Apunte Único: Álgebra I - Práctica 4

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

última actualización 12/02/26 @ 13:23

Choose your destiny:

(dobleclick en los ejercicio para saltar)

- Notas teóricas
- Ejercicios de la guía:

- Ejercicios de Parciales

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

¡Recomendación para sacarle jugo al apunte!

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

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

Ahora sí mirá la solución.

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

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

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

Mirá los videos de las teóricas:
de Teresa que son buenísimos.

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

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

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

Esta Guía 4 que tenés se actualizó por última vez:
12/02/26 @ 13:23
Escaneá el QR para bajarte (quizás) una versión más nueva:

Guía 4

El resto de las guías repo en github para descargar las guías con los últimos updates.

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

Notas teóricas:

Divisibilidad:

- Definición divisibilidad y notación:

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

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

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

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

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

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

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

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

Definición congruencia:

- *Definición congruencia:*

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

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

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

.

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

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

Un caso particular con un simpático resultado:

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

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
- $\underbrace{0 \leq r < |d|}_{\text{cumple condición de resto}} \implies r = r_d(r)$. 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:

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

- El resto es único:

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

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

- 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,

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

y,

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

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 $b \mid a \implies (a:b) = |b|$ con $b \in \mathbb{Z} - \{0\}$
- Útil para ejercicios: $(a:b) = (a:b+na)$ con $n \in \mathbb{Z}$
- Útil para ejercicios: $(a:b) = (a:r_a(b))$ con $n \in \mathbb{Z}$
- Útil para ejercicios: Sean $a,\ b \in \mathbb{Z}$ no ambos nulos, y sea $k \in \mathbb{N}$

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

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

  Sean $a, b \in \mathbb{Z}$ no ambos nulos, entonces $\exists\, s,\ t \in \mathbb{Z}$ tal que $(a:b) = s \cdot a + t \cdot b$.

  - Todos los divisores comunes entre a y b dividen al $(a:b)$. Sean $a, b \in \mathbb{Z}$ no ambos nulos, $d \in \mathbb{Z} - \{0\}$. Entonces:
  $$d \mid a \quad \text{y} \quad d \mid b \iff d \mid \underbrace{(a:b)}_{s\cdot a + t\cdot b}.$$
  - Sea $c \in \mathbb{Z}$ entonces $\exists\, s', t' \in \mathbb{Z}$ con $c = s'a + t'b \iff (a:b) \mid c$.
  - Todos los números múltiplos del MCD se escriben como combinación entera de a y b.
  - Si un número es una combinación entera de a y b entonces es un múltiplo del MCD.

Coprimos:

- Definición coprimos:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\begin{cases} \text{Si } m \,|\, n \implies m = p_1^{\beta_1} \cdots p_k^{\beta_k} \text{ con } 0 \leq \beta_i \leq \alpha_i, \quad \forall i \;\; 1 \leq i \leq k \\ \qquad \text{y la cantidad total de divisores de } n \text{ es} \\ (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_k + 1) = \prod_{i=1}^{k} (\alpha_i + 1) \end{cases}$$

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

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

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

$$d \,|\, a \iff d^n \,|\, a^n.$$

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

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

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

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

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

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

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

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

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

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

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

Este ejercicio clave para el resto de la materia.

a) Esta proposición es verdadera:

$$a \cdot b \mid c \overset{\text{def}}{\iff} c = a \cdot b \cdot q \quad \text{con } q \in \mathbb{Z}$$

Mirando cada número por separado:

$$\begin{cases} c = a \cdot b \cdot q \overset{!}{=} a \cdot q' \overset{\text{def}}{\iff} a \mid c \\ c = a \cdot b \cdot q \overset{!}{=} b \cdot q'' \overset{\text{def}}{\iff} b \mid c \end{cases}$$

b) La proposición es verdadera:

$$4 \mid a^2 \overset{\text{def}}{\iff} a^2 = 4 \cdot q = 2 \cdot 2 \cdot q = 2 \cdot q'$$

Es decir que a^2 es un número par, más aún:

$$a^2 \text{ es par} \iff a \text{ es par} \quad \text{con } a \in \mathbb{Z}$$

Y bueh, si a es par entonces $2 \mid a$.

c) La afirmación es verdadera.

$$2 \mid a \cdot b \overset{\text{def}}{\iff} a \cdot b = 2 \cdot q \quad \bigstar^1$$

El producto de 2 números es par, si y solo si alguno es par:

2 pares:

$$2n \cdot 2m = 2 \cdot \underbrace{(2 \cdot n \cdot m)}_{q'} = 2 \cdot q'$$

1 par y el otro impar

$$2n \cdot (2m - 1) = 2 \cdot \underbrace{(2 \cdot n \cdot m - n)}_{q'} = 2 \cdot q'$$

Con este resultado en $\bigstar^1$ queda:

$$a \cdot b = 2 \cdot q' \iff 2 \mid a \ \vee \ 2 \mid b$$

d) La proposición es falsa.

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

e) La proposición es falsa.

Contraejemplo: Se tiene que $12 \mid 20 + 4$, sin embargo $12 \nmid 20$ ni $12 \nmid 4$

f) La proposición es falsa.

Contraejemplo: Se tiene que $4 \mid 12 \ \wedge \ 6 \mid 12$, sin embargo $24 \nmid 12$

g) La proposición es falsa.

Contraejemplo: Se tiene que $2 \mid -4$, sin embargo $2 \not\leq -4$

h) La proposición es falsa.

Contraejemplo: Se tiene que $4 \mid 0$, sin embargo $|4| > 0$

En el caso en que $b \neq 0$ la proposición es verdadera.

$$a \mid b \underset{q \in \mathbb{Z}_{\neq 0}}{\overset{\text{def}}{\iff}} b = a \cdot q \overset{!}{\Leftrightarrow} |b| = |a \cdot q| \Leftrightarrow |b| = |a| \cdot |q| \overset{!}{\Leftrightarrow} |b| \geq |a|$$

i) La proposición es verdadera.

$$a \mid b + a^2 \overset{\text{def}}{\iff} b + a^2 = a \cdot q \overset{!}{\Leftrightarrow} b = a \cdot (q - a) \Leftrightarrow b = a \cdot q' \overset{\text{def}}{\iff} a \mid b$$

j) La proposición es verdadera.

Pruebo por inducción. Quiero probar que la siguiente proposición es verdadera:

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

Caso base:

$$p(1) : a \mid b \implies a^1 \mid b^1$$

$p(1)$ resultó verdadera.

Paso inductivo:

Asumo que para algún $h \in \mathbb{N}$ la proposición:

$$p(h) : \underbrace{a \mid b \implies a^h \mid b^h}_{\text{hipótesis inductiva}}$$

es verdadera, entonces quiero probar que la proposición:

$$p(h+1) : a \mid b \implies a^{h+1} \mid b^{h+1}$$

también lo sea.

Si:

$$\begin{aligned}
a \mid b &\overset{\text{HI}}{\implies} a^h \mid b^h \\
&\overset{\text{def}}{\iff} b^h = a^h \cdot q \\
&\overset{\times b}{\iff} b^{h+1} = b \cdot a^h \cdot q \\
&\underset{b = a \cdot q'}{\overset{a \mid b}{\iff}} b^{h+1} = a \cdot q' \cdot a^h \cdot q = a^{h+1} \cdot q'' \\
&\overset{\text{def}}{\iff} a^{h+1} \mid b^{h+1}.
\end{aligned}$$

Como $p(1)$, $p(h)$ y $p(h+1)$ resultaron verdaderas, por el principio de inducción la proposición $p(n)$ es verdadera $\forall n \in \mathbb{N}$.

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

$$a \mid b \implies a^n \mid b^n \iff b \equiv 0 \ (a) \implies b^n \equiv 0 \ (a^n) \underset{0 \overset{(a^n)}{\equiv} a^n}{\iff} b^n \equiv a^n \ (a^n)$$

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

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

---

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) Busco eliminar la n del *miembro* derecho.

$$\left\{\begin{array}{l|l} 3n-1 & n+7 \\ 3n-1 & 3n-1 \end{array}\right. \xrightarrow{3F_1 - F_2 \to F_1} \left\{\begin{array}{l|l} 3n-1 & 22 \\ 3n-1 & 3n-1 \end{array}\right.$$

Con ese resultado sé que $3n-1$ es un *posible divisor* de 22:

$$d = 3n-1 \in \{\pm 1, \pm 2, \pm 11, \pm 22\}$$

Pero ahora hay que probar para cuáles valores de n, obtengo alguno de esos valores d.
Probando a manopla:

$$\begin{aligned} d = 1 &\xRightarrow{\text{☠}} n = \varnothing \\ d = 2 &\xRightarrow[\text{con}]{\text{sale}} n = 1 \\ d = 11 &\xRightarrow[\text{con}]{\text{sale}} n = 4 \\ d = 22 &\xRightarrow{\text{☠}} n = \varnothing \end{aligned}$$

b) Trato de sacar la n del lado derecho:

$$\left\{\begin{array}{l|l} 3n-2 & 5n-8 \\ 3n-2 & 3n-2 \end{array}\right. \xrightarrow{3F_1 - 5F_2 \to F_1} \left\{\begin{array}{l|l} 3n-2 & -14 \\ 3n-2 & 3n-2 \end{array}\right.$$

Con ese resultado sé que $3n-2$ es un *posible divisor* de 14:

$$d = 3n-2 \in \{\pm 1, \pm 2, \pm 7, \pm 14\}$$

Pero ahora hay que probar para cuáles valores de n, obtengo alguno de esos valores d:

$$\begin{aligned} d = 1 &\xRightarrow[\text{con}]{\text{sale}} n = 1 \\ d = 2 &\xRightarrow{\text{☠}} n = \varnothing \\ d = 7 &\xRightarrow[\text{con}]{\text{sale}} n = 3 \\ d = 14 &\xRightarrow{\text{☠}} n = \varnothing \end{aligned}$$

c) Trato de sacar la n del lado derecho:

$$\left\{\begin{array}{l|l} 2n+1 & n^2+5 \\ 2n+1 & 2n+1 \end{array}\right. \xrightarrow{nF_2 - 2F_1 \to F_1} \left\{\begin{array}{l|l} 2n+1 & n-10 \\ 2n+1 & 2n+1 \end{array}\right. \xrightarrow{2F_1 - F_2 \to F_1} \left\{\begin{array}{l|l} 2n+1 & -21 \\ 2n+1 & 2n+1 \end{array}\right.$$

Con ese resultado sé que $2n+1$ es un *posible divisor* de 21:

$$d = 2n+1 \in \{\pm 1, \pm 3, \pm 7, \pm 21\}$$

Pero ahora hay que probar para cuáles valores de n, obtengo alguno de esos valores d, pero me da pajilla .

d) A veces se ve y a veces no, pero:

$$\begin{array}{rr|l} n^3 & -8 & n-2 \\ \cline{3-3} -n^3+2n^2 & & n^2+2n+4 \\ \cline{1-1} 2n^2 & & \\ -2n^2+4n & & \\ \cline{1-1} 4n-8 & & \\ -4n+8 & & \\ \cline{1-1} 0 & & \end{array}$$

Por lo que:

$$n^3-8 \overset{!}{=} (n-2)\cdot(n^2+2n+4) \implies n-2 \mid n^3-8 \qquad \forall n \in \mathbb{N}_{\neq 2}$$

---

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

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

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

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

---

a) *Inducción:*

Proposición:

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

Caso Base:

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

$p(1)$ es verdadera. ✓

Paso inductivo:

Asumo que

$$p(k): \underbrace{a-b \mid a^k-b^k}_{\text{hipótesis inductiva}}$$

es verdadera $\implies$ quiero probar que

$$p(k+1): a-b \mid a^{k+1}-b^{k+1}$$

también lo sea.

Parto de algo verdadero, de la hipótesis inductiva:

$$\left\{ \begin{array}{l} a-b \mid a^k-b^k \\ a-b \mid a-b \end{array} \right. \xRightarrow[\times b^k]{\times a} \left\{ \begin{array}{l} a-b \mid a^{k+1}-ab^k \\ a-b \mid ab^k-b^{k+1} \end{array} \right. \xRightarrow{F_1+F_2} \left\{ \ a-b \mid a^{k+1}-b^{k+1} \right.$$

La *epifanía* esa de multiplicar a y b^k se te puede ocurrir o no, si no la viste, no te mortifiques, *la cosa no va por ahí* 😉.

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

b) Sé que

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

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

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

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

$\bigstar^1$ *Inducción:*

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

Caso base:

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

$p(1)$ es verdadera.

Paso inductivo:

Asumo que

$$p(k) : \underbrace{a \equiv -b \ (a+b) \implies a^k \equiv (-1)^k \cdot b^k \ (a+b)}_{\text{hipótesis inductiva}}$$

es verdadera asumo verdadera para algún $k \in \mathbb{Z}$
Entonces quiero probar que:

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

también lo sea.

Partiendo de $p(k)$, la hipótesis inductiva:

$$\begin{aligned} a \equiv -b \ (a+b) \implies a^k \equiv (-1)^k \cdot b^k \ (a+b) \quad &\overset{\times a}{\implies} \quad a \cdot a^k = a^{k+1} \equiv (-1)^k \cdot \overset{\overset{(a+b)}{\equiv} -b}{\overset{\uparrow}{a}} \cdot b^k \ (a+b) \\ &\implies \quad a^{k+1} \equiv (-1)^{k+1} \cdot b^{k+1} \ (a+b) \\ &\overset{\text{def}}{\iff} \quad a+b \mid a^{k+1} - (-1)^{k+1} b^{k+1} \end{aligned}$$

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  .

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Oliv Portero

---

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:

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

Como $a \in \mathbb{Z}$ es impar, puedo escrirla como:

$$a \overset{\bigstar^1}{=} 2m - 1$$

Entonces

$$\begin{aligned}(a-1)\cdot(a+1) &\overset{\bigstar^1}{=} (2m-2)\cdot(2m)\\ &\overset{!}{=} 4\cdot \underbrace{m\cdot(m-1)}_{\substack{\text{seguro}\\ \text{es par}}}\\ &\overset{!!}{=} 4\cdot 2h = 8\cdot h\end{aligned}$$

Es decir que $a^2 - 1 = 8 \cdot h$ con $h \in \mathbb{Z}$. Por lo tanto:

$$8 \,\big|\, 8h = (a-1)\cdot(a+1) \text{ para algún } h \in \mathbb{Z}$$

La proposición $p(1)$ es verdadera.

Paso inductivo:
Asumo que para algún valor de $k \in \mathbb{N}$ que:

$$p(k) : \overbrace{2^{k+2} \,\big|\, a^{2^k} - 1}^{\text{hipótesis inductiva}},$$

es verdadera, entonces quiero probar que la proposición:

$$p(k+1) : 2^{k+3} \,\big|\, a^{2^{k+1}} - 1,$$

también lo sea.

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

$$\overset{\overset{\text{Si } a\,|\,b \;\text{ y }\; c\,|\,d \implies ac\,|\,bd}{\longleftrightarrow}}{\text{hipótesis inductiva}}$$

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

El !! es todo tuyo (*hints:* diferencia de cuadrados, propiedades de exponentes... 👏)
En el último paso se comprueba que $p(k+1)$ es verdadera.
Como $p(1), p(k) \quad$ y $\quad p(k+1)$ resultaron verdaderas, por el principio de inducción también lo será $p(n) \;\; \forall n \in \mathbb{N}$.

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

5.

i) Probar que si n es compuesto, entonces $2^n - 1$ es compuesto.

ii) Probar que si $2^n + 1$ es primo, entonces n es una potencia de 2.

Un número compuesto es un número natural que tiene más de 2 divisores. Un número compuesto n se puede escribir como el producto de 2 números menores, en particular son dos divisores de n, $n = d_1 \cdot d_2$.

i) Mirá el ejercicio **3.** a ver si se te ocurre como usar ese resultado en esta parte.
A partir del resultado dle ejercicio **3.**: $a^n - b^n \equiv 0 \;(a-b) \;\; \forall n \in \mathbb{N} \quad$ y $\quad a \neq b \in \mathbb{Z}$.

$$\begin{aligned}a^n - b^n \equiv 0 \;(a-b) &\overset{\text{def}}{\iff} a^n - b^n = (a-b)\cdot k\\ &\overset{\substack{a=2^{d_1}\\ n=d_2}}{\iff} (2^{d_1})^{d_2} - b = (2^{d_1}-b)\cdot k\\ &\overset{b=1}{\iff} 2^{d_1\cdot d_2} - 1 = (2^{d_1}-1)\cdot k\end{aligned}$$

Por lo tanto una potencia de 2 con un exponente *compuesto* menos 1, es otro número compuesto.

ii) Mirá el ejercicio **4.** a ver si se te ocurre como usar ese resultado en esta parte.

Por contrarrecíproco:

$$(p \implies q) \iff (\neg q \implies \neg p)$$

Entonces, queremos probar que dado n divisible por un primo impar, p, es decir que $n \neq 2^m$, entonces $2^n + 1$ es compuesto, es decir que no es primo ni a palos.

Dado un p impar:

$$p \mid n \overset{\text{def}}{\iff} n = p \cdot q,$$

Asegurando así que $n \neq 2^m$. Del ejercicio **4.** sé que para un natural impar, p en este caso:

$$a + b \mid a^p + b^p \overset{\text{def}}{\iff} a^p + b^p = (a+b) \cdot k \underset{b=1}{\overset{a=2^q}{\iff}} (2^q)^p + 1 = (2^q + 1) \cdot k \Leftrightarrow \boxed{2^{p \cdot q} + 1 = (2^q + 1) \cdot k}$$

El último resultado muestra que:

$$\left(\text{Si } n \neq 2^k \implies 2^n + 1 \text{ no es primo} \right) \iff \left(\text{Si } 2^n + 1 \text{ es primo} \implies n \text{ es una potencia de 2.} \right)$$

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

6.

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

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

---

a) Este es bastante sencillo de ver, tenemos el producto de n enteros consecutivos como:

$$\prod_{i=m}^{n+m-1} i = m \times (m+1) \times \cdots \times (n+m-1)$$

Por ejemplo:

$$\prod_{i=4}^{7} i = 4 \times 5 \times 6 \times 7$$

Tenemos que ver que es divisible por $n!$, si uno se lo pone a pensar intuitivamente, es bastante logico ya que $n!$ va a siempre compartir factores, de hecho el factorial se puede definir como $\prod_{i=1}^{n} i = n!$, asi que si empezamos desde otro indice no cambia nada, igual sigue siendo divisible por $n!$.

Vamos a probarlo por inducción porque es lo más fácil, sino se podría generalizar con productorias pero es un *quilombo de notación.*

Tenemos que nuestra hipotesis inductiva es:

$$p(n) : \prod_{i=m}^{n} i \text{ es divisible por } n!$$

Probemos el caso base $p(1)$:

$$p(1) : \prod_{i=m=1}^{1} i = 1 \text{ es divisible por } 1!$$

Ahora queremos ver que $p(n) \implies p(n+1)$

$$\prod_{i=m}^{n+1} i \text{ es divisible por } (n+1)! \text{ ?}$$

$$(n+1) \times \underbrace{\prod_{i=m}^{n} i}_{\text{hipótesis inductiva}} \text{ es divisible por } \underbrace{n! \times (n+1)}_{=(n+1)!} \bigstar^1$$

Finalmente entonces probamos que $p(n+1)$ es verdadera, completando la prueba.

$\bigstar^1$: Aca usamos que $a \mid b \implies t \cdot a \mid t \cdot b,\ t \in \mathbb{Z}$

b) Expandimos el coeficiente binomial con su fórmula de factoriales:

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$$

Si fuera par, eso significa que al dividirlo por dos obtengo un número entero, entonces la idea va a ser esa:

$$\frac{(2n)!}{(n!)^2} \cdot \frac{1}{2} = \frac{(\cancel{2}n)(2n-1)!}{(n!)^2} \cdot \frac{1}{\cancel{2}}$$

Entonces me basta ver que

$$\frac{n(2n-1)!}{(n!)^2} \quad \in \mathbb{Z}$$

Manipulamos la expresión un poco:

$$\frac{\cancel{n}(2n-1)!}{(n!)\cancel{n}(n-1)!}$$

Ahora podemos ver que esta expresión es lo mismo que $\binom{2n-1}{n-1}$, el cual es un número entero. Concluimos entonces que $\binom{2n}{n}$ es par.

△ Para más intuición, fijarse que en el triángulo de pascal, el coeficiente $\binom{2n}{n}$ es justo la mitad de la fila con n par (en este caso el n seria el $2n$ de nuestro coeficiente binomial), pueden ver que todos los valores que están en el medio en el triángulo de pascal surgen de la suma de los dos de arriba, que son exactamente iguales. △

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

---

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

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

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

c) $56 \mid 13^{2n} + 28n^2 - 84n - 1 \overset{\text{def}}{\iff} 13^{2n} + 28n^2 - 84n - 1 \equiv 0\ (56)$. Procedemos a probar esto por induccion:

$$p(n) : 13^{2n} + 28n^2 - 84n - 1 \equiv 0\ (56)$$

Caso base:

$$p(1) : 13^2 + 28 - 84 - 1 \equiv 0\ (56) \tag{1}$$
$$0 \equiv 0\ (56) \quad \checkmark \tag{2}$$

Asumimos $p(n)$ verdadera, queremos ver que $p(n+1)$ también lo es.

$$13^{2n+2} + 28(n+1)^2 - 84(n+1) - 1 \equiv 0\ (56) \tag{3}$$
$$13^{2n} \cdot 13^2 + 28n^2 + 56n + 28 - 84n - 84 - 1 \equiv 0\ (56) \tag{4}$$
$$\underbrace{13^{2n} + 28n^2 + 56n - 84n}_{\text{hipotesis inductiva}} + 28 - 84 + 13^2 - 1 \equiv 0\ (56) \tag{5}$$
$$28 - 84 + 168 \equiv 0\ (56) \tag{6}$$
$$112 \equiv 0\ (56) \quad \checkmark \tag{7}$$

Se probó que $p(n+1)$ es verdadera, luego $p(n)$ es verdadera para todo $n \in \mathbb{N}$

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

Sale por inducción:

Quiero ver que:

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

O en notación de congruencia:

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

Caso base:

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

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

Paso inductivo:

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

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

es una proposición verdadera. Entonces quiere probar que:

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

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

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

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

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

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

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

Algoritmo de División:

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

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

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

Voy a usar q para el cociente y r para el resto:

⚠ r tiene que cumplir condición de resto: $0 \leq r \leq |d|$. ⚠

Congruencia:

$$d \mid a \overset{\text{def}}{\iff} a \equiv 0\ (d)$$

a) $a = 133 = -14 \cdot \underset{\downarrow q}{-9} + \underset{\downarrow r}{7}$

b) $13 \div 111 \implies 13 = 111 \cdot \underset{\downarrow q}{0} + \underset{\downarrow r}{13}$

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

dividendo →	$a = 3b+7$	-5	-2	1	4	10	13	16	19	22	25	28	31	34
divisor →	b	-4	-3	-2	-1	1	2	3	4	5	6	7	8	9
cociente →	q	2	1	0	-4	10	6	5	4	4	4	4	3	3
resto →	$0 \leq r \leq \lvert d\rvert$	3	1	1	0	0	1	1	3	2	1	0	7	7

Pasando en limpio, para $b \in \mathbb{Z}_{\neq 0}$:

$$\begin{cases} q_b(a) = 3 & \text{para} \quad |b| \geq 8 \\ r_b(a) = 7 & \text{para} \quad |b| \geq 8 \\ \text{ver tabla} & \text{para} \quad |b| < 8 \end{cases}$$

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

Quiero hacer $\frac{a}{b} = \frac{b^2-6}{b}$:

$$b^2 - 6 = \underset{\downarrow}{b} \cdot \overset{\uparrow}{b} - 6 \quad \begin{matrix} q \\ \\ d \end{matrix}$$

Posibles valores para a, b, q y r:

dividendo →	$a = b^2 - 6$	-5	-5	-2	-2	3	3	10	10
divisor →	b	1	-1	2	-2	3	-3	4	-4
cociente →	q	-5	5	-1	1	1	-1	2	-2
resto →	$0 \leq r \leq \lvert d \rvert$	0	0	0	0	0	0	2	2

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

Quiero hacer $\frac{a}{b} = \frac{n^2+5}{n+2}$:

$$\begin{array}{r|l} n^2 + 5 & n+2 \\ \cline{2-2} -n^2 - 2n & n-2 \\ \cline{1-1} -2n + 5 & \\ 2n + 4 & \\ \cline{1-1} 9 & \end{array} \qquad \rightarrow \qquad n^2 + 5 = \underbrace{(n+2)}_{d} \cdot \overbrace{(n-2)}^{q_n} + 9$$

Posibles valores para a, b, q y r:

	n	1	2	3	4	5	6	7	8	9	10	11
dividendo →	$a = n^2 + 5$	6	9	14	21	30	41	54	69	86	105	126
divisor →	$b = n + 2$	3	4	5	6	7	8	9	10	11	12	13
cociente →	q	2	2	2	3	4	5	6	6	7	8	9
resto →	$0 \leq r \leq \lvert d \rvert$	0	1	4	3	2	1	0	9	9	9	9

Entonces en la tabla están los valores de los cocientes. Los primeros están sacados a manopla:

$$\begin{cases} q_b(a) = n - 2 & \text{para} \quad n \geq 8 \\ r_b(a) = 9 & \text{para} \quad n \geq 8 \end{cases}$$

f) Cuando b sea mayor que a el resto va a ser simplemente a, asi que busco cuando esto se cumpla Digo que $n^2 + 1 > n + 3 \Leftrightarrow n^2 - n - 2 > 0 \Leftrightarrow n > 2 \Leftrightarrow n \geq 3$. Hago los casos separados para $n = 1$ y $n = 2$.

$n = 1$. $a = 4$, $b = 2$, $q = 2$, $r = 0$

$n = 2$. $a = 5$, $b = 5$, $q = 1$, $r = 0$

Finalmente

$$q_b(a) = \begin{cases} 2 \text{ si } n = 1 \\ 1 \text{ si } n = 2 \\ 0 \text{ si } n \geq 3 \end{cases} \qquad r_b(a) = \begin{cases} 0 \text{ si } n < 3 \\ n + 3 \text{ si } n \geq 3 \end{cases}$$

---

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

b) Dividir a cualquier valor a por 3 es hacer:

$$a = 3 \cdot q + r_3(a) \bigstar^1$$

Busco que en el algoritmo de división quede como divisor 18 para poder usar el dato de que $r_{18}(a) = 5$. Multiplico en $\bigstar^1$ por 6 ambos miembros:

$$6 \cdot a = 6 \cdot 3 \cdot q + 6 \cdot r_3(a) \iff 6a = 18 \cdot q + \underbrace{6 \cdot r_3(a)}_{\substack{\text{esto debe ser} \\ r_{18}(6a)}}$$

Por lo tanto usando el *dato* de $r_{18}(a) = 5$:

$$r_{18}(6a) = 6 \cdot r_3(a) \underset{\text{dato}}{\overset{!!}{\iff}} 30 = 6 \cdot r_3(a) \Leftrightarrow 5 = r_3(a) \underset{\text{de resto}}{\overset{\text{condición}}{\iff}} \boxed{r_3(a) = 2}$$

c) Dividir a cualquier valor $4a + 1$ por 9 es hacer:

$$4a + 1 = 9 \cdot q + r_9(4a + 1) \bigstar^1$$

Busco que en el algoritmo de división quede como divisor 18 para poder usar el dato de que $r_{18}(a) = 5$. Multiplico en $\bigstar^1$ por 2 ambos miembros:

$$2 \cdot (4a + 1) = 2 \cdot 9 \cdot q + 2 \cdot r_9(4a + 1) \iff 8a + 2 = 18 \cdot q + \underbrace{2 \cdot r_9(4a + 1)}_{\substack{\text{esto debe ser} \\ r_{18}(8a+2)}}$$

Por lo tanto usando el *dato* de $r_{18}(a) = 5$:

$$r_{18}(8a + 2) = 2 \cdot r_9(4a + 1) \underset{\text{dato}}{\overset{!!}{\iff}} 8 \cdot 5 + 2 = 2 \cdot r_9(4a + 1) \Leftrightarrow 21 = r_3(a) \underset{\text{de resto}}{\overset{\text{condición}}{\iff}} \boxed{r_9(4a + 1) = 2}$$

d) A ver el resto de esa expresión:

$$r_{28}(7a^2 + 12) = r_{28}(7 \cdot r_{28}(a)^2 + 12)$$

La pregunta ahora es ¿qué 💩 es $r_{28}(a)\bigstar^1$? Sé por enunciado que:

$$r_{18}(a) = 5 \underset{}{\overset{\text{def}}{\iff}} a = 18 \cdot q + 5$$

La idea ahora es modificar esa expresión para que me quede un 28 de divisor:

$$a = 18 \cdot q + 5 = 2 \cdot 9q + 5 \underset{\text{M.A.M}}{\overset{\times\, 14}{\iff}} 14 \cdot a = \underbrace{14 \cdot 2}_{28} \cdot 9 \cdot q + 70$$

Ahora tengo que *toquetear* esa expresión para que quede algo de la pinta divisor × cociente + resto:

$$14 \cdot a = 28 \cdot 9q + 70 \Leftrightarrow 14 \cdot a = 28 \cdot 9q + 2 \cdot 28 + 14 \overset{!}{=} 28 \cdot \underbrace{(9q + 2)}_{q'} + 14$$

$\downarrow$ también se podría tomar congruencia 28 en ambos miembros

Entonces queda que:

$$14 \cdot a = 28 \cdot q' + 14 \underset{}{\overset{\text{def}}{\iff}} 14a \equiv 14 \ (28) \Leftrightarrow a \equiv 1 \ (28) \Leftrightarrow r_{28}(a) = 1$$

Lo que logré fue encontrar una expresión donde el divisor sea 28 ¡Y así contesté $\bigstar^1$!

Ahora que sé que $r_{28}(a) = 1$ sale que

$$r_{28}(7a^2 + 12) = r_{28}(7 \cdot r_{28}(a)^2 + 12) = r_{28}(7 \cdot 1 + 12) = r_{28}(a) = 19$$

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

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) Queremos hallar el resto, planteemos una ecuacion de congruencia:

$$\sum_{i=1}^{n}(-1)^i \cdot i! \equiv r\ (12)$$

Ahora expandimos la suma para ver el patron que tiene y ver si podemos simplificar algo:

$$-1 + 2 - 6 + 24 - \cdots + (-1)^k \cdot n! \equiv r\ (12)$$

Notemos que el 24 es divisor de 12, además todos los terminos subsiguientes, van a tener de factores $4 \cdot 3$, por lo cual los terminos que le sigue al 24 todos van a ser divisibles por 12, o sea podemos reescribir la ecuacion como:

$$-1 + 2 - 6 + 12h \equiv r\ (12)$$

Luego:

$$-1 + 2 - 6 \equiv r\ (12)$$
$$-5 \equiv r\ (12)$$

Sumo 12 a ambos miembros

$$-5 + 12 \equiv r + 12\ (12)$$

Finalmente

$$7 \equiv r\ (12)$$

Entonces concluimos que el resto para los $n \geq 4$ al dividir por 12 es de 7. Para los primeros terminos va a haber que calcularlo manualmente.
Para $n = 1$, $-1 \equiv 11\ (12)$
Para $n = 2$ $-1 + 2 \equiv 1\ (12)$
Para $n = 3$, $-1 + 2 - 6 \equiv 7\ (12)$
La respuesta final es entonces: Para $n = 1$, $r = 11$, $n = 2$, $r = 1$, $n \geq 3$, $r = 7$

11.

a) Probar que $a^2 \equiv -1\ (5) \iff a \equiv 2\ (5) \quad \text{o} \quad a \equiv 3\ (5)$

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 $5 \mid a^2 + b^2 + 1 \implies 5 \mid a \quad \text{o} \quad 5 \mid b$. ¿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.

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

Más aún:

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

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

→ La tabla muestra que para un dado a

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

b) Empezamos reescribiendo la expresión $a^3 + 7 \equiv -3 + 7\ (7) \longrightarrow a^3 \equiv 4\ (7)$.
Ahora solo nos basta con probar todas las posibilidades para $0 \leq a \leq |6|$ ya que si tuvieramos 7 directamente el resto seria 0, y si tenemos algun numero mayor que 7, la ecuacion se puede reescribir como:

$$(7+m)^3 \equiv 4\ (7)$$

$$(\underbrace{7^3 + 7^2 \cdot m + 7 \cdot m^2}_{\text{divisibles por } 7} + m^3) \equiv 4\ (7)$$

$$m^3 \equiv 4\ (7)$$

Eso se puede seguir haciendo iterativamente hasta eventualmente tener un $m \leq 7$, en donde entrarian nuestros casos base, esto se podria y se deberia enunciar con induccion global para ser mas formal, pero bueno la idea se entiende.
Entonces veamos los $|a| \leq 6$:

Para $|a| = 0$ es trivial, el resto es 0

Para $|a| = 1$, $a^3 = \pm 1$, $1 \equiv 1\ (7)$, $-1 \equiv 6\ (7)$

Para $|a| = 2$, $a^3 = \pm 8$, $8 \equiv 1\ (7)$, $-8 \equiv 6\ (7)$

Para $|a| = 3$, $a^3 = \pm 27$, $27 \equiv 6\ (7)$, $-27 \equiv 1\ (7)$

$$\text{Para } |a| = 4,\ a^3 = \pm 64,\ 64 \equiv 1\ (7),\ -64 \equiv 6\ (7)$$
$$\text{Para } |a| = 5,\ a^3 = \pm 125,\ 125 \equiv 6\ (7),\ -125 \equiv 1\ (7)$$
$$\text{Para } |a| = 6,\ a^3 = \pm 216,\ 216 \equiv 6\ (7),\ -216 \equiv 1\ (7)$$

Como vemos, ninguno es congruente con 4, por ende queda probado que no existe nigun entero a tal que $a^3 \equiv -3\ (7)$

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

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

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

d) Tenemos una doble implicación, asique hay que probar los dos lados:
$\Rightarrow$)
Que $7 \mid a^2 + b^2$ puede reescribirse como $a^2 + b^2 \equiv 0\ (7)$, lo que queremos entonces es que la suma de los restos de dividir por 7 a a^2 y a b^2 sumen 0, para eso podemos armar una tablita, primero veamos cuales son los restos de dividir por 7 a un numero de la forma m^2:
$r_7(0^2) = 0 \quad r_7(1^2) = 1 \quad r_7(2^2) = 4 \quad r_7(3^2) = 2 \quad r_7(4^2) = 2 \quad r_7(5^2) = 4 \quad r_7(6^2) = 1$

Entonces ahora armamos una tablita:

$r_7(b^2)$ \ $r_7(a^2)$	0	1	2	4
0	0	1	2	4
1	1	2	3	5
2	2	3	4	6
4	4	5	6	1

De la tabla vemos que los unicos posibles restos de 7 que sumados dan 0 como resto de 7, son 0 y 0, y el unico numero m del 0 al 6 tal que $r_7(m^2) = 0$ es $m = 0$, o sea que a y b ambos tienen que ser 0. Dicho de otro modo, la solucion de la ecuacion de congruencia $a^2 + b^2 \equiv 0\ (7)$ es $(a, b) = (0, 0)$. Está claro que el 7 divide al 0 asique queda probada la primera implicacion.
$\Leftarrow$)
Ahora el otro lado, este es mas sencillo. Tenemos de hipotesis que $7 \mid a$ y $7 \mid b$, por ende $7 \mid a + b$ y $7 \mid a \cdot b$. Entonces tambien se cumple que $7 \mid (a + b) \cdot (a + b)$, por lo que $7 \mid a^2 + 2a \cdot b + b^2$, y finalmente como $2ab$ es divisible por 7 se puede reescribir finalmente todo como $7 \mid a^2 + b^2$.
Finalmente se han probado las dos implicaciones, por lo tanto la proposicion inicial es verdadera

e) $5 \mid a^2 + b^2 + 1 \Leftrightarrow a^2 + b^2 + 1 \equiv 0 \Leftrightarrow a^2 + b^2 \equiv 4\,(5)$. Ahora armamos una tabla de cuadrados congruencia 5 para ver como se podria formar esta suma.

a	0	1	2	3	4
a^2	0	1	4	4	1

Observamos que la unica forma de que dos cuadrados sumen 4 es que alguno sea 4 y el otro sea 0. Bien, supongamos sin perdida de generalidad que $a^2 \equiv 4\ (5)$ y $b^2 \equiv 0\ (5)$, sigue que $b \equiv 0\ (5) \Leftrightarrow 5 \mid b$, como se queria demostrar (el caso para a es simetrico). Ahora nos piden comprobar si la vuelta se cumple también.

Contraejemplo: $a = 5$ y $b = 4$, $5^2 + 4^2 + 1 = 42$, pero $5 \nmid 42$. Entonces la implicacion inversa no se cumple.

12.

(a) Probar que $2^{5k} \equiv 1\ (31)$ para todo $k \in \mathbb{N}$.

(b) Hallar el resto de la división de 2^{51833} por 31.

(c) Sea $k \in \mathbb{N}$. Sabiendo que $2^k \equiv 39\ (31)$, hallar el resto de la división de k por 5.

(d) Hallar el resto de la división de $43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999}$ por 31.

(a) Probémoslo por inducción.

Sea la proposición

$$P(k) : 2^{5k} \equiv 1\ (31),\ \ \forall k \in \mathbb{N}$$

- *Caso base*:

$$P(1) : 2^{5\cdot 1} \equiv 1\ (31) \iff 32 \equiv 1\ (31) \quad \checkmark$$

Luego, $P(1)$ es verdadera.

- *Paso inductivo* $P(k) \implies P(k+1)$

Asumiendo verdadero $\underbrace{2^{5k} \equiv 1\ (31)}_{\text{hipótesis inductiva}}$, queremos probar que $2^{5(k+1)} \equiv 1\ (31)$ también es verdadero.

De la hipótesis inductiva tenemos que

$$2^{5k} \equiv 1\ (31) \xrightarrow{32 \equiv 1\ (31)} 2^{5k} \cdot 32 \equiv 1 \cdot 1\ (31) \iff 2^{5k} \cdot 2^5 \equiv 1\ (31) \iff 2^{5(k+1)} \equiv 1\ (31) \quad \checkmark$$

Luego, $P(k+1)$ es verdadera.

Como $P(1)$ es verdadera y $P(k) \implies P(k+1),\ \forall\ k \in \mathbb{N}$, por el principio de inducción, $P(k)$ es verdadera para todo $k \in \mathbb{N}$

(b) Queremos hallar el resto de la división de 2^{51833} por 31, lo que es lo mismo que buscar a qué es congruente 2^{51833} módulo 31.

Observemos que $2^5 \equiv 1\ (31)$, con lo que dividiendo 51833 por 5, tenemos que $51833 = 5 \cdot 10366 + 3$. Luego

$$2^{51833} \equiv 2^{5\cdot 10366+3} \equiv 2^{5\cdot 10366} \cdot 2^3 \equiv (2^5)^{10366} \cdot 8 \equiv 1^{10366} \cdot 8 \equiv 8\ (31)$$

Entonces, $\boxed{r_{31}\left(2^{51833}\right) = 8}$

(c) Como $39 \equiv 8\ (31)$, tenemos que $2^k \equiv 8\ (31)$. Busquemos ahora que valores puede tomar k.

Si van probando valores, van a darse cuenta que el 3, 8, 13, 18, ... funcionan, lo que nos permite conjetuar que $k = 3 + 5q,\ q \in \mathbb{N}$. Entonces podemos conjeturar que

$$2^k \equiv 8\ (31) \iff k = 3 + 5q,\ q \in \mathbb{N}$$

Probemos la doble implicación.

($\Leftarrow$) Reemplazando $k = 3 + 5q$, tenemos que

$$2^k \equiv 2^{3+5q} \equiv 2^3 \cdot 2^{5q} \equiv 8 \cdot 32^q \equiv 8 \cdot 1^q \equiv 8\ (31) \quad \checkmark$$

($\Rightarrow$) Tenemos que probar que k solo puede ser de la forma $k = 3 + 5q$. Para esto debemos verificar que si k es igual a $c + 5q$, con $c \in \{0, 1, 2, 4\}$ entonces $2^k \not\equiv 8\ (31)$. Pues así estariamos viendo todas las posibilidades. Reemplacemos entonces $k = c + 5q$:

$$2^k \equiv 2^{c+5q} \equiv 2^c \cdot 2^{5q} \equiv 2^c \cdot 32^q \equiv 2^c \cdot 1^q \equiv 2^c\ (31)$$

Veamos ahora los valores de c

$$\begin{aligned} c = 0 \to 2^k \equiv 2^0 \equiv 1 \not\equiv 8\ (31) \\ c = 1 \to 2^k \equiv 2^1 \equiv 2 \not\equiv 8\ (31) \\ c = 2 \to 2^k \equiv 2^2 \equiv 4 \not\equiv 8\ (31) \\ c = 4 \to 2^k \equiv 2^4 \equiv 16 \not\equiv 8\ (31) \end{aligned}$$

Dado que ninguno es congruente a 8 módulo 31, llegamos a la conclusión de que los únicos valores que puede tomar k son los de la forma $k = 3 + 5q,\ q \in \mathbb{N}$.

Por último, dado que $k = 3 + 5q$, es evidente que $3 + 5q \equiv 3\ (5)$. Entonces $\boxed{r_5(k) = 3}$

(d) Reduzcamos cada término módulo 31.

Es fundamental notar que $2^5 \equiv 1\ (31)$, que $5^3 \equiv 1\ (31)$ y que $61 \equiv -1\ (31)$ Entonces

$$\begin{aligned} 43 &\equiv 12\ (31) \\ 2^{163} \equiv 2^{5\cdot 32+3} &\equiv (2^5)^{32} \cdot 8 \equiv 8\ (31) \\ 5^{221} \equiv 5^{3\cdot 73+2} &\equiv (5^3)^{73} \cdot 25 \equiv 25\ (31) \\ 61^{999} &\equiv (-1)^{999} \equiv -1\ (31) \end{aligned}$$

Juntando todo

$$43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999} \equiv 12 \cdot 8 + 11 \cdot 25 - 1 \equiv 370 \equiv 29\ (31)$$

Luego, $\boxed{r_{31}(43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999}) = 29}$

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

---

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:

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

La congruencia módulo 7 de la sucesión:

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

Quiero probar que $a_n \equiv 3^n \pmod 7$ por inducción:

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

Casos base:

$$\begin{cases} p(1) : a_1 \equiv 3^1 \ (7) \\ p(2) : a_2 = -5 \overset{(7)}{\equiv} 9 \equiv 3^2 \ (7) \end{cases}$$

Las proposiciones $p(1)$ y $p(2)$ son verdaderas.
Paso Inductivo: Asumo que para algún $k \in \mathbb{N}$ y para $k+1$ las proposiciónes:

$$p(k) : \underbrace{a_k \equiv 3^k \ (7)}_{\text{hipótesis inductiva}} \quad \text{y} \quad p(k+1) : \underbrace{a_{k+1} \equiv 3^{k+1} \ (7)}_{\text{hipótesis inductiva}}$$

son verdaderas, entonces quiero probar que:

$$p(k+2) : a_{k+2} \equiv 3^{k+2} \ (7)$$

también lo sea.
Partiendo de mis hipótesis inductivas sé que:

$$\begin{cases} a_{k+1} \equiv 3^{k+1} \pmod 7 \\ a_k \equiv 3^k \pmod 7 \end{cases}$$

Restando miembro a miembro eso me formo a_{k+2} resultado de ★[1]:

$$a_{k+2} \overset{(7)}{\equiv} a_{k+1} - a_k \equiv 3^{k+1} - 3^k = 2 \cdot 3^k \overset{(7)}{\equiv} 9 \cdot 3^k = 3^{k+2} \Leftrightarrow a_{k+2} \equiv 3^{k+2} \ (7)$$

$p(k+2)$ resultó verdadera.
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 $\forall n \in \mathbb{N}$.

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

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.

A veces escribo $(12)_2 = 1100$ para decir *El número* 12 *en base dos es* 1100 y a veces puede ser que se escriba como $12 = (1100)_2$. A mí me gusta la primera, pero bueh, mientras se entienda, .

Para hallar el desarrollo en base 2 de algún número dado su representación decimal, simplemente dividimos por 2, truncamos, anotamos el resto y seguimos iterando hasta que lleguemos a 0, luego escribimos los restos que conseguimos en orden inverso y esta es la representación.

Pequeño ejemplo para que se vea: Consideremos el número 6, que su representación en base 2 es:

$$6 = 2^2 \cdot 1 + 2^1 \cdot 1 + 2^0 \cdot 0 \implies (6)_2 = 110$$

Lo mismo pero usando una notación de $n \xrightarrow{r_2(n)} \lfloor \frac{n}{2} \rfloor$:

$$6 \overset{0}{\to} 3 \overset{1}{\to} 1 \overset{1}{\to} 0 \quad ★[1]$$

Ahora ponemos en reversa los restos que obtuvimos en ★[1], y nos queda:

$$2^2 \cdot 1 + 2^1 \cdot 1 + 2^0 \cdot 0 \implies (6)_2 = 110$$

(a) i.

$$1365 \xrightarrow{1} 682 \xrightarrow{0} 341 \xrightarrow{1} 170 \xrightarrow{0} 85 \xrightarrow{1} 42 \xrightarrow{0} 21 \xrightarrow{1} 10 \xrightarrow{0} 5 \xrightarrow{1} 2 \xrightarrow{0} 1 \xrightarrow{1} 0.$$

Hacemos el display en reversa y nos da:

$$(1365)_2 = 10101010101,$$

cada 1 representa que multiplica al respectivo 2^d y 0 que lo hace cero. En este caso lo escribimos con 0 y 1 porque es más conveniente que andar poniendo tal multiplicado por 2^d

ii.

$$2800 \xrightarrow{0} 1400 \xrightarrow{0} 700 \xrightarrow{0} 350 \xrightarrow{0} 175 \xrightarrow{1} 87 \xrightarrow{1} 43 \xrightarrow{1} 21 \xrightarrow{1} 10 \xrightarrow{0} 5 \xrightarrow{1} 2 \xrightarrow{0} 1 \xrightarrow{1} 0.$$

Hacemos el display en reversa y nos da:

$$(2800)_2 = 10101111000.$$

iii.

$$3 \cdot 2^{12} = (2+1) \cdot 2^{12} = 2^{13} + 2^{12} \overset{!}{=} 2^{13} \cdot 1 + 2^{12} \cdot 1 + \sum_{i=0}^{11} 2^{11-i} \cdot 0$$

Queda como:

$$(3 \cdot 2^{12})_2 = 11000000000000.$$

iv.

$$13 \cdot 2^n + 5 \cdot 2^{n-1} = (2^3 + 2^2 + 2^0) \cdot 2^n + (2^2 + 2^0) \cdot 2^{n-1} = 2^{n+3} + 2^{n+2} + 2^n + 2^{n+1} + 2^{n-1}$$

Para algún $n \in \mathbb{N}$ queda como:

$$(13 \cdot 2^n + 5 \cdot 2^{n-1})_2 = 11111\underbrace{0 \cdots 0}_{n-1 \text{ dígitos}}$$

(b) Así como en base 2, un dígito puede tomar 2 valores, el 0 o el 1, en base 16 cada dígito de nuestro número puede tomar 16 posibles valores:

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ A,\ B,\ C,\ D,\ E \quad \text{o} \quad F$$

Es igual a lo anterior, pero ahora los posibles restos serán valores entre 0 y $\underset{\downarrow}{F}$:
$\scriptstyle 15$

$$2800 \xrightarrow{0} 175 \xrightarrow{F} 10 \xrightarrow{A} 0.$$

Entonces su representación en base 16:

$$(2800)_{16} = AF0$$

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

---

15. Sea $a = (a_d a_{d-1} \dots a_1 a_0)_2$ un número escrito en base 2 (o sea escrito en bits). Determinar simplemente como son las escrituras en base 2 del número $2a$ y del número $a/2$ cuando a es par, o sea las operaciónes "multiplicar por 2" y "dividir por 2" cuando se puede. Estas operaciónes se llaman *shift* en inglés, o sea corrimiento, y son operaciónes que una computadora hacer en forma sencilla.

$$a = (a_d a_{d-1} \dots a_1 a_0)_2$$

podemos escribirlo en base 10 como:

$$\bigstar^1 a = 2^d \cdot a_d + 2^{d-1} \cdot a_{d-1} + \cdots + 2^1 \cdot a_1 + 2^0 \cdot a_0.$$

Multiplicamos por 2 y obtenemos:

$$2a = 2^{d+1} \cdot a_d + 2^d \cdot a_{d-1} + \cdots + 2^1 \cdot a_0 + 2^0 \cdot 0$$

En base 2 este número sería:

$$2a = (a_d a_{d-1} \dots a_1 a_0 0)_2.$$

Vemos que los números se *corrieron a la izquierda*. Esta operación es el *left shift*.

Hacemos lo mismo pero dividiendo ★[1] por 2:

$$\frac{a}{2} = 2^{d-1} \cdot a_d + 2^{d-2} \cdot a_{d-1} + \cdots + 2^1 a_2 + 2^0 a_1 + r,$$

escrito en base 2 sería:

$$\frac{a}{2} = (a_d a_{d-1} \dots a_2 a_1)_2$$

ya que el resto se elimina. Vemos que perdimos información del último dígito, porque dividimos por 2 y truncamos.

---

16. Enunciar y demostrar criterios de divisibilidad por 8 y por 9.

- **Criterio de divisibilidad por 8:**

  Sea $a = (r_n r_{n-1} \dots r_3 r_2 r_1 r_0)_{10}$ el desarrollo decimal de a, con $0 \leq r_k \leq 9$. Entonces

  $$8 \mid a \iff 8 \mid (r_2 r_1 r_0)_{10}$$

  Es decir, a es divisible por 8 si y solo si el número formado por las 3 últimas cifras de a es divisible por 8.

  Demostración:

  Observemos que $10^3 \equiv 0\ (8)$. Probemos entonces por inducción que $P(m) : 10^m \equiv 0\ (8),\ m \geq 3$

  - **Caso Base**: $P(3)$
    $10^3 \equiv 0\ (8)$ ✓
  - **Paso inductivo**: $P(m) \implies P(m+1)$

  $$10^{m+1} \equiv 10^m \cdot 10 \overset{\textbf{(HI)}}{\equiv} 0 \cdot 10 \equiv 0 \pmod 8$$

  Entonces, $P(m)$ es verdadera para todo $m \geq 3$

  Luego, como $a = 10^n r_n + 10^{n-1} r_{n-1} + \cdots + 10^3 r_3 + 10^2 r_2 + 10 r_1 + r_0$, tomando congruencia módulo 8 tenemos que

  $a = 10^n r_n + 10^{n-1} r_{n-1} + \cdots + 10^3 r_3 + 10^2 r_2 + 10 r_1 + r_0 \equiv 0 + 0 + \dots 0 + 10^2 r_2 + 10 r_1 + r_0 \pmod 8$

  Luego,

  $$8 \mid a \iff a \equiv 0\ (8) \iff 10^2 r_2 + 10 r_1 + r_0 \equiv 0\ (8) \iff (r_2 r_1 r_0)_{10} \equiv 0\ (8) \iff 8 \mid (r_2 r_1 r_0)_{10}$$

- **Criterio de divisibilidad por 9:**

  Sea $a = (r_n r_{n-1} \dots r_1 r_0)_{10}$ el desarrollo decimal de a, con $0 \leq r_k \leq 9$. Entonces

  $$9 \mid a \iff 9 \mid r_n + r_{n-1} + \cdots + r_1 + r_0$$

Es decir, a es divisible por 9 si y solo si la suma de los dígitos de a es divisible por 9.

Demostración:

Observemos que $10 \equiv 1\ (9)$, con lo que $10^m \equiv 1\ (9),\ m \in \mathbb{N}_0$

Luego, como $a = 10^n r_n + 10^{n-1} r_{n-1} + \cdots + 10 r_1 + r_0$, tomando congruencia módulo 9 tenemos que

$a = 10^n r_n + 10^{n-1} r_{n-1} + \cdots + 10 r_1 + r_0 \equiv r_n + r_{n-1} + \cdots + r_1 + r_0 \pmod 9$

Luego,

$$9 \mid a \iff a \equiv 0\ (9) \iff r_n + r_{n-1} + \cdots + r_1 + r_0 \equiv 0\ (9) \iff 9 \mid r_n + r_{n-1} + \ldots r_1 + r_0$$

17.

(a) Sea $k \in \mathbb{N}, k = (aaaa)_7$. Probar que $8 \mid k$

(b) Sea $k \in \mathbb{N}, k = (\underbrace{a \ldots a}_{d})_7$. Determinar para qué valores de $d \in \mathbb{N}$ se tiene que $8 \mid k$

(a) Expreamos k en base 10: $7^3 \cdot a + 7^2 \cdot a + 7^1 \cdot a + a = a(7^3 + 7^2 + 7 + 1) = a(400), 8 \mid 400 \implies 8 \mid a(400) = k$

(b) Expresamos k en base 10:

$$a(7^{d-1} + 7^{d-2} + \cdots 7 + 1).$$

Queremos que lo adentro sea múltiplo de 8, motivado por el ejercicio anterior, vemos que si agrupamos dos potencias de 7 contiguas tal que la primera potencia sea par obtenemos un múltiplo de 8, veamos que onda.

Propongo que:

$$8 \mid 7^{2k} + 7^{2k+1} = 7^{2k}(1 + 7),$$

claramente divisible por 8, entonces necesitamos que vengan potencias de 7 de a pares, luego d tiene que ser par. Entonces el enunciado se cumple siempre que $d \equiv 0\ (2)$.

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

---

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

---

i) Para calcular el máximo común divisor hay que usar el *algoritmo de Euclides*, en forma matricial lo que hago es ir restando las filas hasta encontrar el 0, el valor de la fila anterior es le mcd.

Lo que me gusta de este método es que en cada línea vas a escribiendo una combinación entera entre los números sin mucho esfuerzo.

1	0	2532	F_1
0	1	63	F_2
1	-40	12	$F_3 = F_1 - 40F_2$
-5	201	3	$F_4 = F_2 - 5F_3$
–	–	0	$F_5 = F_3 - 4F_4$

El *máximo común divisor* entre 2532 y 63 escrito como combinación entera de los mismos:

$$\boxed{3 = -5 \cdot 2532 + 201 \cdot 63}$$

También se puede encontar el $(2532 : 63)$ haciendo la factorización en primos y agarrando las potencias comunes elevadas al menor exponente:

$$2532 = 2^2 \cdot 3^1 \cdot 211 \quad \text{y} \quad 63 = 3^2 \cdot 7 \implies (2532 : 63) = 3^1$$

ii) Dado que 131 y 23 son dos números primos, sabemos que $(131 : 23)$. El tema es la combinación entera para lo cual vuelvo a usar el método matricial de Euclides.

1	0	131	F_1
0	1	23	F_2
1	-5	16	$F_3 = F_1 - 5F_2$
-1	6	7	$F_4 = F_2 - F_3$
3	-17	2	$F_5 = F_3 - 2F_4$
-10	57	1	$F_6 = F_4 - 3F_5$
–	–	0	$F_7 = F_5 - 2F_6$

El *máximo común divisor* entre 2532 y 63 escrito como combinación entera de los mismos:

$$\boxed{1 = -10 \cdot 131 + 57 \cdot 23}$$

iii) En este caso con estos polinomios hago división polinomial:

$$\begin{array}{rr|l} n^4 & -3 & n^2+2 \\ \cline{3-3} -n^4-2n^2 & & n^2-2 \\ \cline{1-1} -2n^2-3 & & \\ 2n^2+4 & & \\ \cline{1-1} 1 & & \end{array}$$

Tengo según Euclides:

$$(n^4 - 3 : n^2 + 2) = (n^2 + 2 : 1) = 1$$

Por el algoritmo de división sé que:

$$n^4 - 3 = (n^2+2) \cdot (n^2-2) + 1 \Leftrightarrow \boxed{1 = 1 \cdot (n^4 - 3) + -(n^2-2) \cdot (n^2+2)}$$

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

---

19. Sean $a, b \in \mathbb{Z}$. Sabiendo que el resto de dividir a a por b es 27 y que el resto de dividir b por 27 es 21, calcular $(a : b)$

Traducimos lo que nos da el enunciado a congruencias y tenemos:

$$\begin{cases} a \equiv 27 \ (b) & \overset{\text{def}}{\iff} \quad a = b \cdot j + 27 \text{ con } j \in \mathbb{Z} \ ★^1 \\ b \equiv 21 \ (27) & \overset{\text{def}}{\iff} \quad b = 27 \cdot k + 21 \text{ con } k \in \mathbb{Z} \ ★^2. \end{cases}$$

Reescribimos el *máximo común divisor* $(a : b)$:

$$(a : b) \overset{★^1}{=} (b \cdot j + 27 : b) \overset{!}{=} (27 : b) \overset{★^2}{=} \big(27 : (27 \cdot k + 21)\big) \overset{!}{=} (27 : 21) \overset{!}{=} (21 : 6) \overset{!}{=} (6 : 3) = (3^2 : 3^1) = 3$$

Quizás los últimos pasos son medio un *overkill*, pero quedó claro.
Si en los ! te quedás pensando: No es otra cosa que el algoritmo de Euclides.

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

---

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

a) Probar que $(5a+8 : 7a+3) = 1 \quad$ 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 $(2a^2 + 3a - 1 : 5a + 6) = 1 \quad$ 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 $(a^2 - 3a + 2 : 3a^3 - 5a^2) = 2 \quad$ 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) Si $d = (5a + 8 : 7a + 3)$, entonces d divide ambas expresiones:

$$\left\{ \begin{array}{l|l} d & 5a+8 \\ d & 7a+3 \end{array} \right. \xrightarrow{7F_1 - 5F_2 \to F_2} \left\{ \begin{array}{l|l} d & 5a+8 \\ d & 41 \end{array} \right.$$

Para que se cumpla ese último resultado:

$$d \in \{\pm 1, \pm 41\}$$

Pero el *máximo común divisor* es positivo así que:

$$d \in \{1, 41\}$$

Si $a = 1$ queda $d = (13 : 10) = 1$. En el caso en que $a = 23$:

$$d = (123 : 164) \overset{!}{=} (123 : 41) = 41$$

Donde en el ! usé Euclides. Haciendo el algoritmo de Euclides, recordar que el valor del *máximos común divisor* se encuentra en el último resto distinto de 0.

ii) Si $d = (2a^2 + 3a - 1 : 5a + 6)$, entonces d divide ambas expresiones:

$$\left\{ \begin{array}{l|l} d & 2a^2+3a-1 \\ d & 5a+6 \end{array} \right. \xrightarrow{5F_1 - 2aF_2 \to F_1} \left\{ \begin{array}{l|l} d & 3a-5 \\ d & 5a+6 \end{array} \right. \xrightarrow{5F_1 - 3F_2 \to F_2} \left\{ \begin{array}{l|l} d & 3a-5 \\ d & -43 \end{array} \right.$$

Para que se cumpla ese último resultado:

$$d \in \{\pm 1, \pm 43\}$$

Pero el *máximo común divisor* es positivo así que:

$$d \in \{1, 43\}$$

Si $a = 0$ queda $d = (-1 : 6) = 1$. En el caso en que $a = 16$:

$$d = (559 : 86) \overset{!}{=} (86 : 42) \overset{!}{=} (86 : 43) = 43$$

Donde en el ! usé Euclides. Haciendo el algoritmo de Euclides, recordar que el valor del *máximos común divisor* se encuentra en el último resto distinto de 0.

iii) Dado que voy a hacer cuentas en la cuales a no puede ser 0. Me saco de encima eso primero:

$$a = 0 \implies (a^2 - 3a + 2 : 3a^3 - 5a^2) = (0 : -2) = 2$$

Acomodo un poco y hago Euclides haciendo división de polinomios para achicar la expresión:

$$\begin{array}{rr|l} 3a^3 - 5a^2 & & a^2 - 3a + 2 \\ \cline{2-2} -3a^3 + 9a^2 & -6a & 3a + 4 \\ \cline{1-2} 4a^2 & -6a & \\ -4a^2 + 12a & -8 & \\ \cline{1-2} 6a & -8 & \end{array}$$

Con ese resultado:

$$d = (a^2 - 3a + 2 : 3a^3 - 5a^2) = (a^2 - 3a + 2 : 6a - 8)$$

Procedo ahora a encontrar los posibles divisores comunes:

$$\left\{ \begin{array}{l|l} d & a^2 - 3a + 2 \\ d & 6a - 8 \end{array} \right. \xrightarrow[a \neq 0]{6F_1 - 2aF_2 \to F_1} \left\{ \begin{array}{l|l} d & -2a + 12 \\ d & 6a - 8 \end{array} \right. \xrightarrow{3F_1 + F_2 \to F_1} \bigstar^1 \left\{ \begin{array}{l|l} d & 28 \\ d & 6a - 8 \end{array} \right.$$

Para que se cumpla ese último resultado teniendo en cuenta que $28 = 2^2 \cdot 7$:

$$d \in \{\pm 1, \pm 2, \pm 4, \pm 7, \pm 14, \pm 28\}$$

Pero el *máximo común divisor* es positivo así que:

$$d \in \{1, 2, 4, 7, 14, 28\}$$

Hay que sacar posibles valores del MCD. De $\bigstar^1$ necesito que $d \mid 6a - 8$.

Puedo hacer una tabla de restos para estudiar eso:

$r_7(a)$	0	1	2	3	4	5	6
$r_7(6a-8)$	6	5	4	3	2	1	5

La tabla de restos dice que el 7 no divide núnca a la expresión $6a - 8$, por lo que podemos descartar todos los divisores que sean multiplos enteros de 7. Actualizo los posibles valores para d:

$$d \in \{1, 2, 4\}$$

Necesito como dice la **sugerencia**, descartar la posibilidad de que $d = 1$ para algún valor de a:

$r_2(a)$	0	1
$r_2(6a-8)$	0	0

La tabla dice que para todo valor de a la expresión va a ser divisible por 2. Eso descarta que 1 pueda ser *un máximos común divisor*.

$r_4(a)$	0	1	2	3
$r_4(6a-8)$	0	2	0	2

Juntando todos estos resultados se puede concluir:

$$d = \left\{ \begin{array}{lll} 2 & \text{si} & a \equiv 1\ (2) \vee a = 0 \\ 4 & \text{si} & a \equiv 0\ (4) \wedge a \neq 0 \end{array} \right.$$

O puesto de otra manera

$$d = \left\{ \begin{array}{lll} 2 & \text{si} & a \text{ es impar} \vee a = 0 \\ 4 & \text{si} & a \text{ par} \wedge a \neq 0 \end{array} \right.$$

Solo falta el ejemplo de a para que $d = 4$:

$$a = 2 \implies (a^2 - 3a + 2 : 3a^3 - 5a^2) = (0 : 4) = 4$$

---

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

Puedo buscar divisores comunes para ver si son coprimos:

$$\begin{cases} d \mid 7a - 3b \\ d \mid 2a - b \end{cases} \xrightarrow{2F_1 - 7F_2 \to F_1} \begin{cases} d \mid b \\ d \mid 2a - b \end{cases}$$

Pero también:

$$\begin{cases} d \mid 7a - 3b \\ d \mid 2a - b \end{cases} \xrightarrow{F_1 - 3F_2 \to F_2} \begin{cases} d \mid 7a - 3b \\ d \mid a \end{cases}$$

Es decir que d es un divisor común de a y b, peeeeeero por enunciado sé que $(a : b) = 1$. Por lo tanto el único divisor común que tienen 2 números coprimos es 1, así que d puede valer $d = \pm 1$, a los fines del ejercicio $d = 1$:

$$d = 1 = (7a - 3b : 2a - b)$$

La expresiones son números coprimos porque el único divisor común que tienen es 1.

---

22. Sean $a, b \in \mathbb{Z}$ con $(a : b) = 2$. Probar que los valores posibles para $(7a + 3b : 4a - 5b)$ son 2 y 94. Exhibir valores de a y b para los cuales da 2 y para los cuales da 94.

Si $d = (7a + 3b : 4a - 5b)$, entonces d divide a ambas expresiones. Podemos *coprimizar* para hacer las cuentas más chicas:
Dado que $(a : b) = 2$, puedo cambiar las variables:

$$\xrightarrow[\text{variables}]{\text{cambio}} {}^{1}\!\star \begin{cases} a &= 2A \\ b &= 2B \end{cases}$$

Donde ahora $(A : B) = 1$. Reemplazando en la expresión de d obtengo así una para D:

$$d = (7 \cdot 2A + 3 \cdot 2B : 4 \cdot 2A - 5 \cdot 2B) = 2 \cdot \underbrace{(7A + 3B : 4A - 5B)}_{D} \overset{{}^{2}\!\star}{=} 2D \implies D = (7A + 3B : 4A - 5B)$$

Busco posibles divisores de D:

$$\begin{cases} D \mid 7A + 3B \\ D \mid 4A - 5B \end{cases} \xrightarrow[7F_2 \to F_2]{4F_1 \to F_1} \begin{cases} d \mid 28A + 12B \\ d \mid 28A - 35B \end{cases} \implies d \mid 47B$$

$$\begin{cases} D \mid 7A + 3B \\ D \mid 4A - 5B \end{cases} \xrightarrow[3F_2 \to F_2]{5F_1 \to F_1} \begin{cases} D \mid 35A + 15B \\ D \mid 12A - 15B \end{cases} \implies D \mid 47A$$

Como A y B son coprimos los únicos posibles divisores de D son:

$$D \in \{1, 47\}$$

Para obtener el $D = 1$ por inspección saco:

$$A = 1 \ \wedge \ B = 0 \implies D = (7 : 4) = 1$$

Y en las variables originales ★[1]:

$$\boxed{a = 2 \ \wedge \ b = 0 \overset{★[2]}{\Longrightarrow} d = 2}$$

Para obtener el $D = 47$ por inspección saco:

$$A = 5 \ \wedge \ B = 4 \implies D = (47 : 0) = 47$$

Y en las variables originales ★[1]:

$$\boxed{a = 10 \ \wedge \ b = 8 \overset{★[2]}{\Longrightarrow} d = 94}$$

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

23.

a) Determinar todos los $a, b \in \mathbb{Z}$ coprimos tales que $\frac{b+4}{a} + \frac{5}{b} \in \mathbb{Z}$.

b) Determinar todos los $a, b \in \mathbb{Z}$ coprimos tales que $\frac{9a}{b} + \frac{7a^2}{b^2} \in \mathbb{Z}$.

c) Determinar todos los $a \in \mathbb{Z}$ tales que $\frac{2a+3}{a+1} + \frac{a+2}{4} \in \mathbb{Z}$.

---

a) Acomodo el enunciado como:

$$\frac{b+4}{a} + \frac{5}{b} = \frac{b^2 + 4b + 5a}{ab}$$

Quiero que esa fracción sea entera, lo cual es lo mismo que decir:

$$ab \mid b^2 + 4b + 5a$$

Dado que $a \perp b$:

$$\begin{cases} a|b^2 + 4b + 5a \\ b|b^2 + 4b + 5a \end{cases} \Leftrightarrow \begin{cases} a|b^2 + 4b \\ b|5a \end{cases} \overset{\text{sé que } b \nmid a}{\underset{b \text{ debe dividir a } 5}{\Longrightarrow}} \begin{cases} a|b \cdot (b+4) ★[1] \\ b|5 \end{cases}$$

Sale que:

$$b \in \{\pm 1, \pm 5\}$$

Puedo entonces probar valores de b y así ver que valor de a queda:

Si $b = 1$

$$\overset{★[1]}{\Longrightarrow} a \mid 5 \implies (a, b) = \begin{cases} (\pm 1, 1) \\ (\pm 5, 1) \end{cases}$$

Si $b = -1$

$$\overset{★[1]}{\Longrightarrow} a \mid -3 \implies (a, b) = \begin{cases} (\pm 1, -1) \\ (\pm 3, -1) \end{cases}$$

Si $b = 5$

$$\overset{★[1]}{\Longrightarrow} a \mid 45 \implies (a, b) \overset{!!}{=} \begin{cases} (\pm 1, 5) \\ (\pm 3, 5) \\ (\pm 9, 5) \end{cases}$$

Si $b = -5$

$$\overset{★[1]}{\Longrightarrow} a \mid 5 \implies (a, b) \overset{!!}{=} \{ \ (\pm 1, -5)$$

En el !! se usa que $a \perp b$

b) Acomodo el enunciado sacando denominador común:

$$\frac{9a}{b} + \frac{7a^2}{b^2} = \frac{9ab + 7a^2}{b^2}$$

Quiero que esa fracción sea entera, lo cual es lo mismo que decir:

$$b^2 \mid 9ab + 7a^2 \overset{!!!}{\Longrightarrow} b \mid 9ab + 7a^2 \Leftrightarrow b \mid 7a^2 \overset{a \perp b}{\Longleftrightarrow} b \mid 7$$

Sale que:

$$b \in \{\pm 1, \pm 7\}$$

Puedo entonces probar valores de b y así ver que valor de a queda:

Si $b = \pm 1$:

$$\frac{\pm 9a + 7a^2}{1} \in \mathbb{Z} \ \ \forall a \in \mathbb{Z} \implies (a, b) = (a, \pm 1)$$

Si $b = 7$:

$$\frac{9a \cdot 7 + 7a^2}{49} = \frac{9a + a^2}{7}$$

Esto último va a ocurrir cuando:

$$a^2 + 9a \equiv 0 \ (7) \Leftrightarrow a \cdot (a+2) \equiv 0 \ (7) \overset{\substack{a \perp 7 \\ b = 7}}{\Longleftrightarrow} a + 2 \equiv 0 \ (7) \Leftrightarrow a \equiv 5 \ (7)$$

Los pares (a, b) para satisfacer lo pedido son de la forma:

$$(a, b) = (a, 7) \quad \text{con} \quad a \equiv 5 \ (7)$$

Si $b = -7$: El desarrollo es igual que para el caso anterior y los pares quedan:

$$(a, b) = (a, -7) \quad \text{con} \quad a \equiv 2 \ (7)$$

c)

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

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

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

Busco eliminar la a del lado derecho:

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

Las cuentas del ! te las dejo a vos.

$4a + 4$ tiene que dividir a 16, onda $\frac{16}{4a+a} \in \mathbb{Z}$ por lo tanto necesitamos:

$$4a + a \in \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}.$$

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

$$\begin{aligned} 4 \cdot (-5) + 4 &= -16 \\ 4 \cdot (-3) + 4 &= -8 \\ 4 \cdot (-2) + 4 &= -4 \\ 4 \cdot 0 + 4 &= 4 \\ 4 \cdot 1 + 4 &= 8 \\ 4 \cdot 3 + 4 &= 16 \end{aligned}$$

reemplazando esos valores de a en $\bigstar^1$ se obtiene que $\bigstar^1 \in \mathbb{Z}$.

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Juan Iglesias M Poncini

---

24. Probar que existen infinitos primos positivos congruentes a 3 módulo 4.
Sugerencia: probar primero que si $a \in \mathbb{N}$ satisface $a \equiv 3\ (4)$, entonces existe p primo con $p \equiv 3\ (4)$ tal que $p \mid a$. Luego probar que si existieran sólo finitos primos congruentes a 3 módulo 4, digamos $p_1, p_2, \ldots, p_n$, entonces $a = -1 + 4\prod_{i=1}^{n} p_i$ sería mayor que 1 y no es divisible por ningún primo congruente a 3 módulo 4.

Comencemos probando la primera parte de la sugerencia:

$$\text{Dado } a \in \mathbb{N}, a \equiv 3\ (4) \implies \exists p \text{ primo con } p \equiv 3\ (4) \text{ tal que } p \mid a$$

Como $a \equiv 3\ (4) \iff a = 4k + 3$ y dado que $a \in \mathbb{N}$, es evidente que $a > 1$. Luego sabemos que $\exists p$ primo tal que $p \mid a$. Ahora debemos ver que $p \equiv 3\ (4)$. Para esto, apliquemos el TFA:

$$a = (P_1)^{n_1} \cdot (P_2)^{n_2} \cdots (P_r)^{n_r},\ n_1, n_2 \ldots, n_r \in \mathbb{N}$$

Notemos ahora que ninguno de los primos en la factorización de a puede ser 2, pues $a = 4k + 3 = 2(2k + 1) + 1$ es impar. Esto nos descarta que $p \equiv 0\ (4)$ o que $p \equiv 2\ (4)$, pues el único primo que cumple alguna es el 2. De modo que nos quedan dos opciones:

$$p \equiv 1\ (4) \quad \text{o} \quad p \equiv 3\ (4)$$

Prestemos atención a lo siguiente. Si todos los primos en la factorización de a fueran congruentes a 1 módulo 4, esto es

$$P_1 \equiv 1\ (4), P_2 \equiv 1\ (4), \ldots, P_r \equiv 1\ (4) \implies (P_1)^{n_1} \equiv 1\ (4), (P_2)^{n_2} \equiv 1\ (4), \ldots, (P_r)^{n_r} \equiv 1\ (4)$$

tendriamos que

$$a = (P_1)^{n_1} \cdot (P_2)^{n_2} \cdots (P_r)^{n_r} \equiv 1\ (4)$$

lo cual contradice nuestra hipótesis de que $a \equiv 3\ (4)$.
Así, probamos que al menos debe existir un p en la factorización de a (esto asegura que $p \mid a$), que cumpla que $p \equiv 3\ (4)$ si es que tenemos que $a \equiv 3\ (4)$, que era lo que queriamos probar.

Veamos ahora la segunda parte de la sugerencia (no voy a probar eso exactamente, pero es parecido).
Supongamos que existen finitos primos congruentes a 3 módulo 4, digamos $p_1, p_2, \ldots, p_n$. Esto nos permite definir a como $a = -1 + 4\prod_{i=1}^{n} p_i$. Notemos que como $a \in \mathbb{N}$, $a > 1$ y $a \equiv 3\ (4)$, podemos aplicar lo que probamos en la primera parte. Esto es: existe p primo con $p \equiv 3\ (4)$ tal que $p \mid a$. Notemos que este p debe ser alguno de los p_i.
Luego

$$\begin{cases} p_i \mid -1 + 4\prod_{i=1}^{n} p_i \\ p_i \mid 4\prod_{i=1}^{n} p_i \end{cases} \xrightarrow{F_2 - F_1} p_i \mid 1$$

Lo cual es absurdo. Esta contradicción proviene de la única suposición que hicimos, que existen finitos primos congruentes a 3 módulo 4.
Luego, existen infinitos primos congruentes a 3 módulo 4, que era lo que queriamos probar.

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

25. Sea p primo positivo.

(a) Probar que si $0 < k < p$, entonces $p \mid \binom{p}{k}$.

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

(a) Como $0 < k < p$, tenemos que $p \nmid k!$ y que $p \nmid (p-k)!$, pues *p es primo y no divide a ningún factor de ambos números.* Por la misma razón, se tiene que ★[1] $p \nmid k!(p-k)!$. Entonces

$$\frac{p!}{k!(p-k)!} = \binom{p}{k} \Leftrightarrow p! = \binom{p}{k} \cdot k!(p-k)! \Leftrightarrow p(p-1)! = \binom{p}{k} \cdot k!(p-k)! \xRightarrow[!!]{(p-1)! \in \mathbb{Z}} p \mid \binom{p}{k} \cdot k!(p-k)!$$

$$p \mid \binom{p}{k} \cdot k!(p-k)! \xLeftrightarrow[\text{★}^1 p \nmid k!(p-k)!]{p \text{ primo}} p \mid \binom{p}{k} \quad \checkmark$$

(b) Usando el binomio de Newton, tenemos que

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} \cdot a^k \cdot b^{p-k} = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} \cdot a^k \cdot b^{p-k}$$

Como en la nueva sumatoria tenemos que $0 < k < p$, podemos aplicar lo probado en el inciso (a), obteniendo que

$$\sum_{k=1}^{p-1} \binom{p}{k} \cdot a^k \cdot b^{p-k} \equiv 0 \ (p)$$

Ahora solo queda juntar todo

$$(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} \cdot a^k \cdot b^{p-k} \equiv a^p + b^p \pmod{p} \quad \checkmark$$

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

---

26. Decidir si existen enteros a y b no nulos que satisfagan

a) $a^2 = 3b^3$ b) $7a^2 = 8b^2$

---

a) Observando que hay un 3 del lado derecho, a ojo se puede ver que, por ejemplo, $(a, b) = (3^2, 3)$ cumple.

b) A simple vista, no parece haber una solución obvia. Veamos la factorización en primos para ver si encontramos una contradicción.
Por TFA, se tiene que

$$\begin{cases} a = (P_1)^{m_1} ... (P_r)^{m_r}, \ m_1, ..., m_r \in \mathbb{N}_0 \\ b = (P_1)^{n_1} ... (P_r)^{n_r}, \ n_1, ..., n_r \in \mathbb{N}_0 \end{cases} \implies \begin{cases} a^2 = (P_1)^{2m_1} ... (P_r)^{2m_r} \\ b^2 = (P_1)^{2n_1} ... (P_r)^{2n_r} \end{cases}$$

Entonces

$$7a^2 = 8b^2 \iff 7^1 \cdot (P_1)^{2m_1} ... (P_r)^{2m_r} = 2^3 \cdot (P_1)^{2n_1} ... (P_r)^{2n_r}$$

Del lado izquierdo de la igualdad, el 7 aparece con el exponente $2m_7 + 1$.
Del lado derecho de la igualdad, el 7 aparece con el exponente $2n_7$.
Entonces, por unicidad de la factorización, se deberia tener que

$$2m_7 + 1 = 2n_7$$

Lo cual es absurdo, pues un número es impar y el otro par.
Luego, $\nexists\, a, b \in \mathbb{Z}$ no nulos tal que $7a^2 = 8b^2$

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

---

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

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

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

Tomemos $\frac{a}{b}$ como una fracción irreducible, es decir, con a y b coprimos.
Luego,

$$\sqrt[n]{p} = \frac{a}{b} \implies b \cdot \sqrt[n]{p} = a \implies b^n \cdot p = a^n \implies p \,|\, a^n \xrightarrow{p \text{ primo}} p \,|\, a$$

Como $p \,|\, a$, entonces $a = p \cdot k,\ k \in \mathbb{Z}$. Reemplazando, tenemos que

$$b^n \cdot p = a^n \implies b^n \cdot p = (p \cdot k)^n \implies b^n \cdot p = p^n \cdot k^n \overset{!!}{\Rightarrow} b^n = p^{n-1} \cdot k^n \overset{!!!}{\Rightarrow} b^n = p \cdot p^{n-2} \cdot k^n \implies p \,|\, b^n \xrightarrow{p \text{ primo}} p \,|\, b$$

El paso en !! tiene sentido porque $n \in \mathbb{N}$ y en !!! porque $n \geq 2$. Esto asegura que las expresiones p^{n-1} y p^{n-2} pertenezcan $\mathbb{N}_0$.

Así, obtuvimos que $p \,|\, a$ y $p \,|\, b$, lo cual contradice el hecho que a y b son coprimos. La contradicción proviene de la única suposición que hicimos, que $\sqrt[n]{p} \in \mathbb{Q}$. Luego, $\sqrt[n]{p} \notin \mathbb{Q}$, tal como queriamos probar.

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

---

28. Sean p y q primos positivos distintos. Probar que $p^{113} \cdot q^{201} \,|\, a^{378}$ si y sólo si $pq \,|\, a$.

Antes de empezar, notemos que como $p \neq q$ y ambos son primos, se tiene que $(p : q) = 1$

- $p^{113} \cdot q^{201} \,|\, a^{378} \implies pq \,|\, a.$

$$p^{113} \cdot q^{201} \,|\, a^{378} \iff a^{378} = p^{113} \cdot q^{201} \cdot k\ ,\ k \in \mathbb{Z} \implies \begin{cases} p \,|\, a^{378} \xrightarrow{\text{p primo}} p \,|\, a \\ q \,|\, a^{378} \xrightarrow{\text{q primo}} q \,|\, a \end{cases} \xrightarrow{(p\,:\,q) = 1} pq \,|\, a \quad \checkmark$$

- $pq \mid a \implies p^{113} \cdot q^{201} \mid a^{378}$

$$pq \mid a \iff a = pq \cdot k\ ,\ k \in \mathbb{Z} \implies a^{378} = p^{378} \cdot q^{378} \cdot k^{378} \iff a^{378} = p^{113} \cdot q^{201}(p^{265} \cdot p^{177} \cdot k^{378})$$

$$\xrightarrow{(p^{265} \cdot p^{177} \cdot k^{378}) \in \mathbb{Z}} p^{113} \cdot q^{201} \mid a^{378} \quad \checkmark$$

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

---

29. Determinar cuántos divisores positivos tiene 9000, $15^4 \cdot 42^3 \cdot 56^5$ y $10^n \cdot 11^{n+1}$. ¿Y cuántos divisores en total?

Lo único que hay que hacer en este ejercicio es factorizar en primos cada número y utiizar la formula de cantidad de divisores (poco interesante).

- 9000

$$9000 = 2^3 \cdot 3^2 \cdot 5^3 \implies \begin{cases} \#Div_+(9000) = (3+1)(2+1)(3+1) = \boxed{48} \\ \#Div(9000) = 2 \cdot 48 = \boxed{96} \end{cases}$$

- $15^4 \cdot 42^3 \cdot 56^5$

$$15^4 \cdot 42^3 \cdot 56^5 = 2^{18} \cdot 3^7 \cdot 5^4 \cdot 7^8 \implies \begin{cases} \#Div_+(15^4 \cdot 42^3 \cdot 56^5) = (18+1)(7+1)(4+1)(8+1) = \boxed{6840} \\ \#Div(15^4 \cdot 42^3 \cdot 56^5) = 2 \cdot 6840 = \boxed{13680} \end{cases}$$

- $10^n \cdot 11^{n+1}$

$$10^n \cdot 11^{n+1} = 2^n \cdot 5^n \cdot 11^{n+1} \implies \begin{cases} \#Div_+(10^n \cdot 11^{n+1}) = (n+1)(n+1)(n+1+1) = \boxed{(n+2)(n+1)^2} \\ \#Div(10^n \cdot 11^{n+1}) = \boxed{2(n+2)(n+1)^2} \end{cases}$$

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

---

30. Hallar la suma de los divisores positivos de $2^4 \cdot 5^{123}$ y de $10^n \cdot 11^{n+1}$.

- $2^4 \cdot 5^{123}$
  Sabemos que $Div_+(2^4 \cdot 5^{123}) = \{2^i \cdot 5^j,\ 0 \le i \le 4 \quad \text{y} \quad 0 \le j \le 123\}$
  Entonces, la suma de los divisores será igual a:

$$\sum_{i=0}^{4}\sum_{j=0}^{123} 2^i \cdot 5^j = \left(\sum_{i=0}^{4} 2^i\right) \cdot \left(\sum_{j=0}^{123} 5^j\right) = \left(\frac{1-2^{4+1}}{1-2}\right) \cdot \left(\frac{1-5^{123+1}}{1-5}\right) = \boxed{\frac{31}{4}(5^{124}-1)}$$

- $10^n \cdot 11^{n+1}$
  $10^n \cdot 11^{n+1} = 2^n \cdot 5^n \cdot 11^{n+1}$
  Sabemos que $Div_+(10^n \cdot 11^{n+1}) = \{2^i \cdot 5^j \cdot 11^k,\ 0 \le i \le n,\ 0 \le j \le n \quad \text{y} \quad 0 \le k \le n+1\}$
  Entonces, la suma de los divisores será igual a:

$$\sum_{i=0}^{n}\sum_{j=0}^{n}\sum_{k=0}^{n+1} 2^i \cdot 5^j \cdot 11^k = \left(\sum_{i=0}^{n} 2^i\right) \cdot \left(\sum_{j=0}^{n} 5^j\right) \cdot \left(\sum_{k=0}^{n+1} 11^k\right) = \left(\frac{1-2^{n+1}}{1-2}\right) \cdot \left(\frac{1-5^{n+1}}{1-5}\right) \cdot \left(\frac{1-11^{n+1+1}}{1-11}\right) =$$

$$= \boxed{\frac{1}{40}(2^{n+1}-1)(5^{n+1}-1)(11^{n+2}-1)}$$

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

---

31. Hallar el menor número natural n tal que $6552n$ sea un cuadrado, es decir, que exista $k \in \mathbb{N}$ tal que $6552n = k^2$.

Como $k \in \mathbb{N}$ y como claramente $k \neq 1$, por TFA, se tiene que

$$k = (P_1)^{m_1} \cdot (P_2)^{m_2} \cdots (P_r)^{m_r},\ m_1, m_2, \ldots, m_r \in \mathbb{N} \implies k^2 = (P_1)^{2m_1} \cdot (P_2)^{2m_2} \cdots (P_r)^{2m_r}$$

Entonces

$$6552n = k^2 \iff 2^3 \cdot 3^2 \cdot 7 \cdot 13 \cdot n = (P_1)^{2m_1} \cdot (P_2)^{2m_2} \cdots (P_r)^{2m_r}$$

Esto nos dice que todos los primos del lado izquierdo de la igualdad deben estar elevados a un número de la forma $2k,\ k \in \mathbb{N}$.
Para lograr esto, notemos que es necesario que n contenga en su factorización un 2, un 7 y un 13 y como nos piden el menor n, esto resulta suficiente.
Luego, $n = 2 \cdot 7 \cdot 13 = \boxed{182}$

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

---

32. Sean $a, b \in \mathbb{N}, a, b \geq 2$. Probar que si ab es un cuadrado en $\mathbb{N}$ y $(a : b) = 1$, entonces, tanto a como b son cuadrados en $\mathbb{N}$.

$$ab \text{ es un cuadrado en } \mathbb{N} \iff ab = k^2,\ k \in \mathbb{N}$$

Esto implica que todos los primos en la factorización de ab son de la forma $2q$, con $q \in \mathbb{N}$. Es decir

$$ab = (P_1)^{2n_1} \cdots (P_r)^{2n_r},\ n_1, \ldots, n_r \in \mathbb{N}$$

Luego, usando que $(a : b) = 1$, se tiene que a y b no poseen primos en común, de modo que cada primo con su respectivo exponente de ab esta en la factorización de a o de b, pero no en ambas.
Entonces, podemos escribir a ambos números en su factorización correspondiente:

$$a = (Q_1)^{2m_1} \cdots (Q_t)^{2m_t},\ m_1, \ldots, m_t \in \mathbb{N}$$

$$b = (S_1)^{2l_1} \cdots (S_c)^{2l_c},\ l_1, \ldots, l_c \in \mathbb{N}$$

De esta manera

$$\exists\, k_1, k_2 \in \mathbb{N} \text{ con } \begin{cases} k_1 = (Q_1)^{m_1} \cdots (Q_t)^{m_t} \\ k_2 = (S_1)^{l_1} \cdots (S_c)^{l_c} \end{cases} \text{ tal que } \begin{cases} a = (k_1)^2 \\ b = (k_2)^2 \end{cases}$$

Esto precisamente quiere decir que a y b son cuadrados en $\mathbb{N}$, que era lo que queriamos probar.

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

---

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

(a) $(n : 945) = 63$, $(n : 1176) = 84$ y $n \leq 2800$

(b) $(n : 1260) = 70$ y n tiene 30 divisores positivos.

(a) Trabajemos con la primera condición

$$(n : 945) = 63 \iff (n : 3^3 \cdot 5 \cdot 7) = 3^2 \cdot 7$$

De aca tenemos que, en su factorización, n tiene un 3^2, no tiene un 5 y tiene un 7^m, $m \geq 1$.

Veamos ahora la segunda condición

$$(n : 1176) = 84 \iff (n : 2^3 \cdot 3 \cdot 7^2) = 2^2 \cdot 3 \cdot 7$$

De aca tenemos que, en su factorización, n tiene un 2^2, tiene un 3^k, $k \geq 1$ y tiene un 7.
Juntando todo, tenemos que

$$n = 2^2 \cdot 3^2 \cdot 7 \cdot (P_1)^{m_1} \cdots (P_r)^{m_r},\ m_1, \ldots, m_r \in \mathbb{N}_0$$

Veamos ahora la tercer condición.
Si n no tiene ningún primo más, tenemos que $n = 2^2 \cdot 3^2 \cdot 7 = 252 \leq 2800$ ✓
Si n tiene un primo más, sabiendo que el 5 no puede ser, probamos con el 11, que es el que le sigue al 7. Entonces, tenemos que $n = 2^2 \cdot 3^2 \cdot 7 \cdot 11 = 2772 \leq 2800$ ✓
Si agregamos otro 11, ya nos pasamos, pues $n = 2^2 \cdot 3^2 \cdot 7 \cdot 11^2 = 30492$. Por otro lado, si no agregamos el 11 sino el que le sigue, el 13, tenemos que $n = 2^2 \cdot 3^2 \cdot 7 \cdot 13 = 3276$, con lo que también nos pasamos. De este modo, es evidente que con cualquier otro primo mayor a 13 también nos pasariamos. Así, solo puede haber como máximo un 11 más.

Luego, los unicos n que cumplen son

$$n = 2^2 \cdot 3^2 \cdot 7 = \boxed{252}$$
$$n = 2^2 \cdot 3^2 \cdot 7 \cdot 11 = \boxed{2772}$$

(b) Veamos la primera condición

$$(n : 1260) = 70 \iff (n : 2^2 \cdot 3^2 \cdot 5 \cdot 7) = 2 \cdot 5 \cdot 7$$

De aca deducimos que, en su factorización, n tiene un 2, no tiene un 3, tiene un 5^m, $m \geq 1$ y tiene un 7^k, $k \geq 1$.
Así, tenemos que

$$n = 2^1 \cdot 5^m \cdot 7^k \cdot (P_1)^{m_1} \cdots (P_r)^{m_r},\ m_1, \ldots, m_r \in \mathbb{N}_0$$

De la segunda condición tenemos que

$$\#Div_+(n) = 30 \iff 30 = (1+1)(m+1)(k+1)(m_1+1)\cdots(m_r+1) \iff 15 = (m+1)(k+1)(m_1+1)\cdots(m_r+1)$$

Notemos ahora que las únicas maneras de escribir a $15 = 3 \cdot 5$ como un producto de dos o más números es haciendo $15 \cdot 1$ o $3 \cdot 5$

Para empezar, estos nos dice que no hay más primos en la factorización de n, además del 2, 5 y 7. Luego, tenemos que

$$15 = (m+1)(k+1)$$

Como ambos factores son mayores iguales a 2 (pues k y m son mayores a 1), tenemos que la única manera que el producto de 15 es que uno sea igual a 3 y el otro a 5. Con lo que tenemos dos opciones:

$$(m+1) = 3 \quad \text{y} \quad (k+1) = 5$$

$$(m+1) = 5 \quad \text{y} \quad (k+1) = 3$$

De la primera obtenemos que $m = 2$ y que $k = 4$. Con lo que $n = 2 \cdot 5^2 \cdot 7^4$. De la segunda obtenemos que $m = 4$ y que $k = 2$. Con lo que $n = 2 \cdot 5^4 \cdot 7^2$.

Luego, los unicos n que cumplen son

$$\boxed{n = 2 \cdot 5^2 \cdot 7^4 = 120050} \quad \text{y} \quad \boxed{n = 2 \cdot 5^4 \cdot 7^2 = 61250}$$

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

---

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

Trabajemos con la primera condición:

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

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

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

De la segunda condición tenemos que

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

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

- $(i+1) = 6 \quad \text{y} \quad (m_1+1)...(m_k+1) = 1$
- $(i+1) = 3 \quad \text{y} \quad (m_1+1)...(m_k+1) = 2$

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

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

Luego, elegiendo el menor entre los dos, la respuesta es $\boxed{n = 495}$

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

35.

(a) Sea $k \in \mathbb{N}$. Probar que $(2^k + 7^k : 2^k - 7^k) = 1$.

(b) Sea $k \in \mathbb{N}$. Probar que $(2^k + 5^{k+1} : 2^{k+1} + 5^k) = 3 \quad \text{o} \quad 9$, y dar un ejemplo para cada caso.

(c) Caracterizar para cada $k \in \mathbb{N}$ el valor que toma $(12^k - 1 : 12^k + 1286)$.

(a) Sea $d = (2^k + 7^k : 2^k - 7^k) = 1$. Entonces

$$\left\{ \begin{array}{l} d \,|\, 2^k + 7^k \\ d \,|\, 2^k - 7^k \end{array} \right. \left\{ \begin{array}{l} \xrightarrow{F_1 + F_2} d \,|\, 2 \cdot 2^k \\ \xrightarrow{F_1 - F_2} d \,|\, 2 \cdot 7^k \end{array} \right. \implies d \,|\, (2 \cdot 2^k : 2 \cdot 7^k) = 2(2^k : 7^k) \overset{!!}{=} 2 \cdot 1 = 2 \implies d \in \{1, 2\}$$

En !! uso que $(2 : 7) = 1 \iff (2^k : 7^k) = 1$

Ahora nos gustaria descartar que d pueda ser 2, con lo que basta ver que 2 no divide a alguna de las expresiones. Para esto, miremos la congruencia módulo 2 de $2^k + 7^k$:

$$2^k + 7^k \equiv 0^k + 1^k \equiv 1 \pmod 2 \implies r_2(2^k + 7^k) = 1, \ \forall\, k \in \mathbb{N} \implies 2 \nmid 2^k + 7^k, \ \forall\, k \in \mathbb{N}$$

De aca, tenemos que $2 \nmid d$. Entonces, queda que $\boxed{d = 1}$, tal como queriamos probar.

(b) Sea $d = (2^k + 5^{k+1} : 2^{k+1} + 5^k) = 1$. Entonces

$$\left\{ \begin{array}{l} d \,|\, 2^k + 5^{k+1} \\ d \,|\, 2^{k+1} + 5^k \end{array} \right. \left\{ \begin{array}{l} \xrightarrow{2 \cdot F_1} \left\{ \begin{array}{l} d \,|\, 2^{k+1} + 2 \cdot 5^{k+1} \\ d \,|\, 2^{k+1} + 5^k \end{array} \right. \xrightarrow{F_1 - F_2} d \,|\, 9 \cdot 5^k \\ \xrightarrow{5 \cdot F_2} \left\{ \begin{array}{l} d \,|\, 2^k + 5^{k+1} \\ d \,|\, 5 \cdot 2^{k+1} + 5^{k+1} \end{array} \right. \xrightarrow{F_2 - F_1} d \,|\, 9 \cdot 2^k \end{array} \right. \implies d \,|\, (9 \cdot 5^k : 9 \cdot 2^k) = 9(5^k : 2^k) \overset{!!}{=} 9 \cdot 1 = 9$$

$$\implies d \in \{1, 3, 9\}$$

En !! uso que $(5 : 2) = 1 \iff (5^k : 2^k) = 1$

Veamos ahora que d puede ser igual a 3 o a 9:

$$\left\{ \begin{array}{l} k = 1 \to d = (2^1 + 5^{1+1} : 2^{1+1} + 5^1) = (27 : 9) = (9 : 0) = 9 \quad \checkmark \\ k = 2 \to d = (2^2 + 5^{2+1} : 2^{2+1} + 5^2) = (129 : 33) = (33 : 30) = (30 : 3) = (3 : 0) = 3 \quad \checkmark \end{array} \right.$$

En estos pasos usé el algoritmo de Euclides.

Ahors tenemos que ver que d no puede ser 1, con lo que debemos verificar que ambas expresiones son siempre divisibles por 3. Para esto, miramos la congruencia módulo 3:

$$\left\{ \begin{array}{l} 2^k + 5^{k+1} \equiv 2^k + 2^{k+1} \equiv 3 \cdot 2^k \equiv 0 \pmod 3 \implies r_3(2^k + 5^{k+1}) = 0, \ \forall\, k \in \mathbb{N} \\ 2^{k+1} + 5^k \equiv 2^{k+1} + 2^k \equiv 3 \cdot 2^k \equiv 0 \pmod 3 \implies r_3(2^{k+1} + 5^k) = 0, \ \forall\, k \in \mathbb{N} \end{array} \right.$$

Entonces, tenemos que

$$3 \,|\, 2^k + 5^{k+1} \quad \text{y} \quad 3 \,|\, 2^{k+1} + 5^k, \ \forall\, k \in \mathbb{N}$$

Con lo que d no puede ser 1. Entonces $\boxed{d = 3 \quad \text{o} \quad 9}$, tal como queriamos ver.

(c) Sea $d = (12^k - 1 : 12^k + 1286)$.

Notemos que $(12^k + 1286) - (12^k - 1) = 1287$. De modo que, haciendo Euclides, tenemos que

$$d = (12^k - 1 : 12^k + 1286) = (12^k - 1 : 1287) = (12^k - 1 : 3^2 \cdot 11 \cdot 13)$$

Miremos ahora la congruencia módulo 3, 11 y 13 de $12^k - 1$:

- mod 3

$$12^k - 1 \equiv 0^k + 2 \equiv 2 \pmod 3 \implies r_3(12^k - 1) = 2 \implies 3 \nmid 12^k - 1, \ \forall\, k \in \mathbb{N}$$

  Luego, $3 \nmid d$, de modo que $d \in \{11, 13, 11 \cdot 13\}$
- mod 11

$$12^k - 1 \equiv 1^k - 1 \equiv 1 - 1 \equiv 0 \pmod{11} \implies r_{11}(12^k - 1) = 0 \implies 11 \mid 12^k - 1, \ \forall\, k \in \mathbb{N}$$

  Luego, $11 \mid d$, de modo que $d \in \{11, 11 \cdot 13\}$
- mod 13

$$12^k - 1 \equiv (-1)^k - 1 \pmod{13}$$

  Aca se abren dos opciones, dependiendo si k es par o impar.

  Si k es par, tenemos que

$$(-1)^k = 1 \implies 12^k - 1 \equiv 0\ (13) \implies r_{13}(12^k - 1) = 0 \implies 13 \mid 12^k - 1$$

  Luego, tenemos que $13 \mid d$, de modo que $d = 11 \cdot 13 = 143$.

  Si k es impar, tenemos que

$$(-1)^k = -1 \implies 12^k - 1 \equiv 11\ (13) \implies r_{13}(12^k - 1) = 11 \implies 13 \nmid 12^k - 1$$

  Luego, tenemos que $13 \nmid d$, de modo que $d = 11$.

Resumiendo

$$\begin{cases} \boxed{d = 11} \text{ si } k \text{ es impar} \\ \boxed{d = 143} \text{ si } k \text{ es par} \end{cases}$$

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

---

36. Sean $a, b \in \mathbb{Z}$. Probar que si $(a : b) = 1$ entonces $(a^2 \cdot b^3 : a + b) = 1$.

La estrategia es suponer que $(a^2 \cdot b^3 : a + b) \neq 1$ sabiendo que $(a : b) = 1$ y llegar a una contradicción.
Sea $d = (a^2 \cdot b^3 : a + b)$ con $d \neq 1$, entonces $\exists\, p$ primo positivo tal que $p \mid d$.
Luego

$$\begin{cases} d \mid a^2 \cdot b^3 \\ d \mid a + b \end{cases} \xRightarrow{\text{Transitividad}} \begin{cases} p \mid a^2 \cdot b^3 \xRightarrow{\text{p primo}} p \mid a \quad \text{o} \quad p \mid b \\ p \mid a + b \end{cases}$$

Esto nos deja dos opciones:

- Caso $p \mid a$

$$\begin{cases} p \mid a \\ p \mid a + b \end{cases} \xRightarrow{F_2 - F_1} p \mid b$$

  Lo cual es absurdo, pues $p \mid a$ y $p \mid b$, pero dijimos que $(a : b) = 1$.

- Caso $p \mid b$

$$\begin{cases} p \mid b \\ p \mid a+b \end{cases} \xrightarrow{F_2 - F_1} p \mid a$$

Lo cual es absurdo, pues $p \mid a$ y $p \mid b$, pero dijimos que $(a : b) = 1$.

Sea como fuera, en ambos casos llegamos a un absurdo suponiendo que $d \neq 1$. Luego, $d = 1$ ✓

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

---

37. Sean $a, b \in \mathbb{Z}$ tales que $(a : b) = 5$.

(a) Calcular los posibles valores de $(ab : 5a - 10b)$ y dar un ejemplo para cada uno de ellos.

(b) Para cada $k \in \mathbb{N}$, calcular $(a^{k-1}b : a^k + b^k)$.

(a) Coprimizo: defino $5a' = a$ y $5b' = b$, con lo que $(a : b) = (5a' : 5b') = 5(a' : b') = 5$, de modo que $(a' : b') = 1$.

Reemplazo en $d = (ab : 5a - 10b)$:

$$d = (ab : 5a - 10b) = (25a'b' : 25a' - 50b') = 25(a'b' : a' - 2b')$$

Sea ahora $d' = (a'b' : a' - 2b')$. Entonces, $d = 25d'$.
Trabajemos ahora con d'

$$\begin{cases} d' \mid a'b' \\ d' \mid a' - 2b' \end{cases} \begin{cases} \xrightarrow{b' \cdot F_2} \begin{cases} d' \mid a'b' \\ d' \mid a'b' - 2(b')^2 \end{cases} \xrightarrow{F_1 - F_2} d' \mid 2(b')^2 \\ \xrightarrow[2a' \cdot F_2]{4 \cdot F_1} \begin{cases} d' \mid 4a'b' \\ d' \mid 2(a')^2 - 4b'a' \end{cases} \xrightarrow{F_1 + F_2} d' \mid 2(a')^2 \end{cases} \implies d' \mid (2(b')^2 : 2(a')^2)$$

$$\implies d' \mid (2(b')^2 : 2(a')^2) = 2((b')^2 : (a')^2) \overset{!!}{=} 2 \cdot 1 = 2 \implies d' \mid 2 \implies d' \in \{1, 2\}$$

En !! uso que $(b' : a') = 1 \iff ((b')^2 : (a')^2) = 1$

Como $d' = 1$ o 2, entonces $d = 25$ o 50. Veamos ahora que ambos valores son posibles:

$$\begin{cases} (a, b) = (0, 5) \xrightarrow{(0,5) = 5} d = (0 : -50) = 50 & ✓ \\ (a, b) = (5, 15) \xrightarrow{(5,15) = 5} d = (75 : 25 - 150) = (50 : -125) = 25 & ✓ \end{cases}$$

Luego, $\boxed{d = 25 \quad \text{o} \quad 50}$

(b) Coprimizo: defino $5a' = a$ y $5b' = b$, con lo que $(a : b) = (5a' : 5b') = 5(a' : b') = 5$, de modo que $(a' : b') = 1$.

Reemplazo en $d = (a^{k-1}b : a^k + b^k)$:

$$d = (a^{k-1}b : a^k + b^k) = ((5a')^{k-1}5b' : (5a')^k + (5b')^k) = (5^k(a')^{k-1}b' : 5^k(a')^k + 5^k(b')^k) =$$
$$= 5^k((a')^{k-1}b' : (a')^k + (b')^k)$$

Sea $d' = ((a')^{k-1}b' : (a')^k + (b')^k)$, entonces $d = 5^k d'$

Trabajemos ahora con d'

$$\begin{cases} d' \mid (a')^{k-1}b' \\ d' \mid (a')^k + (b')^k \end{cases} \xrightarrow[(a')^k \cdot F_2]{a'(b')^{k-1} \cdot F_1} \begin{cases} d' \mid (a')^k(b')^k \\ d' \mid (a')^{2k} + (b')^k(a')^k \end{cases} \xrightarrow{F_2 - F_1} d' \mid (a')^{2k}$$

$$\begin{cases} d' \mid (a')^{k-1}b' \\ d' \mid (a')^k + (b')^k \end{cases} \xrightarrow[(b')^k \cdot F_2]{a'(b')^{k-1} \cdot F_1} \begin{cases} d' \mid (a')^k(b')^k \\ d' \mid (b')^{2k} + (b')^k(a')^k \end{cases} \xrightarrow{F_2 - F_1} d' \mid (b')^{2k}$$

$$\implies d' \mid ((a')^{2k} : (b')^{2k}) \overset{!!}{=} 1$$

$$\implies d' \mid 1 \implies d' = 1$$

En !! uso que $(a' : b') = 1 \iff ((a')^{2k} : (b')^{2k}) = 1$

Luego, como $d' = 1$, tenemos que $\boxed{d = 5^k, \text{para cada } k \in \mathbb{N}}$

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

38.

(a) Sean $a, b \in \mathbb{Z}$ tales que $(a : b) = 3$. Calcular los posibles valores de $(a^2 + 15b + 57 : 4050)$ y dar un ejemplo en cada caso.

(b) Sean $a, b \in \mathbb{Z}$. Sabiendo que $b \equiv 6\ (24)$ y que $(a : b) = 13$, calcular $(5a^2 + 11b + 117 : 624)$.

(a) Coprimizo: defino $3x = a$ y $3y = b$, con lo que $(a : b) = (3x : 3y) = 3(x : y) = 3$, de modo que $(x : y) = 1$.

Reemplazo en $d = (a^2 + 15b + 57 : 4050)$:

$$d = (a^2 + 15b + 57 : 4050) = (9x^2 + 45y + 57 : 2 \cdot 3^4 \cdot 5^2) = 3(3x^2 + 15y + 19 : 2 \cdot 3^3 \cdot 5^2)$$

Sea ahora $d' = (3x^2 + 15y + 19 : 2 \cdot 3^3 \cdot 5^2)$. Entonces, $d = 3d'$.
Sabiendo todo esto, tenemos que

$$d' \mid 2 \cdot 3^3 \cdot 5^2 \implies d' \in \{1, 2, 3, 5, 6, 9, 10, 15, 18, 25, 27, 30, 45, 50, 54, 75, 90, 135, 150, 225, 270, 450, 675, 1350\}$$

Miremos ahora la congruencia de $3x^2 + 15y + 19$ módulo 3 y 5:

- mod 5
  Notemos que $3x^2 + 15y + 19 \equiv 3x^2 + 4\ (5)$. Entonces, veo la tabla de restos de $3x^2 + 4$.

$r_5(x)$	0	1	2	3	4
$r_5(3x^2 + 4)$	4	2	1	1	2

  De aca tenemos que $5 \nmid 3x^2 + 15y + 19\ \forall\ x \in \mathbb{Z}$. Luego, $5 \nmid d'$. Con lo que

$$d' \in \{1, 2, 3, 6, 9, 18, 27, 54\}$$

- mod 3
  Acá no hace falta ver la tabla de restos, pues notemos que $3x^2 + 15y + 19 \equiv 1\ (3)$. Entonces $5 \nmid 3x^2 + 15y + 19\ \forall\ x \in \mathbb{Z}$. Luego, $3 \nmid d'$. Con lo que

$$d' \in \{1, 2\}$$

Como $d' = 1 \quad o \quad 2$, entonces, $d = 3 \quad o \quad 6$. Veamos ahora ejemplos de que cada uno es posible:

$$\begin{cases} (a,b) = (3,3) \xrightarrow{(3,3)=3} d = (111 : 4050) = (111 : 54) = (54 : 3) = (3 : 0) = 3 \quad \checkmark \\ (a,b) = (6,3) \xrightarrow{(6,3)=3} d = (138 : 4050) = (138 : 48) = (48 : 42) = (42 : 6) = (6 : 0) = 6 \quad \checkmark \end{cases}$$

Luego, $\boxed{d = 3 \quad o \quad 6}$.

(b) Coprimizo: defino $13x = a$ y $13y = b$, con lo que $(a : b) = (13x : 13y) = 13(x : y) = 13$, de modo que $(x : y) = 1$.

Reemplazo en $d = (5a^2 + 11b + 117 : 624)$:

$$d = (5a^2 + 11b + 117 : 624) = (5 \cdot 13^2 \cdot x^2 + 143y + 117 : 2^4 \cdot 3 \cdot 13) = 13(65x^2 + 11y + 9 : 2^4 \cdot 3)$$

Sea ahora $d' = (65x^2 + 11y + 9 : 2^4 \cdot 3)$. Entonces, $d = 13d'$.
Sabiendo todo esto, tenemos que

$$d' \mid 2^4 \cdot 3 \implies d' \in \{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}$$

Antes de mirar las congruencias, veamos la condición que dice que $b \equiv 6\ (24)$. De esta obtenemos lo siguiente

$$b \equiv 6\ (24) \implies \begin{cases} b \equiv 0\ (2) \\ b \equiv 0\ (3) \\ b \equiv 2\ (4) \\ b \equiv 6\ (8) \end{cases}$$

Para obtener condiciones sobre y, usamos $b = 13y$. Entonces

$$\begin{cases} b \equiv 0\ (2) \implies 13y \equiv 0\ (2) \xrightarrow{13 \equiv 1\ (2)} y \equiv 0\ (2) \\ b \equiv 0\ (3) \implies 13y \equiv 0\ (3) \xrightarrow{13 \equiv 1\ (3)} y \equiv 0\ (3) \\ b \equiv 2\ (4) \implies 13y \equiv 2\ (4) \xrightarrow{13 \equiv 1\ (4)} y \equiv 2\ (4) \\ b \equiv 6\ (8) \implies 13y \equiv 6\ (8) \xrightarrow{5 \equiv 5\ (8)} 65y \equiv 30\ (8) \xrightarrow{65 \equiv 1\ (8)} y \equiv 6\ (8) \end{cases}$$

Miremos ahora las congruencias con la expresión $65x^2 + 11y + 9$.

- mod 3
  Usando que $y \equiv 0\ (3)$, tenemos que $65x^2 + 11y + 9 \equiv 2x^2\ (3)$.

  Miremos la tabla de restos con $2x^2$

$r_3(x)$	0	1	2
$r_3(2x^2)$	0	2	2

  Notemos que el resto es 0 si y solo $x \equiv 0\ (3)$, pero esto no puede ser, pues tendriamos que $3 \mid x$ y que $3 \mid y$ y no se cumpliria que $(x : y) = 1$. Luego, $3 \nmid 65x^2 + 11y + 9$, con lo que $3 \nmid d'$. Con lo que

$$d' \in \{1, 2, 4, 8, 16\}$$

- mod 8
  Usando que $y \equiv 6\ (8)$, tenemos que $65x^2 + 11y + 9 \equiv x^2 + 3\ (8)$.

  Miremos la tabla de restos con $x^2 + 3$

$r_8(x)$	0	1	2	3	4	5	6	7
$r_8(x^2+3)$	3	4	7	4	3	4	7	4

  De aca tenemos que $8 \nmid 65x^2 + 11y + 9$. Luego, $8 \nmid d'$. Con lo que

$$d' \in \{1, 2, 4\}$$

- mod 2
  Usando que $y \equiv 0\ (2)$, tenemos que $65x^2 + 11y + 9 \equiv x^2 + 1\ (2)$.

  Miremos la tabla de restos con $x^2 + 1$

$r_2(x)$	0	1
$r_2(x^2+1)$	1	0

  De aca tenemos que el resto es 0 si y solo si $x \equiv 1\ (2)$. Notemos que en realidad esta es la unica opción, pues no puede ser que $x \equiv 0\ (2)$, pues tendriamos que $(x : y) \neq 1$. Luego $2 \mid 65x^2 + 11y + 9$, con lo que $2 \mid d'$. Así tenemos

  $$d' \in \{2, 4\}$$

- mod 4
  Usando que $y \equiv 2\ (4)$, tenemos que $65x^2 + 11y + 9 \equiv x^2 + 3\ (4)$.

  Como del caso anterior obtuvimos que x debe ser impar, basta ver la congruencia módulo 1 y 3:

$r_4(x)$	1	3
$r_4(x^2+3)$	0	0

  Como en ambos casos el resto es 0, tenemos que $4 \mid 65x^2 + 11y + 9$, de modo que $4 \mid d'$. Así, llegamos a que el único valor que puede tomar d' es 4.

Finalmente, tenemos que $d = 13 \cdot 4 = \boxed{52}$

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

---

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

(a) $[n : 130] = 260$.

(b) $[n : 420] = 7560$.

(a)

$$[n : 130] = 260 \iff [n : 2 \cdot 5 \cdot 13] = 2^2 \cdot 5 \cdot 13$$

Como el mínimo común múltiplo se calcula con los primos a la máxima potencia, tenemos que n tiene un 2^2 y luego tenemos que puede tener al 5 y al 13, a ambos o a ninguno, pues el 5 y el 13 ya están en la factorización del 130.
Entonces, los n que cumplen son:

$$n = 2^2 = \boxed{4}$$
$$n = 2^2 \cdot 5 = \boxed{20}$$
$$n = 2^2 \cdot 13 = \boxed{52}$$
$$n = 2^2 \cdot 5 \cdot 13 = \boxed{260}$$

(b)

$$[n : 420] = 7560 \iff [n : 2^2 \cdot 3 \cdot 5 \cdot 7] = 2^3 \cdot 3^3 \cdot 5 \cdot 7$$

Como el mínimo común múltiplo se calcula con los primos a la máxima potencia, tenemos que n tiene un 2^3, un 3^3 y luego tenemos que puede tener al 5 y al 7, a ambos o a ninguno, pues el 5 y el 7 ya están en la factorización del 420.

Entonces, los n que cumplen son:

$$n = 2^3 \cdot 3^3 = \boxed{216}$$
$$n = 2^3 \cdot 3^3 \cdot 5 = \boxed{1080}$$
$$n = 2^3 \cdot 3^3 \cdot 7 = \boxed{1512}$$
$$n = 2^3 \cdot 3^3 \cdot 5 \cdot 7 = \boxed{7560}$$

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

---

40. Hallar todos los $a, b \in \mathbb{N}$ tales que

(a) $(a : b) = 10$ y $[a : b] = 1500$.

(b) $3 \mid a$, $(a : b) = 20$ y $[a : b] = 9000$.

(a) Veamos la primera condición

$$(a : b) = 10 \iff (a : b) = 2 \cdot 5$$

De aca tenemos que tanto a y b poseen en su factorización, como mínimo, un 2 y un 5.

Veamos la segunda condición

$$[a : b] = 1500 \iff [a : b] = 2^2 \cdot 3 \cdot 5^3$$

De aca tenemos que alguno entre a y b tiene un 2^2, pero nos los dos a la vez, pues en el MCD aparece un 2. Por la misma razón, alguno tiene un 3, pero no los dos y alguno tiene un 5^3, pero no los dos.

Resumiendo, tenemos que a y b tienen un 2 y un 5 siempre y debemos repartir un 2, un 3 y un 5^2 para formar todas las combinaciones posibles. Así, todos los a y b son

$$(a, b) = \boxed{(2^2 \cdot 3 \cdot 5^3, 2 \cdot 5)}$$
$$(a, b) = \boxed{(2^2 \cdot 3 \cdot 5, 2 \cdot 5^3)}$$
$$(a, b) = \boxed{(2^2 \cdot 5, 2 \cdot 3 \cdot 5^3)}$$
$$(a, b) = \boxed{(2^2 \cdot 5^3, 2 \cdot 3 \cdot 5)}$$
$$(a, b) = \boxed{(2 \cdot 5, 2^2 \cdot 3 \cdot 5^3)}$$
$$(a, b) = \boxed{(2 \cdot 5^3, 2^2 \cdot 3 \cdot 5)}$$
$$(a, b) = \boxed{(2 \cdot 3 \cdot 5^3, 2^2 \cdot 5)}$$
$$(a, b) = \boxed{(2 \cdot 3 \cdot 5, 2^2 \cdot 5^3)}$$

(b) Veamos la segunda condición

$$(a:b) = 20 \iff (a:b) = 2^2 \cdot 5$$

De aca tenemos que tanto a y b poseen en su factorización, como mínimo, un 2^2 y un 5.

Veamos la tercera condición

$$[a:b] = 9000 \iff [a:b] = 2^3 \cdot 3^2 \cdot 5^3$$

De aca tenemos que alguno entre a y b tiene un 2^3, pero nos los dos a la vez, pues en el MCD aparece un 2^2. Por la misma razón, alguno tiene un 5^3, pero no los dos.

En el caso del 3^2, como tenemos la primera condición que nos dice que $3 \mid a$, el 3^2 debe estar en la factorización de a si o si.

Resumiendo, tenemos que a tiene un 2^2, un 3^2 y un 5, mientras b posee un 2^2 y un 5. Ahora solo queda repartir un 2 y un 5^2 para formar todas las combinaciones posibles. Así, todos los a y b son

$$(a,b) = \boxed{(2^3 \cdot 3^2 \cdot 5^3, 2^2 \cdot 5)}$$
$$(a,b) = \boxed{(2^2 \cdot 3^2 \cdot 5, 2^3 \cdot 5^3)}$$
$$(a,b) = \boxed{(2^3 \cdot 3^2 \cdot 5, 2^2 \cdot 5^3)}$$
$$(a,b) = \boxed{(2^2 \cdot 3^2 \cdot 5^3, 2^3 \cdot 5)}$$

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

Ejercicios de parciales:

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

Factorizo el número a estudiar:

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

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

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

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

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

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

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

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Tobia Loni

---

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

i) $(n : 2528) = 316$

ii) n tiene exáctamente 48 divisores positivos

iii) $27 \nmid n$

Analizo los números:

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

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

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

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

---

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

Arranco *comprimizando:*

$$\begin{cases} a = 5c \\ b = 5d \end{cases} \implies (3ab : a^2 + b^2) = 25 \xLeftrightarrow[!]{\text{coprimizar}} (3cd : c^2 + d^2) = 1$$

Esto último nos dice que las expresiones $3cd$ y $c^2 + d^2$ son coprimas entre sí, en otras palabras, que *no hay ningún* p *primo* que divida ambas expresiones a la vez.
Pruebo por absurdo que no existe p primo que divida a ambas expresiones, es decir que no existe un p, tal que $(3cd : c^2 + d^2) = p$. Supongo que $\exists\, p$ primo tal que:

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

Si ocurre que $p \mid 3 \Leftrightarrow p = 3$. Quiero entonces ver si $3 \mid c^2 + d^2 \Leftrightarrow c^2 + d^2 \overset{(3)}{\equiv} 0$. Hago una tabla para estudiar esa última ecuación, tengo 2 valores, hago <u>todas las combinaciones</u>:

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

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

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

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 $\bigstar^1 p \mid 3$

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

$$\begin{cases} p \mid c \\ p \mid c^2 + d^2 \end{cases} \xrightarrow[F_2 - c \cdot F_1 \to F_2]{} \begin{cases} p \mid c \\ p \mid d^2 \xLeftrightarrow[\text{primo}]{p} p \mid d \end{cases}$$

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

El caso $\bigstar^3$ 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 $\begin{cases} a = 5c \\ b = 5d \end{cases}$

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

---

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

Probar usando propiedades:

$$\begin{aligned} 81 \mid (16n^2 + 8^{2n} - 15n - 7)^{2024} &\overset{!!!}{\iff} 3 \mid (16n^2 + 8^{2n} - 15n - 7)^{506} \\ &\overset{\text{def}}{\iff} (16n^2 + 8^{2n} - 15n - 7)^{506} \equiv 0 \ (3) \\ &\overset{!}{\iff} (n^2)^{506} \equiv 0 \ (3) \\ &\overset{!!}{\iff} n \equiv 0 \ (3) \\ &\overset{\text{def}}{\iff} 3 \mid n \end{aligned}$$

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

Son todas dobles implicaciones. En el !!! uso esto $p^n \mid a^n \Leftrightarrow p \mid a$. En ! son cuentas de congruencia. Y en !! uso esto, $p \mid a^n \iff p \mid a$.

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

---

5. Determinar los posibles valores de $d = (a^2 - 2a - 5 : a - 1)$ para $a \in \mathbb{Z}$. Exhibir un valor de a correspondiente a cada uno de los valores de d hallados.

Parecido a cosas que ya se hicieron en otros ejercicios. Simplificamos si se puede con Euclides y después con tabla de restos filtramos los máximos común divisores que quedaron.

Euclides con División de polinomios

$$\begin{array}{rr|l} a^2 - 2a - 5 & & a - 1 \\ \cline{3-3} -a^2 + a & & a - 1 \\ \cline{1-1} -a - 5 & & \\ a - 1 & & \\ \cline{1-1} -6 & & \end{array}$$

Que en el resto quede un número es una excelente noticia, podemos reescribir al mcd:

$$d = (a^2 - 2a - 5 : a - 1) = (a - 1 : -6)$$

Con ese resultado y dado que $d \mid a - 1$ y también $d \mid 6$:

$$d \in \{1, 2, 3, 6\}$$

Tabla de restos para ver para que valores de a se divide la expresión $a - 1$

$r_2(a)$	0	1
$r_2(a-1)$	1	0

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

$r_6(a)$	0	1	2	3	4	5
$r_6(a-1)$	5	0	1	2	3	4

Ahora hay que elegir un valor a de forma tal que d sea un valor que cumpla con los resultados.
Hay que tener cuidado, porque los conjuntos de a que salen de la tabla de restos no son disjuntos.
Los siguientes valores salen a ojímetro:

$$\begin{aligned} \text{si } a = 0 &\implies d = 1 \\ \text{si } a = 5 &\implies d = 2 \\ \text{si } a = 4 &\implies d = 3 \\ \text{si } a = 7 &\implies d = 6 \end{aligned}$$

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

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* para hacer menos cuentas:

$$(a : b) = 6 \iff \left\{ \begin{array}{l} a = 6A \\ b = 6B \end{array} \right\} \text{ con } (A : B) \overset{\bigstar^1}{=} 1$$

Uso ahora las nuevas variables coprimas entre sí, A y B. Con esto la expresión de d queda:

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

Entonces ahora puedo estudiar $D = (2A + B : 3A - 2B)$. Busco *divisores comunes*:

$$\left\{ \begin{array}{l|l} D & 2A + B \\ D & 3A - 2B \end{array} \right. \overset{!}{\iff} \left\{ \begin{array}{l|l} D & 7B \\ D & 7A \end{array} \right. \Leftrightarrow D = (7A : 7B) = 7 \cdot (A : B) \overset{\bigstar^1}{=} 7$$

Por lo tanto los posibles divisores comúnes:

$$D \in \mathcal{D}_+(7) = \{1, 7\},$$

pero yo quiero encontrar ejemplos de A y B:
Para $D = 7$

$$A = 2 \quad \text{y} \quad B = 3$$

Traduciendo esto para los valores de a, b y d:

$$\boxed{d = 42 \quad \text{y} \quad \left\{ \begin{array}{l} a = 12 \\ b = 18 \end{array} \right.}$$

Para $D = 1$

$$A = 0 \quad \text{y} \quad B = 1$$

Traduciendo esto para los valores de a, b y d:

$$\boxed{d = 6 \quad \text{y} \quad \left\{ \begin{array}{l} a = 0 \\ b = 6 \end{array} \right.}$$

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

---

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

⚠ En este ejercicio no están pidiendo que des el MCD para cada valor de a. Solo hay que contestar cual sería el mayor MCD entre todos los a permitidos. ⚠

Simplifico un poco:

$$32a \equiv 17\ (9) \Leftrightarrow 5a \equiv 8\ (9) \underset{(\Leftarrow) 2 \perp 9}{\overset{\times 2}{\Longleftrightarrow}} a \equiv 7\ (9) \overset{\bigstar^1}{} \quad \checkmark$$

Simplifico la expresión del MCD con euclides:

$$\begin{array}{r|l} a^3 + 4a + 1 & a^2 + 2 \\ \underline{-\,a^3 - 2a} & a \\ 2a + 1 & \end{array}$$

Entonces puedo escribir:

$$d = (a^3 + 4a + 1 : a^2 + 2) = (a^2 + 2 : 2a + 1)$$

Busco potenciales d:

$$\left\{ \begin{array}{l|l} d & a^2 + 2 \\ d & 2a + 1 \end{array} \right. \xrightarrow{2F_1 - aF_2} \left\{ \begin{array}{l|l} d & -a + 4 \\ d & 2a + 1 \end{array} \right. \xrightarrow{2F_1 + F_2} \left\{ \begin{array}{l|l} d & -a + 4 \\ d & 9 \end{array} \right.$$

Por lo tanto la versión más simple quedó en: $d = (-a + 4 : 9)$. Posibles $d : \{1, 3, 9\}$ ✓

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

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

Entonces los a que cumplen $a \equiv 1\ (3)$, son candidatos para obtener $d = 3$. Dado que 9 es una potencia de 3, ya sé más o menos que esperar de lo que viene, ¿O no?
Tabla de restos para $d = 9$:

$r_9(a)$	0	1	2	3	4	5	6	7	8
$r_9(-a+4)$	4	3	2	1	0	−1	−2	−3	−4

Entonces los a que cumplen $a \equiv 4\ (9)$ ★², son candidatos para $d = 9$.
Ahora no olvida que no estamos laburando con cualquier valor de a. Estos resultados deben cumplir la condición ★¹$a \equiv 7\ (9)$ como se pide en el enunciado.
Ese resultado no es compatible con el resultado de la tabla de r_9, (¿Lo ves?):

$$a \equiv 7\ (9) \iff a \overset{★^1}{=} 9 \cdot k + 7 \overset{(9)}{\equiv} 7 \not\equiv 4\ ★^2$$

pero sí con la tabla r_3. Notar que: $a \overset{★^1}{=} 9k + 7 \overset{(3)}{\equiv} 1$, cumple ★².

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

$$\boxed{(a^3 + 4a + 1 : a^2 + 2) = 3}$$

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

---

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

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

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

(a) Por inducción:

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

Primero notar que:

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

Se ve que tiene un período de 6 elementos.

Caso Base: $p(2): a_8 \overset{?}{=}_{\bigstar^1} a_2$ ✓

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 $p(k+1)$

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

Ahora uso la definición de manera sucesiva:

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

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

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

En la sumatoria hay 256 términos. $256 = 42 \cdot 6 + 4$ por lo tanto van a haber 42 bloques que dan 0 y sobreviven los últimos 4 términos. $\sum_{k=0}^{255} a_k = \underbrace{0 + 0 + \cdots + 0}_{42 \text{ ceros}} + a_{252} + a_{253} + a_{254} + a_{255} = \cancel{a_{252}} + a_{253} + a_{254} + \cancel{a_{255}} = a_{253} + a_{254} = 5$

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

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

---

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.

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

$$\bigstar^1 \begin{cases} 10a-15 \mid 4a^2 - 13a + 8 \\ 10a-15 \mid 10a - 15 \end{cases} \overset{!!!}{\iff} \begin{cases} 10a-15 \mid -25 \bigstar^2 \\ 10a-15 \mid 10a - 15 \end{cases}$$

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

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

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

$$\begin{cases} \text{Caso: } d = 10a-15 = 1 & \iff a = \frac{26}{10} \notin \mathbb{Z} \\ \text{Caso: } d = 10a-15 = -1 & \iff a = \frac{14}{10} \notin \mathbb{Z} \\ \text{Caso: } d = 10a-15 = 5 & \iff a = 2 \quad \checkmark \\ \text{Caso: } d = 10a-15 = -5 & \iff a = 1 \quad \checkmark \\ \text{Caso: } d = 10a-15 = 25 & \iff a = 4 \quad \checkmark \\ \text{Caso: } d = 10a-15 = -25 & \iff a = -1 \quad \checkmark \end{cases}$$

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

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

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 ★[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 ★[1] es $a = -1$

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

---

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: ★[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:

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

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 ★[1]:

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

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

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

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

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

$$\begin{array}{rr|l} X^3 & +31 & X^2 - X + 1 \\ \cline{3-3} -X^3 + X^2 - X & & X + 1 \\ \cline{1-1} X^2 - X + 31 & & \\ -X^2 + X - 1 & & \\ \cline{1-1} 30 & & \end{array}$$

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

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

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

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

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

$$a = \underbrace{2k}_{par} \implies (2k)^2 - 2k + 1 = \overbrace{\underbrace{2 \cdot (2k^2 - k)}_{par} + 1}^{impar} \quad \checkmark$$

$$a = \underbrace{2k+1}_{impar} \implies (2k+1)^2 - 2(k+1) + 1 = \overbrace{\underbrace{2 \cdot (2k^2 + 3k + 2)}_{par} + 1}^{impar} \quad \checkmark$$

Hacé lo que más te guste ☺!

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

$$d \mid 30 \quad \text{y} \quad d \equiv 1\ (2) \implies d \in \{1, 3, 5, 15\}\,.$$

Tabla de restos: Siempre empezando por el menor valor

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

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

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

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

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

Dale las gracias y un poco de amor ❤ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Maxi T.

---

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

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

Coprimizar:

$$d = (a^2b^4 : 7^5(-a+b)) \underset{b=7B}{\overset{a=7A}{\iff}} d = 7^6 \cdot (A^2B^4 : B - A) \Leftrightarrow d = 7^6 \cdot D \quad \text{con} \quad (A : B) = 1$$

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

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

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

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

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

---

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

Hay que *comprimizar*, *encontrar posibles divisores*, *interpretar resultado*.
Coprimizar:

$$(a : b) = 3 \Leftrightarrow (\frac{a}{3} : \frac{b}{3}) = 1 \overset{\substack{a = 3A \\ b = 3B}}{\Longleftrightarrow} (A : B) = 1 \Leftrightarrow A \perp B.$$

Reemplazo y acomodo:

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

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

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

Oka, ahí en el !! hice lo de siempre: Multipliqué una fila por A, la otra por B^2 y resté y coso.
Lo que nos queda es algo muy parecido a lo que pasó en el ejercicio éste(click).

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

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

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

---

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

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

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

$$r_{18}(6 \cdot 35^n + 73^{3021} + \sum_{k=1}^{n} 3^k \cdot k!) \overset{!}{=} r_{18}(6 \cdot (-1)^n + 1^{3021} + r_{18}(\sum_{k=1}^{n} 3^k \cdot k!))$$

$$\overset{\bigstar^1}{=} \left\{ \begin{array}{ll} r_{18}(7 + r_{18}(\sum_{k=1}^{n} 3^k \cdot k!)) & \text{si } n \text{ es par} \\ r_{18}(-5 + r_{18}(\sum_{k=1}^{n} 3^k \cdot k!)) & \text{si } n \text{ es impar} \end{array} \right.$$

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

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

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

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

Quiero probar que:

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

Caso base:

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

Por lo que el caso $p(2)$ es verdadero.
Paso inductivo: Asumo que para algún $k \geq 2$

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

es verdadero. Y quiero probar que:

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

también lo sea.
Partiendo de $p(h+1)$

$$\begin{aligned} r_{18}(\sum_{k=2}^{h+1} 3^k \cdot k!) &= r_{18}\big(\sum_{k=2}^{h} 3^k \cdot k! + 3^{h+1} \cdot (h+1)!\big) \\ &\overset{\text{HI}}{=} r_{18}\big(3^{h+1} \cdot (h+1)!\big) \\ &\overset{!}{=} r_{18}\big(3 \cdot 6 \cdot 3^h \cdot \tfrac{(h+1)!}{3!}\big) \\ &= 0 \end{aligned}$$

Ahí en el ! me las arreglé para que aparezca el 18 que hace que el resto de 0. Debe haber otras formas de hacerlo, tenés licencia para dibujar.
Como $p(2), p(h)$ y $p(h+1)$ resultaron verdaderas, por criterio de inducción $p(n)$ también lo es para todo $n \in \mathbb{N}_{\geq 2}$
Volviendo a $\bigstar^2$:

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

por lo tanto en $\bigstar^1$:

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

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Dani Tadd

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

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

$$\begin{cases} d \mid a^2 + 3b^2 \\ d \mid 2a^2 + 11b^2 \end{cases} \xrightarrow{F_2 - 2F_1 \to F_2} \begin{cases} d \mid a^2 + 3b^2 \\ d \mid 5b^2 \end{cases} \quad \text{y} \quad \begin{cases} d \mid a^2 + 3b^2 \\ d \mid 2a^2 + 11b^2 \end{cases} \xrightarrow{11F_1 - 3F_2 \to F_2} \begin{cases} d \mid a^2 + 3b^2 \\ d \mid 5a^2 \end{cases}$$

De esta forma queda que el MCD:

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

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

$$\{1, 5\}$$

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

División por 5: Hay que tener cuidado cuando se hace la tabla de restos y hay dos parámetros, a y b, porque estos no tienen que tener el mismo resto a la vez, entonces se puede proceder así:

Tabla para a:

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

y

Tabla para b:

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

busco una combinación suma que me dé $r_5(a^2 + 3b^2) \overset{(5)}{\equiv} 0$

$$r_5(a^2 + 3b^2) = 0 \Leftrightarrow \begin{cases} a \equiv 0 \ (5) \\ b \equiv 0 \ (5) \end{cases}$$

Fijate que no importa como combines los restos de las tablas, nunca podés formar un 5.
Ese resultado dice que para que suceda que $5 \mid a^2 + 3b^2$ se requiere que:

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

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

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

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
Ale Teran naD GarRaz

---

16. Calcular el resto de dividir

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

por 7.

Nos piden calcular el resto 7 de esa porquería:

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

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

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

Pensar que $6 \equiv -1\ (7)$ y eso nos ayuda a anular muchas cosas:

$$\sum_{k=4}^{134} k^3 = \underbrace{4^3 + 5^3 + 6^3 + 7^3 + 8^3 + \cdots + 130^3 + 131^3 + 132^3 + 134^3}_{131 \text{ términos}}$$

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

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

Se concluye que:

$$r_7\Big(\sum_{k=4}^{134} k^3\Big) = 0 \quad \bigstar^1$$

Ahora quiero ver qué onda con $\sum_{k=4}^{134} k!$.
Noto primero que cuando $k \geq 7$ el número $k!$ es un múltiplo de 7, es decir:

$$k! \equiv 0\ (7) \qquad \text{con } k \in \mathbb{N}_{\geq 7}$$

Por lo tanto me quedaría con los primero 3 términos:

$$\sum_{k=4}^{134} k! = 4! + 5! + 6! + \underbrace{0 + \cdots + 0}_{131 \text{ términos igual a } 0} \equiv 3 + 1 + 6\ (7) \equiv 3 + 1 + 6\ (7) \equiv 3\ (7) \bigstar^2$$

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

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

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Juan Parajó

---

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

Si el mcd es d:

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

Tengo que d es un *divisor común a ambas expresiones:*

$$\left\{ \begin{array}{l|l} d & 7a^2 - a - 3 \\ d & 3a + 6 \end{array} \right. \xrightarrow{3F_1 - 7aF_2 \to F_1} \left\{ \begin{array}{l|l} d & -45a - 9 \\ d & 3a + 6 \end{array} \right. \xrightarrow{F_1 + 15F_2 \to F_1} \left\{ \begin{array}{l|l} d & 81 \\ d & 3a + 6 \end{array} \right.$$

Como $81 = 3^4$, los posibles divisores d:

$$d \in \{1, 3, 9, 27, 81\}$$

Empiezo a ver si es divisible por $d = 3$: Tabla de restos para $d = 3$:

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

Cuando tenga valores de:

$$\begin{cases} a \equiv 0 \ (3) \\ \text{o} \\ a \equiv 1 \ (3) \end{cases} \iff d \neq 1$$

Cuando $a \equiv 2 \ (3)$ no son ambas expresiones divisibles por 3, por eso se descarta.
Dado que los otros posibles divisores (9, 27, 81) son potencias de 3, se concluye que solo valdrá que:

$$d \neq 1 \iff \begin{cases} a \equiv 0 \ (3) \\ \text{o} \\ a \equiv 1 \ (3) \end{cases}$$

Importante que en este ejercicio no pidieron encontrar los posibles valores de d, solo que fueran distintos de uno. De no ser así habría que haber hecho, por ejemplo la tabla de restos 9, para ver si el nuevo era un posible d y así con los posibles divisores.

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Dani Tadd Olivia Portero

---

18. Hallar todos los pares $(a, b) \in \mathbb{N} \times \mathbb{N}$ que cumplen las siguientes condiciones en simultáneo:

$$27 \nmid a \qquad (a : b) = 42 \qquad [a : 5b] = 13230$$

A lo largo de este ejercicio mucho de lo que voy a usar son esas frases del secundario:

El máximo común divisor entre 2 números son los factores (de la factorización en primos) comunes elevados al menor exponente.

El mínimo común múltiplo entre 2 números son los factores (de la factorización en primos) comunes y los no comunes elevados al mayor exponente.

Del enunciado se deduce que:

$$3^3 \nmid a,$$

o sea que quizás $3^1, 3^2$ sí divida a a. También tenemos que el máximo común divisor:

$$(a : b) = 2 \cdot 3 \cdot 7$$

Esto nos dice que en la factorización de a **y de** b hay factores $2^\alpha, 3^\beta$ y 7^γ★[1], donde esos exponentes son ≥ 1. Por último el dato del mínimo común múltiplo:

$$[a : 5b] = 2^1 \cdot 3^3 \cdot 5^1 \cdot 7^2,$$

¿Qué nos dice el 2^1?:
Como sabemos de ★[1] que tanto a como b tienen a 2 como un factor y ahora en el mcm tiene exponente 1. Esto *determina* que tanto a como b tienen 2^1 como factor y ninguna potencia de 2 superior en su factorización en primos.

¿Qué nos dice el 3^3? ★²:
Parecido a lo anterior. ★¹ nos dice que el 3 está en a y b. Acá hay que tener presente que $a \nmid 3^3$. Ahora se *determina* el exponente exacto del factor 3 de b que será 3, y el de a será 1 sino en el máximo cómún divisor habría un exponente mayor en el factor 3.

¿Qué nos dice el 5^1?:
Sale que *b no tiene 5 es su factorización*, porque de tenerlo, el 5 del mcm tendría un exponente mayor debido al 5 que se enchufó ahí de prepo en el $[a : 5b]$. Y a su vez sale que a tiene que tener un 5^δ con $0 \leq \delta \leq 1$ en su factorización

¿Qué nos dice el 7^2?:
Parecido a lo que salió en ★². En este caso ★¹ nos dice que el 7 está en a y b. Ahora tampoco se *determina* el exponente exacto, pero sí sabemos que a y b tienen un factor 7^γ con $1 \leq \beta \leq 2$ en su factorización en primos, pero por ★¹ no pueden tener ambos 2 a la vez.

Recopilando la información de eso:

$$\begin{array}{rcccl} (a,b) & = & (2^1 \cdot 3^1 \cdot 5^1 \cdot 7^2 \ , \ 2^1 \cdot 3^3 \cdot 7^1) & = & (1470, 378) \\ (a,b) & = & (2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1 \ , \ 2^1 \cdot 3^3 \cdot 7^2) & = & (210, 2646) \\ (a,b) & = & (2^1 \cdot 3^1 \cdot 5^0 \cdot 7^2 \ , \ 2^1 \cdot 3^3 \cdot 7^1) & = & (294, 378) \\ (a,b) & = & (2^1 \cdot 3^1 \cdot 5^0 \cdot 7^1 \ , \ 2^1 \cdot 3^3 \cdot 7^2) & = & (42, 2646) \end{array}$$

⚠ *Nota que puede ser relevante:*
Suponiendo que lo que hice está bien, $a \cdot b = (a : b) \cdot [a : b]$, tiene que valer, pero acordate que en el enunciado metieron un 5 ahí que no está ni en a ni en b, ojo con eso.
Fin de nota que puede ser relevante: ⚠

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

---

19. Probar que $6^{2n} - 35n - 1$ es divisible por 245 para todo $n \in \mathbb{N}$.

Noto que:

$$245 = 5^2 \cdot 7$$

Los que nos piden se puede escribir como:

$$6^{2n} - 35n - 1 \equiv 0 \ (245)$$

Inducción:
Quiero probar que:

$$p(n) : 6^{2n} - 35n - 1 \equiv 0 \ (245) \qquad \forall n \in \mathbb{N}$$

Caso base:

$$p(1) : 6^{2 \cdot 1} - 35 \cdot 1 - 1 = 0 \equiv 0 \ (245)$$

Por lo que $p(1)$ resultó ser verdadera.

Paso inductivo: Asumo que

$$p(k) : \underbrace{6^{2 \cdot k} - 35 \cdot k - 1 \equiv 0 \ (245)}_{\text{hipótesis inductiva}}$$

es verdadera para algún $k \in \mathbb{N}$. Entonces quiero probar que:

$$p(k+1) : 6^{2 \cdot (k+1)} - 35 \cdot (k+1) - 1 \equiv 0 \ (245)$$

Partiendo de esto último:

$$6^{2\cdot(k+1)} - 35\cdot(k+1) - 1 = 36\cdot 6^{2k} - 35k - 35 - 1 = 36\cdot(6^{2k}-1) - 35k \equiv 0\ (245)\bigstar^1$$

Acomodo la hipótesis inductiva:

$$6^{2k} - 35\cdot k - 1 \equiv 0\ (245) \iff 6^{2k} - 1 \equiv 35k\ (245)\bigstar^2$$

Uso $\bigstar^2$ eso en $\bigstar^1$

$$36\cdot(35k) - 35k = 35^2k = 5^2\cdot 7^2 = 245\cdot 7 \equiv 0\ (245)\bigstar^1$$

Es así que $p(k+1)$ también es verdadera.

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

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

---

20. Sea $n \in \mathbb{N}$ con $n \equiv 2$ (mód 6). Hallar los posibles valores de $(2n^4+6n^2+10 : n^3+2n)$ y dar un ejemplo para cada uno.

Bautizo al MCD:

$$d = (2n^4+6n^2+10 : n^3+2n)$$

Según Euclides:

$$\begin{array}{r|l} 2n^4+6n^2+10 & n^3+2n \\ \cline{2-2} -2n^4-4n^2 & 2n \\ \cline{1-1} 2n^2+10 & \end{array}$$

Por lo que:

$$d = (2n^4+6n^2+10 : n^3+2n) = (n^3+2n : 2n^2+10)$$

Limpiando un poco eso:

$$\left\{\begin{array}{l} d \mid n^3+2n \\ d \mid 2n^2+10 \end{array}\right. \xrightarrow{2F_1 - nF_2 \to F_1} \left\{\begin{array}{l} d \mid 6n \\ d \mid 2n^2+10 \end{array}\right. \xrightarrow{3F_2 - nF_1 \to F_2} \left\{\begin{array}{l} d \mid 6n \\ d \mid 30 \end{array}\right.$$

Si $d = (6n : 30)$ entonces los *potenciales* posibles valores para el MCD serían:

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

Teniendo en cuenta que los valores de n que interesan son:

$$n \equiv 2\ (6) \overset{\text{def}}{\underset{\bigstar^1}{\iff}} n \in \{k \in \mathbb{Z}_{\geq 0} : 6k+2\}$$

Los n son siempre par, descartando así los valores $\{1,3,5,15\}$. Esto porque siempre va a estar el 2 como factor en d, ya que $d \mid 6n$.

Similarmente:

$$6 \mid 6n,$$

por lo tanto el 2 no puede ser MCD, porque el 6 siempre va a ser un divisor común y obviamente $6 > 2$ ☺.
Hasta el momento los posibles valores que puede tomar el MCD, d:

$$d \in \{6, 10, 30\}$$

Me parece que $d = 10$ *no va a ser un* d, ya que si encuentro algún n es divisible por 5, ocurre lo siguiente:

$$n = 5k \implies d \mid 6\cdot 5k = 30k,$$

por lo que tengo que eliminar al 10 de los posibles d ! Siempre que sea divisible por 10 va a ser divisible por 30.

Ahora busco ese n multiplo de 5, para probar que 30 es un podible d:

$$\overset{\bigstar^1}{\underset{!}{\Longrightarrow}} n = \underbrace{6k+2}_{\bigstar^2} \xrightarrow[\text{es multiplo de } 5]{\text{analizar si } n} 6k+2 \equiv 0\ (5) \Leftrightarrow k \equiv 3\ (5) \xrightarrow{k=3} n \overset{\bigstar^2}{=} 20$$

Es con $n = 20$ que:

$$\boxed{n = 20 \implies d \overset{\checkmark}{=} 30}$$

Es así que los posibles valores para $d = (2n^4 + 6n^2 + 10 : n^3 + 2n)$ son:

$$\boxed{d \in \{6, 30\}, \quad \text{para } n \equiv 2\ (6) \quad \text{y además} \quad \begin{cases} \text{si} \quad n = 2 & \implies & d = 6 \\ \text{si} \quad n = 20 & \implies & d = 30 \end{cases}}$$

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

---

21. Sea $a \in \mathbb{Z}$. Calcule todos los posibles valores de $d = (a^2 + a : a^3 + 3a^2 + 2a + 14)$. Para cada posibilidad de d hallada, caracterice todos los $a \in \mathbb{Z}$ para los cuales se obtiene dicho valor de d.

Simplifico al MCD, d usando Euclides:

$$\begin{array}{rl} a^3 + 3a^2 + 2a + 14 & \big| \, a^2 + a \\ \underline{-\,a^3 \;\; -\,a^2} & \big| \, \overline{a + 2} \\ 2a^2 + 2a & \\ \underline{-\,2a^2 - 2a} & \\ 14 & \end{array}$$

Por lo tanto:

$$d = (a^2 + a : 14) \implies \begin{cases} d \,\big|\, a^2 + a \\ \text{y} \\ d \,\big|\, 14 \end{cases} \qquad d \in \{1, 2, 7, 14\}$$

Tabla de restos:
Empiezo por los números menores.

¿$d = 2$ divide las expresiones?:

$r_2(a)$	0	1
$r_2(a^2 + a)$	0	0

Se concluye que el 2 es un *divisor común* para cualquier valor de a. Peeeeero como yo quiero al *MAYOR divisor común*, sigo probando con los otros posibles valores de d.

¿$d = 7$ divide las expresiones?:

$r_2(a)$	0	1	2	3	4	5	6
$r_2(a^2 + a)$	0	2	6	5	6	2	0

Se concluye que el 7 es un *divisor común* para:

$$a \equiv 0\ (7) \quad \text{o} \quad a \equiv 6\ (7)$$

¿$d = 14$ divide las expresiones?:
No hace falta hacer la tabla. ¿Por qué?

Bueno, resulta que 14 va a ser un *divisor común* ¡Cuando tanto 2 y 7 lo sean! Por lo tanto 14 es un *divisor común* cuando:

$$a \equiv 0 \ (7) \quad \text{o} \quad a \equiv 6 \ (7)$$

Vamos redondeando. Los valores de el MCD, d van a ser:

$$d = \begin{cases} 14 & \Leftrightarrow \begin{cases} a \equiv 0 \ (7) \\ \text{o} \\ a \equiv 6 \ (7) \end{cases} \\ \\ 2 & \Leftrightarrow \text{otro caso} \end{cases} .$$

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Dani Tadd

---

22. [1er cuatrimestre 2025]
Hallar el menor $n \in \mathbb{N}$ tal que $(11n^2 : 2^2 \cdot 3^4 \cdot 5 \cdot 11) = 99$ y que tenga exactamente 12 divisores positivos.

Lindo enunciado. Bautizo:

$$d = (11n^2 : 2^2 \cdot 3^4 \cdot 5 \cdot 11)$$

Factorizando ese d:

$$99 = 3^2 \cdot 11$$

Por la forma en que está expresado el número este ejercicio sale entendiendo que:

> El *máximo común divisor*, $d = (a : b)$, es el producto de los primos, de las factorizaciones de a y b, comunes elevados al menor exponente.

Para que d sea 99 entonces:

$$n = 3^1 \cdot k \quad \text{con } k \in \mathbb{N} .$$

Donde le puse a 3 el exponente 1 para que no rompa la condición del $d = 99$.
Ya está con eso tenemos que $d = 99$ siempre que lo que agreguemos en k no tenga ningún primo en común con:

$$2^2 \cdot 3^4 \cdot 5.$$

Tenemos que agregar entonces la combinación de primos que no rompan nada y que además generen un n con 12 divisores, ya sea $7^\alpha, 11^\beta, 13^\gamma, 17^\delta, \ldots$, peeeeero para que la cantidad de divisores de n sea 12 no puede haber más de 3 primos en la factorización, sino habría más de 3 divisores (Acá un poco de formulitas sobre esto click click).
Armo sistema con los 3 primos más chicos que puedo elegir:

$$\begin{cases} n &= 3^1 \cdot 7^\alpha \cdot 11^\beta \\ (1+1) \cdot (\alpha+1) \cdot (\beta+1) &= 12 \quad \Longleftrightarrow \quad (\alpha+1) \cdot (\beta+1) = 6 \end{cases}$$

Quedan solo 4 opciones:

$$\begin{cases} (\alpha, \beta) = (1,2) & \Longrightarrow \quad n = 3^1 \cdot 7^1 \cdot 11^2 \\ (\alpha, \beta) = (2,1) & \Longrightarrow \quad n = 3^1 \cdot 7^2 \cdot 11^1 \\ (\alpha, \beta) = (5,0) & \Longrightarrow \quad n = 3^1 \cdot 7^0 \cdot 11^5 \\ (\alpha, \beta) = (0,5) & \Longrightarrow \quad n = 3^1 \cdot 7^5 \cdot 11^0 \end{cases}$$

La combinación que da el menor n es:

$$\boxed{n = 3^1 \cdot 7^2 \cdot 11^1}$$

---

23. [(7/10/25) primer parcial]

Probar que para todo $n \in \mathbb{N}$ vale que $36 \mid 19^n - 18n^2 - 1$.

Acomodo el enunciado como:

$$36 \mid 19^n - 18n^2 - 1 \overset{\text{def}}{\iff} 19^n - 18n^2 - 1 \equiv 0 \ (36)$$

Inducción: Quiero probar que la proposición $p(n)$:

$$p(n) : 19^n - 18n^2 - 1 \equiv 0 \ (36) \ \ \forall n \in \mathbb{N}$$

es verdadera.

Caso base: Quiero ver que para $n = 1$ la proposición es verdadera.

$$p(1) : 19^1 - 18 \cdot 1^2 - 1 = 0 \equiv 0 \ (36).$$

Por lo tanto $p(1)$ es verdadera.
Paso inductivo: Para algún $k \in \mathbb{N}$ asumo que la proposición:

$$p(k) : \underbrace{19^k - 18k^2 - 1 \equiv 0 \ (36)}_{\text{hipótesis inductiva}}$$

es verdadera. Entonces quiero probar que:

$$p(k+1) : 19^{k+1} - 18(k+1)^2 - 1 \equiv 0 \ (36)$$

también lo sea.
Partiendo del paso $k+1$:

$$\begin{aligned} 19^{k+1} - 18(k+1)^2 - 1 &\overset{!}{=} 19 \cdot 19^k - 18k^2 - 36k - 19 \\ &= 19 \cdot (19^k - 1) - 18k^2 - 36k \\ &\overset{(36)}{\equiv} 19 \cdot (19^k - 1) - 18k^2 \bigstar^1 \end{aligned}$$

Usando la hipótesis inductiva:

$$19^k - 18k^2 - 1 \equiv 0 \ (36) \overset{\bigstar^2}{\iff} 19^k - 1 \equiv 18k^2 \ (36)$$

puedo escribir a $\bigstar^1$ como:

$$\begin{aligned} \bigstar^1 \to 19 \cdot (19^k - 1) - 18k^2 &\overset{(36)}{\underset{\bigstar^2}{\equiv}} 19 \cdot (18k^2) - 18k^2 \\ &= 18 \cdot (18k^2) \\ &= 18^2 k^2 \\ &\overset{(36)}{\underset{!}{\equiv}} 0 \end{aligned}$$

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

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

24. [(7/10/25) primer parcial]
Sean a y $b \in \mathbb{Z}$ tales que $(a : b) = 5^2$. Hallar los posibles valores de $(a^2b : 5^4(a^2 + b^2))$. Dar ejemplo de cada caso posible.

Arranco coprimizando:

$$(a : b) = 5^2 \xrightarrow[(A:B)=1]{\text{coprimizar}} \bigstar^1 \begin{cases} a &= A \cdot 5^2 \\ b &= B \cdot 5^2 \end{cases}$$

Quedando el MCD como:

$$d = (a^2b : 5^4(a^2 + b^2)) \overset{\bigstar^1}{\iff} d = 5^6 \cdot (A^2B : 5^2(A^2 + B^2))$$

Laburo ahora con:

$$(A : B) = 1 \quad \text{y} \quad D = (A^2B : 5^2(A^2 + B^2)) \ \bigstar^2$$

Dado que D es un *divisor común*:

$$\begin{cases} D \mid A^2B \\ D \mid 5^2(A^2 + B^2) \end{cases} \overset{\text{¿?}}{\Longrightarrow} \begin{cases} \begin{cases} D \mid A^2B \\ D \mid 5^2B^3 \end{cases} \\ \text{y} \\ \begin{cases} D \mid A^2B \\ D \mid 5^2A^4 \end{cases} \end{cases}$$

Dado que A y B no comparten ningún primo en su factorización, *because* coprimos los posibles valores que puede tomar D:

$$D \in \{1, 5, 25\}\,.$$

Si encuentro valores de A y B con $A \perp B$ para esos D, gané. Miro fuerte la expresión de D en $\bigstar^2$. Probando valores razonables a *ojímetro*:

$$(A, B) = (1, 1) \implies D = (1, 5^2) = 1 \xRightarrow{\bigstar^1} \begin{cases} (a, b) &= (5^2, 5^2) \\ d &= 5^6 \end{cases}$$

$$(A, B) = (1, 5) \implies D \overset{!}{=} (5, 5^2 \cdot 13 \cdot 2) = 5 \xRightarrow{\bigstar^1} \begin{cases} (a, b) &= (5^2, 5^3) \\ d &= 5^7 \end{cases}$$

$$(A, B) = (0, 1) \implies D = (0, 25) = 25 \xRightarrow{\bigstar^1} \begin{cases} (a, b) &= (0, 5^2) \\ d &= 5^8 \end{cases}$$

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

---

25. [11/02/26 Ejercicio de la Práctica]
Sea $b \in \mathbb{Z}$ impar y sea a_n la sucesión de enteros dada por

$$\begin{cases} a_1 &= -6 \\ a_{n+1} &= 41a_n + b^{2n} + 7 \end{cases}.$$

Probar que $a_n \equiv 2\ (8), \quad \forall n \in \mathbb{N}$.

Sale por inducción:

Dada una sucesión definida por recurrencia $\begin{cases} a_1 &= -6 \\ a_{n+1} &= 41a_n + b^{2n} + 7 \end{cases}$

Quiero probar que la siguiente proposición es verdadera:

$$p(n) : a_n \equiv 2\ (8)$$

Caso base:
Quiero probar que

$$p(1) : a_1 \equiv 2 \ (8)$$

es verdadera.
Es trivialmente verdadera dado que $a_1 \overset{\text{def}}{=} -6 \overset{(8)}{\equiv} 2$.

Paso inductivo:
Para algún $k \in \mathbb{N}$ asumo que la proposición:

$$p(k) : \underbrace{a_k \equiv 2 \ (8)}_{\text{hipótesis inductiva}}$$

es verdadera. Entonces quiero ver que la proposición:

$$p(k+1) : a_{k+1} \equiv 2 \ (8)$$

también lo sea.
Usando la hipótesis inductiva en la definición de la sucesión:

$$a_{k+1} = 41a_k + b^{2k} + 7 \overset{(8)}{\underset{\text{HI!!}}{\equiv}} 2 + b^{2k} + 7$$

$$\overset{(8)}{\equiv} b^{2k} + 1 \ \bigstar^1$$

Si puedo probar que $b^{2k} \equiv 1 \ (8)$ listo gané, dado que me quedaría que $a_{k+1} \equiv 2 \ (8)$. Lo voy a probar de 2 formas distintas, cuál se te ocurre a vos es cosa tuya. La primera es más *"creativa y elegante"*, la segunda más *"intuitiva y mecánica"*.

Mirar los ejercicios **4.** y **13.** puede servir de inspiración. Anyways, si no salió ahí va.

¿Cómo verga se hace esto? Es un salto creativo para pensar un ratito y probar cositas hasta que salga.

Resulta que b es impar:

$$b \overset{\bigstar^2}{=} 2i+1 \implies \begin{cases} b^{2k} = (b^2)^k \\ \overset{\bigstar^2}{=} ((2i+1)^2)^k \\ \overset{!}{=} (4\underbrace{i(i+1)}_{\substack{\text{esto es} \\ \text{siempre} \\ \text{par}}} + 1)^k \\ \overset{!!!}{=} (8j+1)^k \\ \overset{(8)}{\equiv} (1)^k = 1 \end{cases}$$

Si te perdiste en los !, en uno son cuentas y en otro escribo un número par en su forma genérica.

Estás pensando:
¡Eso no se me ocurre ni en pedo en un parcial! Fair enough, tabla de restos

$r_8(i)$	0	1	2	3	4	5	6	7
$r_8((2i+1)^2)$	1	1	1	1	1	1	1	1

Mucho más fácil honestamente, menos elegante y *mathy snoby*, pero mucho más fácil. Elige tu propia aventura.
Así queda demostrado $\bigstar^1$ que $a_{k+1} \equiv 2 \ (8)$.

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

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
Ivan Doumerc · naD GarRaz · Diego Moros