Álgebra I
Práctica 4 Resuelta

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

Choose your destiny:

- Notas teóricas
- Ejercicios de la guía:

1.	**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.**
🔥**2.**	🔥**4.**	🔥**6.**	🔥**8.**	

Notas teóricas:

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

Algoritmo de división:

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

$$\left\{ \begin{array}{c} a = k \cdot d + r, \\ \text{con } 0 \leq r < |d|. \end{array} \right\}$$

  Y además estos k y r son *únicos*.

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

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

Sistema de numeración:

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

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

  con $0 \leq r_i < d$ para $0 \leq i \leq n$ con $r_n, \ldots, r_0$ son únicos en esas condiciones.
- *Notación:* $a = (r_n r_{n-1} \cdots r_1 r_0)_d = \begin{cases} 2020 = (2020)_{10} \\ 2020 = (7E4)_{16} \\ 2020 = (31040)_5 \end{cases}$
- $d^n = (1\underbrace{0 \cdots 0}_{n})$
- ¿Cuál es el número más grande que puedo escribir usando n cifras en base d?
  $(\underbrace{d-1 \quad d-1 \quad \cdots \quad d-1}_{n \text{ cifras}})_d = \sum\limits_{i=0}^{n-1} (d-1) d^i = d^n - 1$
- ¿Cuántos números hay con $\leq n$ cifras?
  Hay del 0 hasta el $d^n - 1$, es decir d^n.
- ¿Cuál es la forma más rápida de calcular 2^{16}

Máximo común divisor:

- Sean $a, b \in \mathbb{Z}$, no ambos nulos. El MCD entre a y b es el mayor de los divisores común entre a y b y se nota $(a : b)$
- $(a : b) \in \mathbb{N}$ (pues $(a : b) \geq 1$) siempre existe. $\mathcal{D}com_+(a, b) = \mathcal{D}_+(a) \cap \mathcal{D}_+(b) \neq \varnothing$ pues $1 \in \mathcal{D}com_+(a, b)$. Se ve también que está acotado por el menor entre a y b, pues si $d \mid a \wedge d \mid b \Rightarrow d \leq |a| \wedge d \leq |b|$ y es único.
- Sean a y $b \in \mathbb{Z}$, no ambos nulos.
  - $(a : b) = (\pm a : \pm b)$
  - $(a : b) = (b : a)$
  - $(a : 1) = 1$
  - $(a : 0) = |a|, \quad \forall a \in \mathbb{Z} - \{0\}$
  - si $b \mid a \Rightarrow (a : b) = |b|$ si $b \in \mathbb{Z} - \{0\}$
  - $(a : b) = (a : b + na)$ con $n \in \mathbb{Z}$
  - $(a : b) = (a : r_a(b))$ con $n \in \mathbb{Z}$
- *Algoritmo de Euclides*: Sean $a, b \in \mathbb{Z}$ con $b \neq 0$, entonces, $\forall k \in \mathbb{Z}$, se tiene: $(a : b) = (b : a - kb)$. En particular, como $r_b(a) = a - kb$, con k el cociente (para $b \neq 0$), se tiene $(a : b) = (b : r_b(a))$

- *Combinacion Entera*: Sean $a, b \in \mathbb{Z}$ no ambos nulos, entonces $\exists\, s,\ t \in \mathbb{Z}$ tal que $(a : b) = s \cdot a + t \cdot b$.
  - Todos los divisores comunes entre a y b dividen al $(a : b)$. Sean $a, b \in \mathbb{Z}$ no ambos nulos, $d \in \mathbb{Z} - \{0\}$. Entonces:
  $$d \,|\, a \text{ y } d \,|\, b \iff d \,|\, \underbrace{(a : b)}_{s \cdot a + t \cdot b}$$
  .
  - 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.
  - Sean $a,\ b \in \mathbb{Z}$ no ambos nulos, y sea $k \in \mathbb{N}$
  $$(ka : kb) = k(a : b)$$

- *Coprimos:*
  - Dados $a, b \in \mathbb{Z}$, no ambos nulos, se dice que son *coprimos* si $(a : b) = 1$
  $$a \perp b \iff (a : b) = 1$$
  $$a \perp b \iff \exists\, s,\ t \in \mathbb{Z} \text{ tal que } 1 = s \cdot a + t \cdot b$$
  - Sean $a, b \in \mathbb{Z}$, no ambos nulos. Entonces $\frac{a}{(a:b)} \perp \frac{b}{(a:b)}$.
  - Coprimizar es : $\left\{ \begin{array}{l} a = (a : b) \cdot a' \\ b = (a : b) \cdot b' \end{array} \right\} \to a'$ y b' son coprimos.
  - Sean $a, c, d \in \mathbb{Z}$ con c, d no nulos. Entonces:
  $$c \,|\, a \text{ y } d \,|\, a \text{ y } c \perp d \iff c \cdot d \,|\, a$$
  - Sean $a, b, d \in \mathbb{Z}$ con $d \neq 0$. Entonces:
  $$d \,|\, a \cdot b \text{ y } d \perp a \Rightarrow d \,|\, b$$

- *Primos y Factorización:*
  - Sea p primo y sean $a, b \in \mathbb{Z}$. Entonces:
  $$p \,|\, a \cdot b \Rightarrow p \,|\, a \vee p \,|\, b$$
  - *Si p divide a algún producto de números, tiene que dividir a alguno de los factores* $\to$ Sean $a_1, \dots, a_n \in \mathbb{Z}$:
  $$\left\{ \begin{array}{l} p \,|\, a_1 \cdot a_2 \cdots a_n \Rightarrow p \,|\, a_i \text{ para algún } i \text{ con } 1 \leq i \leq n. \\ p \,|\, a^n \Rightarrow p \,|\, a. \end{array} \right.$$
  - Si $a \in \mathbb{Z}$, p primo:
  $$\left\{ \begin{array}{l} (a : p) = 1 \iff p \nmid a \\ (a : p) = p \iff p \,|\, a \end{array} \right.$$

– 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:

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

– 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 $a, b, c \in \mathbb{Z}$ no nulos:

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

– Si $a \,|\, m \ \wedge\ b \,|\, m$, entonces $[a : b] \,|\, m$

– $(a : b) \cdot [a : b] = |a \cdot b|$

Ejercicios de la guía:

Divisibilidad

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

i) $a \cdot b \,|\, c \Rightarrow a \,|\, c$ y $b \,|\, c$

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

ii) $4 \,|\, a^2 \Rightarrow 2 \,|\, a$

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

iii) $2 \,|\, a \cdot b \Rightarrow 2 \,|\, a$ o $2 \,|\, b$

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

iv) $9 \,|\, a \cdot b \Rightarrow 9 \,|\, a$ o $9 \,|\, b$

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

v) $a \,|\, b + c \Rightarrow a \,|\, b$ o $a \,|\, c$

$12 \,|\, 20 + 4 \Rightarrow 12 \nmid 20$ y $12 \nmid 4$

vi)

Falta hacerlo!

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

vii)

Falta hacerlo!

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

viii) ______________________________

Falta hacerlo!

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

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

____

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

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

____

Pruebo por inducción. $p(n) \ : \ a \mid b \Rightarrow a^n \mid b^n$
$$\left\{ \begin{array}{l} \text{Caso base: } n = 1 \Rightarrow a|b \Rightarrow a^1 \mid b^1 \quad \checkmark \\ \text{Paso inductivo: } \quad \forall h \in \mathbb{N}, p(h) \ V \Rightarrow p(h+1) \ V? \\ \text{Si } a \mid b \Rightarrow a^k \mid b^k \Rightarrow a^k \cdot c = b^k \xrightarrow[b \text{ M.A.M}]{\text{multiplico por}} b \cdot a^k \cdot c = b^{k+1} \xrightarrow[a \cdot d = b]{a \mid b} a \cdot d \cdot a^k \cdot c = a^{k+1} \cdot (cd) = b^{k+1} \\ \xrightarrow[\text{que}]{\text{concluyendo}} a^{k+1} \mid b^{k+1} \text{como quería mostrarse.} \end{array} \right.$$
Como $p(1) \wedge p(k) \wedge p(k+1)$ resultaron verdaderas, por el principio de inducción $p(n)$ es verdadera $\forall n \in \mathbb{N}$

Este resultado es importante y se va a ver en muchos ejercicios.

$$a \mid b \Rightarrow a^n \mid b^n \iff b \equiv 0 \ (a) \Rightarrow b^n \equiv \underbrace{0}_{\stackrel{(a^n)}{\equiv} a^n} \ (a^n) \iff b^n \equiv a^n \ (a^n)$$

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

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

____

Busco eliminar la n del *miembro* derecho.
$$\left\{ \begin{array}{l} 3n - 1 \mid n + 7 \xrightarrow[a \mid k \cdot c]{a|c \Rightarrow} 3n - 1 \mid 3 \cdot (n + 7) = 3n + 21 \\ \xrightarrow[\Rightarrow a \mid b \pm c]{a \mid b \wedge a \mid c} 3n - 1 \mid 3n + 21 - (3n - 1) = 22 \end{array} \right\} \to 3n - 1 \mid 22$$
$$\xrightarrow[\text{para que}]{\text{busco } n} \frac{22}{3n-1} \in \mathcal{D}(22) = \{1 \pm 1, \pm 2, \pm 11, \pm 22\} \xrightarrow{\text{probando}} n \in \{1, 4\} \quad \checkmark$$

ii)

iii)

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

____

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

---

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

i) Probar que $a-b \mid a^n - b^n$ para todo $n \in \mathbb{N}$ y $a \neq b \in \mathbb{Z}$

ii) Probar que si n es un número natural par y $a \neq -b$, entonces $a+b \mid a^n - b^n$.

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

---

i) *Inducción:*

Proposición:

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

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.

$$\begin{cases} a-b \mid a^k - b^k \\ a-b \mid a^k - b^k \end{cases} \overset{\times a}{\underset{\times b}{\Longrightarrow}} \begin{cases} a-b \mid a^{k+1} - ab^k \\ a-b \mid ba^k - b^{k+1} \end{cases} \overset{+}{\Longrightarrow} \{\ a-b \mid a^{k+1} - b^{k+1}. \qquad \checkmark$$

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

ii) Sé que

$$a+b \mid a+b \overset{\text{def}}{\iff} a \equiv -b\ (a+b)$$

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

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

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

★[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:

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

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

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

iii) Hecho en el anterior.

---

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

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

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.

$$2^{k+3} \mid a^{2^{k+1}} - 1 \overset{!}{\Leftrightarrow} 2^{k+2} \cdot 2 \mid (a^{2^k} - 1) \cdot \overbrace{(a^{2^k} + 1)}^{\text{par !}}$$
$$\xLeftarrow[\text{hipótesis inductiva}]{\text{Si } a \mid b \text{ y } c \mid d \Rightarrow ac \mid bd}$$
$$2^{k+2} \cdot 2 \mid (a^{2^k} - 1) \cdot \underbrace{(a^{2^k} + 1)}_{\text{par}}.$$

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. Falta hacerlo!

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

6. Falta hacerlo!

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

7.

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

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

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

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

---

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

$$\begin{cases} \xrightarrow[\text{que}]{\text{sé}} 100 \equiv 1\ (99) \iff 100^2 \equiv \underbrace{100}_{\overset{(99)}{\equiv} 1}\ (99) \to 100^2 \equiv 1\ (99) \iff \dots \iff 100^n \equiv 1\ (99) \\ Tengoquedemostrareserenglnporinduccinocon"propiedaddecongruencia"funciona? \end{cases}$$

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

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

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

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

iii) Falta hacerlo!

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

iv) Falta hacerlo!

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

Algoritmo de División:

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

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

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

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

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

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

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

---

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

ii)

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

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

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

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

---

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

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

ii) la división de a por 3.

iii) la división de $4a + 1$ por 9.

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

---

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

---

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

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

---

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

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

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

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

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.

i) Si $a \equiv 22\ (14)$, hallar el resto de dividir a a por 14, por 2 y por 7.

ii) Si $a \equiv 13\ (5)$, hallar el resto de dividir a $33a^3 + 3a^2 - 197a + 2$ por 5.

iii) Hallar, para cada $n \in \mathbb{N}$, el resto de la división de $\sum_{i=1}^{n} (-1)^i \cdot i!$ por 12

---

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

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

iii) Falta hacerlo!

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

11.

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

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

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

iv) Probar que $7 \mid a^2 + b^2 \iff 7 \mid a \wedge 7 \mid b$.

v) Probar que $5 \mid a^2 + b^2 + 1 \iff 5 \mid a \vee 5 \mid b$. ¿Vale la recíproca?

---

i) Me piden que pruebe una congruencia es válida solo para ciertos $a \in \mathbb{Z}$. Pensado en términos de *restos* quiero que el resto al poner los a en cuestión cumplan la congruencia.

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

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

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

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

ii) Falta hacerlo!

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

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

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

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:

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

iv)

v)

12. Falta hacerlo!

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

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

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

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.

$\xrightarrow[\text{enunciado feo}]{\text{acomodo}} r_7(a_{n+2}) = r_7(r_7(a_{n+1}) - \underbrace{r_7(36)^n}_{\overset{(7)}{\equiv} 1} \cdot r_7(a_n) + \underbrace{r_7(21)^n}_{\overset{(7)}{\equiv} 0} \cdot r_7(n)^{21}) = \underbrace{r_7(a_{n+2}) = r_7(a_{n+1}) - r_7(a_n)}_{\star^1}$ ✓

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:

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

$$\begin{cases} \text{Casos base:} & \begin{cases} p(n=1) \; : \; a_1 \equiv 3^1 \; (7) \text{Verdadera} \\ p(n=2) \; : \; a_2 \equiv 3^2 \; (7) \overset{(7)}{\equiv} 2 \overset{(7)}{\equiv} -5 \text{Verdadera} \end{cases} \\ \text{Paso Inductivo:} & \begin{cases} p(k) \; : \; a_k \equiv 3^k \pmod 7 \text{ Verdadera} \\ \wedge \\ p(k+1) \; : \; a_{k+1} \equiv 3^{k+1} \pmod 7 \text{ Verdadera} \\ \Rightarrow p(k+1) \; : \; a_{k+2} \equiv 3^{k+2} \pmod 7 \text{ Verdadera?} \end{cases} \\ \text{Hipótesis inductiva:} & \begin{cases} a_k \equiv 3^k \pmod 7 \\ a_{k+1} \equiv 3^{k+1} \pmod 7 \\ \xrightarrow[\text{pensando en } \star^1]{\text{sumo}} \underbrace{a_{k+1} - a_k}_{a_{k+2}} \equiv \underbrace{3^{k+1} - 3^k}_{2 \cdot 3^k} \pmod 7 \\ \xrightarrow[\text{limpio}]{\text{paso en}} a_{k+2} \equiv \underbrace{9}_{\overset{(7)}{\equiv} 2} \cdot 3^k \; (7) \overset{(7)}{\equiv} 3^{k+2} \to \boxed{a_{k+2} \equiv 3^{k+2} \; (7)} \end{cases} \end{cases}$$

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

14.

i) Hallar el desarrollo en base 2 de

(a) 1365

(b) 2800

(c) $3 \cdot 2^{12}$

(d) $13 \cdot 2^n + 5 \cdot 2^{n-1}$

Hacer!

15. Falta hacerlo!

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

16. Falta hacerlo!

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

17. Falta 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. Falta hacerlo!

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

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

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

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

c) Probar que $(a^2 - 3a + 2 : 3a^3 - 5a^2) = 2$ o 4, y exhibir un valor de a para cada caso.
(Para este item es **indispensable** mostrar que el máximo común divisor nunca puede ser 1).

---

i) Falta hacerlo!

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

ii) Falta hacerlo!

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

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

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

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

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.

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

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

22. Falta 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) $\frac{b+4}{a} + \frac{5}{b} = \frac{b^2+4b+5a}{ab} \xrightarrow{\text{quiero que}} ab \,|\, b^2 + 4b + 5a$

$\xrightarrow[\text{coprimitusibilidad}]{\text{por}} \begin{cases} a|b^2 + 4b + 5a \\ b|b^2 + 4b + 5a \end{cases} \to \begin{cases} a|b^2 + 4b \\ b|5a \end{cases} \xrightarrow[\text{debe dividr a 5}]{\text{es seguro que } b \not| a} \begin{cases} a|b \cdot (b+4) \\ b|5 \end{cases}$

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

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

ii) Hacer!

iii) Falta 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. Falta hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

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

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

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

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

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

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

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

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

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

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

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

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

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

40. Falta 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: $\sum_{i=0}^{4} \sum_{j=0}^{2} \sum_{k=0}^{1} 2^i \cdot 5^j \cdot 11^k = \left(\sum_{i=0}^{4} 2^i \right) \cdot \left(\sum_{j=0}^{2} 5^j \right) \cdot \left(\sum_{k=0}^{1} 11^k \right)$

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

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

i) $(n : 2528) = 316$

ii) n tiene exáctamente 48 divisores positivos

iii) $27 \nmid n$

$$\left\{ \begin{array}{l} \xrightarrow[2528]{\text{factorizo}} 2528 = 2^5 \cdot 79 \quad \checkmark \\ \xrightarrow[316]{\text{factorizo}} 316 = 2^2 \cdot 79 \quad \checkmark \\ \xrightarrow[\text{condición}]{\text{reescribo}} (n : 2^5 \cdot 79) = 2^2 \cdot 79 \end{array} \right.$$

$\xrightarrow[\text{encontrar}]{\text{quiero}} n = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdot 5^{\alpha_5} \cdot 7^{\alpha_7} \cdots 79^{\alpha_{79}} \cdots.$

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

$$\xrightarrow[\text{el primo más chico que haya}]{\text{la estrategia sigue con}} \left\{ \begin{array}{l} 48 = \underbrace{(\alpha_2 + 1)}_{2+1} \cdot (\alpha_3 + 1) \cdots \\ 48 = 3 \cdot (\alpha_3 + 1) \cdots \\ 16 = (\alpha_3 + 1) \cdot (\alpha_5 + 1) \cdot (\alpha_7 + 1) \cdots \underbrace{(\alpha_{79} + 1)}_{=2 \text{ quiero el menor}} \cdots \\ 8 = (\alpha_3 + 1) \cdot (\alpha_5 + 1) \cdot (\alpha_7 + 1) \cdots \\ 8 = \underbrace{(\alpha_3 + 1)}_{=2} \cdot \underbrace{(\alpha_5 + 1)}_{=2} \cdot \underbrace{(\alpha_7 + 1)}_{=2} \cdot 1 \cdots 1 \end{array} \right. \quad \text{El } n \text{ que cumple lo pedido}$$

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

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

Coprimizar: $\left\{ \begin{array}{l} c = \frac{a}{5} \\ d = \frac{b}{5} \end{array} \right. \to (a : b) = 5 \cdot \underbrace{(c : d)}_{1} = 5$

$\to \left\{ \xrightarrow[\text{enunciado}]{\text{según}} 25 = (3ab : a^2 + b^2) \xrightarrow{\text{reemplazo}} 25 = 25 \cdot \underbrace{(3cd : c^2 + d^2)}_{1} \right.$

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

$$\xrightarrow[\text{no lo fuera}]{\text{Supongo que}} \exists p \to \left\{ p \,|\, (3cd : c^2+d^2) \to \left\{ \begin{array}{l} p \,|\, 3cd \to \left\{ \begin{array}{l} p \,|\, 3 \to p = 3 \xrightarrow[r_3(c^2+d^2)]{\text{tabla}} \left\{ \begin{array}{lll} 0 & \text{si} & \underbrace{c,d \equiv 0\ (3)}_{noup!(c:d)=1} \\ \neq 0 & \text{si} & \text{otro caso} \end{array} \right. \\ p \,|\, c \to \left\{ \xrightarrow{\text{como}} p \,|\, c^2+d^2 \Rightarrow p \,|\, d^2 \to \underbrace{p \,|\, d}_{noup!(c:d)=1} \right. \\ p \,|\, d \to noup!idem \end{array} \right. \\ p \,|\, c^2+d^2 \end{array} \right. \right.$$

Si ningún primo p divide a $(3cd : c^2 + d^2) \Rightarrow (3cd : c^2 + d^2) = 1$

4.

i) Calcular los posibles valores de: $(7^{n-1} + 5^{n+2} : 5 \cdot 7^n - 5^{n+1})$.

ii) Encontrar n tales que el mcd para ese n tome 3 valores distintos.

Busco independencia de n en algún lado del $(a : b)$. Si $d = (7^{n-1} + 5^{n+2} : 5 \cdot 7^n - 5^{n+1}) \to$

$$\left\{ \begin{array}{l} d \,|\, 7^{n-1} + 5^{n+2} \\ d \,|\, 5 \cdot 7^n - 5^{n+1} \end{array} \right. \to \left\{ \begin{array}{l} d \,|\, \underbrace{7^{n-1} + 5^{n+2}}_{\overset{(5)}{\equiv} 2^n} \\ d \,|\, 5 \cdot (7^n - 5^n) \end{array} \right. \xrightarrow[\Rightarrow p \,|\, k]{p \not| \, d \wedge d \,|\, p \cdot k} \left\{ \begin{array}{l} d \,|\, 7^{n-1} + 5^{n+2} \\ d \,|\, 7^n - 5^n \end{array} \right.$$

$$\to \left\{ \begin{array}{l} d \,|\, 176 \cdot 5^n \\ d \,|\, 7^n - 5^n \end{array} \right. \xrightarrow[\Rightarrow p \,|\, k]{p \not| \, d \wedge d \,|\, p \cdot k} \left\{ \begin{array}{l} d \,|\, 176 \\ d \,|\, 7^n - 5^n \end{array} \right. \to d = (176 : 7^n - 5^n) \quad \checkmark$$

Factorizo: $176 = 2^4 \cdot 11 \to \mathcal{D}_+(176) = \{1, 2, 4, 8, 11, 16, 22, 44, 88, 176\}$.

$$\text{Descarto} \to \left\{ \begin{array}{lllll} 1 & \to & 7^n - 5^n \equiv 2^n\ (5) & \to & d \text{ tiene que ser par y } 2 > 1 \\ 11 & \to & 7^n - 5^n \equiv 2^n\ (5) & \to & d \text{ tiene que ser par} \end{array} \right.$$

$\mathcal{D}_+(d) = \{2, 4, 8, 16, 22, 44, 88, 176\}$

$$\text{Estudio congruencia de los pares e impares: } \left\{ \begin{array}{l} 7^{2k} - 5^{2k} \equiv 1^k - 25^k\ (8) \to 1 - \underbrace{1}_{\overset{(8)}{\equiv} 25} \equiv 0\ (8) \\ 7^{2k+1} - 5^{2k+1} \equiv 3 - 1\ (4) \overset{(4)}{\equiv} 2 \end{array} \right.$$

Puedo descartar a los múltiplos de 4 que no sean múltiplos de 8. $\to \mathcal{D}_+(d) = \{2, 8, 16, 22, 88, 176\}$

No lo terminé, no entiendo bien este paso y como descartar algún otro.

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 $2 \not| \, A \Rightarrow 2 \cdot k \not| \, A$ tampoco.

Se ve fácil contrarecíproco: $\underbrace{2k}_{par} \,|\, A \Rightarrow 2 \,|\, A$. Porque existe un k tal que $2 \cdot c \cdot k = A \Rightarrow 2 \cdot (c \cdot k) = A$.

Ahora cuentas para simplificar la expresión y encontrar número del lado derecho.

$$\left\{ \begin{array}{l} d \,|\, a^3 + 1 \\ d \,|\, a^2 - a + 1 \end{array} \right. \to d \,|\, 30 \to \mathcal{D}_+(d) = \{1, 2, 3, 5, 6, 10, 15, 30\} \xrightarrow[\text{no hay divisores pares}]{\text{por lo de antes}} \mathcal{D}_+(d) = \{1, 3, 5, 15\}$$

$$\xrightarrow[\text{empezar por los números chicos}]{\text{hacer tabla de restos}} \left\{ \begin{array}{ccc} r_3(a^3+1) = 0 & \text{si} & a \equiv 2\ (3) \\ \wedge & & \\ r_3(a^2-a+1) = 0 & \text{si} & a \equiv 2\ (3) \end{array} \right\} \to \left\{\ r_5(a^3+1) \neq 0 \quad \forall a \in \mathbb{Z}\ \right\}.$$

Luego si $5 \not| \ (a^3+1 : a^2-a+1) \Rightarrow \underbrace{15}_{5\cdot 3} \not| \ (a^3+1 : a^2-a+1) \xrightarrow[\text{conjunto de divisores}]{\text{se achica el}} \mathcal{D}_+(d) = \{1,3\}$

$$d = \left\{ \begin{array}{lll} 3 & \text{si} & a \equiv 2\ (3) \\ 1 & \text{si} & a \equiv 1 \vee 2\ (3) \end{array} \right.$$

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 $(A : B)^{\bigstar^1} = 1$

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

$\to d^{\bigstar^2} = 6D \xrightarrow[\text{comunes}]{\text{busco divisores}} \left\{ \begin{array}{l} D \,|\, 2A + B \\ D \,|\, 3A - 2B \end{array} \right. \xrightarrow[\dots]{\text{operaciones}} \left\{ \begin{array}{l} D \,|\, 7B \\ D \,|\, 7A \end{array} \right. \Rightarrow D = (7A : 7B) = 7 \cdot (A : B)^{\bigstar^1} = 7$

Por lo tanto $D \in \mathcal{D}_+(7) = \{1, 7\}$, pero yo quiero encontrar ejemplos de a y b:

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

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

$32a \equiv 17\ (9) \to 5a \equiv 8\ (9) \xrightarrow[\text{por } 2]{\text{multiplico}} a \equiv 7\ (9) \quad \checkmark$

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

$\xrightarrow[\text{divisores}]{\text{buscar}} \left\{ \begin{array}{l} d \,|\, a^2 + 2 \\ d \,|\, 2a + 1 \end{array} \right. \xrightarrow{2F_1 - aF_2} \left\{ \begin{array}{l} d \,|\, -a + 4 \\ d \,|\, 2a + 1 \end{array} \right. \xrightarrow{2F_1 + F_2} \left\{ \begin{array}{l} d \,|\, -a + 4 \\ d \,|\, 9 \end{array} \right.$

$\to d = (-a + 4 : 9) \xrightarrow[\text{candidatos a MCD}]{\text{divisores}} \{1, 3, 9\} \quad \checkmark$

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

Caso Base: Primero notar que,

$$\to \begin{Bmatrix} a_0 = 1 \\ a_1 = 3 \\ a_2 \overset{\text{def}}{=} 2 \\ a_3 \overset{\text{def}}{=} -1 \\ a_4 \overset{\text{def}}{=} -3 \\ a_5 \overset{\text{def}}{=} -2 \end{Bmatrix} \to \begin{Bmatrix} a_6 \overset{\text{def}}{=} 1 \\ a_7 \overset{\text{def}}{=} 3 \\ a_8 \overset{\text{def}}{=} 2 \\ a_9 \overset{\text{def}}{=} -1 \\ a_{10} \overset{\text{def}}{=} -3 \\ a_{11} \overset{\text{def}}{=} -2 \end{Bmatrix} \to \cdots \text{ Se ve que tiene un período de 6 elementos.}$$

$p(n = 2)$ Verdadero? ? $\to a_8 \overset{?}{=} a_2 \quad \checkmark$

Paso inductivo: Supongo $p(k)$ Verdadero? $\Rightarrow p(k+1)$ Verdadero? ?

Hipótesis inductiva: Supongo $a_{k+6} = a_k \ \ \forall k \in \mathbb{N}_0$ Verdadero? , quiero ver que $a_{k+7} = a_{k+1}$

$$a_{k+7} \overset{\text{def}}{=} a_{k+6} - a_{k+5} \overset{\text{HI}}{=} a_k - a_{k+5} \overset{\text{def}}{=} a_k - (\underbrace{a_k + a_{k+4}}_{a_{k+5}}) = -a_{k+4}$$

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

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

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

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

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.

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

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

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

$$10a-15 \mid -25 \iff 10a-25 \in \{\pm1, \pm5, \pm25\} \star^3 \text{ para algún } a \in \mathbb{Z}\,. \quad \checkmark$$

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

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

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.

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

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:

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

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

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