrow m = \pm 2^\alpha \cdot 5^\beta \cdot 11^\gamma \quad \text{con} \quad \begin{cases} 0 \leq \alpha \leq 4 \\ 0 \leq \beta \leq 2 \\ 0 \leq \gamma \leq 1 \end{cases}$$

Acá un poco de teoría sobre esto. Hay entonces un total de  $(4+1) \cdot (2+1) \cdot (1+1) = 30$  divisores positivos y 60 enteros.

Busco ahora la suma de esos divisores:

$$\sum_{i=0}^4 \sum_{j=0}^2 \sum_{k=0}^1 2^i \cdot 5^j \cdot 11^k \stackrel{!}{=} \left( \sum_{i=0}^4 2^i \right) \cdot \left( \sum_{j=0}^2 5^j \right) \cdot \left( \sum_{k=0}^1 11^k \right) \stackrel{!!}{=} \frac{2^{4+1} - 1}{2 - 1} \cdot \frac{5^{2+1} - 1}{5 - 1} \cdot \frac{11^{1+1} - 1}{11 - 1} = 31 \cdot 31 \cdot 12 = 11532.$$

Donde se separaran las sumatorias, porque los factores son independientes y luego se usó la fórmula geométrica.

Concluyendo hay un total de 60 divisores distintos, cuya suma es 11532.

Dale las gracias y un poco de amor ❤️ a los que contribuyeron! Gracias por tu aporte:

👉 Nad Garraz 🐼

👉 Tobia Loni 🐼

🔥2. Hallar el menor  $n \in \mathbb{N}$  tal que:

- i)  $(n : 2528) = 316$
- ii)  $n$  tiene exactamente 48 divisores positivos
- iii)  $27 \nmid n$

Analizo los números:

$$\left\{ \begin{array}{l} \xrightarrow[\text{factorizo}]{2528} 2528 = 2^5 \cdot 79 \quad \checkmark \\ \xrightarrow[\text{factorizo}]{316} 316 = 2^2 \cdot 79 \quad \checkmark \\ \xrightarrow[\text{reescribo}]{\text{condición}} (n : 2^5 \cdot 79) = 2^2 \cdot 79 \end{array} \right. \quad \xrightarrow[\text{encontrar}]{\text{quiero}} n = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdot 5^{\alpha_5} \cdot 7^{\alpha_7} \dots 79^{\alpha_{79}} \dots$$


$$\xrightarrow{\text{como}} (n : 2^5 \cdot 79) = 2^2 \cdot 79 \xrightarrow[\text{que}]{\text{tengo}} \left\{ \begin{array}{l} \alpha_2 = 2, \\ \alpha_{79} \geq 1, \\ \xrightarrow[\text{que}]{\text{notar}} \alpha_3 < 3 \end{array} \right. \quad \begin{array}{l} \text{dado que } 2^2 \cdot 79 \mid n. \text{ busco el menor } n!. \\ \text{Al igual que antes.} \\ \text{si no } 3^3 = 27 \mid n \end{array}$$

La estrategia sigue con el primo más chico que haya:

🐼 ¿Errores? Avisá así se corrige y ganamos todos.

$$\left\{ \begin{array}{l} 48 = \underbrace{(\alpha_2 + 1)}_{2+1} \cdot (\alpha_3 + 1) \cdots \\ 48 = 3 \cdot (\alpha_3 + 1) \cdots \\ 16 = (\alpha_3 + 1) \cdot (\alpha_5 + 1) \cdot (\alpha_7 + 1) \cdots \underbrace{(\alpha_{79} + 1)}_{=2 \text{ quiero el menor}} \cdots \\ 8 = (\alpha_3 + 1) \cdot (\alpha_5 + 1) \cdot (\alpha_7 + 1) \cdots \\ 8 = \underbrace{(\alpha_3 + 1)}_{=2} \cdot \underbrace{(\alpha_5 + 1)}_{=2} \cdot \underbrace{(\alpha_7 + 1)}_{=2} \cdot 1 \cdots 1 \end{array} \right.$$

El  $n$  que cumple lo pedido sería  $n = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 79^1$

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

Arranco *comprimizando*:

$$\left\{ \begin{array}{l} a = 5c \\ b = 5d \end{array} \right. \Rightarrow (3ab : a^2 + b^2) = 25 \xrightarrow[\text{!}]{\text{coprimizar}} (3cd : c^2 + d^2) = 1$$

Esto último nos dice que las expresiones  $3cd$  y  $c^2 + d^2$  son coprimas entre sí, en otras palabras, que *no hay ningún  $p$  primo* que divida ambas expresiones a la vez.

Pruebo por absurdo que no existe  $p$  primo que divida a ambas expresiones, es decir que no existe un  $p$ , tal que  $(3cd : c^2 + d^2) = p$ . Supongo que  $\exists p$  primo tal que:

$$p \mid 3 \cdot c \cdot d \Leftrightarrow \left\{ \begin{array}{l} p \mid 3 \quad \star^1 \\ \text{o} \\ p \mid c \quad \star^2 \\ \text{o} \\ p \mid d \quad \star^3 \end{array} \right.$$

Si ocurre que  $p \mid 3 \Leftrightarrow p = 3$ . Quiero entonces ver si  $3 \mid c^2 + d^2 \Leftrightarrow c^2 + d^2 \stackrel{(3)}{\equiv} 0$ . Hago una tabla para estudiar esa última ecuación:

$r_3(c)$	0	1	2
$r_3(d)$	0	1	2
$r_3(c^2 + d^2)$	0	2	2

De la tabla concluimos que para que  $c^2 + d^2 \stackrel{(3)}{\equiv} 0$  debe ocurrir que:  $c \stackrel{(3)}{\equiv} 0$  y también que  $d \stackrel{(3)}{\equiv} 0$ , es decir que tanto  $c$  como  $d$  sean múltiplos de 3. Esto es una contradicción, ya que *no puede* ocurrir porque  $(c : d) = 1$ . Por lo tanto no puede ser que  $\star^1 p \mid 3$

Si ocurre ahora que  $\star^2 p \mid c$ , estudio a ver si también  $p \mid c^2 + d^2$ :

$$\left\{ \begin{array}{l} p \mid c \\ p \mid c^2 + d^2 \end{array} \right. \xrightarrow{F_2 - c \cdot F_1 \rightarrow F_2} \left\{ \begin{array}{l} p \mid c \\ p \mid d^2 \end{array} \right. \xleftrightarrow[p]{p} p \mid d$$

Entonces si  $p \mid c$  y también  $p \mid c^2 + d^2$  debe ocurrir que  $p \mid d$ . Nuevamente contradicción ya que *no puede ocurrir* debido a que  $(c : d) = 1$ .

El caso  $\star^3$  es lo mismo que el caso  $\star^2$ .

Se concluye entonces que  $(3cd : c^2 + d^2) = 1$  con  $(c : d) = 1$ . Así probando que  $(3ab : a^2 + b^2) = 25$  con

$$\left\{ \begin{array}{l} a = 5c \\ b = 5d \end{array} \right.$$







Entonces los  $a$  que cumplen  $a \equiv 4 \text{ (9)}$ , son candidatos para obtener  $d$ .

Tabla de restos para  $d = 3$ :

$r_3(a)$	0	1	2
$r_3(-a + 4)$	2	0	2

Entonces los  $a$  que cumplen  $a \equiv 1 \text{ (3)}$ , también son candidatos para obtener  $d$ .

Estos resultados deben cumplir la condición  $\star^1 a \equiv 7 \text{ (9)}$  como se pide en el enunciado, lo cual no es compatible con el resultado de la tabla de  $r_9$ , pero sí con la tabla  $r_3$ . Notar que:  $a = 9k + 7 \stackrel{(3)}{\equiv} 1$ .

Finalmente el MCD con  $a \in \mathbb{Z}$  que cumplan que  $32a \equiv 17 \text{ (9)}$

$$(a^3 + 4a + 1 : a^2 + 2) = 3 \quad \checkmark$$

8. Sea  $(a_n)_{n \in \mathbb{N}_0}$  con  $\begin{cases} a_0 = 1 \\ a_1 = 3 \\ a_n = a_{n-1} - a_{n-2} \quad \forall n \geq 2 \end{cases}$

a) Probar que  $a_{n+6} = a_n$

b) Calcular  $\sum_{k=0}^{255} a_k$

(a) Por inducción:

$$p(n) : a_{n+6} = a_n \quad \forall n \geq \mathbb{N}_0$$

Primero notar que:

$$\left\{ \begin{array}{l} a_0 = 1 \\ a_1 = 3 \\ a_2 \stackrel{\text{def}}{=} 2 \star^1 \\ a_3 \stackrel{\text{def}}{=} -1 \\ a_4 \stackrel{\text{def}}{=} -3 \\ a_5 \stackrel{\text{def}}{=} -2 \end{array} \right\} \rightarrow \left\{ \begin{array}{l} a_6 \stackrel{\text{def}}{=} 1 \\ a_7 \stackrel{\text{def}}{=} 3 \\ a_8 \stackrel{\text{def}}{=} 2 \star^1 \\ a_9 \stackrel{\text{def}}{=} -1 \\ a_{10} \stackrel{\text{def}}{=} -3 \\ a_{11} \stackrel{\text{def}}{=} -2 \end{array} \right\}$$

Se ve que tiene un período de 6 elementos.

Caso Base:  $p(2) : a_8 \stackrel{?}{=} a_2 \quad \checkmark$

Paso inductivo: Asumo que

$$p(k) : \underbrace{a_{k+6} = a_k}_{\text{hipótesis inductiva}} \text{ para algún } k \geq \mathbb{N}_{\geq 2}$$

entonces quiero probar que,

$$p(k+1) : a_{k+1+6} = a_{k+1}$$

también sea verdadera.

Parto desde  $p(k+1)$

$$a_{k+7} \stackrel{\text{def}}{=} a_{k+6} - a_{k+5} \stackrel{\text{HI}}{=} a_k - a_{k+5} \stackrel{\text{def}}{=} a_k - (a_k + a_{k+4}) = -a_{k+4} \Rightarrow a_{k+7} = -a_{k+4} \quad \checkmark$$

Ahora uso la definición de manera sucesiva:

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

Como  $p(2), p(3), p(4), p(5), p(k)$  y  $p(k+1)$  son verdaderas por el principio de inducción  $p(n)$  también es verdadera  $\forall n \in \mathbb{N}_{\geq 2}$

$$(b) \sum_{k=0}^{255} a_k = \underbrace{a_0 + a_1 + a_2 + a_3 + a_4 + a_5}_{=0} + \underbrace{a_6 + a_7 + a_8 + a_9 + a_{10} + a_{11}}_{=0} + \cdots + a_{252} + a_{253} + a_{254} + a_{255}$$

En la sumatoria hay **256 términos**.  $256 = 42 \cdot 6 + 4$  por lo tanto van a haber 42 bloques que dan 0 y sobreviven los últimos 4 términos.  $\sum_{k=0}^{255} a_k = \underbrace{0 + 0 + \cdots + 0}_{42 \text{ ceros}} + a_{252} + a_{253} + a_{254} + a_{255} =$

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

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

**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.

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

$$\star^1 \left\{ \begin{array}{l} 10a - 15 \mid 4a^2 - 13a + 8 \\ 10a - 15 \mid 10a - 15 \end{array} \right. \xrightarrow[\text{varias}]{\text{operaciones}} \left\{ \begin{array}{l} 10a - 15 \mid -25 \star^2 \\ 10a - 15 \mid 10a - 15 \end{array} \right.$$

Para que ocurra  $\star^1$ , debe ocurrir  $\star^2$ .

$$10a - 15 \mid -25 \iff 10a - 25 \in \{\pm 1, \pm 5, \pm 25\} \star^3 \text{ para algún } a \in \mathbb{Z}. \quad \checkmark$$

De paso observo que  $|10a - 25| \leq 25$ . Busco  $a$ :

$$\begin{cases} \text{Caso: } d = 10a - 15 = 1 & \iff a = \frac{8}{5} \quad \text{☹} \\ \text{Caso: } d = 10a - 15 = -1 & \iff a = \frac{8}{5} \quad \text{☹} \\ \text{Caso: } d = 10a - 15 = 5 & \iff a = 2 \quad \checkmark \\ \text{Caso: } d = 10a - 15 = -5 & \iff a = 1 \quad \checkmark \\ \text{Caso: } d = 10a - 15 = 25 & \iff a = 4 \quad \checkmark \\ \text{Caso: } d = 10a - 15 = -25 & \iff a = -1 \quad \checkmark \end{cases}$$

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

$$\begin{array}{llll} d = 5 & a = 2 & \Rightarrow 4 \cdot 2^2 - 13 \cdot 2 + 8 = -2 & \rightarrow 5 \nmid -2 \quad \text{☹} \\ d = -5 & a = 1 & \Rightarrow 4 \cdot 1^2 - 13 \cdot 1 + 8 = 1 & \rightarrow -5 \nmid 1 \quad \text{☹} \\ d = 25 & a = 4 & \Rightarrow 4 \cdot 4^2 - 13 \cdot 4 + 8 = 4 & \rightarrow 25 \nmid 4 \quad \text{☹} \\ d = -25 & a = -1 & \Rightarrow 4 \cdot (-1)^2 - 13 \cdot (-1) + 8 = 25 & \rightarrow -25 \mid 25 \quad \checkmark \end{array}$$

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

*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:

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

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

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

**10.** Sea  $(a_n)_{n \in \mathbb{N}}$  la sucesión dada por recurrencia:

$$\begin{cases} a_1 = 30, \\ a_2 = 16, \\ a_{n+2} = 24a_{n+1} + 65^n a_n + 96n^4 \quad \forall n \geq 1. \end{cases}$$

Probar que  $a_n \equiv 3^n - 5^n \pmod{32}$ ,  $\forall n \geq 1$ .

Ejercicio intimidante a primera vista. Acomodemos un poco el enunciado así hacemos inducción.

Estoy buscando el módulo 32,  $a_{n+2}$  queda más amigable:  $\star^1 a_{n+2} \stackrel{(32)}{\equiv} 24a_{n+1} + a_n \quad \checkmark$

*Inducción:*

$$p(n) : a_n \equiv 3^n - 5^n \pmod{32} \quad \forall n \in \mathbb{N}$$

*Casos base:*

$$\begin{cases} p(1) : a_1 \equiv 3 - 5 \pmod{32} & \iff a_1 \equiv 30 \pmod{32} & \checkmark & p(1) \text{ resultó verdadera.} \\ p(2) : a_2 \equiv 3^2 - 5^2 \pmod{32} & \iff a_2 \equiv 16 \pmod{32} & \checkmark & p(2) \text{ resultó verdadera.} \end{cases}$$

*Pasos inductivos:*

Para algún  $k \in \mathbb{Z}$ :

$$\begin{cases} p(k) : \overbrace{a_k \equiv 3^k - 5^k \pmod{32}}^{\text{hipótesis inductiva}} & \text{Se asume verdadera.} \\ p(k+1) : \overbrace{a_{k+1} \equiv 3^{k+1} - 5^{k+1} \pmod{32}}^{\text{también hipótesis inductiva}} & \text{También se asume verdadera.} \end{cases}$$

Y queremos probar entonces que:

$$p(k+2) : a_{k+2} \equiv 3^{k+2} - 5^{k+2} \pmod{32}$$


Arranco con la definición de la sucesión que se cocinó un poco en  $\star^1$ :

$$a_{k+2} \stackrel{\text{def}}{=} 24a_{k+1} + 65^k a_k + 96k^4 \stackrel{(32)}{\equiv} 24(\overbrace{3^{k+1} - 5^{k+1}}^{HI}) + \overbrace{3^k - 5^k}^{!!} \stackrel{!!}{=} 73 \cdot 3^k - 121 \cdot 5^k \stackrel{(32)}{\equiv} 9 \cdot 3^k - 25 \cdot 5^k = 3^{k+2} - 5^{k+2} \checkmark$$


Si te quedaste picando en  $!!$ , seguí mirando ese paso, porque son cuentas que tenés que poder encontrar mirando fijo el tiempo que sea necesario. Por mi parte 🍷.

Y así fue como comprobamos que el enunciado ladraba pero no mordía.

Como  $p(1)$ ,  $p(2)$ ,  $p(k)$ ,  $p(k+1)$  y  $p(k+2)$  son verdaderas, por el principio de inducción también lo será  $p(n) \forall n \in \mathbb{N}$ .

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

 **11.** Estudiar los valores para **todos** los  $a \in \mathbb{Z}$  de  $(a^3 + 31 : a^2 - a + 1)$ .

Simplifico la expresión  $(a^3 + 31 : a^2 - a + 1)$  con el querido algoritmo de Euclides:

$$\begin{array}{r} X^3 \qquad \qquad + 31 \mid X^2 - X + 1 \\ - X^3 + X^2 - X \qquad \qquad \mid X + 1 \\ \hline X^2 - X + 31 \\ - X^2 + X \qquad - 1 \\ \hline 30 \end{array}$$

Por lo tanto el mcd  $d = (a^3 + 31 : a^2 - a + 1) = (a^2 - a + 1 : 30)$ , es decir que:


$$d \mid 30 \Rightarrow d \in \{1, 2, 3, 5, 6, 10, 15, 30\}$$

Muchos divisores. Se pueden eliminar unos cuantos notando que  $a^2 - a + 1$  es una expresión siempre impar. Una forma de mostrar esto:

$$a^2 - a + 1 \text{ es impar} \Leftrightarrow a^2 - a + 1 \equiv 1 \pmod{2} \stackrel{!}{\Leftrightarrow} a \cdot (a - 1) \equiv 0 \pmod{2}$$

La última expresión  $a \cdot (a - 1)$  es siempre **par**, dado que es un número multiplicado por su consecutivo. Otra forma de mostrar la paridad sería reemplazando por  $2k$  y luego por  $2k + 1$  y ver que los resultados son siempre impares.

$$\begin{aligned} a = \underbrace{2k}_{\text{par}} &\Rightarrow (2k)^2 - 2k + 1 = \overbrace{2 \cdot (2k^2 - k) + 1}^{\text{impar}} \quad \checkmark \\ a = \underbrace{2k + 1}_{\text{impar}} &\Rightarrow (2k + 1)^2 - 2(k + 1) + 1 = \overbrace{2 \cdot (2k^2 + 3k + 2) + 1}^{\text{impar}} \quad \checkmark \end{aligned}$$

Hacé lo que más te guste 

Dado que esa expresión es impar podemos reducir el conjunto de divisores a:

$$d \mid 30 \quad \text{y} \quad d \equiv 1 \pmod{2} \Rightarrow d \in \{1, 3, 5, 15\}.$$

*Tabla de restos:* Siempre empezando por el menor valor


$r_3(a)$	0	1	2
$r_3(a^2 - a + 1)$	1	1	<b>0</b>

Obtenemos que 3 *es un potencial mcd* cuando  $r_3(a) = 2$  o dicho de otro modo  $a \equiv 2 \pmod{3}$ .

$r_5(a)$	0	1	2	3	4
$r_5(a^2 - a + 1)$	1	1	3	2	3


Obtenemos que 5 *no es un potencial mcd*, por lo que 15 tampoco será un divisor de la expresión  $a^2 - a + 1$ . Con la información obtenida se puede concluir que:

$$d = \begin{cases} 3 & \text{si } a \equiv 2 \pmod{3} \\ 1 & \text{si } a \not\equiv 2 \pmod{3} \end{cases}$$

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

 Maxi T. 

 **12.** Determinar para cada par  $(a, b) \in \mathbb{Z}^2$  tal que  $(a : b) = 7$  el valor de

$$(a^2 b^4 : 7^5(-a + b)).$$

*Coprimizar:*

$$d = (a^2 b^4 : 7^5(-a + b)) \xleftrightarrow[b=7B]{a=7A} 7^6 \cdot (A^2 B^4 : B - A) \Leftrightarrow d = 7^6 \cdot D$$

$$\begin{cases} D \mid A^2 B^4 \\ D \mid B - A \xleftrightarrow{\text{def}} B \equiv A(D) \star^1 \end{cases}$$

$$\begin{cases} D \mid A^2 B^4 \xleftrightarrow{\star^1} \boxed{B^6 \equiv 0(D)} \\ \text{y también} \\ D \mid A^2 B^4 \xleftrightarrow{\star^1} \boxed{A^6 \equiv 0(D)} \end{cases}$$

El resultado dice que  $D \mid A^6$  y que  $D \mid B^6$  lo cual está complicado porque  $A$  y  $B$  son coprimos, por lo tanto  $A^6$  y  $B^6$  también y  $(A^6 : B^6) \star^2 = 1 = D$ .


$\star^2$  la factorización en primos lo muestra, mismos factores elevados a la 6, no puede cambiar la coprimisimilitubilidad.

Creo que hay que justificar con algo más, pero no sé, con algo de primos? Bueh, algo así:


Si  $D \mid A^6$  entonces la *descomposición en primos* de  $D = p_1^{i_d} \cdots p_n^{j_d}$  tiene que tener solo factores de la *descomposición en primos* de  $A^6 = p_1^i \cdots p_n^j \cdot p_{n+1}^k \cdots p_m^l$  con los exponentes de los factores de  $D (i_d, j_d, \dots)$ , menores o iguales a los exponentes de  $A^6 (i, j, \dots)$  de manera que al dividir:

$$\frac{A^6}{D} = \frac{p_1^i \cdots p_n^j \cdot p_{n+1}^k \cdots p_m^l}{p_1^{i_d} \cdots p_n^{j_d} \cdot p_{n+1}^{k_d} \cdots p_m^{l_d}} = \frac{\overbrace{p_1^{i-i_d}}^{0 \leq} \cdots \overbrace{p_n^{j-j_d}}^{0 \leq} \cdot \overbrace{p_{n+1}^{k-k_d}}^{0 \leq} \cdots \overbrace{p_m^{l-l_d}}^{0 \leq}}{1},$$

es decir que se cancele todo de manera que quede un **1** en el denominador. Eso es que  $D \mid A^6$  ni más ni menos.

Y sí, *muy rico todo*, pero esa cantinela es la misma para  $D \mid B^6$ , **pero** la *descomposición en primos* de  $B^6$  tiene los  $p_i$  **distintos** a los de  $A^6$ , porque  $(A^6 : B^6) = 1!$  y ahí llegamos al absurdo.  $D$  no puede dividir a ambos a la vez, **porque son coprimos** , a menos que  $D = 1$  ✓.

$$D = 1 \Rightarrow \boxed{d = 7^6}, \text{ para cada } (a, b) \in \mathbb{Z}^2 / (a : b) = 7$$

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

 **13.** Calcular  $(a \cdot b^2 : 3a^2 + 3b^2)$  para cada par de enteros  $a$  y  $b$  tales que  $(a : b) = 3$ .

Hay que *coprimizar*, encontrar posibles divisores, interpretar resultado.

*Coprimizar:*

$$(a : b) = 3 \Leftrightarrow \left(\frac{a}{3} : \frac{b}{3}\right) = 1 \xleftrightarrow[b=3B]{a=3A} (A : B) = 1 \Leftrightarrow A \perp B.$$

Reemplazo y acomodo:

$$d = (a \cdot b^2 : 3a^2 + 3b^2) \xrightarrow{!} d = 27(A \cdot B^2 : A^2 + B^2) \xleftrightarrow{d=27D} D = (A \cdot B^2 : A^2 + B^2) \text{ con } A \perp B$$

Dado que  $D$  es el mcd, tiene que cumplir que:

$$\left\{ \begin{array}{l} D \mid A \cdot B^2 \\ D \mid A^2 + B^2 \end{array} \right. \xrightarrow{!!} \left\{ \begin{array}{l} D \mid A^3 \\ D \mid B^4 \end{array} \right.$$

Oka, ahí en el **!!** hice lo de siempre: Multiplique una fila por  $A$  o  $B$  y resté y coso.


Lo que nos queda es algo muy parecido a lo que pasó en el ejercicio [éste](#)(click).

Interpretación:

Tenemos que  $D$  por su condición de divisor común debe dividir a dos número *coprimos*, dado que si  $A \perp B$  también sucede que  $A^3 \perp B^4$ , because *primos and shit*, y bueh, ¿Puede ser eso posible?.. Sí! Cuando  $D = 1$ .

Entonces:

$$D = 1 \Rightarrow d = 27 \text{ para cada par } (a, b) \in \mathbb{Z} / (a : b) = 3$$

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

 **14.** Calcular, para cada  $n \in \mathbb{N}$ , el resto de dividir por 18 a

$$6 \cdot 35^n + 73^{3021} + \sum_{k=1}^n 3^k \cdot k!$$

Simplifiquemos esa expresión espantosa calculando el  $r_{18}$  y aplicando las propiedades:

$$\begin{aligned} r_{18}(6 \cdot 35^n + 73^{3021} + \sum_{k=1}^n 3^k \cdot k!) &\stackrel{!}{=} r_{18}(6 \cdot (-1)^n + 1^{3021} + r_{18}(\sum_{k=1}^n 3^k \cdot k!)) \\ &\stackrel{\star^1}{=} \begin{cases} r_{18}(7 + r_{18}(\sum_{k=1}^n 3^k \cdot k!)) & \text{si } n \text{ es par} \\ r_{18}(-5 + r_{18}(\sum_{k=1}^n 3^k \cdot k!)) & \text{si } n \text{ es impar} \end{cases} \end{aligned}$$

La para está ahora en calcular:  $r_{18}(\sum_{k=1}^n 3^k \cdot k!)$

Dado que tiene un 3 ahí dando vueltas y que la  $k!$  en algún momento tendrá el factor  $6 = 3! = 2 \cdot 3$ , es esperable que el término general de la sumatoria sea un múltiplo de 18.

Acomodo la expresión:

$$r_{18}(\sum_{k=1}^n 3^k \cdot k!) = r_{18}(3 + \sum_{k=2}^n 3^k \cdot k!) \stackrel{\star^2}{=} 3 + r_{18}(\sum_{k=2}^n 3^k \cdot k!)$$

A ojo se puede ver que  $r_{18}(\sum_{k=2}^n 3^k \cdot k!) = 0 \quad \forall n \in \mathbb{N}_{\geq 2}$  Pero como no sabemos si el que nos corrige está de mal humor probemos eso por inducción:



Quiero probar que:

$$p(n) : r_{18}\left(\sum_{k=2}^n 3^k \cdot k!\right) = 0 \quad \forall n \in \mathbb{N}_{\geq 2}$$

Caso base:

$$p(2) : r_{18}\left(\sum_{k=2}^2 3^k \cdot k!\right) = r_{18}(3^2 \cdot 2) = 0$$

Por lo que el caso  $p(2)$  es verdadero.

Paso inductivo: Asumo que para algún  $k \geq 2$

$$p(h) : r_{18}\left(\underbrace{\sum_{k=2}^h 3^k \cdot k!}_{\text{hipótesis inductiva}}\right) = 0$$

es verdadero. Y quiero probar que:

$$p(h+1) : r_{18}\left(\sum_{k=2}^{h+1} 3^k \cdot k!\right) = 0$$

también lo sea.

Partiendo de  $p(h+1)$

$$\begin{aligned} r_{18}\left(\sum_{k=2}^{h+1} 3^k \cdot k!\right) &= r_{18}\left(\sum_{k=2}^h 3^k \cdot k! + 3^{h+1} \cdot (h+1)!\right) \\ &\stackrel{\text{HI}}{=} r_{18}(3^{h+1} \cdot (h+1)!) \\ &\stackrel{!}{=} r_{18}(3 \cdot 6 \cdot 3^h \cdot \frac{(h+1)!}{3!}) \\ &= 0 \end{aligned}$$

Ahí en el  $!$  me las arreglé para que aparezca el 18 que hace que el resto de 0. Debe haber otras formas de hacerlo, tenés licencia para dibujar.


Como  $p(2), p(h)$  y  $p(h+1)$  resultaron verdaderas, por criterio de inducción  $p(n)$  también lo es para todo  $n \in \mathbb{N}_{\geq 2}$

Volviendo a  $\star^2$ :

$$r_{18}\left(\sum_{k=1}^n 3^k \cdot k!\right) = 3$$


por lo tanto en  $\star^1$ :

$$r_{18}(6 \cdot 35^n + 73^{3021} + \sum_{k=1}^n 3^k \cdot k!) = \begin{cases} r_{18}(6 + 1 + 3) = 10 & \text{si } n \text{ es par} \\ r_{18}(-6 + 1 + 3) \stackrel{!}{=} 16 & \text{si } n \text{ es impar} \end{cases}$$

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

 Dani Tadd 

 **15.** Sean  $a, b \in \mathbb{Z}$  tales que  $(a : b) = 1$ . Calcular los posibles valores de  $(a^2 + 3b^2 : 2a^2 + 11b^2)$  y dar un ejemplo para cada uno de ellos.

Si  $d = (a^2 + 3b^2 : 2a^2 + 11b^2)$  entonces deber suceder:

$$\left\{ \begin{array}{c} d \mid a^2 + 3b^2 \\ d \mid 2a^2 + 11b^2 \end{array} \right\} \xleftrightarrow{F_2 - 2F_1 \rightarrow F_2} \left\{ \begin{array}{c} d \mid a^2 + 3b^2 \\ d \mid 5b^2 \end{array} \right\} \quad \text{y} \quad \left\{ \begin{array}{c} d \mid a^2 + 3b^2 \\ d \mid 2a^2 + 11b^2 \end{array} \right\} \xleftrightarrow{11F_1 - 3F_2 \rightarrow F_2} \left\{ \begin{array}{c} d \mid a^2 + 3b^2 \\ d \mid 5a^2 \end{array} \right\}$$

De esta forma queda que el MCD:

$$d = (5a^2 : 5b^2) \Leftrightarrow d = 5(a^2 : b^2) \Leftrightarrow d = 5(a : b)^2 \xleftrightarrow{a \perp b} d = 5$$

Si el *máximo común divisor* de  $(a^2 + 3b^2 : 2a^2 + 11b^2)$  es 5, los valores que puede *potencialmente* tomar la expresión son:

$$\{1, 5\}$$

*División por 1:*

El uno está por ejemplo para el par  $(a, b) = (1, 2)$  donde  $a \perp b$ .

*División por 5:*

$r_5(a)$	0	1	2	3	4
$r_5(a^2)$	0	1	4	4	1

y

$r_5(b)$	0	1	2	3	4
$r_5(3b^2)$	0	3	2	2	3

y


$r_5(a^2 + 3b^2)$	0	4	1	1	4
-------------------	---	---	---	---	---

Ese resultado dice que para que suceda que  $5 \mid a^2 + 3b^2$  se requiere que:

$$a \equiv 0 \pmod{5} \quad \text{y} \quad b \equiv 0 \pmod{5}$$

Peeeeero, por enunciado  $(a : b) = 1$  así que se concluye que no hay par de  $(a, b)$  con  $a \perp b$  tal que  $5 \mid a^2 + 3b^2$ .

Así que el único valor que puede tomar la expresión  $(a^2 + 3b^2 : 2a^2 + 11b^2)$  es 1.

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Ale Teran 

 Nad Garraz 

 **16.** Calcular el resto de dividir

$$\sum_{k=4}^{134} (k! + k^3)$$

por 7.

Nos piden calcular el resto 7 de esa porquería:

$$\sum_{k=4}^{134} (k! + k^3) = \sum_{k=4}^{134} k! + \sum_{k=4}^{134} k^3$$

Arranco por estudiar  $\sum_{k=4}^{134} k^3$ . Tabla de restos 7 de  $k^3$ :

$r_7(k)$	0	1	2	3	4	5	6
$r_7(k^3)$	0	1	1	6	1	6	6

Pensar que  $6 \equiv -1 \pmod{7}$  y eso nos ayuda a anular muchas cosas:

$$\sum_{k=4}^{134} k^3 = 4^3 + 5^3 + 6^3 + 7^3 + 8^3 + \dots + 130^3 + 131^3 + 132^3 + 134^3$$

131 términos

Todos esos términos tienen  $r_7$  igual a 0, 1 o  $-1$ . Sumando 7 términos consecutivos se obtiene como resultado 0. Organizo los términos teniendo en cuenta que  $131 = 18 \cdot 7 + 5$ , es decir que tengo 18 sumas de 7 términos que dan 0 y me sobran los últimos 5 términos:

$$\begin{aligned} \sum_{k=4}^{134} k^3 &= 4^3 + 5^3 + 6^3 + 7^3 + 8^3 + 9^3 + 10^3 + \dots + 126^3 + 124^3 + 125^3 + 126^3 + 127^3 + 128^3 + 129^3 + 130^3 + 131^3 + 132^3 + 133^3 + 134^3 \\ &\equiv \underbrace{1 + (-1) + (-1) + 0 + 1 + 1 + (-1)}_{=0} + \dots + \underbrace{1 + (-1) + (-1) + 0 + 1 + 1 + (-1)}_{=0} + \underbrace{1 + (-1) + (-1) + 0 + 1}_{=0} \pmod{7} \\ &\stackrel{!}{=} 18 \cdot 0 + 0 \pmod{7} \equiv 0 \pmod{7} \end{aligned}$$

Se concluye que:

$$r_7\left(\sum_{k=4}^{134} k^3\right) = 0 \quad \star^1$$

Ahora quiero ver qué onda con  $\sum_{k=4}^{134} k!$ .

Noto primero que cuando  $k \geq 7$  el número  $k!$  es un múltiplo de 7, es decir:


$$k! \equiv 0 \pmod{7} \quad \text{con } k \in \mathbb{N}_{\geq 7}$$

Por lo tanto me quedaría con los primeros 3 términos:

$$\sum_{k=4}^{134} k! = 4! + 5! + 6! + \underbrace{0 + \dots + 0}_{131 \text{ términos igual a } 0} \equiv 3 + 1 + 6 \pmod{7} \equiv 3 + 1 + 6 \pmod{7} \equiv 3 \pmod{7} \quad \star^2$$


Por último juntando los resultados de  $\star^1$  y  $\star^2$ :

$$r_7\left(\sum_{k=4}^{134} (k! + k^3)\right) = 3$$

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

 Juan Parajó 

 **17.** Hallar todos los valores de  $a \in \mathbb{Z}$  tales que  $(3a + 6 : 7a^2 - a - 3) \neq 1$ .

Si el mcd es  $d$ :

$$d = (3a + 6 : 7a^2 - a - 3)$$

Puedo usar Euclides para simplificar la expresión del mcd:

$$\begin{array}{r|l} 7a^2 & -a & -3 \\ -7a^2 - 14a & & \\ \hline & -15a & -3 \\ & 15a + 30 & \\ \hline & & 27 \end{array}$$

Por lo tanto  $d$  queda:

$$d = (3a + 6 : 7a^2 - a - 3) = (3a + 6 : 27)$$

Por lo tanto como  $d \mid 27$ :

$$d \in \{1, 3, 9, 27\} = \{1, 3, 3^2, 3^3\}$$

¿Para que valor de  $a$  valdrá  $d = 1$ ? Empiezo a ver si es divisible por 3:


Tabla de restos para  $d = 3$ :

$r_3(a)$	0	1	2
$r_3(3a + 6)$	0	0	0
$r_3(7a^2 - a - 3)$	0	0	2

Dado que el resto de los posibles divisores, 9 y 27 son potencias de 3, se concluye que:

$$d = 1 \iff a \equiv 2 \pmod{3}$$

Dado que para esos valores de  $a$  la expresión  $7a^2 - a - 3$  no es divisible por ninguna potencia de 3

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 