Álgebra I
Práctica 4 Resuelta

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

Choose your destiny:

(dobleclick 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 Extras

🔥1.	**🔥3.**	**🔥5.**	**🔥7.**	**🔥9.**	**🔥11.**	**🔥13.**
🔥2.	**🔥4.**	**🔥6.**	**🔥8.**	**🔥10.**	**🔥12.**	

Notas teóricas:

Divisibilidad:

- Definición divisibilidad:

$$d \text{ divide a } a \xLeftrightarrow[\text{que decir}]{\text{es lo mismo}} a \text{ es un múltiplo entero de } d$$
$$d \,|\, a \iff \exists k \in \mathbb{Z} \text{ tal que } a = k \cdot d$$

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

- $d \,|\, 0$, dado que $0 = 0 \cdot d$. Se desprende que $\mathcal{D}(0) = \{\mathbb{Z} - \{0\}\}$

- A la hora de divisibilidad *los signos no importan:*

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

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

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

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

Definición congruencia:

- *Definición congruencia:*

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

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

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

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

$$\begin{cases} a_1 \equiv b_1 \ (d) \\ \quad \vdots \\ a_n \equiv b_n \ (d) \end{cases} \Rightarrow a_1 \cdots a_n \equiv a_b \cdots b_n \ (d)$$

Un caso particular con un simpático resultado:

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

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 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 a entre d:
$$a \equiv r_d(a)\ (d).$$
- Si d divide al número a, entonces el resto de la división es 0:
$$r_d(a) = 0 \iff d \,|\, a \iff a \equiv 0\ (d)$$
- 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,
$$\left\{ \begin{array}{c} a \equiv r_d(a)\ (d) \\ b \equiv r_d(b)\ (d) \end{array} \right\} \xRightarrow[\text{ecuaciones}]{\text{sumo}} a + b \equiv r_d(a) + r_d(b)\ (d)$$
y,
$$\left\{ \begin{array}{c} a \equiv r_d(a)\ (d) \\ b \equiv r_d(b)\ (d) \end{array} \right\} \xRightarrow[\text{ecuaciones}]{\text{multiplico}} a \cdot b \equiv r_d(a) \cdot r_d(b)\ (d)$$

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:
$$\boxed{\text{máximo común divisor: MCD} = (a : b)}$$
- $(a : b) \in \mathbb{N}$ (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 $(a : 0) = |a|, \quad \forall a \in \mathbb{Z} - \{0\}$
- si $b \,|\, a \Rightarrow (a : b) = |b|$ 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 feos. Hay que saber hacer esto. Fin. ¡Se usa de acá hasta el final de la materia!.
- *Combinacion Entera*: Otra herramienta gloriosa que sale de hacer *Euclides*. ¡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:

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

  - Sea $c \in \mathbb{Z}$ entonces $\exists\, s', t' \in \mathbb{Z}$ con $c = s'a + t'b \iff (a : b) \,|\, c$.
  - 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 $(a : b) = 1$

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

- Sean $a, b \in \mathbb{Z}$ no ambos nulos.*coprimizar* los números es dividirlos por su máximos 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:

$$c \,|\, a \quad \text{y} \quad d \,|\, a \quad \text{y} \quad c \perp d \overset{!!}{\iff} c \cdot d \,|\, a$$

  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:

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

  - *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:

$$\begin{cases} (a : p) = 1 \iff p \not\mid a \\ (a : p) = p \iff p \mid a \end{cases}$$

  - 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

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

  - 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.
    * $(a : b) = 1 \quad \text{y} \quad (a : c) = 1 \iff (a : bc) = 1$
    * $(a : b) = 1 \iff (a^m : b^n) = 1, \quad \forall m, n \in \mathbb{N}$
    * $(a^n : b^n) = (a : b)^n \;\; \forall n \in \mathbb{N}$
  - 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) $a \cdot b \mid c \Rightarrow a \mid c \quad \text{y} \quad b \mid c$

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

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

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

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

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

g) $a \mid b \Rightarrow a \leq b$

h) $a \mid b \Rightarrow |a| \leq |b|$

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

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

---

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

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

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

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

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 →, o mejor aún si querés subirlo en LaTeX→.

g) ______________________________

... hay que hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

h) ______________________________

... hay que hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

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

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

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

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:

$$a \mid b \overset{\text{HI}}{\Longrightarrow} a^k \mid b^k \Leftrightarrow a^k \cdot c = b^k \overset{\times b}{\Longleftrightarrow} b \cdot a^k \cdot c = b^{k+1} \underset{a \cdot d = b}{\overset{a \mid b}{\Longleftrightarrow}} a \cdot d \cdot a^k \cdot c = a^{k+1} \cdot (cd) = b^{k+1} \Leftrightarrow a^{k+1} \mid b^{k+1}.$$

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:

$$a \mid b \Rightarrow a^n \mid b^n \iff b \equiv 0 \ (a) \Rightarrow b^n \equiv 0 \ (a^n) \xLeftrightarrow{0 \overset{(a^n)}{\equiv} a^n} b^n \equiv a^n \ (a^n)$$

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

---

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

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

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

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

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

---

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

Busco eliminar la n del *miembro* derecho.

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

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

b)

c)

d) $n-2 \,|\, n^3-8$

$\xrightarrow[\Rightarrow a\,|\,k\cdot b]{a\,|\,b} n-2 \,|\, \underbrace{(n-2)\cdot(n^2+2n+4)}_{n^3-8}$ Esto va a dividir para todo $n \neq 2$

---

3. Sean $a.b \in \mathbb{Z}$.

a) Probar que $a-b \,|\, a^n-b^n$ 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 $a+b \,|\, a^n-b^n$.

c) Probar que si n es un número natural impar y $a \neq -b$, entonces $a+b \,|\, a^n+b^n$.

---

a) *Inducción:*

Proposición:

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

Caso Base:

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

$p(1)$ es verdadera. ✓

Paso inductivo:

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

$$\begin{cases} a-b \,|\, a^k-b^k \\ a-b \,|\, a^k-b^k \end{cases} \overset{\times a}{\underset{\times b}{\Longrightarrow}} \begin{cases} a-b \,|\, a^{k+1}-ab^k \\ a-b \,|\, ba^k-b^{k+1} \end{cases} \overset{+}{\Longrightarrow} \left\{ \, a-b \,|\, a^{k+1}-b^{k+1}. \quad \checkmark \right.$$

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

b) Sé que

$$a+b \,|\, a+b \overset{\text{def}}{\Longleftrightarrow} a \equiv -b \; (a+b)$$

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

$$\begin{cases} a\cdot a = a^2 \overset{(a+b)}{\equiv} a\cdot(-b) \overset{(a+b)}{\equiv} (-1)^2 b \\ \quad\vdots \qquad \leftarrow \bigstar^1 \\ a^n \overset{(a+b)}{\equiv} (-1)^n\cdot b^n \rightarrow \begin{cases} a^n \equiv b^n \; (a+b) & \text{con n par} \\ a^n \equiv (-1)^n\cdot b^n \; (a+b) & \text{con n impar} \end{cases} \end{cases}$$

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

$\bigstar^1$ *Inducción:*

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

Caso base:

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

$p(1)$ 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

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

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

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:

$$p(1) \ : \ 2^3 = 8 \mid a^2 - 1 = (a-1) \cdot (a+1)$$

$$\xrightarrow[a = 2m-1]{a \text{ es impar, si } m \in \mathbb{Z}} \star^1$$

$$(a-1) \cdot (a+1) \overset{\star^1}{=} (2m-2) \cdot (2m) \overset{!}{=} 4 \cdot \underbrace{m \cdot (m-1)}_{par:\ 2h,\ h \in \mathbb{Z}} = 4 \cdot 2h = 8 * h$$

$$\xrightarrow[\text{tanto}]{\text{por lo}}$$

$$8 \mid 8h = (a-1) \cdot (a+1) \text{ para algún } h \in \mathbb{Z} \quad \checkmark$$

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

Paso inductivo:

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

$$2^{k+3} \mid a^{2^{k+1}} - 1 \overset{!}{\iff} 2^{k+2} \cdot 2 \mid (a^{2^k} - 1) \cdot \overbrace{(a^{2^k} + 1)}^{\text{par !}}$$

$$\xLeftarrow[\text{hipótesis inductiva}]{\text{Si } a \mid b \text{ y } c \mid d \Rightarrow ac \mid bd}$$

$$2^{k+2} \cdot 2 \mid (a^{2^k} - 1) \cdot \underbrace{(a^{2^k} + 1)}_{\text{par}}.$$

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

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

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

---

5. ... hay que hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

6.

a) Probar que el producto de n enteros consecutivos es divisible por $n!$

b) Probar que $\binom{2n}{n}$ es divisible por 2.

... hay que hacerlo!

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

---

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

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

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

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

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

---

a) $99 \mid 10^{2n} + 197 \overset{\text{def}}{\iff} 10^{2n} + 197 \equiv 0\ (99) \to 10^{2n} + 198 \equiv 1\ (99) \to 10^{2n} + \underbrace{198}_{\overset{(99)}{\equiv} 0} \equiv 1\ (99) \to 100^n \equiv 1\ (99) \to$

$$\left\{ \xrightarrow[\text{que}]{\text{sé}} 100 \equiv 1\ (99) \iff 100^2 \equiv \underbrace{100}_{\overset{(99)}{\equiv} 1}\ (99) \to 100^2 \equiv 1\ (99) \iff \dots \iff 100^n \equiv 1\ (99) \right.$$

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

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

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

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

c) ... hay que hacerlo!

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

d) ... hay que hacerlo!

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

Algoritmo de División:

---

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

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

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

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

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

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

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

---

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

b)

c) $a = 3b + 7 \to$ me interesa: $\to \left\{ \begin{array}{l} |b| \leq |a| \quad \checkmark \\ 0 \leq r < |b| \quad \checkmark \end{array} \right\} \to$

$$\to \left\{ \begin{array}{l} \text{Si: } |b| > 7 \to (q, r) = (3, 7) \\ \text{Si: } |b| \leq 7 \to (q, r) = (3, 7) \\ \begin{array}{|c|c|c|c|c|c|c|} \hline (a,b) & (-14,-7) & (-11,-6) & (-8,-5) & (-5,-4) & (4,-1) & \dots \\ \hline (q,r) & (2,0) & (2,1) & (2,2) & (2,3) & (4,0) & \dots \\ \hline \end{array} \end{array} \right.$$

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

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

---

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

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

---

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

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

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

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

Ahora que sé que $r_{28}(a) = 1$ 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 $a \equiv 22\ (14)$, hallar el resto de dividir a a por 14, por 2 y por 7.

b) Si $a \equiv 13\ (5)$, 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) $$\begin{cases} a \equiv 22\ (14) \to a = 14 \cdot q + \underbrace{22}_{14+8} = 14 \cdot (q+1) + 8 \xrightarrow[\text{es}]{\text{el resto}} r_{14}(a) = 8 \quad \checkmark \\ a \equiv 22\ (14) \to a = \underbrace{14 \cdot q}_{2\cdot(7\cdot q)} + \underbrace{22}_{2\cdot 11} = 2 \cdot (7q + 11) + 0 \xrightarrow[\text{es}]{\text{el resto}} r_2(a) = 0 \quad \checkmark \\ a \equiv 22\ (14) \to a = \underbrace{14 \cdot q}_{7\cdot(2\cdot q)} + \underbrace{22}_{1+7\cdot 3} = 7 \cdot (2q + 3) + 1 \xrightarrow[\text{es}]{\text{el resto}} r_7(a) = 1 \quad \checkmark \end{cases}$$

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

c) ... hay que hacerlo!

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

11.

a) Probar que $a^2 \equiv -1\ (5) \iff a \equiv 2\ (5) \vee a \equiv 3\ (5)$

b) Probar que no existe ningún entero a tal que $a^3 \equiv -3\ (7)$

c) Probar que $a^7 \equiv a\ (7)\ \ \forall a \in \mathbb{Z}$

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.

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

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

$\to$ La tabla muestra que para un dado a

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

b) ... hay que hacerlo!

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

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.

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

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

$\to$ Cómo para todos los a, alguno de los factores del resto siempre se anula, es decir:

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

d)

e)

---

12. ... hay que hacerlo!
Si querés mandarlo: Telegram $\to$, o mejor aún si querés subirlo en LaTeX $\to$.

---

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

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

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.

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

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

Quiero probar que $a_n \equiv 3^n \pmod 7 \to$ inducción completa:
$p(n) : a_n \equiv 3^n \pmod 7 \ \ \forall n \in \mathbb{N}$

Casos base:
$$\begin{cases} p(1): a_1 \equiv 3^1\ (7) \quad \checkmark, \quad p(1) \text{ es verdadera} \\ p(2): a_2 \equiv 3^2\ (7) \overset{(7)}{\equiv} 2 \overset{(7)}{\equiv} -5 \quad \checkmark, \quad p(2) \text{ es verdadera} \end{cases}$$

Paso Inductivo:
$$\begin{cases} p(k): a_k \equiv 3^k \pmod 7 \quad \checkmark, \quad p(k) \text{ la asumo verdadera} \\ \text{y} \\ p(k+1): a_{k+1} \equiv 3^{k+1} \pmod 7 \quad \checkmark, \quad p(k+1) \text{ también asumo verdadera} \\ \Rightarrow p(k+2): a_{k+2} \equiv 3^{k+2} \pmod 7 \text{ quiero probar que es verdadera} \end{cases}$$

Hipótesis inductiva:
$$\begin{cases} a_k \equiv 3^k \pmod 7 \\ a_{k+1} \equiv 3^{k+1} \pmod 7 \\ \xrightarrow[\bigstar^1]{\text{sumo}} a_{k+2} = a_{k+1} - a_k \equiv 3^{k+1} - 3^k = 2 \cdot 3^k \overset{(7)}{\equiv} 9 \cdot 3^k = 3^{k+2}\ (7) \quad \checkmark \\ p(k+2) \text{ resultó ser verdadera.} \end{cases}$$

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 LaTeX→.

15. ... hay que hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

16. ... hay que hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

17. ... hay que hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

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 LaTeX→.

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

a) Probar que $(5a+8 : 7a+3) = 1 \quad \text{o} \quad 41$. Exhibir un valor de a para el cual da 1, y verificar que efectivamente para $a = 23$ da 41.

b) Probar que $(2a^2+3a : 5a+6) = 1 \quad \text{o} \quad 43$. Exhibir un valor de a para el cual da 1, y verificar que efectivamente para $a = 16$ da 43

c) Probar que $(a^2-3a+2 : 3a^3-5a^2) = 2 \quad \text{o} \quad 4$, 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) ... hay que hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

ii) ... hay que hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

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

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

$$\begin{cases} a = 1 & (0 : -2) = 2 \\ a = 2 & (0 : 4) = 4 \end{cases}$$

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 $7a-3b \quad \text{y} \quad 2a-b$ son coprimos.

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

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 LaTeX→.

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

$$\xrightarrow[\text{coprimitusibilidad}]{\text{por}} \begin{cases} a \mid b^2+4b+5a \\ b \mid b^2+4b+5a \end{cases} \to \begin{cases} a \mid b^2+4b \\ b \mid 5a \end{cases} \xrightarrow[\text{debe dividr a 5}]{\text{es seguro que } b \nmid a} \begin{cases} a \mid b \cdot (b+4) \\ b \mid 5 \end{cases}$$

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

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

ii) Hacer!

iii) ... hay que hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

Primos y factorización:

24. ______________________________

25. Sea p primo positivo.

i) Probar que si $0 < k < p \,|\, \binom{p}{k}$.

ii) Probar que si $a, b \in \mathbb{Z}$, entonces $(a + b)^p \equiv a^p + b^p \ (p)$.

____

26. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

27. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

28. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

29. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

30. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

31. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

32. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

33. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

34. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→ .

35. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→ .

36. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→ .

37. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→ .

38. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→ .

39. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→ .

40. ... hay que hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→ .

Ejercicios extras:

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

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

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

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

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

---

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

i) $(n : 2528) = 316$

ii) n tiene exáctamente 48 divisores positivos

iii) $27 \nmid n$

Analizo los números:

$$\left\{ \begin{array}{l} \xrightarrow[2528]{\text{factorizo}} 2528 = 2^5 \cdot 79 \quad \checkmark \\ \xrightarrow[316]{\text{factorizo}} 316 = 2^2 \cdot 79 \quad \checkmark \\ \xrightarrow[\text{condición}]{\text{reescribo}} (n : 2^5 \cdot 79) = 2^2 \cdot 79 \end{array} \right. \xrightarrow[\text{encontrar}]{\text{quiero}} n = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdot 5^{\alpha_5} \cdot 7^{\alpha_7} \cdots 79^{\alpha_79} \cdots .$$

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

La estrategia sigue con el primo más chico que haya:

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

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:*

$$\begin{cases} a = 5c \\ b = 5d \end{cases} \Rightarrow (3ab : a^2 + b^2) = 25 \overset{\text{coprimizar}}{\underset{!}{\Longleftrightarrow}} (3cd : c^2 + d^2) = 1$$

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:

$$p \,|\, 3 \cdot c \cdot d \Leftrightarrow \begin{cases} p \,|\, 3 & \bigstar^1 \\ \text{o} & \\ p \,|\, c & \bigstar^2 \\ \text{o} & \\ p \,|\, d & \bigstar^3 \end{cases}$$

Si ocurre que $p \,|\, 3 \Leftrightarrow p = 3$. Quiero entonces ver si $3 \,|\, c^2 + d^2 \Leftrightarrow c^2 + d^2 \overset{(3)}{\equiv} 0$. 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 concluímos que para que $c^2 + d^2 \overset{(3)}{\equiv} 0$ debe ocurrir que: $c \overset{(3)}{\equiv} 0$ y también que $d \overset{(3)}{\equiv} 0$, 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 $\bigstar^1$ $p \,|\, 3$

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

$$\begin{cases} p \,|\, c \\ p \,|\, c^2 + d^2 \end{cases} \xRightarrow[F_2 - c \cdot F_1 \to F_2]{} \begin{cases} p \,|\, c \\ p \,|\, d^2 \overset{p}{\underset{\text{primo}}{\Longleftrightarrow}} p \,|\, d \end{cases}$$

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

El caso $\bigstar^3$ es lo mismo que el caso $\bigstar^2$.
Se concluye entonces que $(3cd : c^2 + d^2) = 1$ con $(c : d) = 1$. Así probando que $(3ab : a^2 + b^2) = 25$ con $\begin{cases} a = 5c \\ b = 5d \end{cases}$

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.

... hay que hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

5. 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:
$\left\{ \begin{array}{l} (2k-1)^2 - (2k-1) + 1 \overset{(2)}{\equiv} (-1)^2 - 1 + 1 \overset{(2)}{\equiv} 1 \\ (2k)^2 - (2k) + 1 \overset{(2)}{\equiv} (0)^2 - 0 + 1 \overset{(2)}{\equiv} 1. \end{array} \right\}$ Por lo tanto 2 no puede ser un divisor de ambas expresiones y si $2 \nmid A \Rightarrow 2 \cdot k \nmid A$ tampoco.
Se ve fácil contrarecíproco: $\underbrace{2k}_{par} \mid A \Rightarrow 2 \mid A$. 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.
$\left\{ \begin{array}{l} d \mid a^3 + 1 \\ d \mid a^2 - a + 1 \end{array} \right. \to d \mid 30 \to \mathcal{D}_+(d) = \{1, 2, 3, 5, 6, 10, 15, 30\} \xrightarrow[\text{no hay divisores pares}]{\text{por lo de antes}} \mathcal{D}_+(d) = \{1, 3, 5, 15\}$
$\xrightarrow[\text{empezar por los números chicos}]{\text{hacer tabla de restos}} \left\{ \begin{array}{ccc} r_3(a^3+1) = 0 & \text{si} & a \equiv 2\ (3) \\ \wedge & & \\ r_3(a^2 - a + 1) = 0 & \text{si} & a \equiv 2\ (3) \end{array} \right\} \to \{\ r_5(a^3+1) \neq 0 \quad \forall a \in \mathbb{Z}\ \}.$
Luego si $5 \nmid (a^3 + 1 : a^2 - a + 1) \Rightarrow \underbrace{15}_{5 \cdot 3} \nmid (a^3 + 1 : a^2 - a + 1) \xrightarrow[\text{conjunto de divisores}]{\text{se achica el}} \mathcal{D}_+(d) = \{1, 3\}$
$d = \left\{ \begin{array}{lll} 3 & \text{si} & a \equiv 2\ (3) \\ 1 & \text{si} & a \equiv 1 \vee 2\ (3) \end{array} \right.$

---

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*: $(a : b) = 6 \iff \left\{ \begin{array}{l} a = 6A \\ b = 6B \end{array} \right\}$ con $(A : B)^{\star 1} = 1$
$d = (2 \cdot 6A + 6B : 3 \cdot 6A - 2 \cdot 6B) = (6 \cdot (2 \cdot A + B) : 6 \cdot (3 \cdot A - 2 \cdot B)) = 6 \cdot \underbrace{(2A + B : 3A - 2B)}_{D}$
$\to d^{\star 2} = 6D \xrightarrow[\text{comunes}]{\text{busco divisores}} \left\{ \begin{array}{l} D \mid 2A + B \\ D \mid 3A - 2B \end{array} \right. \xrightarrow[\dots]{\text{operaciones}} \left\{ \begin{array}{l} D \mid 7B \\ D \mid 7A \end{array} \right. \Rightarrow D = (7A : 7B) = 7 \cdot (A : B)^{\star 1} = 7$
Por lo tanto $D \in \mathcal{D}_+(7) = \{1, 7\}$, pero yo quiero encontrar ejemplos de a y b:

$$\star^2 \to \left\{ \begin{array}{l} d = 6 \cdot 7 = 42 \left\{ \begin{array}{l} \text{Si:}\quad A = 2 \to a = 12 \\ \qquad\ \ B = 3 \to b = 18 \\ (7:0) \Rightarrow D = 7 \to d = (42 : 0) = \underbrace{42}_{6 \cdot D} \end{array} \right. \\ \qquad\qquad\qquad\qquad \vee \\ d = 6 \cdot 1 = 6 \left\{ \begin{array}{l} \text{Si:}\quad A = 0 \to a = 0 \\ \qquad\ \ B = 1 \to b = 6 \\ (1 : -2) \Rightarrow D = 1 \to d = (6 : -12) = \underbrace{6}_{6 \cdot D} \end{array} \right. \end{array} \right.$$

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

$32a \equiv 17\ (9) \to 5a \equiv 8\ (9) \xrightarrow[\text{por 2}]{\text{multiplico}} a \equiv 7\ (9) \quad \checkmark$
$d = (a^3 + 4a + 1 : a^2 + 2) \xrightarrow{\text{Euclides}} \left\{ \begin{array}{r|l} a^3 + 4a + 1 & a^2 + 2 \\ \cline{2-2} -\ a^3 - 2a & a \\ \hline 2a + 1 & \end{array} \right\} \to d = (a^2 + 2 : 2a + 1) \quad \checkmark$
$\xrightarrow[\text{divisores}]{\text{buscar}} \left\{ \begin{array}{l} d \mid a^2 + 2 \\ d \mid 2a + 1 \end{array} \right. \xrightarrow{2F_1 - aF_2} \left\{ \begin{array}{l} d \mid -a + 4 \\ d \mid 2a + 1 \end{array} \right. \xrightarrow{2F_1 + F_2} \left\{ \begin{array}{l} d \mid -a + 4 \\ d \mid 9 \end{array} \right.$
$\to d = (-a + 4 : 9) \xrightarrow[\text{candidatos a MCD}]{\text{divisores}} \{1, 3, 9\} \quad \checkmark$

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
$r_9(-a+4)$	4	3	2	1	0	-1	-2	-3	-4

$\to a \equiv 4\ (9)$, valores de a candidatos para obtener MCD.

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

$\to a \equiv 1\ (3)$, valores de 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 $a = 9k+7 \overset{(3)}{\equiv} 1$.

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

---

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 $\sum\limits_{k=0}^{255} a_k$

(a) Por inducción:

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

Primero notar que:

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

Se ve que tiene un período de 6 elementos.

Caso Base: $p(2) : a_8 \underset{\bigstar^1}{\overset{?}{=}} a_2 \quad \checkmark$

Paso inductivo: Asumo que

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

entonces quiero probar que,

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

también sea verdadera.

Parto desde $p(k+1)$

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

Ahora uso la definición de manera sucesiva:

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

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

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. $\sum\limits_{k=0}^{255} a_k = \underbrace{0 + 0 + \cdots + 0}_{42 \text{ ceros}} + a_{252} + a_{253} + a_{254} + a_{255} =$

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

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

---

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.

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

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

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:

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

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 númerador sea un múltiplo del denominador para el valor de a usado.

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

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 $\bigstar^{3}$, calcularía:

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

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

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

---

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

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

Probar que $a_n \equiv 3^n - 5^n \ (32), \qquad \forall n \geq 1.$

Ejercicio intimidante a primera vista. Acomodemos un poco el enunciado así hacemos inducción.
Estoy buscando el módulo 32, a_{n+2} queda más amigable: $\bigstar^{1}\ a_{n+2} \overset{(32)}{\equiv} 24a_{n+1} + a_n \quad \checkmark$
Inducción:

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

Casos base:

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

Pasos inductivos:
Para algún $k \in \mathbb{Z}$:

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

Y queremos probar entonces que:

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

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

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

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 $p(n) \in \mathbb{N}$.

11. Caracterizar, para **cada** $a \in \mathbb{Z}$, el valor de $(a^3 + 31 : a^2 - a + 1)$.

... hay que hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

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

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

Coprimizar:

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

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

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

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 $(A^6 : B^6) \overset{\bigstar^2}{=} 1 = D$.

$\bigstar^2$ 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:

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

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 $D = 1$ ✓.

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

13. Sea $n \in \mathbb{N}$. Probar que $81 \mid (16n^2 + 8^{2n} - 15n - 7)^{2024}$ si y solo si $3 \mid n$.

$\Rightarrow$)

$$81 \mid (16n^2 + 8^{2n} - 15n - 7)^{2024} \overset{!!!}{\Longrightarrow} 3 \mid (16n^2 + 8^{2n} - 15n - 7)^{506} \overset{\text{def}}{\Longleftrightarrow}$$

$$\overset{\text{def}}{\Longleftrightarrow} (16n^2 + 8^{2n} - 15n - 7)^{2024} \equiv 0\ (3) \overset{!}{\Leftrightarrow} (n^2)^{2024} \equiv 0\ (3) \Leftrightarrow n^{4048} \equiv 0\ (3) \overset{!!}{\Rightarrow} n \equiv 0\ (3)$$

$$\boxed{81 \mid (16n^2 + 8^{2n} - 15n - 7)^{2024} \Rightarrow 3 \mid n}$$

En el !!! uso esto $p^n \mid a^n \Leftrightarrow p \mid a$. En ! son cuentas de congruencia. Y en !! uso esto, $p \mid a^n \Rightarrow p \mid a$.

$\Leftarrow$)

$$3 \mid n \overset{\text{def}}{\Longleftrightarrow} n \equiv 0\ (3) \overset{!}{\Leftrightarrow} n^2 \equiv 0\ (3) \overset{!}{\Leftrightarrow} 16n^2 + 8^{2n} - 15n - 7 \equiv 0\ (3) \overset{!}{\Leftrightarrow}$$

$$\overset{!}{\Leftrightarrow} (16n^2 + 8^{2n} - 15n - 7)^4 \equiv 0\ (3^4) \overset{!}{\Rightarrow} (16n^2 + 8^{2n} - 15n - 7)^{2024} \equiv 0\ (3^4)$$

$$\boxed{3 \mid n \Rightarrow 81 \mid (16n^2 + 8^{2n} - 15n - 7)^{2024}}$$

En el último ! uso que $n \equiv 0\ (d) \Rightarrow n^m \equiv 0\ (d)$ y en los otros la mismas propiedades que antes... *maomeno*