

Práctica 4 de álgebra 1

Comunidad algebraica

última compilacion: 29/06/2024

1 Definiciones y fórmulas útiles

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

Algoritmo de división:

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

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

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.
- $r_d(a) = 0 \iff d \mid a \iff a \equiv 0 \pmod{d}$
- $a \equiv r_d(a) \pmod{d}$. Tiene mucho sentido.
- $a \equiv r \pmod{d}$ con $\underbrace{0 \leq r < |d|}_{\text{cumple condición de resto}} \Rightarrow r = r_d(a)$
- $r_1 \equiv r_2 \pmod{d}$ con $\underbrace{0 \leq r_1, r_2 < |d|}_{\text{cumple condición de resto}} \Rightarrow r_1 = r_2$
- $a \equiv b \pmod{d} \iff r_d(a) = r_d(b)$. Dos números que son congruentes, tienen igual resto.
- $r_d(a + b) = r_d(r_d(a) + r_d(b))$ ya que si $\left\{ \begin{array}{l} a \equiv r_d(a) \pmod{d} \\ b \equiv r_d(b) \pmod{d} \end{array} \right\} \rightarrow a + b \equiv r_d(a) + r_d(b) \pmod{d}$
- $r_d(a \cdot b) = r_d(r_d(a) \cdot r_d(b))$ ya que si $\left\{ \begin{array}{l} a \equiv r_d(a) \pmod{d} \\ b \equiv r_d(b) \pmod{d} \end{array} \right\} \rightarrow a \cdot b \equiv r_d(a) \cdot r_d(b) \pmod{d}$

Sistema de numeración:

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

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

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

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

$$\underbrace{(d-1 \quad d-1 \quad \dots \quad d-1)}_{n \text{ cifras}}_d = \sum_{i=0}^{n-1} (d-1)d^i = d^n - 1$$
- ¿Cuántos números hay con $\leq n$ cifras?
 Hay del 0 hasta el $d^n - 1$, es decir d^n .
- ¿Cuál es la forma más rápida de calcular 2^{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. $\mathcal{D}com_+(a, b) = \mathcal{D}_+(a) \cap \mathcal{D}_+(b) \neq \emptyset$ pues $1 \in \mathcal{D}com_+(a, b)$. Se ve también que está acotado por el menor entre a y b , pues si $d \mid a \wedge d \mid b \Rightarrow d \leq |a| \wedge d \leq |b|$ y es único.
- Sean a y $b \in \mathbb{Z}$, no ambos nulos.

- $(a : b) = (\pm a : \pm b)$
- $(a : b) = (b : a)$
- $(a : 1) = 1$
- $(a : 0) = |a|, \forall a \in \mathbb{Z} - \{0\}$
- 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:

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

- Sea $c \in \mathbb{Z}$ entonces $\exists s', t' \in \mathbb{Z}$ con $c = s'a + t'b \iff (a : b) \mid c$.
- Todos los números múltiplos del MCD se escriben como combinación entera de a y b .
- Si un número es una combinación entera de a y b entonces es un múltiplo del MCD.
- Sean $a, b \in \mathbb{Z}$ no ambos nulos, y sea $k \in \mathbb{N}$

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

- *Coprimos:*

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

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

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

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

- 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:

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

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

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

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

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

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

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

- Sean a y $b \in \mathbb{Z}$ no nulos, con $\begin{cases} a = \pm p_1^{m_1} \cdots p_r^{m_r} \text{ con } m_1, \dots, m_r \in \mathbb{Z}_0 \\ b = \pm p_1^{n_1} \cdots p_r^{n_r} \text{ con } n_1, \dots, n_r \in \mathbb{Z}_0 \\ \Rightarrow (a : b) = p_1^{\min\{m_1, n_1\}} \cdots p_r^{\min\{m_r, n_r\}} \\ \Rightarrow [a : b] = p_1^{\max\{m_1, n_1\}} \cdots p_r^{\max\{m_r, n_r\}} \end{cases}$

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

$$* a \perp b \iff \text{no tienen primos en común.}$$

$$* (a : b) = 1 \wedge (a : c) = 1 \iff (a : bc) = 1$$

$$* (a : b) = 1 \iff (a^m, b^n) = 1, \forall m, n \in \mathbb{Z}$$

$$* (a^n : a^m) = (a : b)^n$$

- Si $a \mid m \wedge b \mid m$, entonces $[a : b] \mid m$

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

Ejercicios dados en clase:

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

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

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

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

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

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

i) $(n : 2528) = 316$

ii) n tiene exáctamente 48 divisores positivos

iii) $27 \nmid n$

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

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

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

dido 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: $\left\{ \begin{array}{l} c = \frac{a}{5} \\ d = \frac{b}{5} \end{array} \right. \rightarrow (a : b) = 5 \cdot \underbrace{(c : d)}_1 = 5$

$\rightarrow \left\{ \begin{array}{l} \xrightarrow[\text{enunciado}]{\text{según}} 25 = (3ab : a^2 + b^2) \xrightarrow{\text{reemplazo}} 25 = 25 \cdot \underbrace{(3cd : c^2 + d^2)}_1 \end{array} \right.$

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

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

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

4. Ejercicio parcial

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

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

$$\begin{cases} d \mid 7^{n-1} + 5^{n+2} \\ d \mid 5 \cdot 7^n - 5^{n+1} \end{cases} \rightarrow \begin{cases} d \mid \underbrace{7^{n-1} + 5^{n+2}}_{\equiv 2^n \pmod{5}} \\ d \mid 5 \cdot (7^n - 5^n) \end{cases} \xrightarrow[p \nmid k]{p \nmid d \wedge d \mid p \cdot k} \begin{cases} d \mid 7^{n-1} + 5^{n+2} \\ d \mid 7^n - 5^n \end{cases}$$
$$\rightarrow \begin{cases} d \mid 176 \cdot 5^n \\ d \mid 7^n - 5^n \end{cases} \xrightarrow[p \mid k]{p \nmid d \wedge d \mid p \cdot k} \begin{cases} d \mid 176 \\ d \mid 7^n - 5^n \end{cases} \rightarrow d = (176 : 7^n - 5^n) \quad \checkmark$$

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

Descarto $\rightarrow \begin{cases} 1 \rightarrow 7^n - 5^n \equiv 2^n \pmod{5} \rightarrow d \text{ tiene que ser par y } 2 > 1 \\ 11 \rightarrow 7^n - 5^n \equiv 2^n \pmod{5} \rightarrow d \text{ tiene que ser par} \end{cases}$

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

Estudio congruencia de los pares e impares: $\begin{cases} 7^{2k} - 5^{2k} \equiv 1^k - 25^k \pmod{8} \rightarrow 1 - \underbrace{1}_{\equiv 25 \pmod{8}} \equiv 0 \pmod{8} \\ 7^{2k+1} - 5^{2k+1} \equiv 3 - 1 \pmod{4} \rightarrow \equiv 2 \pmod{4} \end{cases}$

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

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

5. Parcial del primer cuatrimestre 2024

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

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

$$\left\{ \begin{array}{l} (2k-1)^2 - (2k-1) + 1 \stackrel{(2)}{\equiv} (-1)^2 - 1 + 1 \stackrel{(2)}{\equiv} 1 \\ (2k)^2 - (2k) + 1 \stackrel{(2)}{\equiv} (0)^2 - 0 + 1 \stackrel{(2)}{\equiv} 1. \end{array} \right\} \text{ Por lo tanto 2 no puede ser un divisor de ambas}$$

expresiones y si $2 \nmid A \Rightarrow 2 \cdot k \nmid A$ tampoco.

Se ve fácil contrarecíproco: $\underbrace{2k}_{\text{par}} \mid A \Rightarrow 2 \mid A$. 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.

$$\begin{cases} d \mid a^3 + 1 \\ d \mid a^2 - a + 1 \end{cases} \rightarrow d \mid 30 \rightarrow \mathcal{D}_+(d) = \{1, 2, 3, 5, 6, 10, 15, 30\} \xrightarrow[\text{no hay divisores pares}]{\text{por lo de antes}} \mathcal{D}_+(d) = \{1, 3, 5, 15\}$$
$$\xrightarrow[\text{empezar por los números chicos}]{\text{hacer tabla de restos}} \left\{ \begin{array}{ll} r_3(a^3 + 1) = 0 & \text{si } a \equiv 2 \pmod{3} \\ \wedge \\ r_3(a^2 - a + 1) = 0 & \text{si } a \equiv 2 \pmod{3} \end{array} \right\} \rightarrow \{ r_5(a^3 + 1) \neq 0 \quad \forall a \in \mathbb{Z} \}.$$

Luego si $5 \nmid (a^3 + 1 : a^2 - a + 1) \Rightarrow \underbrace{15}_{5 \cdot 3} \nmid (a^3 + 1 : a^2 - a + 1) \xrightarrow[\text{conjunto de divisores}]{\text{se achica el}} \mathcal{D}_+(d) = \{1, 3\}$

$$d = \begin{cases} 3 & \text{si } a \equiv 2 \pmod{3} \\ 1 & \text{si } a \equiv 1 \vee 0 \pmod{3} \end{cases}$$

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

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

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

$$\rightarrow d \star^2 = 6D \xrightarrow[\text{comunes}]{\text{busco divisores}} \begin{cases} D \mid 2A + B \\ D \mid 3A - 2B \end{cases} \xrightarrow[\dots]{\text{operaciones}} \begin{cases} D \mid 7B \\ D \mid 7A \end{cases} \Rightarrow D = (7A : 7B) = 7 \cdot (A : B) \star^1 = 7$$

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

$$\star^2 \rightarrow \begin{cases} d = 6 \cdot 7 = 42 \begin{cases} \text{Si: } A = 2 \rightarrow a = 12 \\ B = 3 \rightarrow b = 18 \\ (7 : 0) \Rightarrow D = 7 \rightarrow d = (42 : 0) = \underbrace{42}_{6 \cdot D} \end{cases} \\ d = 6 \cdot 1 = 6 \begin{cases} \text{Si: } A = 0 \rightarrow a = 0 \\ B = 1 \rightarrow b = 6 \\ (1 : -2) \Rightarrow D = 1 \rightarrow d = (6 : -12) = \underbrace{6}_{6 \cdot D} \end{cases} \end{cases} \quad \checkmark$$

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

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

$$d = (a^3 + 4a + 1 : a^2 + 2) \xrightarrow{\text{Euclides}} \left\{ \begin{array}{l} a^3 + 4a + 1 \mid a^2 + 2 \\ -a^3 - 2a \mid a^2 + 2 \\ \hline 2a + 1 \mid a^2 + 2 \end{array} \right\} \rightarrow d = (a^2 + 2 : 2a + 1) \quad \checkmark$$

$$\xrightarrow[\text{divisores}]{\text{buscar}} \begin{cases} d \mid a^2 + 2 \\ d \mid 2a + 1 \end{cases} \xrightarrow{2F_1 - aF_2} \begin{cases} d \mid -a + 4 \\ d \mid 2a + 1 \end{cases} \xrightarrow{2F_1 + F_2} \begin{cases} d \mid -a + 4 \\ d \mid 9 \end{cases}$$

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

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

$\rightarrow a \equiv 4 \pmod{9}$, valores de a candidatos para obtener MCD.

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

$\rightarrow a \equiv 1 \pmod{3}$, valores de a candidatos para obtener MCD.

La condición $a \equiv 7 \pmod{9}$ no es compatible con el resultado de la tabla de r_9 , pero sí con r_3 . Notar que $a = 9k + 7 \stackrel{(3)}{\equiv} 1$.

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

Ejercicios de la guía: Divisibilidad

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

Calcular

i) $a \cdot b \mid c \Rightarrow a \mid c$ y $b \mid c$

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

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

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

iii) $2 \mid a \cdot b \Rightarrow 2 \mid a$ o $2 \mid b$

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

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

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

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

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

vi) _____
Hacer!

vii) _____
Hacer!

viii) _____
Hacer!

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

$$a \mid b + a^2 \Rightarrow b + a^2 = k \cdot a \xrightarrow{\text{acomodo}} b = (k - a) \cdot a = h \cdot a \Rightarrow a \mid b \quad \checkmark$$
$$\xrightarrow[\text{decir si:}]{\text{tambi\u00e9n puedo}} \left\{ \begin{array}{c} a \mid a^2 \\ a \mid b - a^2 \end{array} \right\} \xrightarrow[\text{propiedad}]{\text{por}} a \mid (b - a^2) + (a^2) = b \Rightarrow a \mid b \quad \checkmark$$

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

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

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

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.

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

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

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

Busco eliminar la n del *miembro* derecho.

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

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

ii)

iii)

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

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

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

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

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 $a + b \mid a^n + b^n$.

$$\text{i) Si } a-b \mid a^n - b^n \xLeftrightarrow{\text{def}} a^n \equiv b^n (a-b) \iff \left\{ \begin{array}{l} a \equiv b (a-b) \\ a^2 \equiv \underbrace{a}_{\substack{(a-b) \\ \equiv b}} \cdot b (a-b) \rightarrow a^2 \equiv b^2 (a-b) \\ \vdots \\ a^n \equiv b^n (a-b) \end{array} \right\}$$

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

$$\text{ii) Sé que } a \equiv -b (a+b) \iff \left\{ \begin{array}{l} a^2 \equiv \underbrace{a}_{\substack{(a-b) \\ \equiv -b}} \cdot b (a+b) \xrightarrow[\text{congruencia}]{\text{propiedad}} a^2 \equiv (-1)^2 \cdot b^2 (a+b) \\ \vdots \quad \star^1 \leftarrow \\ a^n \equiv (-1)^n \cdot b^n (a+b) \rightarrow \left\{ \begin{array}{ll} a^n \equiv b^n (a+b) & \text{con n par} \\ a^n \equiv (-1)^n \cdot b^n (a+b) & \text{con n impar} \end{array} \right\} \star^2 \end{array} \right\}$$

$$\star^2 \left\{ \begin{array}{l} \text{Con } n \text{ par: } a^n \equiv b^n (a+b) \Rightarrow a+b \mid a^n - b^n \\ \text{Con } n \text{ impar: } a^n \equiv -b^n (a+b) \Rightarrow a+b \mid a^n + b^n \end{array} \right.$$

\star^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:

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

Hipótesis inductiva:

$$p(k) \text{ V} \Rightarrow p(k+1) \text{ V?}$$

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

Parto de $p(k)$:

$$\left\{ \begin{array}{l} a^k \equiv (-1)^k \cdot b^k (a+b) \\ \xrightarrow[\text{por } a]{\text{multiplico}} a \cdot a^k \equiv (-1)^k \cdot \underbrace{a}_{\substack{(a-b) \\ \equiv -b}} \cdot b^k (a+b) \\ \xrightarrow{\text{y acomodo}} a^{k+1} \equiv (-1)^{k+1} \cdot b^{k+1} (a+b) \quad \checkmark \end{array} \right.$$

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: $p(n) : 2^{n+2} \mid a^{2^n} - 1$

$$\left\{ \begin{array}{l} \text{Caso base: } p(1) : 2^3 \mid a^2 - 1 = (a-1) \cdot (a+1) \xrightarrow[a=2m-1]{a \text{ es impar}} (2m-2) \cdot (2m) = \\ 4 \cdot \underbrace{m \cdot (m-1)}_{\text{par}} = 4 \cdot (2 \cdot h) = 8 \cdot h \xrightarrow[\text{tanto}]{\text{por lo}} 8 \mid 8 \cdot h \text{ con } h \text{ entero. } \checkmark \\ \text{Paso inductivo: } p(k) V \Rightarrow p(k+1) V? \xrightarrow[\text{decir}]{\text{es}} 2^{k+2} \mid a^{2^k} - 1 \Rightarrow 2^{k+3} \mid a^{2^{k+1}} - 1 V? \\ \text{Hipótesis inductiva:} \\ \left\{ \begin{array}{l} 2^{k+3} \mid a^{2^{k+1}} - 1 \xrightarrow[\text{diferencia cuadrados}]{\text{acomodar}} 2 \cdot 2^k \mid (a^{2^k})^2 - 1 = \\ (a^{2^k} - 1) \cdot (a^{2^k} + 1) \\ \left\{ \begin{array}{l} \text{par} \quad \text{par} \\ \frac{a \mid b}{a \cdot c \mid b \cdot d} \iff \frac{a \cdot k_1 = b}{a \cdot c \cdot \underbrace{k_3}_{k_1 \cdot k_2} = b \cdot d} \end{array} \right\} \xrightarrow{\text{Si } a \mid b \text{ y } c \mid d} \underbrace{2^{k+2}}_a \cdot \underbrace{2}_c \mid \underbrace{(a^{2^k} - 1)}_b \cdot \underbrace{(a^{2^k} + 1)}_d \Rightarrow 2^{k+3} \mid a^{2^{k+1}} - 1 \quad V \quad \checkmark \end{array} \right. \end{array} \right\}$$

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

5. _____

6. _____

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) $99 \mid 10^{2n} + 197 \xLeftrightarrow{def} 10^{2n} + 197 \equiv 0 \pmod{99} \rightarrow 10^{2n} + 198 \equiv 1 \pmod{99} \rightarrow 10^{2n} + \underbrace{198}_{\substack{(99) \\ \equiv 0}} \equiv 1 \pmod{99} \rightarrow$

$$100^n \equiv 1 \pmod{99} \rightarrow \left\{ \begin{array}{l} \xrightarrow[\text{que}]{\text{sé}} 100 \equiv 1 \pmod{99} \iff 100^2 \equiv \underbrace{100}_{\substack{(99) \\ \equiv 1}} \pmod{99} \rightarrow 100^2 \equiv 1 \pmod{99} \iff \dots \iff 100^n \equiv 1 \pmod{99} \\ \text{\textcolor{red}{Tengo que demostrar ser en gl n por inducción con "propiedad de congruencia" funciona?}} \end{array} \right.$$

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

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

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

0 (9)

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

iii) **Hacer!**

iv) **Hacer!**

Algoritmo de División:

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

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

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

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

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

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

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

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

ii)

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

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

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

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:

iv) 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) $\left\{ \begin{array}{l} a = 3 \cdot q + r_3(a) \\ 6 \cdot a = 18 \cdot q + \underbrace{6 \cdot r_3(a)}_{r_{18}(6a)} \end{array} \right\} \rightarrow r_{18}(6a) = r_{18}(r_{18}(6) \cdot r_{18}(a)) = r_{18}(30) = 12$
 $\Rightarrow 6 \cdot r_3(a) = r_{18}(6a) \rightarrow r_3(a) = 2$

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

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

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

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

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

10.

- i) Si $a \equiv 22 \pmod{14}$, hallar el resto de dividir a a por 14, por 2 y por 7.
- ii) Si $a \equiv 13 \pmod{5}$, 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

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

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

$$\xrightarrow[r_5(a)=3]{\text{como } a \equiv 13 \pmod{5}} r_5(33a^3 + 3a^2 - 197a + 2) = 4$$

iii) **Hacer!**

11.

- i) Probar que $a^2 \equiv -1 \pmod{5} \iff a \equiv 2 \pmod{5} \vee a \equiv 3 \pmod{5}$
- ii) Probar que no existe ningún entero a tal que $a^3 \equiv -3 \pmod{7}$
- iii) Probar que $a^7 \equiv a \pmod{7} \quad \forall a \in \mathbb{Z}$
- 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.

$$\left\{ \begin{array}{l} a^2 \equiv -1 \pmod{5} \iff a^2 \equiv 4 \pmod{5} \iff a^2 - 4 \equiv 0 \pmod{5} \iff (a-2) \cdot (a+2) \equiv 0 \pmod{5} \\ \xrightarrow[\text{resto sea } 0]{\text{quiero que el}} r_5(a^2 + 1) = r_5(a^2 - 4) = r_5(r_5(a-2) \cdot r_5(a+2)) = \underbrace{r_5((r_5(a)-2) \cdot (r_5(a)+2))}_{\star^1} = 0 \\ \\ \xrightarrow[0 \text{ cuando}]{\text{el resto será}} r_5(a^2 + 1) = 0 \star^1 \iff r_5((r_5(a)-2) \cdot (r_5(a)+2)) = 0 \left\{ \begin{array}{l} r_5(a) = 2 \iff a \equiv 2 \pmod{5} \quad \checkmark \\ r_5(a) = -2 \iff a \equiv \underbrace{3}_{\substack{(5) \\ \equiv -2}} \pmod{5} \quad \checkmark \end{array} \right. \end{array} \right.$$

Más aún:

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

a	0	1	2	3	4
-----	---	---	---	---	---

$r_5(a)$ 0 1 2 3 4 \rightarrow La tabla muestra que para un dado a

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

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

- ii) **Hacer!**

- 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.

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

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

\rightarrow Cómo para todos los a , alguno de los factores del resto siempre

se anula, es decir:

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

iv)

v)

12. _____

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

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

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.

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

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

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

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

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

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

15. _____

16. _____

17. _____

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

19. _____

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

- i) Probar que $(5a + 8 : 7a + 2) = 1$ o 41. Exhibir un valor de a para el cual da 1, y verificar que efectivamente para $a = 23$ da 43
 - ii) Probar que $(2 \cdot a^2 + 3a : 5a + 6) = 1$ o 43. Exhibir un valor de a para el cual da 1, y verificar que efectivamente para $a = 16$ da 43
 - iii) 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). que efectivamente para $a = 16$ da 43
-

i) **Pasar!**

ii) **Hacer!**

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

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

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

Parecido al hecho en clase.

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

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

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

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

22.

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

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

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

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

ii) **Hacer!**

iii) **Hacer!**

Primos y factorización:

24.

25. Sea p primo positivo.

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