Apéndice A

EJERCICIOS

A.1. Ejercicios Propuestos

A.1.1. Números Enteros

Ejercicio 1 *Demostrar que* $\forall n \in \mathbb{N}: \quad 6|(n(n+1)(n^2+n+1))$.

Ejercicio 2 *Demostrar que* $\forall n \in \mathbb{N}: \quad 30|(n^5-n)$.

Ejercicio 3 *Demostrar que* $\forall n \in \mathbb{Z}: \quad 4$ *no divide a* n^2-n.

Ejercicio 4 *Demostrar que el producto de dos números enteros impares da un entero impar.*

Ejercicio 5 *Si* $b|c$ *y* $(a,c)=1$ *entonces* $(a,b)=1$.

Ejercicio 6 *Sean* $x, y, r \in \mathbb{Z}$ *tales que* $(r,11)=1$, $r|(2x-y)$, $r|(x+5y)$. *Demuestre que* $r|x$

Ejercicio 7 *Si* $n \in \mathbb{Z}^+$. *Calcular* $(n, n+1), \quad [n, n+1]$

Ejercicio 8 *Encontrar el máximo común divisor MCD en los siguientes caso:*

i) $(232, 548)$

ii) $(54, 138, 1104)$

Ejercicio 9 *Determinar la solución general de cada ecuación diofántica lineal.*

i) $598 \cdot x + 767 \cdot y = 26$

ii) $3 \cdot x + 9 \cdot y + 13 \cdot z = 1$

A.1.2. Números Enteros Módulo m

Ejercicio 10 *Calcular el orden de:*

i) $\overline{3} \in (\mathbb{Z}_{69}, +)$

ii) $\overline{5} \in (\mathcal{U}(\mathbb{Z}_{31}), \cdot)$

iii) $\overline{7} \in (\mathcal{U}(\mathbb{Z}_{29}), \cdot)$

Ejercicio 11 *Hacer la tabla del grupo:*

i) $(\mathbb{Z}_8, +)$

ii) $(\mathcal{U}(\mathbb{Z}_{11}), \cdot)$

Ejercicio 12 *Hacer la tabla y determinar los generadores de* $\mathcal{U}(\mathbb{Z}_{10})$

Ejercicio 13 *Calcular el número y las raíces primitivas o los generadores:*

i) $(\mathbb{Z}_{24}, +)$

ii) $(\mathbb{Z}_{30}, +)$

iii) $(\mathbb{Z}_{300}, +)$

iv) $(\mathbb{Z}_{890}, +)$

v) $(\mathcal{U}(\mathbb{Z}_{11}), \cdot)$

vi) $(\mathcal{U}(\mathbb{Z}_{12}), \cdot)$

vii) $(\mathcal{U}(\mathbb{Z}_{18}), \cdot)$

viii) $(\mathcal{U}(\mathbb{Z}_{25}), \cdot)$

ix) $(\mathcal{U}(\mathbb{Z}_{43}), \cdot)$

Ejercicio 14 *Determinar generadores y subgrupos de:*

i) $\mathcal{C}_{13} = \{\overline{x}^3 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{13})\}$

ii) $\mathcal{C}_{31} = \{\overline{x}^3 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{31})\}$

Ejercicio 15 *Calcular el reticulado de los subgrupos de* $(\mathbb{Z}_{16}, +)$

Ejercicio 16 *Sea* $\mathcal{G} =< g >$ *grupo cíclico tal que* $|\mathcal{G}| = 12$. *Calcular el reticulado de los subgrupos de* $\mathcal{G}$.

Ejercicio 17 *Determine si* $(\mathcal{U}(\mathbb{Z}_{23}), \cdot)$ *es un grupo cíclico, en caso afirmativo encuentre un generador.*

Ejercicio 18 *Determinar el resto al dividir:*

i) 7^{2702} *por* 31

ii) $2^{100} + 3^{20} + 7^{89}$ *por* 19

iii) 473^{38} *por* 5

Ejercicio 19 *¿Cuál es el dígito de las unidades en la representación decimal de* 3^{400}*?*

Ejercicio 20 *Encontrar el menor entero positivo que deja restos* $2, 3, 2$ *cuando es divido por* $3, 5, 7$ *respectivamente.*

Ejercicio 21 *Calcular los elementos, generadores y hacer la tabla de:*

i) $\square_{17}$

ii) $\square_{22}$

Ejercicio 22 *Determine el número de soluciones en cada caso*

i) $x^2 \equiv 5 (\texttt{mod } 73)$

ii) $x^2 \equiv 226 (\texttt{mod } 563)$

iii) $x^3 \equiv 8 (\texttt{mod } 719)$

iv) $x^2 \equiv 150 (\texttt{mod } 1009)$

v) $x^4 \equiv 9 (\texttt{mod } 4003)$

vi) $x^6 \equiv 1 (\texttt{mod } 19)$

Ejercicio 23 *Resolver las siguientes ecuaciones*

i) $x^2 \equiv 5 (\texttt{mod } 29)$

ii) $x^2 \equiv 2 (\texttt{mod } 97)$

iii) $x^{954} + 2x - 1 \equiv 0 (\texttt{mod } 953)$

iv) $x^3 \equiv 8 (\texttt{mod } 31)$

v) $x^6 + 2x^3 + 3 \equiv 0 (\texttt{mod } 23)$

vi) $x^{15} - x^{10} + 4x - 3 \equiv 0 (\texttt{mod } 7)$

vii) $x^8 + x^2 \equiv 0 (\texttt{mod } 7) \quad 0 \leq x \leq 30$

viii) $x^5 - x^3 \equiv 0 (\texttt{mod } 43)$

Ejercicio 24 *Resolver en* $\mathbb{Z}_{21}$*:*

$$\overline{x} + \overline{73} = \overline{68}$$

Ejercicio 25 *Determinar todos los* $\overline{x} \in \mathbb{Z}_7$ *tal que*

$$\overline{2} \cdot \overline{x}^2 + \overline{x} + \overline{6} = \overline{0}$$

Ejercicio 26 *Demostrar que para todo entero* a, n *tales que son primo relativos con* 31 *entonces* $31 | n^{30} - a^{30}$

Ejercicio 27 *Determinar todos los* p *primos impares tal que* $\left(\frac{5}{p}\right) = -1$

Ejercicio 28 *Resolver:*

a. $\left.\begin{array}{rcl} 3x + 2y & \equiv & 1 (\bmod 7) \\ 2x + 5y & \equiv & 2 (\bmod 7) \end{array}\right|$ *b.* $\left.\begin{array}{rcl} x + 12y & \equiv & 9 (\bmod 13) \\ 3x + 11y & \equiv & 8 (\bmod 13) \end{array}\right|$

c. $\left.\begin{array}{rcl} x + y + z & \equiv & 2 (\bmod 7) \\ x + 2y + 3z & \equiv & 3 (\bmod 7) \\ 2x + y + 4z & \equiv & 1 (\bmod 7) \end{array}\right|$ *d.* $\left.\begin{array}{rcl} x + 2y + 4z & \equiv & 5 (\bmod 13) \\ 5x + y + 8z & \equiv & 7 (\bmod 13) \\ 6x + 8y + 7z & \equiv & 1 (\bmod 13) \end{array}\right|$

e. $\left.\begin{array}{rcl} x & \equiv & 7 (\bmod 9) \\ x & \equiv & 10 (\bmod 4) \\ x & \equiv & 1 (\bmod 7) \end{array}\right|$ *f.* $\left.\begin{array}{rcl} x & \equiv & 1 (\bmod 4) \\ x & \equiv & 0 (\bmod 3) \\ x & \equiv & 5 (\bmod 7) \end{array}\right|$

g. $\left.\begin{array}{rcl} 3x & \equiv & 1 (\bmod 5) \\ 4x & \equiv & 6 (\bmod 14) \\ 5x & \equiv & 11 (\bmod 3) \end{array}\right|$ *h.* $\left.\begin{array}{rcl} x - y & \equiv & 5 (\bmod 47) \\ xy & \equiv & 6 (\bmod 47) \end{array}\right|$

i. $\left.\begin{array}{rcl} x^2 + y^2 & \equiv & 1 (\bmod 13) \\ xy & \equiv & 2 (\bmod 13) \end{array}\right|$

Ejercicio 29 *Determinar los* $\alpha \in \mathbb{Z}_{41}$ *tal que*

$$\left.\begin{array}{rcl} x - y & = & \alpha \\ x \cdot y & = & 1 \end{array}\right|$$

el sistema no tenga solución.

Ejercicio 30 *Si* $p \equiv 3 (\bmod 4)$*. Determine si existen* $x, y \in \mathbb{Z}$ *tal que* $x^2 + y^2 = p$

Ejercicio 31 *Sea* p *primo impar. Demostrar:* $\sum_{\overline{x} \in \mathbb{Z}_p^*} \overline{x}^{-1} \equiv 0 (mod, p)$

Ejercicio 32 *Sea* p *primo impar. Calcular* $\prod_{\overline{x} \in \square_p} \overline{x}$

Ejercicio 33 *Calcular* $\sum_{\overline{x} \in \square_p} \overline{x}$

Ejercicio 34 *Determinar todos los* $x, y \in \mathbb{Z}$ *que cumplan con:* $x, y \in \mathbb{Z}^+$, $x + y = 100$ *y* $(x, y) = 5$

Ejercicio 35 *Probar que si* x, y *son impares entonces* $x^2 + y^2$ *es par pero no divisible por cuatro.*

Ejercicio 36 *Sean* $a, b \in \mathbb{Z}$ *entonces demuestre que:*
Si $a^2 = 2 \cdot b^2$ *entonces* a *y* b *son pares.*

Ejercicio 37 *Sean* $a, b \in \mathbb{Z}$ *entonces demuestre que:*
Si $(a, 4) = 2, \quad (b, 4) = 2$ *entonces* $(a + b, 4) = 4$

A.1.3. Números Complejos

Ejercicio 38 *Determinar* $z \in \mathbb{C}$ *tal que:*

i) $\overline{z} + 2z = 4 + i$

ii) $\overline{z} + 5z + 6 = z^2$

iii) $z^2 + |z| = 0$

iv) $\left|\frac{z-12}{z-8i}\right| = \frac{5}{3}$

Ejercicio 39 *Demostrar:*

i) $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

ii) $|z_1 + z_2|^2 + |z_1 - z_2|^2 = 2|z_1|^2 + 2|z_2|^2$

Ejercicio 40 *Determinar el lugar geométrico de:*

i) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad 4 \leq |z - 1| + |z + 1| \leq 8\}$

ii) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad \frac{1}{2} \leq |z| \leq 1\}$

iii) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z - 1 + i| = 4\}$

iv) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z - 2| = |1 - 2\overline{z}|\}$

v) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad Re(\overline{z} - i) = 2\}$

vi) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad 0 \leq Im(z) \leq 2\}$

vii) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad 0 \leq Re(z) \leq 2\}$

viii) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z - 4i| + |z + 4i| = 10\}$

ix) *Sean* $a, c \in \mathbb{R}, b \in \mathbb{C}$ *fijos* $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad a \cdot z \cdot \overline{z} + Re(b \cdot \overline{z}) + c = 0\}$

Ejercicio 41 *Sean* $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z| = 3\}, \quad \mathcal{B} = \{z \in \mathbb{C} \quad | \quad |z-1| = |z-i|\}$.
Calcular $\mathcal{A} \cap \mathcal{B}$

Ejercicio 42 *Si* $|z| = 1$ *y* $w, z \in \mathbb{C}$, *demuestre que* $|z + w| = |\overline{z}w + 1|$

Ejercicio 43 *Encontrar el Arg(z) cuando:*

I) $z = -2 + 2\sqrt{3}i$

II) $z = -\frac{2}{1+\sqrt{3}i}$

Ejercicio 44 *Escriba en forma polar:*

I) $-\sqrt{2} - \sqrt{2}i$

II) $z = -\frac{2}{1+\sqrt{3}i}$

Ejercicio 45 *Encuentre el valor de:*

I) $\frac{(-\sqrt{2}-\sqrt{2}i)^{16}}{(-1+i)^4}$

II) $\left(\frac{1+\sqrt{3}i}{1-i}\right)^{40}$

III) $(1+i)^n + (1-i)^n$

Ejercicio 46 *Determinar todos los* $z \in \mathbb{C}$ *tal que:* $\left(\frac{1-z}{i+z}\right)^3 = 1$

Ejercicio 47 *Encuentre en cada caso, las siguientes raíces n-esima de:*

I) $-i \qquad n = 3$

II) $-1 \qquad n = 4$

III) $2 - 2\sqrt{3}i \qquad n = 2$

IV) $-\frac{\sqrt{3}}{2} + \frac{1}{2}i \qquad n = 3$

Ejercicio 48 *Determine si* $2 + 3i$ *divide* $4 + 8i$ *en* $\mathbb{Z}[i]$ *Justifique.*

Ejercicio 49 *Determine si* $7 + 5i$ *es primo en* $\mathbb{Z}[i]$ *Justifique*

Ejercicio 50 *Determine si* 7 *es primo en* $\mathbb{Z}[i]$*? Justifique*

Ejercicio 51 *Sea* $p(x) = x^4 + ax^2 + bx + 5$. *Determinar* a, b *si* 1 *y* -2 *son raíces de* $p(x)$.

A.1.4. Polinomios

Ejercicio 52 *Determinar todas las raíces de* $x^8 + x^4 + 1$

Ejercicio 53 *Sea* $p(x) = 3x^3 + 2x^2 + cx - k$*. Determinar* $c, k \in \mathbb{R}$ *tal que al dividir* $p(x)$ *por* $x + 2$ *el resto es* 37 *y al dividir* $p(x)$ *por* $x - 1$ *el resto es* -2*.*

Ejercicio 54 *Sea* $p(x) = 2x^3 + bx^2 + cx + d$*. Determinar los valores de* $b, c, \in \mathbb{R}$ *de modo que se cumplan. El resto al dividir* $p(x)$ *por* x *es* $2 + b$*, el resto al dividir* $p(x)$ *por* $x + 1$ *es* $b + d$*,* 1 *es raíz de* $p(x)$

Ejercicio 55 *Sea* $p(x) \in \mathbb{R}[x]$*. Al dividir* $p(x)$ *por* $x-3$ *el resto es 2. Al dividir* $p(x)$ *por* $x-4$ *es resto es 6 y 2 es raíz de* $p(x)$ *Calcular el resto al dividir* $p(x)$ *por* $(x-2)\cdot(x-3)\cdot(x-4)$*.*

Ejercicio 56 *Determinar* $a, b \in \mathbb{R}$ *para que* -1 *sea raíz doble (o de multiplicidad dos) de* $p(x) = x^4 + ax^3 + (a-b)x^2 + bx + 1$

Ejercicio 57 *Sea* $p(x) = 6x^3 + tx^2 + kx - 3t$ *encontrar los valores de* $t, k \in \mathbb{R}$ *tal que al dividir* $p(x)$ *por* $x - 2$ *el resto es* 21 *y* 1 *es raíz de* $p(x)$*.*

Ejercicio 58 *Sea* $p(x) = 2x^4 + ax^3 + 28x^2 + bx + 6$*. Determine los valores de* $a, b \in \mathbb{R}$ *para que* 1 *y* $\frac{1}{2}$ *sean raíces de* $p(x)$*.*

Ejercicio 59 *Sea* $p(x) \in \mathbb{R}[x]$*. Al dividir* $p(x)$ *por* $x + 1$ *el resto es 2. Al dividir* $p(x)$ *por* $x - 1$ *es resto es 3. Calcular el resto al dividir* $p(x)$ *por* $(x+1)\cdot(x-1)$*.*

Ejercicio 60 *Sea* $p(x) = x^6 - 1$*. Descomponer en factores irreducibles el polinomio* $p(x)$ *en* $\mathbb{Q}[x]$*,* $\mathbb{R}[x]$*,* $\mathbb{C}[x]$

Ejercicio 61 *Sea* $p(x) = 2x^4 + ax^3 + 28x^2 + bx + 6$*. Determinar los valores de* $a, b \in \mathbb{R}$ *para que* 1 *y* $\frac{1}{2}$ *sean raíces de* $p(x)$ *y factoricé* $p(x)$ *como producto de polinomios irreducibles en* $\mathbb{R}[x]$*.*

Ejercicio 62 *Sea* $p(x) = x^6 - x^5 - 5x^4 + 5x^3 - 36x^2 + 36x$

i) *Determine las raíces racionales de* $p(x)$

ii) *Factorize* $p(x)$ *como producto de polinomios irreducibles en* $\mathbb{R}[x]$

iii) *Factorize* $p(x)$ *como producto de polinomios irreducibles en* $\mathbb{C}[x]$

Ejercicio 63 *Descomponer* $x^8 + x^4 + \overline{1} \in \mathbb{Z}_7[x]$ *en factores irreducibles.*

Ejercicio 64 *Exprese* $x^4 + \overline{4} \in \mathbb{Z}_5[x]$ *como el producto de polinomios irreducibles.*

Ejercicio 65 *Sea* $p(x) = x^4 + x^3 + x^2 + x + \overline{1} \in \mathbb{Z}_5[x]$*. Descomponer* $p(x)$ *en factores irreducibles.*

Ejercicio 66 *Dadas las raíces* a, b, c *de* $x^3+x^2+x+1=0$, *construya un polinomio de grado* 3 *cuyas raíces son* a^2, b^2, c^2

Ejercicio 67 *Dadas las raíces* a, b, c *de* $x^3+2x^2+3x+1=0$, *construya un polinomio de grado* 3 *cuyas raíces son* a^2, b^2, c^2

Ejercicio 68 *Si* a, b, c *son las raíces del polinomio* x^3-x^2-1. *Determine el polinomio de grado* 3 *cuyas raíces son* $a+b, a+c, b+c$

Ejercicio 69 *Exprese* $x^8+\overline{4} \in \mathbb{Z}_5[x]$ *como el producto de polinomios irreducibles.*

Ejercicio 70 *Hacer la tabla de suma y multiplicación del siguiente anillo* $\mathbb{Z}_3[x]/ < x^2-\overline{1} >$

Ejercicio 71 *Sea el cuerpo* $\mathbb{F}_{27} = \mathbb{Z}_3[x]/ < x^3+2x+1 >$. *Sea* $\overline{x^4+\overline{1}} \in \mathbb{F}_{27}$. *Calcule* $\overline{x^4+\overline{1}}^{-1}$

Ejercicio 72 *Sea* $\mathbb{F}_{25} = \mathbb{Z}_5[x]/ < x^2+x+1 >$. *Calcule* $[x^7+x^5+x^4+4]^{-1}$

Ejercicio 73 $\mathbb{F}_8^* = \mathcal{U}(\mathbb{Z}_2[x]/ < x^3+x+1 >)$ *es cíclico?*

Ejercicio 74 *Sea* $\mathbb{F}_9 = \mathbb{Z}_3[x]/ < x^2+1 >$. *En el grupo* $(\mathbb{F}_9^*, \cdot)$. *Determine el orden de cada elemento.*

Ejercicio 75 $\mathbb{Z}_{19}[x]/ < x^2-8 >$ *es un cuerpo?*

Ejercicio 76 *Hacer la tabla del grupo de los cuadrados de* $\mathbb{F}_9$

Ejercicio 77 *Determine* α *para que* $\mathbb{Z}_7[x]/ < x^2-\alpha >$ *no sea un cuerpo.*

A.2. Respuesta Ejercicios Propuestos

A.2.1. Números Enteros

Solución 1. La demostración se realizar usando el principio de inducción.

Sea $p(n) : 6|n(n+1)(n^2+n+1)$

Primer paso: $p(0) : 6|0$, es verdadero.

Segundo paso: Supongamos $p(n) : 30|(n(n+1)(n^2+n+1)$ es verdadero, y demostremos que $p(n+1)$ es verdadero

Para ello notemos primero que

$$6|(n+1)(n+2)((n+1)^2+(n+1)+1) \Leftrightarrow (n+1)(n+2)(n^2+3n+3) = 6\cdot q; \quad q \in \mathbb{Z}.$$

de otro modo tenemos

$$\begin{aligned}
& (n+1)(n+2)(n^2+3n+3) \\
= \;& n(n+1)(n^2+3n+3) + 2(n+1)(n^2+3n+3) \\
= \;& n(n+1)(n^2+n+1) + 2(n+1)n(n+1) + 2(n+1)(n^2) + 6(n+1)^2 \\
= \;& n(n+1)(n^2+n+1) + 2(n+1)(n^2+n+n^2) + 6(n+1)^2 \\
= \;& n(n+1)(n^2+n+1) + 2(n+1)n(2n+1) + 6(n+1)^2
\end{aligned}$$

Por hipótesis de inducción el primer sumando es múltiplo de 6, el segundo es 12 veces la suma de los primeros naturales al cuadrado, y el tercero es múltiplo de 6, luego $p(n+1)$ es verdadero y por el principio de inducción se tiene que:

$$\forall n \in \mathbb{N} : \quad 6|(n(n+1)(n^2+n+1)).$$

♡

Solución 2. La demostración se realizar usando el principio de inducción.

Sea $p(n) : 30|(n^5 - n)$

Primer paso: $p(0) : 30|0$, es verdadero.

Segundo paso: Supongamos $p(n) : 30|(n^5 - n)$ es verdadero, y demostremos que $p(n+1)$ es verdadero.

Para ello notemos primero que

$$30|((n+1)^5 - (n+1)) \Leftrightarrow (n+1)^5 - (n+1) = 30 \cdot q; \quad q \in \mathbb{Z}.$$

Desarrollando el binomio obtenemos

$$\begin{aligned} (n+1)^5 - (n+1) &= n^5 + 5 \cdot n^4 + 10 \cdot n^3 + 10 \cdot n^2 + 5 \cdot n + 1 - n - 1 \\ &= n^5 - n + 5 \cdot (n^4 + 2 \cdot n^3 + 2 \cdot n^2 + n) \end{aligned}$$

Aplicando hipótesis de inducción tenemos

$$(n+1)^5 - (n+1) = 30 \cdot k + 5 \cdot (n^4 + 2 \cdot n^3 + 2 \cdot n^2 + n)$$

Para poder concluir necesitamos que

$$\forall n \in \mathbb{N} : \quad 6|(n^4 + 2 \cdot n^3 + 2 \cdot n^2 + n) \Leftrightarrow n(n+1)(n^2+n+1) = 6 \cdot r; \quad r \in \mathbb{Z},$$

lo cuál esta demostrado en el ejercicio anterior, por ello obtenemos

$$\begin{aligned} (n+1)^5 - (n+1) &= 30 \cdot k + 5 \cdot 6 \cdot r \\ &= 30 \cdot k + 30 \cdot r \\ &= 30 \cdot (k + r) \end{aligned}$$

De este modo obtenemos que $p(n+1)$ es verdadero y por el principio de inducción se obtiene que

$$\forall n \in \mathbb{N} : \quad 30|(n^5 - n).$$

♡

Solución 3. La demostración se realizara por el método del absurdo.

Para ello supongamos que existe $n \in \mathbb{Z}$ tal que $4|(n^2+2) \Leftrightarrow n^2 + 2 = 4 \cdot q; \quad q \in \mathbb{Z}$.

Notemos que al dividir un número por 2 se obtiene 2 posibles resto $0, 1$, lo cual significa que

$$\mathbb{Z} = \{2 \cdot k \mid k \in \mathbb{Z}\} \cup \{2 \cdot k + 1 \mid k \in \mathbb{Z}\}$$

Recordemos que $a|b \wedge a|c$ entonces $a|(bx+cy)$

Caso Supongamos $n = 2\cdot k$ de lo cual obtenemos $n^2 = 4\cdot k^2$, reemplazando obtenemos

$$4|(4\cdot k^2 + 2) \Rightarrow 4|2.$$

lo que es una contradicción.

Por lo tanto 4 no divide a n^2+2, con $n = 2\cdot k$.

Caso Supongamos $n = 2\cdot k+1$ de lo cual $n^2 = (2\cdot k+1)^2 = 4k^2+4k+1$, reemplazando obtenemos

$$4|(4\cdot k^2 + 4k + 1 + 2) \Rightarrow 4|3$$

lo que es una contradicción.

Por lo tanto 4 no divide a n^2+2 con $n = 2\cdot k+1$

Por ello se tiene que $\forall n \in \mathbb{Z}: \quad 4$ no divide a n^2+2. ♡

Solución 4. Sean m, n números impares, luego $m = 2\cdot k+1; \quad k \in \mathbb{Z}$, $n = 2\cdot q+1; \quad q \in \mathbb{Z}$

$$\begin{aligned} m\cdot n &= (2\cdot k+1)\cdot(2\cdot q+1) \\ &= 4\cdot k\cdot q + 2\cdot q + 2\cdot q + 1 \\ &= 2\cdot(2\cdot q\cdot k + q + k) + 1 \\ &= 2\cdot r + 1; \quad \text{con } r = 2\cdot q\cdot k + q + k \end{aligned}$$

Por lo tanto, el producto de dos números enteros impares es un entero impar. ♡

Solución 5. Supongamos que $b|c$ y $(a,c) = 1$, como $b|c \Leftrightarrow c = b\cdot r; \quad r \in \mathbb{Z}$, además existen $x, y \in \mathbb{Z}$ tales que $1 = a\cdot x + c\cdot y$.

$$\begin{aligned} 1 &= a\cdot x + c\cdot y \\ &= a\cdot x + b\cdot r\cdot y \\ &= a\cdot x + b\cdot y_0; \quad y_0 = r\cdot y, \end{aligned}$$

es decir, existen $x_0, y_0 \in \mathbb{Z}$, tales que $a\cdot x + b\cdot y_0 = 1$, por ende, se tiene que $(a,b) = 1$. ♡

Solución 6. Sean $x, y, r \in \mathbb{Z}$ tales que $(r, 11) = 1$, $r|(2x-y)$, $r|(x+5y)$. Por demostrar $r|x$

Como

$$r|(2x-y) \quad \wedge \quad r|(x+5y)$$

Luego existen $q_1, q_2 \in \mathbb{Z}$, tale que

$$2x - y = r\cdot q_1; \quad x + 5y = r\cdot q_2$$

Además $(r, 11) = 1$, por lo cual, existen $a, b \in \mathbb{Z}$ tal que $ra + 11b = 1$. Es decir,

$$\begin{array}{rcl|} 1 &=& ra + 11b \\ 2x-y &=& r\cdot q_1 \\ x+5y &=& r\cdot q_2 \\ \hline \end{array}$$

Amplificando por 5, la segunda ecuación y sumando a la tercera obtenemos

$$11x = r \cdot (5q_1 + q_2) = r \cdot k; \quad k = 5q_1 + q_2$$

Ahora amplificando por x la primera ecuación y reemplazando $11x$

$$\begin{aligned} x &= rax + 11xb \\ x &= rax + rkb = r \cdot (ax + kb) \end{aligned}$$

Por lo tanto $r|x$ $\heartsuit$

Solución 7. Dado $n \in \mathbb{Z}^+$. Calcular $(n, n+1)$, $[n, n+1]$.
Para ello notemos que

$$(n+1) \cdot (1) + n \cdot (-1) = 1$$

Por lo tanto $(n, n+1) = 1$

$$[n, n+1] = \frac{n \cdot (n+1)}{(n, n+1)}$$

Por lo tanto $[n, n+1] = n \cdot (n+1)$. $\heartsuit$

Solución 8.

I) Calcular $(232, 548)$, para ello

$$548 = 232 \cdot 2 + 84; \quad 232 = 84 \cdot 2 + 64; \quad 84 = 64 \cdot 1 + 20;$$
$$64 = 20 \cdot 3 + 4; \quad 20 = 4 \cdot 5 + 0.$$

Por lo tanto $(232, 548) = 4$

II) Calcular $(54, 138, 1104)$, para ello

$$138 = 54 \cdot 2 + 30; \quad 54 = 30 \cdot 1 + 24; \quad 30 = 24 \cdot 1 + 6;$$
$$24 = 6 \cdot 4; \quad 1104 = 6 \cdot 184.$$

Por lo tanto $(54, 138, 1104) = ((54, 138), 1104) = (6, 1104) = 6$

$\heartsuit$

Solución 9.

I) Resolver $598 \cdot x + 767 \cdot y = 26$

$$767 = 598 \cdot 1 + 169; \quad 598 = 169 \cdot 3 + 91; \quad 169 = 91 \cdot 1 + 78;$$
$$91 = 78 \cdot 1 + 13; \quad 78 = 13 \cdot 6.$$

Por lo tanto $(598, 767) = 13$, determines una solución

$$\begin{aligned}
13 &= 91 - 78 \cdot 1 = 91 - 1 \cdot (169 - 91 \cdot 1)\\
&= 91 - 169 \cdot 1 + 91 \cdot 1 = 91 \cdot 2 - 169 \cdot 1\\
&= 2 \cdot (598 - 169 \cdot 3) - 169 \cdot 1 = 598 \cdot 2 - 169 \cdot 6 - 169 \cdot 1\\
&= 598 \cdot 2 - 169 \cdot 7 = 598 \cdot 2 - 7 \cdot (767 - 598 \cdot 1)\\
&= 598 \cdot 2 - 767 \cdot 7 + 598 \cdot 7 = 598 \cdot (9) + 767 \cdot (-7)
\end{aligned}$$

Luego amplificando por 2 obtenemos

$$26 = 598 \cdot (18) + 767 \cdot (-14)$$

Por lo tanto, una solución particular es $x_0 = 18$, $y_0 = -14$

Solución general:

$$\begin{array}{ll}
x = 18 + \dfrac{767}{13} \cdot t & y = -14 - \dfrac{598}{13} \cdot t \quad t \in \mathbb{Z}\\
x = 18 + 59 \cdot t & y = -14 - 46 \cdot t \quad t \in \mathbb{Z}
\end{array}$$

II) Resolver $3 \cdot x + 9 \cdot y + 13 \cdot z = 1$.

Notemos que $(3, 9) = 3$, luego la ecuación

$$3 \cdot x + 9 \cdot y = 3 \cdot t; \Longleftrightarrow x + 3 \cdot y = t; \quad t \in \mathbb{Z},$$

siempre tiene solución.

Primero resolvemos: $3 \cdot t + 13 \cdot z = 1$

$$13 = 3 \cdot 4 + 1; \qquad 3 = 1 \cdot 3 + 0.$$

Por lo tanto $(3, 13) = 1$.

$$1 = 3 \cdot (-4) + 13 \cdot (1),$$

luego una solución particular es $t_0 = -4,\ z_0 = 1$.

Veamos la solución general de la primera parte

$$t = -4 + 13 \cdot s \qquad z = 1 - 3 \cdot s \quad s \in \mathbb{Z}.$$

Ahora veremos la solución del problema original $x + 3 \cdot y = -4 + 13 \cdot s$. Pero

$$\begin{aligned}
1 &= 1 \cdot (-2) + 3 \cdot (1) \quad / \cdot -4 + 13 \cdot s\\
-4 + 13 \cdot s &= 1 \cdot (8 - 26 \cdot s) + 3 \cdot (-4 + 13 \cdot s)
\end{aligned}$$

Por lo tanto $x_0 = 8 - 26 \cdot s$, $y_0 = -4 + 13 \cdot s$

Solución general es:

$$x = 8 - 26s + 3r, \quad y = -4 + 13s - r, \quad z = 1 - 3s, \quad \text{con } r, s \in \mathbb{Z}$$

o bien

$$S = \{\ (8 - 26s + 3r, -4 + 13s - r, 1 - 3s) \mid r, s \in \mathbb{Z}\}$$

♡

A.2.2. Números Enteros Módulo m

Solución 10.

i) $\overline{3} \in (\mathbb{Z}_{69}, +)$, el orden aditivo de un elemento esta dado por $|\overline{x}| = \frac{n}{(n,x)}$. Veamos el máximo común divisor

$$69 = 3 \cdot 23 + 0; \quad (69, 3) = 3$$

Luego

$$|3| = \frac{69}{(69,3)} = \frac{69}{3} = 23$$

Por lo tanto, el orden de $\overline{3}$ es 23.

ii) $\overline{5} \in (\mathcal{U}(\mathbb{Z}_{31}), \cdot)$ Veamos el subgrupo generador por el elemento

$$< \overline{5} > \;\; = \;\; \{\overline{5}, \overline{25}, \overline{1}\}$$

Por lo tanto el orden multiplicativo de $\overline{5}$ es 3

iii) $\overline{7} \in (\mathcal{U}(\mathbb{Z}_{29}), \cdot)$

$$< \overline{7} > \;\; = \;\; \{\overline{7}, \overline{20}, \overline{24}, \overline{23}, \overline{16}, \overline{25}, \overline{1}\}$$

Por lo tanto el orden de $\overline{7}$ es 7

Solución 11.

$+_8$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{7}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$

$\cdot_{11}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{10}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$	$\overline{9}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{10}$	$\overline{2}$	$\overline{5}$	$\overline{8}$
$\overline{4}$	$\overline{4}$	$\overline{8}$	$\overline{1}$	$\overline{5}$	$\overline{9}$	$\overline{2}$	$\overline{6}$	$\overline{10}$	$\overline{3}$	$\overline{7}$
$\overline{5}$	$\overline{5}$	$\overline{10}$	$\overline{4}$	$\overline{9}$	$\overline{3}$	$\overline{8}$	$\overline{2}$	$\overline{7}$	$\overline{1}$	$\overline{6}$
$\overline{6}$	$\overline{6}$	$\overline{1}$	$\overline{7}$	$\overline{2}$	$\overline{8}$	$\overline{3}$	$\overline{9}$	$\overline{4}$	$\overline{10}$	$\overline{5}$
$\overline{7}$	$\overline{7}$	$\overline{3}$	$\overline{10}$	$\overline{6}$	$\overline{2}$	$\overline{9}$	$\overline{5}$	$\overline{1}$	$\overline{8}$	$\overline{4}$
$\overline{8}$	$\overline{8}$	$\overline{5}$	$\overline{2}$	$\overline{10}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{9}$	$\overline{6}$	$\overline{3}$
$\overline{9}$	$\overline{9}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{10}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{10}$	$\overline{10}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

♡

Solución 12. Ya que $10 = 2 \cdot 5$, por lo tanto $\mathcal{U}(\mathbb{Z}_{10})$ es un grupo cíclico, luego $|\mathcal{U}(\mathbb{Z}_{10})| = \phi(10) = 4$.

$$\mathcal{U}(\mathbb{Z}_{10}) = \{\overline{a} \in \mathbb{Z}_{10} \quad | \quad (\overline{a}, 10) = 1\} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$$

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
$\overline{3}$	$\overline{3}$	$\overline{9}$	$\overline{1}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{1}$	$\overline{9}$	$\overline{3}$
$\overline{9}$	$\overline{9}$	$\overline{7}$	$\overline{3}$	$\overline{1}$

Como $\mathcal{U}(\mathbb{Z}_{10})$ es cíclico, las raíces primitivas es lo mismo que los generadores.

$$\phi(\phi(10)) = \phi(4) = \phi(2^2) = 2^2 \cdot \left(1 - \frac{1}{2}\right) = 2^2 \cdot \frac{1}{2} = 2$$

Por lo tanto $\mathcal{U}(\mathbb{Z}_{10})$ tiene dos raíces primitivas. Ahora buscamos el primer generador de $\mathcal{U}(\mathbb{Z}_{10})$.

$$< \overline{3} >= \{\overline{3}, \overline{9}, \overline{7}, \overline{1}\}$$

Por otro lado necesitamos determinar los primos relativos con $\phi(10)$, lo cuales son: $1, 3$

Por lo tanto las raíces primitivas de $\mathcal{U}(\mathbb{Z}_{10})$ son, $\overline{3}^1 = \overline{3}, \quad \overline{3}^3 = \overline{7}$. ♡

Solución 13.

I) Veremos el número de generadores de $(\mathbb{Z}_{24}, +)$, para ello $24 = 2^3 \cdot 3$

$$\phi(24) = 2^3 \cdot 3 \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 2^3 \cdot 3 \cdot \frac{1}{2} \cdot \frac{2}{3} = 8$$

Por lo tanto $(\mathbb{Z}_{24}, +)$ tiene 8 generadores, que van a hacer los primos relativos con 24. Luego, los generadores de $(\mathbb{Z}_{24}, +)$ son:

$$\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}.$$

II) Veremos el número de generadores de $(\mathbb{Z}_{30}, +)$, para ello $30 = 2 \cdot 3 \cdot 5$

$$\phi(30) = 2 \cdot 3 \cdot 5 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 2 \cdot 3 \cdot 5 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$$

Por lo tanto $(\mathbb{Z}_{30}, +)$ tiene 8 generadores, que van a hacer los primos relativos con 30. Los generadores de $(\mathbb{Z}_{30}, +)$ son:

$$\overline{1}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{29}.$$

III) Veremos el número de generadores de $(\mathbb{Z}_{300}, +)$, para ello $300 = 2^2 \cdot 3 \cdot 5^2$

$$\phi(300) = 2^3 \cdot 3 \cdot 5^2 \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 2^3 \cdot 3 \cdot 5^2 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 80$$

Por lo tanto $(\mathbb{Z}_{300}, +)$ tiene 80 generadores.

IV) Veremos el número de generadores de $(\mathbb{Z}_{890}, +)$, para ello $890 = 2 \cdot 5 \cdot 89$

$$\phi(890) = 2 \cdot 5 \cdot 89 \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{89}\right) = 2^3 \cdot 5^3 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{88}{89} = 352$$

Por lo tanto $(\mathbb{Z}_{890}, +)$ tiene 352 generadores.

V) Veremos los generadores de $(\mathcal{U}(\mathbb{Z}_{11}), \cdot)$, como 11 es primo es cíclico. $\phi(11) = 10$ y $\phi(10) = 4$, luego tiene cuatro generadores

$$< \overline{2} > \;\; = \;\; \{\overline{2}, \overline{4}, \overline{8}, \overline{5}, \overline{10}, \overline{9}, \overline{7}, \overline{3}, \overline{6}, \overline{1}\}$$

Los primos relativos con 10 son $1, 3, 7, 9$, por lo tanto los generadores son

$$\overline{2}^1 = \overline{2},\ \overline{2}^3 = \overline{8},\ \overline{2}^7 = \overline{7},\ \overline{2}^9 = \overline{6}$$

Por lo tanto generadores de $(\mathcal{U}(\mathbb{Z}_{11}), \cdot)$ son $\overline{2}, \overline{6}, \overline{7}, \overline{8}$. ♡

VI) Veremos los generadores de $(\mathcal{U}(\mathbb{Z}_{12}), \cdot)$, las unidades de $\mathbb{Z}_{12}$, son los primos relativos con el 12.

$$< \overline{5} >= \{\overline{5}, \overline{1}\}; \quad < \overline{7} >= \{\overline{7}, \overline{1}\}; \quad < \overline{11} >= \{\overline{11}, \overline{1}\}.$$

Por lo tanto $(\mathcal{U}(\mathbb{Z}_{12}), \cdot)$ no tiene generadores.

VII) Veremos los generadores de $(\mathcal{U}(\mathbb{Z}_{18}), \cdot)$, las unidades de $\mathbb{Z}_{18}$, son lo primos relativos con el 18. además $18 = 2 \cdot 3^2$ luego es cíclico. $\phi(18) = 6$ y $\phi(6) = 2$, luego tiene dos generadores

$$< \overline{5} >= \{\overline{5}, \overline{7}, \overline{17}, \overline{13}, \overline{11}, \overline{1}\}$$

Por lo tanto $(\mathcal{U}(\mathbb{Z}_{18}), \cdot)$ tiene dos generadores $\overline{5}, \overline{11}$

VIII) $\mathcal{U}(\mathbb{Z}_{25})$, como $25 = 5^2$, luego $\mathcal{U}(\mathbb{Z}_{25})$ es cíclico, y el numero de elementos esta dado por:

$$\phi(25) = \phi\left(5^2 \cdot \left(1 - \frac{1}{5}\right)\right) = \left(5^2 \cdot \frac{4}{5}\right) = 20$$

y estos son

$$\mathcal{U}(\mathbb{Z}_{25}) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17}, \overline{18}, \overline{19}, \overline{20}, \overline{21}, \overline{22}, \overline{23}, \overline{24}\}$$

El número de generados

$$\phi(20) \;\; = \;\; \phi(2^2 \cdot 5) = 2^2 \cdot 5 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 2^2 \cdot 5 \cdot \frac{1}{2} \cdot \frac{4}{5} = 8$$

Por lo tanto $\mathbb{Z}_{25}$ tiene 8 raíces primitivas.

Buscamos el primer generador de $\mathcal{U}(\mathbb{Z}_{25})$.

$$< \overline{2} > \;\; = \;\; \{\overline{2}, \overline{4}, \overline{8}, \overline{16}, \overline{7}, \overline{14}, \overline{3}, \overline{6}, \overline{12}, \overline{24}, \overline{23}, \overline{21}, \overline{17}, \overline{9}, \overline{18}, \overline{11}, \overline{22}, \overline{19}, \overline{13}, \overline{1}\}$$

Luego, buscamos los primos relativos con $\phi(25) = 20$ que son: $1, 3, 7, 9, 11, 13, 17, 19$.

Por lo tanto las raíces primitivas módulo 25 son:

$$\overline{2}^1 = \overline{2}, \quad \overline{2}^3 = \overline{8}, \quad \overline{2}^7 = \overline{3}, \quad \overline{2}^9 = \overline{12}, \quad \overline{2}^{11} = \overline{23}, \quad \overline{2}^{13} = \overline{17}, \quad \overline{2}^{17} = \overline{22}, \quad \overline{2}^{19} = \overline{13}$$

IX) $\mathcal{U}(\mathbb{Z}_{43})$, como 43 es primo entonces $\mathcal{U}(\mathbb{Z}_{43})$ es cíclico.

$$\begin{aligned}\mathcal{U}(\mathbb{Z}_{43}) &= \{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7},\overline{8},\overline{9},\overline{10},\overline{11},\overline{12},\overline{13},\overline{14},\overline{15},\overline{16},\overline{17},\overline{18},\overline{19},\overline{20},\overline{21},\overline{22},\overline{23},\\ &\quad \cdots,\overline{24},\overline{25},\overline{26},\overline{27},\overline{28},\overline{29},\overline{30},\overline{31},\overline{32},\overline{33},\overline{34},\overline{35},\overline{36},\overline{37},\overline{38},\overline{39},\overline{40},\overline{41},\overline{42}\}\end{aligned}$$

Veremos la cantidad de generadores, ara ello calculemos $\phi(43) = 42 = 2\cdot 3\cdot 7$

$$\phi(\phi(43)) = 2\cdot 3\cdot 7\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{7}\right) = 12$$

Por lo tanto $\mathbb{Z}_{43}$ tiene 12 raíces primitivas. Buscamos el primer generador de $\mathcal{U}(\mathbb{Z}_{43})$.

$$\begin{aligned}<\overline{2}> &= \{\overline{2},\overline{4},\overline{8},\overline{16},\overline{32},\overline{21},\overline{42},\overline{41},\overline{39},\overline{35},\overline{27},\overline{11},\overline{22},\overline{1}\}\\ <\overline{3}> &= \{\overline{3},\overline{9},\overline{27},\overline{38},\overline{28},\overline{41},\overline{37},\overline{25},\overline{32},\overline{10},\overline{30},\overline{4},\overline{12},\overline{36},\overline{22},\overline{23},\overline{26},\overline{35},\overline{19},\overline{14},\overline{42},\overline{40},\overline{34},\\ &\quad \overline{16},\overline{5},\overline{15},\overline{2},\overline{6},\overline{18},\overline{11},\overline{33},\overline{13},\overline{39},\overline{31},\overline{7},\overline{21},\overline{20},\overline{17},\overline{8},\overline{24},\overline{29},\overline{1}\}\end{aligned}$$

Luego, buscamos los primos relativos con $\phi(43) = 42$ que son: $1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41$.

Por lo tanto las raíces primitivas módulo 43 son:

$$\begin{gathered}\overline{3}^1 = \overline{3},\quad \overline{3}^5 = \overline{28},\quad \overline{3}^{11} = \overline{30},\quad \overline{3}^{13} = \overline{12},\quad \overline{3}^{17} = \overline{26},\quad \overline{3}^{19} = \overline{19},\\ \overline{3}^{23} = \overline{34},\quad \overline{3}^{25} = \overline{5},\quad \overline{3}^{29} = \overline{18},\quad \overline{3}^{31} = \overline{33},\quad \overline{3}^{37} = \overline{20},\quad \overline{3}^{41} = \overline{29}\end{gathered}$$

♡

Solución 14.

I) $\mathcal{C}_{13} = \{\overline{x}^3 \mid \overline{x}\in\mathcal{U}(\mathbb{Z}_{13})\}$. Como 13 es primo luego $\mathcal{U}(\mathbb{Z}_{13})$ es cíclico, además $13 \equiv 1(\texttt{mod}\ 3)$, luego $|\mathcal{C}_{13}| = \frac{13-1}{3} = 4$, $\phi(4) = 2$ por lo tanto tiene dos generadores

$$\mathcal{C}_{13} = \{\overline{1},\overline{8},\overline{12},\overline{5}\}$$

Veremos los generados

$$<\overline{8}>= \{\overline{8},\overline{12},\overline{5},\overline{1}\};\quad <\overline{12}>= \{\overline{12},\overline{1}\};\quad <\overline{5}>= \{\overline{5},\overline{12},\overline{8},\overline{1}\}.$$

Por lo tanto los generadores de $\mathcal{C}_{13}$ son $\overline{8},\overline{5}$

orden	subgrupo
1	$<\overline{1}>$
2	$<\overline{12}>$
4	$<\overline{8}>, <\overline{5}>$

II) $\mathcal{C}_{31} = \{\overline{x}^3 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{31})\}$. Como 31 es primo luego $\mathcal{U}(\mathbb{Z}_{31})$ es cíclico, además $31 \equiv 1(\texttt{mod}\ 3)$, luego $|\mathcal{C}_{31}| = \frac{31-1}{3} = 10, \phi(10) = 4$ por lo tanto tiene cuatro generadores

$$\mathcal{C}_{31} = \{\overline{1}, \overline{8}, \overline{27}, \overline{2}, \overline{30}, \overline{16}, \overline{29}, \overline{23}, \overline{4}, \overline{15}\}$$

Veremos los generados

$$\begin{array}{rl}
<\overline{8}>= \{\overline{8}, \overline{2}, \overline{16}, \overline{4}, \overline{1}\}; & <\overline{27}>= \{\overline{27}, \overline{16}, \overline{29}, \overline{8}, \overline{30}, \overline{4}, \overline{15}, \overline{2}, \overline{23}, \overline{1}\}; \\
<\overline{2}>= \{\overline{2}, \overline{4}, \overline{8}, \overline{16}, \overline{1}\}; & <\overline{23}>= \{\overline{23}, \overline{2}, \overline{15}, \overline{9}, \overline{30}, \overline{8}, \overline{29}, \overline{16}, \overline{27}, \overline{1}\}; \\
<\overline{16}>= \{\overline{16}, \overline{8}, \overline{4}, \overline{2}, \overline{1}\}; & <\overline{29}>= \{\overline{29}, \overline{4}, \overline{23}, \overline{16}, \overline{30}, \overline{2}, \overline{27}, \overline{8}, \overline{15}, \overline{1}\}; \\
<\overline{4}>= \{\overline{4}, \overline{16}, \overline{2}, \overline{8}, \overline{1}\}; & <\overline{15}>= \{\overline{15}, \overline{8}, \overline{27}, \overline{2}, \overline{30}, \overline{16}, \overline{23}, \overline{4}, \overline{29}, \overline{1}\}; \\
<\overline{30}>= \{\overline{30}, \overline{1}\}; & <\overline{1}>= \{\overline{1}\}.
\end{array}$$

Por lo tanto los generadores de $\mathcal{C}_{31}$ son $\overline{15}, \overline{23}, \overline{27}, \overline{29}$

orden	subgrupo
1	$<\overline{1}>$
2	$<\overline{30}>$
5	$<\overline{2}>, <\overline{4}>, <\overline{8}>, <\overline{16}>$
10	$<\overline{15}>, <\overline{23}>, <\overline{27}>, <\overline{29}>$

♡

Solución 15.

$\mathcal{H} \leq \mathcal{G} = (\mathbb{Z}_{16}, +) \Leftrightarrow |\mathcal{H}|\ |16$ luego $|\mathcal{H}| \in \{1, 2, 4, 8, 16\}$, además existe sólo un subgrupo de orden un divisor de 16 y es cíclico.

$$\mathbb{Z}_{16} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}\}$$

El orden de $\overline{2}$ es $16/(16, 2) = 8$, el orden $\overline{4}$ es $16/(16, 4) = 4$ y el orden $\overline{8}$ es $16/(16, 8) = 2$
Resumiendo tenemos

orden	subgrupo
1	$<\overline{0}>$
2	$<\overline{8}>$
4	$<\overline{4}>, <\overline{12}>$
8	$<\overline{2}>, <\overline{6}>, <\overline{10}>, <\overline{14}>$
16	$<\overline{1}>, <\overline{3}>, <\overline{5}>, <\overline{7}>, <\overline{9}>, <\overline{13}>, <\overline{15}>$

$$<\overline{0}>\subset<\overline{8}>\subset<\overline{4}>\subset<\overline{2}>\subset<\overline{1}>$$

Reticulado:

$$<\overline{0}> \rightarrow <\overline{8}> \rightarrow <\overline{4}> \rightarrow <\overline{2}> \rightarrow <\overline{1}>$$

Solución 16.

$\mathcal{H} \leq \mathcal{G}$, luego $|\mathcal{H}|\ |12$ es decir $|\mathcal{H}| \in \{1,2,3,4,6,12\}$. además existe un solo subgrupo de orden un divisor de 12 y es cíclico.

$$\mathcal{G} = \{g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, e\}$$

Calculemos directamente los subgrupos

$$\begin{aligned}
< g > &= \{g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, e\} \\
< g^2 > &= \{g^2, g^4, g^6, g^8, g^{10}, e\} \\
< g^3 > &= \{g^3, g^6, g^9, e\} \\
< g^4 > &= \{g^4, g^8, e\} \\
< g^5 > &= \{g^5, g^{10}, g^3, g^8, g, g^6, g^{11}, g^4, g^9, g^2, g^7, e\} \\
< g^6 > &= \{g^6, e\} \\
< g^7 > &= \{g^7, g^2, g^9, g^4, g^{11}, g^6, g, g^8, g^3, g^{10}, g^5, e\} \\
< g^8 > &= \{g^8, g^4, e\} \\
< g^9 > &= \{g^9, g^6, g^3, e\} \\
< g^{10} > &= \{g^{10}, g^8, g^6, g^4, g^2, e\} \\
< g^{11} > &= \{g^{11}, g^{10}, g^9, g^8, g^7, g^6, g^5, g^4, g^3, g^2, g^1, e\} \\
< e > &= \{e\}
\end{aligned}$$

orden	subgrupo
1	$< e >$
2	$< g^6 >$
3	$< g^4 >, < g^8 >$
4	$< g^3 >, < g^9 >$
6	$< g^2 >, < g^{10} >$
12	$< g >, < g^5 >, < g^7 >, < g^{11} >$

$$\begin{array}{ccccccc}
< e > & \subset & < g^6 > & \subset & < g^3 > & \subset & < g > \\
< e > & \subset & < g^4 > & \subset & < g^2 > & \subset & < g > \\
< e > & \subset & < g^6 > & \subset & < g^2 > & \subset & < g >
\end{array}$$

Reticulado:

$$\begin{tikzcd}
 & < g > & \\
< g^2 > \arrow[ur] & & < g^3 > \arrow[ul] \\
< g^4 > \arrow[u] & & < g^6 > \arrow[u] \arrow[ull] \\
 & < g^0 > \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

♡

Solución: 17 Ya que 23 es un número primo entonces el grupo es cíclico.

$\mathcal{U}(\mathbb{Z}_{23}) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17}, \overline{18}, \overline{19}, \overline{20}, \overline{21}, \overline{22}\}$

$$\begin{aligned}
< \overline{1} > &= \{\overline{1}\}\\
< \overline{2} > &= \{\overline{2}, \overline{4}, \overline{8}, \overline{16}, \overline{9}, \overline{18}, \overline{13}, \overline{3}, \overline{6}, \overline{12}, \overline{1}\}\\
< \overline{3} > &= \{\overline{3}, \overline{9}, \overline{4}, \overline{12}, \overline{13}, \overline{16}, \overline{2}, \overline{6}, \overline{18}, \overline{8}, \overline{1}\}\\
< \overline{4} > &= \{\overline{4}, \overline{16}, \overline{18}, \overline{3}, \overline{12}, \overline{2}, \overline{8}, \overline{9}, \overline{13}, \overline{6}, \overline{1}\}\\
< \overline{5} > &= \{\overline{5}, \overline{2}, \overline{10}, \overline{4}, \overline{20}, \overline{8}, \overline{17}, \overline{16}, \overline{11}, \overline{9}, \overline{22}, \overline{18}, \overline{21}, \overline{13}, \overline{19}, \overline{3}, \overline{15}, \overline{6}, \overline{7}, \overline{12}, \overline{14}, \overline{1}\}
\end{aligned}$$

Por lo tanto $\mathcal{U}(\mathbb{Z}_{23}) =< \overline{5} >$, es decir, $(\mathcal{U}(\mathbb{Z}_{23}), \cdot)$ es cíclico y esta generado por $\overline{5}$ es un generador. ♡

Solución: 18

I) 7^{2702} por 31, como $(7, 31) = 1$, luego $7^{\phi(31)} \equiv 1(\texttt{mod } 31)$. Se tiene que $\phi(31) = 30$ y además $2702 = 30 \cdot 90 + 2$

$$7^{2702} \equiv 7^{30\cdot 90+2} \equiv (7^{30})^{90}7^2 \equiv 49 \equiv 18(\texttt{mod } 31)$$

Por lo tanto el resto al dividir 7^{2702} por 31 es 18

II) $2^{100} + 3^{20} + 7^{89}$ por 19, como $(2, 19) = 1$, luego $2^{\phi(19)} \equiv 2^{18} \equiv 1(\texttt{mod } 19)$, además $100 = 18 \cdot 5 + 10$.

$$\begin{aligned}
2^{100} &\equiv 2^{18\cdot 5+10} \equiv (2^{18})^5 2^{10} \equiv 2^{10}(\texttt{mod } 19)\\
&\equiv 2^{2\cdot 5} \equiv (32)^2 \equiv 13^2 \equiv 169 \equiv 17(\texttt{mod } 19)
\end{aligned}$$

De modo similar tenemos que $(3, 19) = 1$, es decir, $3^{18} \equiv 1(\texttt{mod } 19)$, además $20 = 18 \cdot 1 + 2$

$$3^{20} \equiv 3^{18}3^2 \equiv 9(\texttt{mod } 19)$$

También tenemos $(7, 19) = 1$, luego $7^{18} \equiv 1(\texttt{mod } 19)$, además $89 = 18 \cdot 4 + 17$, es decir, necesitamos calcular 7^{17}, para ello veremos

$$< \overline{7} >= \{\overline{7}, \overline{11}, \overline{1}\},$$

de lo cual obtenemos $89 = 3 \cdot 29 + 2$

$$7^{89} \equiv 7^{3\cdot 29+2} \equiv 7^2 \equiv 11(\texttt{mod } 19)$$

Reemplazando los valores obtenidos

$$\begin{aligned}
2^{100} + 3^{20} + 7^{89} &\equiv 17 + 9 + 11(\texttt{mod } 19)\\
2^{100} + 3^{20} + 7^{89} &\equiv 37 \equiv 18(\texttt{mod } 19)
\end{aligned}$$

Por lo tanto el resto al dividir $2^{100} + 3^{20} + 7^{89}$ por 19 es 18.

III) 473^{38} por 5, notemos que $473 \equiv 3(\texttt{mod } 5)$, luego

$$473^{38} \equiv 3^{38} \equiv 3^{4\cdot 9+2} \equiv 3^2 \equiv 9 \equiv 4(\texttt{mod } 5)$$

Por lo tanto el resto al dividir 473^{38} por 5 es 4

♡

Solución 19. ¿Cuál es el dígito de las unidades en la representación decimal de 3^{400}?
Ya que $(3,10)=1$, y

$$\phi(10) \;=\; 2\cdot 5\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{5}\right)=2\cdot 5\cdot\frac{1}{2}\cdot\frac{4}{5}=4$$

luego $3^{\phi(10)} \equiv 3^4 \equiv 1(\texttt{mod } 10)$

$$3^{400} \equiv (3^4)^{100} \equiv 1(\texttt{mod } 10)$$

Por lo tanto, el último dígito de 3^{400} es 1. ♡

Solución 20.

$$\left.\begin{array}{rcl} x & \equiv & 2(\texttt{mod } 3) \\ x & \equiv & 3(\texttt{mod } 5) \\ x & \equiv & 2(\texttt{mod } 7) \end{array}\right|$$

Primero verifiquemos que los módulo, son primos dos a dos

$$(3,7)=1, \quad (5,7)=1, \quad (3,5)=1$$

Los coeficientes del teorema Chino de los Restos

$$a_1=2, a_2=3, a_3=2, \quad m_1=3, m_2=5, m_3=7, \quad m=m_1\cdot m_2\cdot m_3=105,$$

ahora calculemos los coeficientes b_i,

$$\begin{array}{rcl} \frac{m}{m_1}\cdot b_1 & \equiv & 1(\texttt{mod } m_1) \\ 35\cdot b_1 & \equiv & 1(\texttt{mod } 3) \\ 2b_1 & \equiv & 1(\texttt{mod } 3) \\ 2b_1 & \equiv & 4(\texttt{mod } 3) \\ b_1 & \equiv & 2(\texttt{mod } 3) \end{array} \quad \begin{array}{rcl} \frac{m}{m_2}\cdot b_2 & \equiv & 1(\texttt{mod } m_2) \\ 21\cdot b_2 & \equiv & 1(\texttt{mod } 5) \\ b_2 & \equiv & 1(\texttt{mod } 5) \\ & & \\ & & \end{array} \quad \begin{array}{rcl} \frac{m}{m_3}\cdot b_3 & \equiv & 1(\texttt{mod } m_3) \\ 15\cdot b_3 & \equiv & 1(\texttt{mod } 7) \\ b_3 & \equiv & 3(\texttt{mod } 7) \\ & & \\ & & \end{array}$$

Luego una solución particular es

$$\begin{array}{rcl} x_0 & = & a_1\cdot b_1\cdot\dfrac{m}{m_1}+a_2\cdot b_2\cdot\dfrac{m}{m_2}+a_3\cdot b_3\cdot\dfrac{m}{m_3} \\ x_0 & = & 2\cdot 2\cdot 35+3\cdot 1\cdot 21+2\cdot 1\cdot 15=2331 \end{array}$$

$$x \equiv x_0 \equiv 233 \equiv 23(\texttt{mod } 105)$$

El menor entero positivo es 23. ♡

Solución 21.

I) $\square_{17} = \{\overline{x}^2 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{17})\}$

$$\begin{array}{rcl} \mathcal{U}(\mathbb{Z}_{17}) & = & \{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7},\overline{8},\overline{9},\overline{10},\overline{11},\overline{12},\overline{13},\overline{14},\overline{15},\overline{16}\} \\ \square_{17} & = & \{\overline{1},\overline{4},\overline{9},\overline{16},\overline{8},\overline{2},\overline{15},\overline{13}\} \end{array}$$

$|\square_{17}| = 8$ y $\phi(8) = 4$. Por lo tanto hay 4 generadores de $\square_{17}$. Buscamos el primer generador:

$$\begin{array}{rcl} <\overline{1}> & = & \{\overline{1}\} \\ <\overline{4}> & = & \{\overline{4},\overline{16},\overline{13},\overline{1}\} \\ <\overline{9}> & = & \{\overline{9},\overline{13},\overline{15},\overline{16},\overline{8},\overline{4},\overline{2},\overline{1}\} \end{array}$$

Ahora necesitamos los primos relativos a 8, que son: $1, 3, 5, 7$.

Generadores del grupo de los $\square_{17}$ son: $\overline{9}^1 = \overline{9}, \quad \overline{9}^3 = \overline{15}, \quad \overline{9}^5 = \overline{8}, \quad \overline{9}^7 = \overline{2}$.

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{9}$	$\overline{13}$	$\overline{15}$	$\overline{16}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{9}$	$\overline{13}$	$\overline{15}$	$\overline{16}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{16}$	$\overline{1}$	$\overline{9}$	$\overline{13}$	$\overline{15}$
$\overline{4}$	$\overline{4}$	$\overline{8}$	$\overline{16}$	$\overline{15}$	$\overline{2}$	$\overline{1}$	$\overline{9}$	$\overline{13}$
$\overline{8}$	$\overline{8}$	$\overline{16}$	$\overline{15}$	$\overline{13}$	$\overline{4}$	$\overline{2}$	$\overline{1}$	$\overline{9}$
$\overline{9}$	$\overline{9}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{13}$	$\overline{15}$	$\overline{16}$	$\overline{8}$
$\overline{13}$	$\overline{13}$	$\overline{9}$	$\overline{1}$	$\overline{2}$	$\overline{15}$	$\overline{16}$	$\overline{8}$	$\overline{4}$
$\overline{15}$	$\overline{15}$	$\overline{13}$	$\overline{9}$	$\overline{1}$	$\overline{16}$	$\overline{8}$	$\overline{4}$	$\overline{2}$
$\overline{16}$	$\overline{16}$	$\overline{15}$	$\overline{13}$	$\overline{9}$	$\overline{8}$	$\overline{4}$	$\overline{2}$	$\overline{13}$

II) Ya que $22 = 2 \cdot 11$ se tiene que $\mathcal{U}(\mathbb{Z}_{22})$ es cíclico, luego $\square_{22} = \{\overline{x}^2 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{22})\}$ es cíclico.

$$\begin{array}{rcl} \mathcal{U}(\mathbb{Z}_{22}) & = & \{\overline{1},\overline{3},\overline{5},\overline{7},\overline{9},\overline{13},\overline{15},\overline{17},\overline{19},\overline{21}\} \\ \square_{22} & = & \{\overline{1},\overline{9},\overline{3},\overline{5},\overline{15}\} \end{array}$$

$|\square_{22}| = 5$ y $\phi(5) = 4$. Por lo tanto hay 4 generadores de $\square_{22}$, es decir son todo salvo el neutro.

Generadores del grupo de los $\square_{22}$ son $\overline{3},\overline{5},\overline{9},\overline{15}$, y la tabla de multiplicar

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{9}$	$\overline{15}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{9}$	$\overline{15}$
$\overline{3}$	$\overline{3}$	$\overline{9}$	$\overline{15}$	$\overline{5}$	$\overline{1}$
$\overline{5}$	$\overline{5}$	$\overline{15}$	$\overline{3}$	$\overline{1}$	$\overline{9}$
$\overline{9}$	$\overline{9}$	$\overline{5}$	$\overline{1}$	$\overline{15}$	$\overline{3}$
$\overline{15}$	$\overline{15}$	$\overline{1}$	$\overline{9}$	$\overline{3}$	$\overline{5}$

♡

Solución 22. Determine el número de soluciones en cada caso

I) $x^2 \equiv 5(\texttt{mod } 73)$

$$\begin{aligned}
\left(\frac{5}{73}\right) \cdot \left(\frac{73}{5}\right) &= (-1)^{\frac{73-1}{2}\cdot\frac{5-1}{2}}; \quad 73 \equiv 3(\texttt{mod } 5) \\
\left(\frac{5}{73}\right) \cdot \left(\frac{3}{5}\right) &= 1
\end{aligned}$$

Pero,

$$\begin{aligned}
\left(\frac{3}{5}\right) \cdot \left(\frac{5}{3}\right) &= (-1)^{\frac{5-1}{2}\cdot\frac{3-1}{2}}; \quad 5 \equiv 2(\texttt{mod } 3) \\
\left(\frac{3}{5}\right) \cdot \left(\frac{2}{3}\right) &= 1
\end{aligned}$$

Además

$$\left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$$

Por lo tanto, $\left(\frac{3}{5}\right) = -1$, luego $\left(\frac{5}{73}\right) = -1$, de lo cual obtenemos $5 \notin \Box_{73}$, es decir, la ecuación $x^2 \equiv 5(\texttt{mod } 73)$ no tiene solución.

II) $x^2 \equiv 226(\texttt{mod } 563)$, sabemos que $226 = 2 \cdot 113$, donde 2 y 113 son primos

$$\begin{aligned}
\left(\frac{226}{563}\right) &= \left(\frac{2}{563}\right) \cdot \left(\frac{113}{563}\right) \\
&= (-1)^{\frac{563^2-1}{8}} \cdot (-1)^{\frac{563-1}{2}\cdot\frac{113-1}{2}} \cdot \left(\frac{563}{113}\right); \quad 563 \equiv 111(\texttt{mod } 113) \\
&= (-1)(1)\left(\frac{111}{113}\right) \\
&= (-1)(-1)^{\frac{113-1}{2}\cdot\frac{111-1}{2}}\left(\frac{113}{111}\right); \quad 113 \equiv 2(\texttt{mod } 111) \\
&= (-1)\left(\frac{2}{111}\right) \\
&= (-1)(-1)^{\frac{111^2-1}{8}} = -1
\end{aligned}$$

De lo cual obtenemos

$$\left(\frac{226}{563}\right) = -1$$

Por lo tanto $226 \notin \Box_{563}$, es decir, la ecuación $x^2 \equiv 5(\texttt{mod } 73)$ no tiene solución.

III) $x^3 \equiv 8(\text{mod } 719)$, notemos que 719 es un número primo

$$\begin{aligned} x^3 &\equiv 8(\text{mod } 719) \\ x^3 - 8 &\equiv 0(\text{mod } 719) \\ x^3 - 2^3 &\equiv 0(\text{mod } 719) \\ (x-2)\cdot(x^2+2x+4) &\equiv 0(\text{mod } 719) \end{aligned}$$

Luego $x - 2 \equiv 0(\text{mod } 719)$ o $x^2 + 2x + 4 \equiv 0(\text{mod } 719)$.

de la primera ecuación obtenemos

$$x - 2 \equiv 0(\text{mod } 719) \Longleftrightarrow x \equiv 2(\text{mod } 719)$$

Para la otro ecuación $x^2 + 2x + 4 \equiv 0(\text{mod } 719)$, debemos calcular su discriminante

$$\Delta = 2^2 - 4\cdot 1\cdot 4 = 4 - 16 = -12 = -1\cdot 2^2\cdot 3$$

Ahora veremos si el discriminante es un cuadrado, para ello veremos los factores

$$\left(\frac{-1}{719}\right) = (-1)^{\frac{719-1}{2}} = -1$$

También tenemos

$$\left(\frac{2^2}{719}\right) = 1$$

Nos falta ver el último factor

$$\begin{aligned} \left(\frac{3}{719}\right) &= (-1)^{\frac{719-1}{2}\cdot\frac{3-1}{2}}\cdot\left(\frac{719}{3}\right); \quad 719 \equiv 2(\text{mod } 3) \\ \left(\frac{3}{719}\right) &= -1\cdot\left(\frac{2}{3}\right) = (-1)\cdot(-1)^{\frac{3^2-1}{8}} = 1 \end{aligned}$$

Luego $\left(\frac{3}{719}\right) = 1$

$$\left(\frac{-12}{719}\right) = \left(\frac{-1}{719}\right)\cdot\left(\frac{2^2}{719}\right)\cdot\left(\frac{3}{719}\right) = -1\cdot 1\cdot 1 = -1$$

Por lo tanto $-12 \notin \square_{719}$, es decir, la ecuación $x^2 + 2x + 4 \equiv 0(\text{mod } 719)$ no tiene solución.

De lo cual, se obtiene que $x^3 \equiv 8(\text{mod } 719)$ tiene exactamente una solución.

IV) $x^2 \equiv 150(\text{mod } 1009)$, notemos que 1009 es primo,y que $150 = 2\cdot 3\cdot 5^2$ analizaremos los factores

$$\begin{aligned}
\left(\frac{150}{1009}\right) &= \left(\frac{2}{1009}\right)\cdot\left(\frac{3}{1009}\right)\cdot\left(\frac{5^2}{1009}\right)\\
&= (-1)^{\frac{1009^2-1}{8}}\cdot(-1)^{\frac{1009-1}{2}\cdot\frac{3-1}{2}}\cdot\left(\frac{1009}{3}\right)\cdot(1)\\
&= \left(\frac{1}{3}\right)=1
\end{aligned}$$

Por lo tanto $150 \in \square_{1009}$, es decir, la ecuación $x^2 \equiv 150(\texttt{mod } 1009)$ tiene dos soluciones módulo 1009.

V) $x^4 \equiv 9(\texttt{mod } 4003)$, notemos que 4003 es un número primo.

$$\begin{aligned}
x^4 &\equiv 9(\texttt{mod } 4003)\\
x^4-9 &\equiv 0(\texttt{mod } 4003)\\
(x^2-3)\cdot(x^2+3) &\equiv 0(\texttt{mod } 4003)
\end{aligned}$$

Luego tenemos que

$$\begin{aligned}
(x^2-3)\equiv 0(\texttt{mod } 4003) &\quad\vee\quad (x^2+3)\equiv 0(\texttt{mod } 4003)\\
x^2\equiv 3(\texttt{mod } 4003) &\quad\vee\quad x^2\equiv -3(\texttt{mod } 4003)
\end{aligned}$$

Debemos determinar si 3 o -3 son cuadrado.

$$\begin{aligned}
\left(\frac{3}{4003}\right) &= (-1)^{\frac{4003-1}{2}\cdot\frac{3-1}{2}}\cdot\left(\frac{4003}{3}\right); \quad 4003\equiv 1(\texttt{mod } 3)\\
&= -1\cdot\left(\frac{1}{3}\right)=-1
\end{aligned}$$

Para el otro valor

$$\left(\frac{-3}{4003}\right)=\left(\frac{-1}{4003}\right)\cdot\left(\frac{3}{4003}\right)=(-1)\cdot(-1)=1$$

Por lo tanto $3\notin\square_{4003}$ y $-3\in\square_{4003}$, es decir, la ecuación $x^4\equiv 9(\texttt{mod } 4003)$ tiene dos soluciones.

VI) $x^6\equiv 1(\texttt{mod } 19)$

$$\begin{aligned}
x^6 &\equiv 1(\texttt{mod } 19)\\
x^6-1 &\equiv 0(\texttt{mod } 19)\\
(x^3-1)\cdot(x^3+1) &\equiv 0(\texttt{mod } 19)\\
(x+1)\cdot(x^2-x+1)\cdot(x-1)\cdot(x^2+x+1) &\equiv 0(\texttt{mod } 19)
\end{aligned}$$

Debemos resolver los cuatro factores, par los lineales tenemos

$$\begin{array}{rl} x+1 \equiv 0(\texttt{mod } 19) & x-1 \equiv 0(\texttt{mod } 19) \\ x \equiv -1(\texttt{mod } 19) & x \equiv 1(\texttt{mod } 19) \\ x \equiv 18(\texttt{mod } 19) & x \equiv 1(\texttt{mod } 19) \end{array}$$

Ahora las cuadráticas $x^2 - x + 1 \equiv 0(\texttt{mod } 19)$ y su discriminante es

$$\Delta = 1 - 4 = -3 = -1 \cdot 3$$

Determine si es un cuadrado, analizando los factores

$$\begin{aligned} \left(\frac{-3}{19}\right) &= \left(\frac{-1}{19}\right) \cdot \left(\frac{3}{19}\right) \\ &= (-1)^{\frac{19-1}{2}} \cdot (-1)^{\frac{19-1}{2} \cdot \frac{3-1}{2}} \cdot \left(\frac{19}{3}\right); \quad 19 \equiv 1(\texttt{mod } 3) \\ &= (-1) \cdot (-1) \cdot \left(\frac{1}{3}\right) = 1 \end{aligned}$$

Así tenemos que $\left(\frac{-3}{19}\right) = 1$, luego $-3 \in \square_{19}$, es decir, la ecuación $x^2 - x + 1 \equiv 0(\texttt{mod } 19)$ tiene dos soluciones y son distintas a las anteriores

Ahora la cuadrática $x^2 + x + 1 \equiv 0(\texttt{mod } 19)$ tiene el mismo discriminante $\Delta = -3$, por tanto tiene dos soluciones distintas, es fácil notar que las soluciones de una cuadrática son distintas a la de la otra (basta restar las ecuaciones). Por lo tanto $x^6 \equiv 1(\texttt{mod } 19)$ tiene 6 soluciones.

♡

Solución 23.

I) $x^2 \equiv 5(\texttt{mod } 29)$, notemos que 29 es primo

$$\begin{aligned} \left(\frac{5}{29}\right) &= (-1)^{\frac{29-1}{2} \cdot \frac{5-1}{2}} \cdot \left(\frac{29}{5}\right); \quad 29 \equiv 2^2(\texttt{mod } 5) \\ \left(\frac{5}{29}\right) &= 1 \cdot \left(\frac{4}{5}\right) = 1 \end{aligned}$$

Por lo tanto $5 \in \square_{29}$, es decir, la ecuación $x^2 \equiv 5(\texttt{mod } 29)$ tiene dos soluciones.

Determinemos las soluciones

$$\begin{aligned} x^2 &\equiv 5(\texttt{mod } 29); \quad 5 \equiv 121(\texttt{mod } 29) \\ x^2 &\equiv 121(\texttt{mod } 29) \\ x^2 - 121 &\equiv 0(\texttt{mod } 29) \\ x^2 - 11^2 &\equiv 0(\texttt{mod } 29) \\ (x-11) \cdot (x+11) &\equiv 0(\texttt{mod } 29) \end{aligned}$$

Luego tenemos

$$\begin{aligned} x-11 &\equiv 0(\texttt{mod } 29) & \qquad x+11 &\equiv 0(\texttt{mod } 29)\\ x &\equiv 11(\texttt{mod } 29) & x &\equiv -11 \equiv 18(\texttt{mod } 29)\end{aligned}$$

Por lo tanto las soluciones de $x^2 \equiv 5(\texttt{mod } 29)$ son:

$$x \equiv 11(\texttt{mod } 29), \quad x \equiv 18(\texttt{mod } 29)$$

II) $x^2 \equiv 2(\texttt{mod } 97)$, Notemos que 97 es primo.

$$\left(\frac{2}{97}\right) = (-1)^{\frac{97^2-1}{8}} = 1$$

Por lo tanto $2 \in \square_{97}$, es decir, la ecuación $x^2 \equiv 2(\texttt{mod } 97)$ tiene dos soluciones.

$$\begin{aligned} x^2 &\equiv 2(\texttt{mod } 97); \quad 2 \equiv 196(\texttt{mod } 97)\\ x^2 &\equiv 196(\texttt{mod } 97)\\ x^2-196 &\equiv 0(\texttt{mod } 97)\\ x^2-14^2 &\equiv 0(\texttt{mod } 97)\\ (x-14)\cdot(x+14) &\equiv 0(\texttt{mod } 97)\end{aligned}$$

De lo cual,

$$\begin{aligned} x-14 &\equiv 0(\texttt{mod } 97) & \qquad x+14 &\equiv 0(\texttt{mod } 97)\\ x &\equiv 14(\texttt{mod } 97) & x &\equiv -14 \equiv 83(\texttt{mod } 97)\end{aligned}$$

Por lo tanto las soluciones de $x^2 \equiv 2(\texttt{mod } 397)$ son:

$$x \equiv 14(\texttt{mod } 97), \quad x \equiv 83(\texttt{mod } 97)$$

III) $x^{954} + 2x - 1 \equiv 0(\texttt{mod } 953)$. Notemos que 953 es un primo y que cero no es solución.

$$\begin{aligned} x^{953} &\equiv x(\texttt{mod } 953) \quad / \cdot x\\ x^{954} &\equiv x^2(\texttt{mod } 953)\\ x^2+2x-1 &\equiv 0(\texttt{mod } 953)\end{aligned}$$

El discriminante es

$$\Delta = 2^2 - 4 \cdot 1 \cdot -1 = 4 + 4 = 8 = 2^2 \cdot 2$$

Falta determinar si 2 es un cuadrado

$$\left(\frac{8}{953}\right) = \left(\frac{2^2}{953}\right) \cdot \left(\frac{2}{953}\right) = 1 \cdot \left(\frac{2}{953}\right) = (-1)^{\frac{953^2-1}{8}} = 1$$

Por lo tanto $8 \in \square_{953}$, es decir, la ecuación $x^{953} + 2x - 1 \equiv 0(\texttt{mod } 953)$ tiene dos soluciones.

Para determinar las soluciones sea $z = 2ax + b = 2x + 2$, luego

$$\begin{aligned}
z^2 &\equiv \Delta(\texttt{mod } 953) \\
z^2 &\equiv 8(\texttt{mod } 953) \quad 8 \equiv 961(\texttt{mod } 953) \\
z^2 &\equiv 961(\texttt{mod } 953) \\
z^2 - 961 &\equiv 0(\texttt{mod } 953) \\
z^2 - 31^2 &\equiv 0(\texttt{mod } 953) \\
(z-31)\cdot(z+31) &\equiv 0(\texttt{mod } 953)
\end{aligned}$$

De lo cual obtenemos,

$$\begin{array}{rl}
z - 31 \equiv 0(\texttt{mod } 953) & z + 31 \equiv 0(\texttt{mod } 953) \\
z \equiv 31(\texttt{mod } 953) & z \equiv -31(\texttt{mod } 953) \\
2\cdot x + 2 \equiv 31(\texttt{mod } 953) & 2\cdot x + 2 \equiv -31(\texttt{mod } 953) \\
2\cdot x \equiv 29(\texttt{mod } 953) & 2\cdot x \equiv -33(\texttt{mod } 953) \\
2\cdot x \equiv 982(\texttt{mod } 953) & 2\cdot x \equiv 920(\texttt{mod } 953) \\
x \equiv 491(\texttt{mod } 953) & x \equiv 460(\texttt{mod } 953)
\end{array}$$

Por lo tanto las soluciones de $x^{954} + 2x - 1 \equiv 0(\texttt{mod } 953)$ son:

$$x \equiv 491(\texttt{mod } 953), \quad x \equiv 460(\texttt{mod } 953)$$

IV) $x^3 \equiv 8(\texttt{mod } 31)$, notemos que 31 es primo,

$$\begin{aligned}
x^3 &\equiv 8(\texttt{mod } 31) \\
x^3 - 8 &\equiv 0(\texttt{mod } 31) \\
x^3 - 2^3 &\equiv 0(\texttt{mod } 31) \\
(x-2)\cdot(x^2 + 2x + 4) &\equiv 0(\texttt{mod } 31)
\end{aligned}$$

De lo cual obtenemos

$$(x-2) \equiv 0(\texttt{mod } 31) \quad \vee \quad x^2 + 2x + 4 \equiv 0(\texttt{mod } 31)$$

De la ecuación lineal obtenemos

$$x - 2 \equiv 0(\texttt{mod } 31) \Longleftrightarrow x \equiv 2(\texttt{mod } 31)$$

Ahora veremos la ecuación cuadrática $x^2 + 2x + 4 \equiv 0(\texttt{mod } 31)$, para ello, calculemos el discriminate

$$\Delta = 2^2 - 4\cdot 1\cdot 4 = 4 - 16 = -12 = -1\cdot 2^2\cdot 3$$

Veremos si es un cuadrado

$$\begin{aligned}
\left(\frac{-12}{31}\right) &= \left(\frac{-1}{31}\right)\cdot\left(\frac{2^2}{31}\right)\cdot\left(\frac{3}{31}\right)\\
&= (-1)^{\frac{31-1}{2}}\cdot(1)\cdot(-1)^{\frac{31-1}{2}\cdot\frac{3-1}{2}}\cdot\left(\frac{31}{3}\right); \quad 31\equiv 1(\texttt{mod } 3)\\
&= (-1)(-1)\left(\frac{1}{3}\right)=1
\end{aligned}$$

Por lo tanto $-12\in\square_{31}$, es decir, la ecuación $x^2+2x+4\equiv 0(\texttt{mod } 31)$ tiene dos soluciones.

Usando el cambio de Variable $z=2ax+b=2x+2$ Obtenemos

$$\begin{aligned}
z^2 &\equiv -12(\texttt{mod } 31) \quad -12\equiv 81(\texttt{mod } 31)\\
z^2 &\equiv 81(\texttt{mod } 31)\\
z^2-81 &\equiv 0(\texttt{mod } 31)\\
(z-9)\cdot(z+9) &\equiv 0(\texttt{mod } 31)
\end{aligned}$$

De este modo obtenemos,

$$\begin{array}{rl}
z-9\equiv 0(\texttt{mod } 31) & z+9\equiv 0(\texttt{mod } 31)\\
2\cdot x+2\equiv 9(\texttt{mod } 31) & 2\cdot x+2\equiv -9(\texttt{mod } 31)\\
2\cdot x\equiv 7(\texttt{mod } 31) & 2\cdot x\equiv -11(\texttt{mod } 31)\\
2\cdot x\equiv 38(\texttt{mod } 31) & 2\cdot x\equiv 20(\texttt{mod } 31)\\
x\equiv 19(\texttt{mod } 31) & x\equiv 10(\texttt{mod } 31)
\end{array}$$

Por lo tanto las soluciones de $x^3\equiv 8(\texttt{mod } 31)$ son:

$$x\equiv 2(\texttt{mod } 31),\quad x\equiv 10(\texttt{mod } 31),\quad x\equiv 19(\texttt{mod } 31)$$

v) $x^6+2x^3+3\equiv 0(\texttt{mod } 23)$, realicemos el siguiente cambio de variable

$$\begin{aligned}
u &= x^3\\
u^2 &= x^6\\
u^2+2u+3 &\equiv 0(\texttt{mod } 23)
\end{aligned}$$

El discriminante de la ecuación cuadrática es

$$\Delta = 2^2-4\cdot 3=4-12=-8=-1\cdot 2^2\cdot 2$$

Veremos si los factores son cuadrados

$$\left(\frac{-1}{23}\right)=(-1)^{\frac{23-1}{2}}=-1;\quad \left(\frac{2^2}{23}\right)=1;\quad \left(\frac{2}{23}\right)=(-1)^{\frac{23^2-1}{8}}=1.$$

Por último tenemos

$$\left(\frac{-8}{23}\right) = \left(\frac{-1}{23}\right)\cdot\left(\frac{2^2}{23}\right)\cdot\left(\frac{2}{23}\right) = -1\cdot 1\cdot 1 = -1$$

Por lo tanto, $-8 \notin \square_{23}$, es decir $u^2+2u+3\equiv 0(\texttt{mod }23)$ no tiene solución, de lo cual obtenemos $x^6+2x^3+3\equiv 0(\texttt{mod }23)$ no tiene solución.

vi) $x^{15}-x^{10}+4x-3\equiv 0(\texttt{mod }7)$, como 7 es primo y cero no es solución de la ecuación tenemos que $x^6\equiv 1(\texttt{mod }7)$.

De lo cual obtenemos que

$$x^{10}\equiv x^4(\texttt{mod }7);\quad x^{15}\equiv x^3(\texttt{mod }7)$$

Luego la ecuación es equivalente a

$$x^3-x^4+4x-3\equiv 0(\texttt{mod }7)$$

El desarrollo de este ejercicio será por evaluación,

$$\begin{array}{lllllll}
x & = & 0 & : & 0^3-0^4+4\cdot 0-3 & = & -3=4\not\equiv 0(\texttt{mod }7)\\
x & = & 1 & : & 1^3-1^4+4\cdot 1-3 & = & 1\not\equiv 0(\texttt{mod }7)\\
x & = & 2 & : & 2^3-2^4+4\cdot 2-3 & = & -3=4\not\equiv 0(\texttt{mod }7)\\
x & = & 3 & : & 3^3-3^4+4\cdot 3-3 & = & -45=4\not\equiv 0(\texttt{mod }7)\\
x & = & 4 & : & 4^3-4^4+4\cdot 4-3 & = & -179=3\not\equiv 0(\texttt{mod }7)\\
x & = & 5 & : & 5^3-5^4+4\cdot 5-3 & = & -483\equiv 0(\texttt{mod }7) \qquad \checkmark\\
x & = & 6 & : & 6^3-6^4+4\cdot 6-3 & = & -1059=5\not\equiv 0(\texttt{mod }7)
\end{array}$$

Por lo tanto la solución de $x^{15}-x^{10}+4x-3\equiv 0(\texttt{mod }7)$ es

$$x\equiv 5(\texttt{mod }7)$$

vii) $x^8+x^2\equiv 0(\texttt{mod }7)\quad 0\le x\le 30$, notemos que $x^7\equiv x(\texttt{mod }7)$

$$\begin{aligned}
x^8+x^2 &\equiv 0(\texttt{mod }7)\\
x^2+x^2 &\equiv 0(\texttt{mod }7)\\
2x^2 &\equiv 0(\texttt{mod }7)\\
x^2 &\equiv 0(\texttt{mod }7)\\
x &\equiv 0(\texttt{mod }7)
\end{aligned}$$

Por lo tanto $x\in\{0,7,14,21,28\}$

viii) $x^5-x^3\equiv 0(\texttt{mod }43)$, recuerde que 43 es primo

$$\begin{aligned}
x^5-x^3 &\equiv 0(\texttt{mod }43)\\
x^3\cdot(x^2-1) &\equiv 0(\texttt{mod }43)\\
x^3\cdot(x-1)\cdot(x+1) &\equiv 0(\texttt{mod }43)
\end{aligned}$$

$$\begin{array}{ccc} x^3 \equiv 0(\texttt{mod}\ 43) & x-1 \equiv 0(\texttt{mod}\ 43) & x+1 \equiv 0(\texttt{mod}\ 43) \\ x \equiv 0(\texttt{mod}\ 43) & x \equiv 1(\texttt{mod}\ 43) & x \equiv -1(\texttt{mod}\ 43) \\ x \equiv 0(\texttt{mod}\ 43) & x \equiv 1(\texttt{mod}\ 43) & x \equiv 42(\texttt{mod}\ 43) \end{array}$$

Por lo tanto las soluciones de $x^5 - x^3 \equiv 0(\texttt{mod}\ 43)$ son:

$$x \equiv 0(\texttt{mod}\ 43), \quad x \equiv 1(\texttt{mod}\ 43), \quad x \equiv 42(\texttt{mod}\ 43)$$

Solución 24. Resolver $\overline{x} + \overline{73} = \overline{68}$ en $\mathbb{Z}_{21}$

$$\begin{aligned} \overline{x} + \overline{73} &= \overline{68} \\ \overline{x} &= \overline{68} - \overline{73} \\ \overline{x} &= -\overline{5}; \quad -5+21=16 \\ \overline{x} &= \overline{16} \end{aligned}$$

♡

Solución 25. Resolver $\overline{2} \cdot \overline{x}^2 + \overline{x} + \overline{6} = \overline{0}$ en $\mathbb{Z}_7$, recordemos que $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$

$$\begin{array}{ccccccc} \overline{x} & = & \overline{0} & : & \overline{2}\cdot\overline{0}^2+\overline{0}+\overline{6} & = & \overline{6} \neq \overline{0} & \\ \overline{x} & = & \overline{1} & : & \overline{2}\cdot\overline{1}^2+\overline{1}+\overline{6} & = & \overline{9} = \overline{2} \neq \overline{0} & \\ \overline{x} & = & \overline{2} & : & \overline{2}\cdot\overline{2}^2+\overline{2}+\overline{6} & = & \overline{16} = \overline{2} \neq \overline{0} & \\ \overline{x} & = & \overline{3} & : & \overline{2}\cdot\overline{3}^2+\overline{3}+\overline{6} & = & \overline{27} = \overline{6} \neq \overline{0} & \\ \overline{x} & = & \overline{4} & : & \overline{2}\cdot\overline{4}^2+\overline{4}+\overline{6} & = & \overline{42} = \overline{0} & \checkmark \\ \overline{x} & = & \overline{5} & : & \overline{2}\cdot\overline{5}^2+\overline{5}+\overline{6} & = & \overline{61} = \overline{5} \neq \overline{0} & \\ \overline{x} & = & \overline{6} & : & \overline{2}\cdot\overline{6}^2+\overline{6}+\overline{6} & = & \overline{84} = \overline{0} & \checkmark \end{array}$$

Por lo tanto todos los $\overline{x} \in \mathbb{Z}_7$ tal que $\overline{2} \cdot \overline{x}^2 + \overline{x} + \overline{6} = \overline{0}$ son $\overline{x} = \overline{4}, \overline{x} = \overline{6}$ ♡

Solución 26. Demostrar que $\forall a, n \in \mathbb{Z}$ tal que a, n son primo relativos con 31 entonces $31 | n^{30} - a^{30}$, para ello tenemos que

$$n^{\phi(31)} \equiv 1(\texttt{mod}\ 31) \quad a^{\phi(31)} \equiv 1(\texttt{mod}\ 31)$$

Luego

$$n^{30} \equiv 1(\texttt{mod}\ 31) \quad a^{30} \equiv 1(\texttt{mod}\ 31)$$

Restando obtenemos

$$n^{30} - a^{30} \equiv 1 - 1 \equiv 0(\texttt{mod}\ 31)$$

De lo cual obtenemos $31 | (n^{30} - a^{30})$ ♡

Solución: 27 Sea p un número primo impar

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}} \cdot \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$$

Como $\left(\frac{5}{p}\right) = -1$, luego $\left(\frac{p}{5}\right) = -1$, analicemos los casos

i) $p \equiv 1(\texttt{mod } 5)$, luego
$\left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1$, lo que es una contradicción

ii) $p \equiv 2(\texttt{mod } 5)$
$\left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$

iii) $p \equiv 3(\texttt{mod } 5)$, luego $\left(\frac{p}{5}\right) = \left(\frac{3}{5}\right)$. Calculemos

$$\begin{aligned}\left(\frac{3}{5}\right) &= (-1)^{\frac{5-1}{2}\cdot\frac{3-1}{2}} \cdot \left(\frac{5}{3}\right); \quad 5 \equiv 2(\texttt{mod } 3)\\ \left(\frac{3}{5}\right) &= 1 \cdot \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} - 1\end{aligned}$$

Por lo tanto $\left(\frac{3}{5}\right) = -1$.

iv) $p \equiv 4(\texttt{mod } 5)$
$\left(\frac{p}{5}\right) = \left(\frac{4}{5}\right) = 1$, lo que es una contradicción

De este modo todos los primos impares p, tal que $\left(\frac{5}{p}\right) = -1$ son

$$p \equiv 2(\texttt{mod } 5) \vee p \equiv 3(\texttt{mod } 5)$$

♡

Solución 28.

I) $\begin{array}{rcl|} 3x+2y & \equiv & 1(\texttt{mod } 7)\\ 2x+5y & \equiv & 2(\texttt{mod } 7) \\ \hline \end{array}$

Note que 7 es un numero primo, todos lo números salvo los múltiplo de 7 son invertibles. Amplificamos las ecuaciones

$$\begin{array}{rcll|} 3x+2y & \equiv & 1(\texttt{mod } 7) & /\cdot 2\\ 2x+5y & \equiv & 2(\texttt{mod } 7) & /\cdot -3 \\ \hline \end{array}$$

$$\begin{array}{rcr|} 6x+4y & \equiv & 1(\texttt{mod } 7)\\ -6x-15y & \equiv & -6(\texttt{mod } 7) \\ \hline \end{array}$$

Sumando las ecuaciones, se obtiene

$$\begin{aligned} -11y &\equiv -4(\texttt{mod } 7)\\ 3y &\equiv 3(\texttt{mod } 7)\\ y &\equiv 1(\texttt{mod } 7)\end{aligned}$$

Reemplazando en $2x \equiv 2 - 5y (\text{mod } 7)$

$$\begin{aligned} 2x &\equiv 2 - 5 (\text{mod } 7) \\ 2x &\equiv -3 \equiv 4 (\text{mod } 7) \\ x &\equiv 2 (\text{mod } 7) \end{aligned}$$

$$S = \{\ (x, y) \mid x \equiv 2 (\text{mod } 7) \quad y \equiv 1 (\text{mod } 7)\}$$

II) $\left.\begin{array}{rcl} x + 12y & \equiv & 9 (\text{mod } 13) \\ 3x + 11y & \equiv & 8 (\text{mod } 13) \end{array}\right|$

De manera análoga tenemos que 13 es primo.

$$\left.\begin{array}{rcll} x + 12y & \equiv & 9 (\text{mod } 13) & / \cdot -3 \\ 3x + 11y & \equiv & 8 (\text{mod } 13) & \end{array}\right|$$

$$\left.\begin{array}{rcl} -3x - 36y & \equiv & -27 (\text{mod } 13) \\ 3x + 11y & \equiv & 8 (\text{mod } 13) \end{array}\right|$$

sumando obtenemos

$$\begin{aligned} -25y &\equiv -19 (\text{mod } 13) \\ y &\equiv 7 (\text{mod } 13) \end{aligned}$$

Reemplazando en $x \equiv 9 - 12y (\text{mod } 13)$

$$\begin{aligned} x &\equiv 9 - 12 \cdot 7 (\text{mod } 13) \\ x &\equiv -75 \equiv 3 (\text{mod } 13) \end{aligned}$$

$$S = \{\ (x, y) \mid x \equiv 3 (\text{mod } 13) \quad y \equiv 7 (\text{mod } 13)\}$$

III) $\left.\begin{array}{rcl} x + y + z & \equiv & 2 (\text{mod } 7) \\ x + 2y + 3z & \equiv & 3 (\text{mod } 7) \\ 2x + y + 4z & \equiv & 1 (\text{mod } 7) \end{array}\right|$

Despejando obtenemos $x \equiv 3 - 2y - 3z (\text{mod } 7)$ y reemplazando en

$$\begin{array}{rcll} 2x + y + 4z & \equiv & 1 (\text{mod } 7) & \\ 2 \cdot (3 - 2y - 3z) + y + 4z & \equiv & 1 (\text{mod } 7) & \\ -3y & \equiv & -5 + 2z (\text{mod } 7) & \\ 4y & \equiv & 2 + 2z (\text{mod } 7) & / \cdot 2 \\ y & \equiv & 4 + 4z (\text{mod } 7) & \end{array}$$

En la ecuación original

$$\begin{aligned}
x &\equiv 3 - 2y - 3z (\texttt{mod } 7)\\
x &\equiv 3 - 2\cdot(4+4z) - 3z (\texttt{mod } 7)\\
x &\equiv -5 - 11z (\texttt{mod } 7)\\
x &\equiv 2 + 3z (\texttt{mod } 7)
\end{aligned}$$

Reemplazando en la primera ecuación

$$\begin{aligned}
x + y + z &\equiv 2 (\texttt{mod } 7)\\
(2+3z) + (4+4z) + z &\equiv 2 (\texttt{mod } 7)\\
z &\equiv 3 (\texttt{mod } 7)
\end{aligned}$$

Reemplazando el valor de z

$$\begin{array}{rl}
x \equiv 2 + 3z (\texttt{mod } 7) & \quad y \equiv 4 + 4z (\texttt{mod } 7)\\
x \equiv 2 + 3\cdot 3 (\texttt{mod } 7) & \quad y \equiv 4 + 4\cdot 3 (\texttt{mod } 7)\\
x \equiv 11 (\texttt{mod } 7) & \quad y \equiv 16 (\texttt{mod } 7)\\
x \equiv 4 (\texttt{mod } 7) & \quad y \equiv 2 (\texttt{mod } 7)
\end{array}$$

La solución del sistema es:

$$x \equiv 4(\texttt{mod } 7) \quad \wedge \quad y \equiv 2(\texttt{mod } 7) \quad \wedge \quad z \equiv 3(\texttt{mod } 7)$$

o bien

$$S = \{\ (x,y,z) \mid x \equiv 4(\texttt{mod } 7) \quad y \equiv 2(\texttt{mod } 7) \quad z \equiv 3(\texttt{mod } 7)\}$$

IV) $$\left.\begin{aligned}
x + 2y + 4z &\equiv 5 (\texttt{mod } 13)\\
5x + y + 8z &\equiv 7 (\texttt{mod } 13)\\
6x + 8y + 7z &\equiv 1 (\texttt{mod } 13)
\end{aligned}\right|$$

Despejando obtenemos $x \equiv 5 - 2y - 4z (\texttt{mod } 13)$ y reemplazando en

$$\begin{aligned}
5x + y + 8z &\equiv 7 (\texttt{mod } 13)\\
5(5 - 2y - 4z) + y + 8z &\equiv 7 (\texttt{mod } 13)\\
-9y &\equiv -18 + 12z (\texttt{mod } 13)\\
4y &\equiv 8 + 12z (\texttt{mod } 13)\\
y &\equiv 2 + 3z (\texttt{mod } 13)
\end{aligned}$$

En la ecuación original

$$\begin{aligned}
x &\equiv 5 - 2y - 4z (\texttt{mod } 13)\\
x &\equiv 5 - 2\cdot(2+3z) - 4z (\texttt{mod } 13)\\
x &\equiv 1 + 3z (\texttt{mod } 13)
\end{aligned}$$

Reemplazando en la tercera ecuación

$$\begin{aligned} 6x+8y+7z &\equiv 1(\text{mod } 13) \\ 6\cdot(1+3z)+8\cdot(2+3z)+7z &\equiv 1(\text{mod } 13) \\ 10z &\equiv 5(\text{mod } 13) \quad /\cdot 4 \\ 40z &\equiv 20(\text{mod } 13) \\ z &\equiv 7(\text{mod } 13) \end{aligned}$$

Reemplazando el valor de z en

$$\begin{array}{rl} x \equiv 1+3z(\text{mod } 13) & y \equiv 2+3z(\text{mod } 13) \\ x \equiv 1+3\cdot 7(\text{mod } 13) & y \equiv 2+3\cdot 7(\text{mod } 13) \\ x \equiv 22(\text{mod } 13) & y \equiv 23(\text{mod } 13) \quad 23-13=10 \\ x \equiv 9(\text{mod } 13) & y \equiv 10(\text{mod } 13) \end{array}$$

La solución del sistema es:

$$x \equiv 9(\text{mod } 13) \quad \wedge \quad y \equiv 10(\text{mod } 13) \quad \wedge \quad z \equiv 7(\text{mod } 13)$$

o bien

$$S = \{\ (x,y,z) \mid x \equiv 9(\text{mod } 13) \quad y \equiv 10(\text{mod } 13) \quad z \equiv 7(\text{mod } 13)\}$$

v) $$\left.\begin{array}{rcl} x & \equiv & 7(\text{mod } 9) \\ x & \equiv & 10(\text{mod } 4) \\ x & \equiv & 1(\text{mod } 7) \end{array}\right|$$

Como $(9,4)=1, \quad (9,7)=1, \quad (4,7)=1$, luego tenemos

$$a_1 = 7, a_2 = 10, a_3 = 1,\ m_1 = 9, m_2 = 4, m_3 = 7,\ m = m_1\cdot m_2\cdot m_3 = 252$$

calculemos los coeficiente de la solución particular

$$\begin{array}{rrr} \frac{m}{m_1}\cdot b_1 \equiv 1(\text{mod } m_1) & \frac{m}{m_2}\cdot b_2 \equiv 1(\text{mod } m_2) & \frac{m}{m_3}\cdot b_3 \equiv 1(\text{mod } m_3) \\ 28\cdot b_1 \equiv 1(\text{mod } 9) & 63\cdot b_2 \equiv 1(\text{mod } 4) & 36\cdot b_3 \equiv 1(\text{mod } 7) \\ b_1 \equiv 1(\text{mod } 9) & -1\cdot b_2 \equiv 1(\text{mod } 4) & b_3 \equiv 1(\text{mod } 7) \\ & b_2 \equiv 3(\text{mod } 4) & \end{array}$$

Luego la solución particular

$$\begin{aligned} x_0 &= a_1\cdot b_1\cdot\frac{m}{m_1} + a_2\cdot b_2\cdot\frac{m}{m_2} + a_3\cdot b_3\cdot\frac{m}{m_3} \\ x_0 &= 7\cdot 1\cdot 28 + 10\cdot 3\cdot 63 + 1\cdot 1\cdot 36 = 2122 \end{aligned}$$

y la solución general

$$\begin{aligned} x &\equiv x_0(\text{mod } m) \\ x &\equiv 2122 \equiv 106(\text{mod } 252) \end{aligned}$$

VI) $\left.\begin{array}{rcl} x & \equiv & 1(\texttt{mod } 4) \\ x & \equiv & 0(\texttt{mod } 3) \\ x & \equiv & 5(\texttt{mod } 7) \end{array}\right|$

Como $(3,7)=1, \quad (4,7)=1, \quad (3,4)=1$, luego tenemos

$$a_1=1, a_2=0, a_3=5,\; m_1=4, m_2=3, m_3=7,\; m=m_1\cdot m_2\cdot m_3=84$$

Los coeficiente de para obtener la solución particular

$$\begin{array}{rrl} \dfrac{m}{m_1}\cdot b_1\equiv 1(\texttt{mod } m_1) & \frac{m}{m_2}\cdot b_2\equiv 1(\texttt{mod } m_2) & \dfrac{m}{m_3}\cdot b_3\equiv 1(\texttt{mod } m_3) \\ 21\cdot b_1\equiv 1(\texttt{mod } 4) & 28\cdot b_2\equiv 1(\texttt{mod } 3) & 12\cdot b_3\equiv 1(\texttt{mod } 7) \\ b_1\equiv 1(\texttt{mod } 4) & b_2\equiv 1(\texttt{mod } 3) & 5\cdot b_3\equiv 15(\texttt{mod } 7) \\ & & b_3\equiv 3(\texttt{mod } 7) \end{array}$$

Luego la solución particular

$$\begin{array}{rcl} x_0 & = & a_1\cdot b_1\cdot\dfrac{m}{m_1}+a_2\cdot b_2\cdot\dfrac{m}{m_2}+a_3\cdot b_3\cdot\dfrac{m}{m_3} \\ x_0 & = & 1\cdot 1\cdot 21+0\cdot 1\cdot 28+5\cdot 3\cdot 12=201 \end{array}$$

y la solución general

$$\begin{array}{rcl} x & \equiv & x_0(\texttt{mod } m) \\ x & \equiv & 201\equiv 33(\texttt{mod } 84) \end{array}$$

VII) $\left.\begin{array}{rcl} 3x & \equiv & 1(\texttt{mod } 5) \\ 4x & \equiv & 6(\texttt{mod } 14) \\ 5x & \equiv & 11(\texttt{mod } 3) \end{array}\right|$

Simplifiquemos

$$\begin{array}{rrr} 3x\equiv 1(\texttt{mod } 5) & 2x\equiv 3(\texttt{mod } 7) & 5x\equiv 11(\texttt{mod } 3) \\ 3x\equiv 6(\texttt{mod } 5) & 2x\equiv 10(\texttt{mod } 7) & 2x\equiv 2(\texttt{mod } 3) \\ x\equiv 2(\texttt{mod } 5) & x\equiv 5(\texttt{mod } 7) & x\equiv 1(\texttt{mod } 3) \end{array}$$

Por lo tanto hay que resolver:

$$\begin{array}{rcl} x & \equiv & 2(\texttt{mod } 5) \\ x & \equiv & 5(\texttt{mod } 7) \\ x & \equiv & 1(\texttt{mod } 3) \end{array}$$

Como $(5,14)=1, \quad (3,5)=1, \quad (14,3)=1$, luego tenemos

$$a_1=2, a_2=5, a_3=1,\; m_1=5, m_2=7, m_3=3,\; m=m_1\cdot m_2\cdot m_3=105$$

Los coeficiente de para obtener la solución particular

$$\begin{array}{rrl}
\dfrac{m}{m_1}\cdot b_1 \equiv 1(\texttt{mod } m_1) & \frac{m}{m_2}\cdot b_2 \equiv 1(\texttt{mod } m_2) & \dfrac{m}{m_3}\cdot b_3 \equiv 1(\texttt{mod } m_3) \\
21\cdot b_1 \equiv 1(\texttt{mod } 5) & 15\cdot b_2 \equiv 1(\texttt{mod } 7) & 35\cdot b_3 \equiv 1(\texttt{mod } 3) \\
b_1 \equiv 1(\texttt{mod } 5) & b_2 \equiv 1(\texttt{mod } 7) & 2b_3 \equiv 1(\texttt{mod } 3 \\
 & & b_3 \equiv 2(\texttt{mod } 3)
\end{array}$$

Luego debemos determinar la solución particular

$$\begin{aligned}
x_0 &= a_1\cdot b_1\cdot \frac{m}{m_1} + a_2\cdot b_2\cdot \frac{m}{m_2} + a_3\cdot b_3\cdot \frac{m}{m_3} \\
x_0 &= 2\cdot 1\cdot 21 + 15\cdot 1\cdot 15 + 1\cdot 2\cdot 35 = 187
\end{aligned}$$

y la solución general

$$\begin{aligned}
x &\equiv x_0(\texttt{mod } m) \\
x &\equiv 187 \equiv 82(\texttt{mod } 105)
\end{aligned}$$

VIII) $\left.\begin{array}{rcl} x-y & \equiv & 5(\texttt{mod } 47) \\ xy & \equiv & 6(\texttt{mod } 47) \end{array}\right|$

Notemos que 47 es un número primo y amplifiquemos por $-y$ la primera ecuación y sumando obtenemos

$$y^2+5y-6 \equiv 0(\texttt{mod } 47)$$

El discriminante es

$$\Delta = 5^2 - 4\cdot 1\cdot 6 = 25-24 = 1 = 1^2$$

luego debemos resolver

$$(2y+5)^2 \equiv 1^2(\texttt{mod } 47)$$

$$\begin{array}{rl}
2y+5 \equiv 1(\texttt{mod } 47) & 2y+5 \equiv -1(\texttt{mod } 47) \\
2y \equiv -4(\texttt{mod } 47) & 2y \equiv -6(\texttt{mod } 47) \\
y \equiv -2(\texttt{mod } 47) & y \equiv -3(\texttt{mod } 47) \\
y \equiv 45(\texttt{mod } 47) & y \equiv 44(\texttt{mod } 47)
\end{array}$$

Reemplazando en la ecuación lineal obtenemos que la solución del sistema es

$$(x \equiv 3(\texttt{mod } 47) \wedge y \equiv 45(\texttt{mod } 47)) \vee (x \equiv 2(\texttt{mod } 47) \wedge y \equiv 44(\texttt{mod } 47))$$

IX) $\left.\begin{array}{rcl} x^2+y^2 & \equiv & 1(\texttt{mod } 13) \\ xy & \equiv & 2(\texttt{mod } 13) \end{array}\right|$

Eliminemos una variable del sistema

$\left.\begin{array}{rcll} x^2+y^2 & \equiv & 1(\texttt{mod } 13) & /\cdot -x^2 \\ xy & \equiv & 2(\texttt{mod } 13) & /()^2 \end{array}\right|$

Recuerde que el paso anterior, no es una equivalencia, pero si una implicación

$$\left.\begin{array}{rcl} -x^4 - x^2y^2 & \equiv & -x^2 (\texttt{mod } 13) \\ x^2y^2 & \equiv & 4 (\texttt{mod } 13) \end{array}\right|$$

Luego

$$x^4 - x^2 + 4 \equiv 0 (\texttt{mod } 13)$$

Cuyo discriminante es

$$\Delta = 1 - 16 = -15 = -2 = (-1) \cdot 2$$

Para determinar si -2 es un cuadrado, veremos

$$\left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right) \cdot \left(\frac{2}{13}\right) = (-1)^{\frac{13-1}{2}} \cdot (-1)^{\frac{13^2-1}{8}} = -1$$

Por lo tanto $-2 \notin \square_{13}$, es decir, $\left.\begin{array}{rcl} x^2 + y^2 & \equiv & 1 (\texttt{mod } 13) \\ xy & \equiv & 2 (\texttt{mod } 13) \end{array}\right|$ no tiene solución.

♡

Solución 29.

Determinar los $\alpha \in \mathbb{Z}_{41}$ tal que

$$\left.\begin{array}{rcl} x - y & = & \alpha \\ x \cdot y & = & 1 \end{array}\right|$$

el sistema no tenga solución. Para ello amplificando por x, la primera ecuación obtenemos

$$\left.\begin{array}{rcl} x^2 - x \cdot y & = & \alpha \cdot x \\ x \cdot y & = & 1 \end{array}\right|$$

Sumando las ecuaciones tenemos

$$x^2 - \alpha \cdot x - 1 = 0$$

El valor del discriminante es

$$\Delta = \alpha^2 + 4 \notin \square_{41} \cup \{0\}$$

Además los cuadrado son

$$\begin{array}{rcl} \square_{41} & = & \{\overline{1}, \overline{4}, \overline{9}, \overline{16}, \overline{25}, \overline{36}, \overline{8}, \overline{23}, \overline{40}, \overline{18}, \overline{39}, \overline{21}, \overline{5}, \overline{32}, \overline{20}, \overline{10}, \overline{2}, \overline{37}, \overline{33}, \overline{31}\} \\ & = & \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{8}, \overline{9}, \overline{10}, \overline{16}, \overline{18}, \overline{20}, \overline{21}, \overline{23}, \overline{25}, \overline{31}, \overline{32}, \overline{33}, \overline{36}, \overline{37}, \overline{39}, \overline{40}\} \end{array}$$

Ahora veremos

$$\square_{41} + \overline{4} = \{\overline{5}, \overline{6}, \overline{8}, \overline{9}, \overline{12}, \overline{13}, \overline{14}, \overline{20}, \overline{22}, \overline{24}, \overline{25}, \overline{27}, \overline{29}, \overline{35}, \overline{36}, \overline{37}, \overline{40}, \overline{0}, \overline{2}, \overline{3}\}$$

por intersección tenemos que

$$\alpha^2 \in \{\overline{2}, \overline{8}, \overline{9}, \overline{10}, \overline{18}, \overline{20}, \overline{23}, \overline{25}, \overline{31}, \overline{40}\}$$

Por lo tanto

$$\alpha \in \{\overline{3},\overline{5},\overline{7},\overline{8},\overline{9},\overline{10},\overline{15},\overline{16},\overline{17},\overline{20},\overline{21},\overline{24},\overline{25},\overline{26},\overline{31},\overline{32},\overline{33},\overline{34},\overline{36},\overline{38}\}$$

♡

Solución 30. Sea $p \equiv 3(\texttt{mod}\ 4)$ y supongamos que existen $x, y \in \mathbb{Z}$ tal que $x^2 + y^2 = p$. Note que si uno de ellos es múltiplo de p entonces el otro también, clo cual nos conduce a una contradicción.

$$\begin{aligned}
x^2 + y^2 &= p \\
x^2 + y^2 &\equiv 0(\texttt{mod}\ p) \\
x^2 &\equiv -y^2(\texttt{mod}\ p) \quad y \neq 0 \\
\left(\frac{x}{y}\right)^2 &\equiv -1(\texttt{mod}\ p) \\
\left(\frac{-1}{p}\right) &= 1 \\
(-1)^{\frac{p-1}{2}} &= 1 \\
\frac{p-1}{2} &= 2 \cdot t \quad t \in \mathbb{Z} \\
p - 1 &= 4 \cdot t \\
p &\equiv 1(\texttt{mod}\ 4)
\end{aligned}$$

Pero $p \equiv 3(\texttt{mod}\ 4)$. Por lo tanto no existen $x, y \in \mathbb{Z}$ tal que $x^2 + y^2 = p$ ♡

Solución 31. Sea p primo impar, luego $p \neq 2$, y además $p - 1$ es par, por lo tanto $p - 1 = 2 \cdot k; \quad k \in \mathbb{Z}$.

Sea $\overline{x} \in \mathcal{U}(\mathbb{Z}_p)$ luego existe un único $\overline{x}^{-1} \in \mathcal{U}(\mathbb{Z}_p)$

$$\sum_{\overline{x} \in \mathbb{Z}_p^*} \overline{x}^{-1} = \sum_{\overline{y} \in \mathbb{Z}_p^*} \overline{y}$$

$$\sum_{\overline{x} \in \mathbb{Z}_p^*} \overline{x}^{-1} = \overline{1} + \overline{2} + \cdots + \overline{p-1} = \overline{\frac{p \cdot (p-1)}{2}} = \overline{\frac{2 \cdot k \cdot p}{2}} = \overline{k \cdot p}$$

De lo obtenemos

$$\sum_{\overline{x} \in \mathbb{Z}_p^*} \overline{x}^{-1} = 0(\texttt{mod}\ p)$$

♡

Solución: 32 Veamos unos ejemplos primero

$$\square_3 = \{\overline{1}\}; \qquad \prod_{\overline{x}\in\square_3} \overline{x} = \overline{1}$$
$$\square_5 = \{\overline{1}, \overline{4}\}; \qquad \prod_{\overline{x}\in\square_5} \overline{x} = \overline{1}\cdot\overline{4} = \overline{4}$$
$$\square_7 = \{\overline{1}, \overline{4}, \overline{2}\}; \qquad \prod_{\overline{x}\in\square_7} \overline{x} = \overline{1}\cdot\overline{4}\cdot\overline{2} = \overline{8} = \overline{1}$$

Note que $\square_p$ es un subgrupo multiplicativo y en este producto esta el inverso de cada elemento, además los únicos elementos que son su propio inverso son $\overline{1}, \overline{-1}$ por lo tanto, el resultado depende solamente si $\overline{-1}$ es un cuadrado

Conclusión:

Si $p = 4\cdot t - 1 \quad t \in \mathbb{Z}$ entonces $\prod_{\overline{x}\in\square_p} \overline{x} = \overline{1}$

Si $p = 4\cdot t + 1 \quad t \in \mathbb{Z}$ entonces $\prod_{\overline{x}\in\square_p} \overline{x} = \overline{p-1}$ ♡

Solución 33.

$$\square_2 = \{\overline{1}\}; \qquad \sum_{\overline{x}\in\square_2} \overline{x} = \overline{1}$$
$$\square_3 = \{\overline{1}\}; \qquad \sum_{\overline{x}\in\square_3} \overline{x} = \overline{1}$$
$$\square_5 = \{\overline{1}, \overline{4}\}; \qquad \sum_{\overline{x}\in\square_5} \overline{x} = \overline{1}+\overline{4} = \overline{5} = \overline{0}$$
$$\square_7 = \{\overline{1}, \overline{4}, \overline{2}\}; \qquad \sum_{\overline{x}\in\square_7} \overline{x} = \overline{1}+\overline{4}+\overline{2} = \overline{7} = \overline{0}$$

Sea p un primo mayor que 3, y δ un no cuadrado distinto de -1, luego $\delta\square_p$ es el conjunto de los no cuadrado y recordemos el ejemplo 102

$$0 = \sum_{\overline{x}\in\mathbb{Z}_p^*} \overline{x} = \sum_{\overline{y}\in\square_p} \overline{y} + \sum_{\overline{z}\in\delta\square_p} \overline{z}$$

Simplificando

$$\begin{aligned} 0 &= \sum_{\overline{y}\in\square_p} \overline{y} + \delta \sum_{\overline{y}\in\square_p} \overline{y} \\ 0 &= (1+\delta) \sum_{\overline{y}\in\square_p} \overline{y} \end{aligned}$$

De lo cual obtenemos la siguiente conclusión:

Si $p = 2$ ó 3 entonces $\sum_{\overline{x}\in\square_p} \overline{x} = \overline{1}$

Si $p \neq 2$ y 3 entonces $\sum_{\overline{x}\in\square_p} \overline{x} = \overline{0}$ ♡

Solución: 34 Sean $x, y \in \mathbb{Z}^+$ tales que $(x, y) = 5$, luego $5|x$ y $5|y$

Como $5|x \Leftrightarrow x = 5\cdot q; \quad q \in \mathbb{Z}$ y $5|y \Leftrightarrow y = 5\cdot k; \quad k \in \mathbb{Z}$, con k, q primos relativos.

Además $x+y=100$, luego reemplazando obtenemos $5(q+k)=100$ y simplificando obtenemos $q+k=20$

q	k	x	y	(x,y)	$x+y$	
1	19	5	95	5	100	✓
2	18	10	90	10	100	
3	17	15	85	5	100	✓
4	16	20	80	20	100	
5	15	25	75	25	100	
6	14	30	70	10	100	
7	13	35	65	5	100	✓
8	12	40	60	20	100	
9	11	45	55	5	100	✓
10	10	50	50	50	100	

Por lo tanto hay 8 soluciones que están dadas por:

$$S=\{\ (5,95),(15,85),(35,65),(45,55),(55,45),(65,35),(85,15),(95,5)\ \}\subset\mathbb{Z}\times\mathbb{Z}$$

♡

Solución 35.

Sean x,y números impares luego $y=2\cdot k+1;\quad k\in\mathbb{Z},\quad x=2\cdot q+1;\quad q\in\mathbb{Z}$, reemplazando y simplificando obtenemos

$$\begin{aligned} x^2+y^2 &= (2\cdot k+1)^2+(2\cdot q+1)^2 \\ &= 4\cdot k^2+4\cdot k+1+4\cdot q^2+4\cdot q+1 \\ &= 2\cdot(2\cdot k^2+2\cdot k+2\cdot q^2+2\cdot q+1) \\ &= 2\cdot r;\quad r=2\cdot k^2+2\cdot k+2\cdot q^2+2\cdot q+1 \end{aligned}$$

Por lo tanto x^2+y^2 es par.

Ahora supongamos que $4|(x^2+y^2)$ luego $x^2+y^2=4\cdot a$ con $a\in\mathbb{Z}$, volviendo a la identidad anterior tenemos

$$\begin{aligned} x^2+y^2 &= 4\cdot a \\ 4\cdot k^2+4\cdot k+1+4\cdot q^2+4\cdot q+1 &= 4\cdot a \\ 4\cdot(k^2+k+q^2+q-a) &= -2 \end{aligned}$$

Por lo tanto $4|2$, lo que es una contradicción, lo que implica que 4 no divide a x^2+y^2

♡

Solución 36. Sean $a,b\in\mathbb{Z}$ tales que $a^2=2\cdot b^2$, luego $2|a^2$ lo que implica que $2|a$, por tanto a es par. Reemplazando $a=2k$, obtenemos

$$\begin{aligned} a^2 &= 2\cdot b^2 \\ (2k)^2 &= 2\cdot b^2 \\ 4k^2 &= 2b^2 \\ 2k^2 &= b^2 \end{aligned}$$

De igual manera $2|b^2$ por ende $2|b$, lo cual determina que b es par. ♡

Solución 37. Sean $a, b \in \mathbb{Z}$ tales que $(a,4) = 2, \quad (b,4) = 2$, luego a divisible por 2 y no por 4, de igual manera b

Por lo anterior tenemos $a = 2 \cdot k_1$ y $b = 2 \cdot k_2$, donde k_1, k_2 son impares es decir,

$$k_1 = 2 \cdot q_1 + 1, \quad k_2 = 2 \cdot q_2 + 1, \quad q_1, q_2 \in \mathbb{Z}$$

Reemplazando tenemos

$$a + b \;=\; 2k_1 + 2k_2 = 2(2q_1 + 1) + 2(2q_2 + 1) = 4(q_1 + q_2 + 1)$$

Por lo tanto $4|a + b$, luego $(a + b, 4) = 4$. ♡

A.2.3. Números Complejos

Solución: 38

I) $\overline{z} + 2z = 4 + i$

Sea $z = a + bi, \quad \overline{z} = a - bi$, luego $\overline{z} + 2z = a - bi + 2a + 2bi$.

Reemplazando se tiene

$$3a + bi \;=\; 4 + i$$

Luego

$$3a = 4; \quad b = 1$$

Por lo tanto $z = \frac{4}{3} + i$

II) $\overline{z} + 5z + 6 = z^2$

Sea $z = a + bi$, con $a, b \in \mathbb{R}$ luego $\overline{z} = a - bi, \quad z^2 = a^2 - b^2 + 2abi$, reemplazando

$$\begin{aligned} \overline{z} + 5z + 6 &= z^2 \\ a - bi + 5a + 5bi + 6 &= a^2 - b^2 + 2abi \end{aligned}$$

de lo cual tenemos

$$\begin{array}{rcl|} 6a + 6 & = & a^2 - b^2 \\ 4b & = & 2ab \\ \hline \end{array}$$

De la segunda ecuación

$$\begin{aligned} 2ab - 4b &= 0 \\ b(2a - 4) &= 0 \end{aligned}$$

luego

$$b = 0 \quad \vee \quad a = 2$$

Si $b = 0$ entonces

$$\begin{aligned} a^2 - b^2 - 6a &= 6 \\ a^2 - 6a - 6 &= 0 \\ a &= \frac{6 \pm \sqrt{36 + 4 \cdot 6}}{2} \\ a &= \frac{6 \pm \sqrt{60}}{2} \\ a &= 3 \pm \sqrt{15} \end{aligned}$$

Si $a = 2$ entonces

$$\begin{aligned} a^2 - b^2 - 6a &= 6 \\ 4 - b^2 - 12 &= 6 \\ b^2 &= -14 \end{aligned}$$

Imposible, ya que b es real. Por lo tanto $z_1 = 3 + \sqrt{15} + 0i, \quad z_2 = 3 - \sqrt{15} + 0i$

III) $z^2 + |z| = 0$

Sea $z = a + bi, \quad z^2 = a^2 + 2abi - b^2, \quad |z| = \sqrt{a^2 + b^2}$

$$\begin{aligned} z^2 + |z| &= 0 \\ a^2 + 2abi - b^2 + \sqrt{a^2 + b^2} &= 0 \\ a^2 - b^2 + \sqrt{a^2 + b^2} + 2abi &= 0 \end{aligned}$$

De lo cual, obtenemos

$$\left.\begin{aligned} a^2 - b^2 + \sqrt{a^2 + b^2} &= 0 \\ 2ab &= 0 \end{aligned}\right|$$

De la segunda ecuación obtenemos

$$a = 0 \quad \vee \quad b = 0$$

Si $a = 0$

$$\begin{aligned} -b^2 + b &= 0 \\ b \cdot (1 - b) &= 0 \\ b = 0 \quad &\vee \quad b = 1 \end{aligned}$$

Si $b = 0$

$$\begin{aligned} a^2 + a &= 0 \\ a \cdot (1 - a) &= 0 \\ a = 0 \quad &\vee \quad a = -1 \end{aligned}$$

Por lo tanto $z \in \{i, -1, 0\}$

IV) $\left|\frac{z-12}{z-8i}\right| = \frac{5}{3}$

Sea $z = a + bi$

$$\begin{aligned}
\frac{|z-12|}{|z-8i|} &= \frac{5}{3}\\
3\cdot|z-12| &= 5\cdot|z-8i|\\
3\cdot|a+bi-12| &= 5\cdot|a+bi-8i|\\
3\cdot|a-12+bi| &= 5\cdot|a+(b-8)i|\\
3\cdot\sqrt{(a-12)^2+b^2} &= 5\cdot\sqrt{a^2+(b-8)^2} \quad /()^2\\
9\cdot(a^2-24a+144+b^2) &= 25\cdot(a^2+b^2-16b+64)\\
9a^2-216a+1296+9b^2 &= 25a^2+25b^2-400b+1600\\
16a^2+216a+16b^2-400b+304 &= 0 \quad /\div 16\\
a^2+\frac{27}{2}a+b^2-25b &= -19
\end{aligned}$$

Para determinar cuales son estos puntos, completemos cuadrado

$$\begin{aligned}
\left(a+\frac{27}{4}\right)^2-\left(\frac{27}{4}\right)^2+\left(b-\frac{25}{2}\right)^2-\left(\frac{25}{2}\right)^2 &= -19\\
\left(a+\frac{27}{4}\right)^2+\left(b-\frac{25}{2}\right)^2 &= -19+\frac{729}{16}+\frac{625}{4}\\
\left(a+\frac{27}{4}\right)^2+\left(b-\frac{25}{2}\right)^2 &= \frac{2925}{16}\\
\left(a+\frac{27}{4}\right)^2+\left(b-\frac{25}{2}\right)^2 &= \left(\frac{5\cdot\sqrt{117}}{4}\right)^2
\end{aligned}$$

representa una circunferencia en el plano cartesiano. ♡

Solución 39.

I) $\overline{z_1\cdot z_2} = \overline{z_1}\cdot\overline{z_2}$

Sean $z_1 = a+bi, \quad z_2 = c+di$

$$\begin{aligned}
\overline{z_1\cdot z_2} &= \overline{(a+bi)\cdot(c+di)}\\
\overline{z_1\cdot z_2} &= \overline{ac+adi+bci-bd}\\
\overline{z_1\cdot z_2} &= \overline{ac-bd+(ad+bc)i}\\
\overline{z_1\cdot z_2} &= ac-bd-adi-bci\\
\overline{z_1\cdot z_2} &= (a-bi)\cdot(c-di)\\
\overline{z_1\cdot z_2} &= \overline{z_1}\cdot\overline{z_2}
\end{aligned}$$

II) $|z_1+z_2|^2+|z_1-z_2|^2 = 2|z_1|^2+2|z_2|^2$

Sean $z_1 = a+bi, \quad z_2 = c+di$

$$\begin{array}{rcl}
|z_1+z_2|^2+|z_1-z_2|^2 &=& |a+bi+c+di|^2+|a+bi-c-di|^2 \\
|z_1+z_2|^2+|z_1-z_2|^2 &=& |a+c+(b+d)i|^2+|a-c+(b-d)i|^2 \\
|z_1+z_2|^2+|z_1-z_2|^2 &=& \sqrt{(a+c)^2+(b+d)^2}^2+\sqrt{(a-c)^2+(b-d)^2}^2 \\
|z_1+z_2|^2+|z_1-z_2|^2 &=& (a+c)^2+(b+d)^2+(a-c)^2+(b-d)^2 \\
|z_1+z_2|^2+|z_1-z_2|^2 &=& 2(a^2+b^2)+2(c^2+d^2) \\
|z_1+z_2|^2+|z_1-z_2|^2 &=& 2\sqrt{a^2+b^2}^2+2\sqrt{c^2+d^2}^2 \\
|z_1+z_2|^2+|z_1-z_2|^2 &=& 2|z_1|^2+2|z_2|^2
\end{array}$$

♡

Solución 40.

I) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad 4 \leq |z-1|+|z+1| \leq 8\}$

Sea $z = a+bi$

$$\begin{array}{rcl}
|a+bi-1|+|a+bi+1| &\leq& 8 \\
|a-1+bi|+|a+1+bi| &\leq& 8 \\
\sqrt{(a-1)^2+b^2}+\sqrt{(a+1)^2+b^2} &\leq& 8 \\
\sqrt{(a-1)^2+b^2} &\leq& 8-\sqrt{(a+1)^2+b^2} \quad /()^2 \qquad (*) \\
a^2-2a+1+b^2 &\leq& 64-16\sqrt{(a+1)^2+b^2}+a^2+2a+1+b^2 \\
16\sqrt{(a+1)^2+b^2} &\leq& 64+4a \quad / \div 4 \\
4\sqrt{(a+1)^2+b^2} &\leq& 16+a \quad /()^2 \\
16a^2+32a+16+16b^2 &\leq& 256+32a+a^2 \\
15a^2+16b^2 &\leq& 240 \quad / \div 240 \\
\dfrac{a^2}{16}+\dfrac{b^2}{15} &\leq& 1
\end{array}$$

Tenga presente que falta analizar una restricción $(*)$, luego $0 \leq 8-\sqrt{(a+1)^2+b^2}$, es decir $(a+1)^2+b^2 \leq 8^2$, es un disco de radio 8 y centro $(-1,0)$, donde la elipse esta contenida en el disco.

veamos la otra condición

$$\begin{array}{rcl}
4 &\leq& |a+bi-1|+|a+bi+1| \\
4 &\leq& |a-1+bi|+|a+1+bi| \\
4 &\leq& \sqrt{(a-1)^2+b^2}+\sqrt{(a+1)^2+b^2} \\
4-\sqrt{(a+1)^2+b^2} &\leq& \sqrt{(a-1)^2+b^2} \quad /()^2 \qquad (*) \\
16-8\sqrt{(a+1)^2+b^2}+a^2+2a+1+b^2 &\leq& a^2-2a+1+b^2 \\
16+4a &\leq& 8\sqrt{(a+1)^2+b^2} \quad / \div 2
\end{array}$$

$$\begin{array}{rcl} 4+a & \leq & 2\sqrt{(a+1)^2+b^2} \quad /()^2 \\ 16+8a+a^2 & \leq & 4a^2+8a+4+4b^2 \\ 12 & \leq & 3a^2+4b^2 \quad / \div 12 \\ 1 & \leq & \dfrac{a^2}{4}+\dfrac{b^2}{3} \end{array}$$

Falta analizar $(*)$, en este caso ha dos posibilidades, si $4^2 < \sqrt{(a+1)^2+b^2}$, cumple todo los valores y si es interior al disco $4^2 \geq (a+1)^2+b^2$ se tiene que $1 \leq \frac{a^2}{4}+\frac{b^2}{3}$, pero la elipse esta contenida en el disco, luego los valores que obtenemos son los exteriores a la elipse.

De este modo obtenemos.

Por lo tanto $\mathcal{A} = \{a+bi \in \mathbb{C}^2 \quad | \quad 1 \leq \frac{a^2}{4}+\frac{b^2}{3} \quad \wedge \quad \frac{a^2}{16}+\frac{b^2}{15} \leq 1\}$.

II) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad \frac{1}{2} \leq |z| \leq 1\}$

Sea $z = a+bi$

$$\begin{array}{rcl} \dfrac{1}{2} \leq & |z| & \leq 1 \\ \dfrac{1}{2} \leq & |a+bi| & \leq 1 \\ \dfrac{1}{2} \leq & \sqrt{a^2+b^2} & \leq 1 \quad /()^2 \\ \dfrac{1}{4} \leq & a^2+b^2 & \leq 1 \end{array}$$

Por lo tanto $\mathcal{A} = \{a+bi \in \mathbb{C} \quad | \quad \frac{1}{4} \leq a^2+b^2 \leq 1\}$.

III) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z-1+i| = 4\}$

Sea $z = a+bi$

$$\begin{array}{rcl} |z-1+i| & = & 4 \\ |a+bi-1+i| & = & 4 \\ |a-1+(b+1)i| & = & 4 \\ \sqrt{(a-1)^2+(b+1)^2} & = & 4 \quad /()^2 \\ (a-1)^2+(b+1)^2 & = & 4^2 \end{array}$$

Por lo tanto $\mathcal{A} = \{a+bi \in \mathbb{C} \quad | \quad (a-1)^2+(b+1)^2 = 16\}$, $\mathcal{A}$ es una circunferencia en $\mathbb{R}^2$.

IV) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z-2| = |1-2\overline{z}|\}$

Sea $z = a + bi, \quad \overline{z} = a - bi$

$$\begin{aligned} |z-2| &= |1-2\overline{z}| \\ |a+bi-2| &= |1-2a+2bi| \\ |a-2+bi| &= |1-2a+2bi| \\ \sqrt{(a-2)^2+b^2} &= \sqrt{(1-2a)^2+4b^2} \quad /()^2 \\ a^2-4a+4+b^2 &= 1-4a+4a^2+4b^2 \\ 3 &= 3a^2+3b^2 \quad / \div 3 \\ 1 &= a^2+b^2 \end{aligned}$$

Por lo tanto $\mathcal{A} = \{a + bi \in \mathbb{C} \quad | \quad a^2 + b^2 = 1\}$, $\mathcal{A}$ es una circunferencia en $\mathbb{R}^2$.

v) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad Re(\overline{z} - i) = 2\}$
Sea $z = a + bi, \quad \overline{z} = a - bi$

$$\begin{aligned} Re(\overline{z}-i) &= 2 \\ Re(a-bi-i) &= 2 \\ a &= 2 \end{aligned}$$

Por lo tanto $\mathcal{A} = \{a + bi \in \mathbb{C} \quad | \quad a = 2\}$, $\mathcal{A}$ es una recta en $\mathbb{R}^2$.

vi) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad 0 \leq Im(z) \leq 2\}$
Sea $z = a + bi$

$$\begin{array}{ccc} 0 \leq & Im(z) & \leq 2 \\ 0 \leq & Im(a+bi) & \leq 2 \\ 0 \leq & b & \leq 2 \end{array}$$

Por lo tanto $\mathcal{A} = \{a + bi \in \mathbb{C} \quad | \quad 0 \leq b \leq 2\}$, $\mathcal{A}$ es la intersección de dos semi planos en $\mathbb{R}^2$.

vii) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad 0 \leq Re(z) \leq 2\}$
Sea $z = a + bi$

$$\begin{array}{ccc} 0 \leq & Re(z) & \leq 2 \\ 0 \leq & Re(a+bi) & \leq 2 \\ 0 \leq & a & \leq 2 \end{array}$$

Por lo tanto $\mathcal{A} = \{a + bi \in \mathbb{C} \quad | \quad 0 \leq a \leq 2\}$, $\mathcal{A}$ es la intersección de dos semiplanos en $\mathbb{R}^2$.

viii) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z - 4i| + |z + 4i| = 10\}$

Sea $z = a + bi$

$$\begin{aligned}
|z-4i| + |z+4i| &= 10 \\
|a+bi-4i| + |a+bi+4i| &= 10 \\
\sqrt{a^2+(b-4)^2} + \sqrt{a^2+(b+4)^2} &= 10 \\
\sqrt{a^2+(b-4)^2} &= 10 - \sqrt{a^2+(b+4)^2} \quad /()^2 \qquad (*) \\
a^2+b^2-8b+16 &= 100 - 20\sqrt{a^2+(b+4)^2} + a^2+b^2+8b+16 \\
20\sqrt{a^2+(b+4)^2} &= 100+16b \quad / \div 4 \\
5\sqrt{a^2+(b+4)^2} &= 25+4b \quad /()^2 \\
25a^2+25b^2+200b+400 &= 625+200b+16b^2 \\
25a^2+9b^2 &= 225 \quad / \div 225 \\
\frac{a^2}{9}+\frac{b^2}{25} &= 1
\end{aligned}$$

Tenga presente, que falta analizar una restricción $(*)$, debe ser interior a la circunferencia de radio 1 y centro $(0,-4)$, lo cual esta considerada en la conclusión

Por lo tanto $\mathcal{A} = \{a+bi \in \mathbb{C} \quad | \quad \frac{a^2}{9}+\frac{b^2}{25} = 1\}$, $\mathcal{A}$ es representa una elipse en $\mathbb{R}^2$.

IX) Sean $a, c \in \mathbb{R}, b \in \mathbb{C}$ fijos

$$a \cdot z \cdot \overline{z} + Re(b \cdot \overline{z}) + c = 0$$

Sea $z = x+yi, \quad \overline{z} = x - yi, \quad b = d + ei$

$$\begin{aligned}
a \cdot z \cdot \overline{z} + Re(b \cdot \overline{z}) + c &= 0 \\
a \cdot (x+yi)\cdot(x-yi) + Re((d+ei)\cdot(x-yi)) + c &= 0 \\
a \cdot (x^2+y^2) + xd + ye + c &= 0 \quad / \div a \\
x^2+y^2+\frac{xd}{a}+\frac{ye}{a} &= -\frac{c}{a} \\
\left(x+\frac{d}{2a}\right)^2 - \frac{d^2}{4a^2} + \left(y+\frac{e}{2a}\right)^2 - \frac{e^2}{4a^2} &= -\frac{c}{a} \\
\left(x+\frac{d}{2a}\right)^2 + \left(y+\frac{e}{2a}\right)^2 &= -\frac{c}{a} + \frac{1}{4a^2}\cdot\left(d^2+e^2\right) \\
\left(x+\frac{d}{2a}\right)^2 + \left(y+\frac{e}{2a}\right)^2 &= \left(\sqrt{\frac{1}{4a^2}\cdot|b|^2 - \frac{c}{a}}\right)^2
\end{aligned}$$

Condición:

$$\begin{aligned}
\frac{1}{4a^2}\cdot|b|^2 - \frac{c}{a} &\geq 0 \\
|b|^2 &\geq 4ac
\end{aligned}$$

Por lo tanto. Si $|b|^2 > 4ac$ entonces el lugar geométrico es una circunferencia. Si $|b|^2 = 4ac$ entonces el lugar geométrico es un punto. Y en los otros caso es vacío. ♡

Solución 41. Sean $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z| = 3\}, \quad \mathcal{B} = \{z \in \mathbb{C} \quad | \quad |z-1| = |z-i|\}$, denotemos $z = a + bi$.

Como $z \in \mathcal{A}$, luego

$$\begin{array}{rcl} |z| & = & \sqrt{a^2+b^2} \\ 3 & = & \sqrt{a^2+b^2} \quad /()^2 \\ 3^2 & = & a^2+b^2 \end{array}$$

Además $z \in \mathcal{B}$, luego

$$\begin{array}{rcl} |z-1| & = & |z-i| \\ |a+bi-1| & = & |a+bi-i| \\ |a-1+bi| & = & |a+(b-1)i| \\ \sqrt{(a-1)^2+b^2} & = & \sqrt{a^2+(b-1)^2} \quad /()^2 \\ a^2-2a+1+b^2 & = & a^2+b^2-2b+1 \\ a & = & b \end{array}$$

Por lo tanto

$$\begin{array}{rcl} \mathcal{A}\cap\mathcal{B} & = & \{a+bi \in \mathbb{C} \quad | \quad a^2+b^2 = 3^2 \wedge a = b\} \\ \mathcal{A}\cap\mathcal{B} & = & \{a+bi \in \mathbb{C} \quad | \quad 2b^2 = 3^2 \wedge a = b\} \\ \mathcal{A}\cap\mathcal{B} & = & \left\{a+bi \in \mathbb{C} \quad | \quad b = \pm\dfrac{3}{\sqrt{2}} \wedge a = b\right\} \\ \mathcal{A}\cap\mathcal{B} & = & \left\{\dfrac{3}{\sqrt{2}} + \dfrac{3}{\sqrt{2}}i, -\dfrac{3}{\sqrt{2}} - \dfrac{3}{\sqrt{2}}i\right\} \end{array}$$

♡

Solución 42. Sea $|z| = 1$ y $w, z \in \mathbb{C}$, si $z = a + bi, \quad \overline{z} = a - bi, \quad w = c + di$

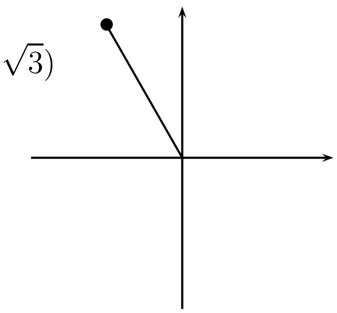
$$\begin{array}{rcl} |\overline{z}w+1| & = & |(a-bi)\cdot(c+di)+1| \\ |\overline{z}w+1| & = & |ac+adi-cbi+bd+1| \\ |\overline{z}w+1| & = & |(ac+bd+1)+(ad-bc)i| \\ |\overline{z}w+1| & = & \sqrt{(ac+bd+1)^2+(ad-bc)^2} \\ |\overline{z}w+1| & = & \sqrt{a^2c^2+b^2d^2+1+2abcd+2bd+2ac+a^2d^2-2abcd+c^2d^2} \\ |\overline{z}w+1| & = & \sqrt{a^2\cdot(c^2+d^2)+b^2\cdot(c^2+d^2)+2ac+2bd+1} \\ |\overline{z}w+1| & = & \sqrt{(a^2+b^2)\cdot(c^2+d^2)+2ac+2bd+1}; \quad |z| = 1 \\ |\overline{z}w+1| & = & \sqrt{c^2+d^2+2ac+2bd+a^2+b^2} \\ |\overline{z}w+1| & = & \sqrt{(a+c)^2+(b+d)^2} \\ |\overline{z}w+1| & = & |z+w| \end{array}$$

♡

Solución 43. Encontrar el Arg(z)

i) $z = -2 + 2\sqrt{3}i$

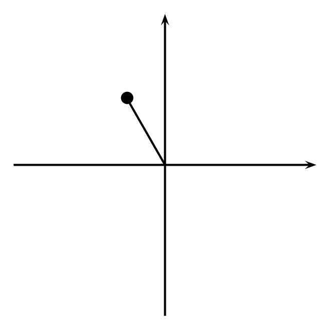
$$\begin{aligned} Arg(z) &= \text{tg}^{-1}\left(\frac{2\sqrt{3}}{-2}\right) = \text{tg}^{-1}(-\sqrt{3}) \\ Arg(z) &= = -60 \\ Arg(z) &= -\frac{\pi}{3} + \pi = \frac{2\pi}{3} \end{aligned}$$



ii) $z = -\dfrac{2}{1 + \sqrt{3}i}$

$$\begin{aligned} z &= -\frac{2}{1+\sqrt{3}i} \cdot \frac{1-\sqrt{3}i}{1-\sqrt{3}i} \\ z &= \frac{-2+2\sqrt{3}i}{1+3} \\ z &= -\frac{1}{2} + \frac{1\sqrt{3}i}{2} \end{aligned}$$

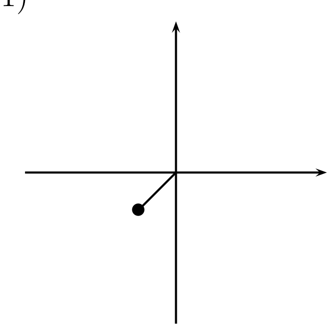
$$\begin{aligned} Arg(z) &= \text{tg}^{-1}\left(\frac{\frac{1}{2}\sqrt{3}}{-\frac{1}{2}}\right) = \text{tg}^{-1}(-\sqrt{3}) \\ Arg(z) &= -60 \\ Arg(z) &= -\frac{\pi}{3} + \pi = \frac{2\pi}{3} \end{aligned}$$



Solución 44.

i) $-\sqrt{2} - \sqrt{2}i$

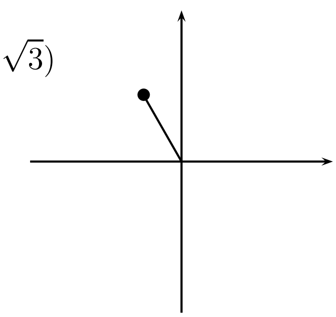
$$\begin{aligned} Arg(z) &= \text{tg}^{-1}\left(\frac{-\sqrt{2}}{-\sqrt{2}}\right) = \text{tg}^{-1}(1) \\ Arg(z) &= 45 \\ Arg(z) &= \frac{\pi}{4} + \pi = \frac{5\pi}{4} \\ |z| &= \sqrt{2+2} = 2 \\ z &= 2 \cdot cis\left(\frac{5\pi}{4}\right) \end{aligned}$$



II) $z = -\dfrac{2}{1+\sqrt{3}i}$

$$\begin{aligned} z &= -\frac{2}{1+\sqrt{3}i} \cdot \frac{1-\sqrt{3}i}{1-\sqrt{3}i} \\ z &= \frac{-2+2\sqrt{3}i}{1+3} \\ z &= -\frac{1}{2} + \frac{1\sqrt{3}i}{2} \end{aligned}$$

$$\begin{aligned} Arg(z) &= \operatorname{tg}^{-1}\left(\frac{\frac{1}{2}\sqrt{3}}{-\frac{1}{2}}\right) = \operatorname{tg}^{-1}(-\sqrt{3}) \\ Arg(z) &= -60 \\ Arg(z) &= -\frac{\pi}{3} + \pi = \frac{2\pi}{3} \\ |z| &= \sqrt{\frac{1}{4}+\frac{3}{4}} = 1 \\ z &= 1 \cdot cis\left(\frac{2\pi}{3}\right) \end{aligned}$$

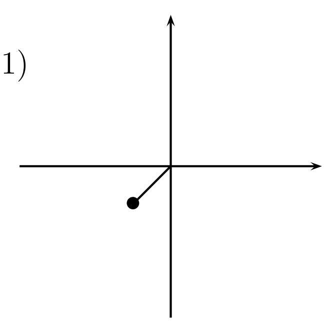


Solución: 45

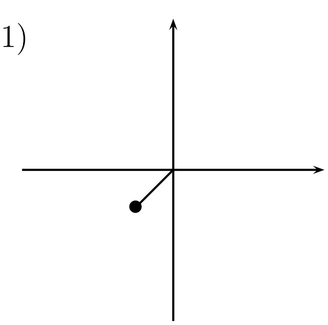
I) $\frac{(-\sqrt{2}-\sqrt{2}i)^{16}}{(-1+i)^4}$

Sean $z_1 = -\sqrt{2} - \sqrt{2}i, \quad z_2 = -1 + i$

$$\begin{aligned} Arg(z_1) &= \operatorname{tg}^{-1}\left(\frac{-\sqrt{2}}{-\sqrt{2}}\right) = \operatorname{tg}^{-1}(1) \\ Arg(z_1) &= 45 \\ Arg(z_1) &= \frac{\pi}{4} + \pi = \frac{5\pi}{4} \\ |z_1| &= \sqrt{2+2} = 2 \\ z_1 &= 2 \cdot cis\left(\frac{5\pi}{4}\right) \end{aligned}$$



$$\begin{aligned} Arg(z_2) &= \operatorname{tg}^{-1}\left(\frac{1}{-1}\right) = \operatorname{tg}^{-1}(-1) \\ Arg(z_2) &= -45 \\ Arg(z_2) &= -\frac{\pi}{4} + \pi = \frac{3\pi}{4} \\ |z_2| &= \sqrt{2} \\ z_2 &= 2^{\frac{1}{2}} \cdot cis\left(\frac{5\pi}{4}\right) \end{aligned}$$



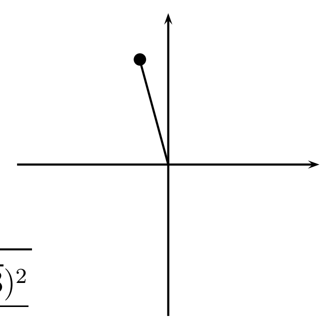
$$\begin{aligned}
\frac{z_1^{16}}{z_2^4} &= \frac{\left(2\cdot cis\left(\frac{5\pi}{4}\right)\right)^{16}}{\left(2^{\frac{1}{2}}\cdot cis\left(\frac{3\pi}{4}\right)\right)^4} = \frac{2^{16}\cdot cis\left(\frac{16\cdot 5\pi}{4}\right)}{2^{\frac{4}{2}}\cdot cis\left(\frac{4\cdot 3\pi}{4}\right)}\\
\frac{z_1^{16}}{z_2^4} &= 2^{14}\cdot cis(20\pi - 3\pi)\\
\frac{z_1^{16}}{z_2^4} &= 2^{14}\cdot(\cos(17\pi) + i\,\mathrm{sen}(17\pi))\\
\frac{z_1^{16}}{z_2^4} &= 2^{14}\cdot(-1+0i)\\
\frac{z_1^{16}}{z_2^4} &= -2^{14}
\end{aligned}$$

II) $\left(\frac{1+\sqrt{3}i}{1-i}\right)^{40}$

Sea $z = \frac{1+\sqrt{3}i}{1-i}$

$$\begin{aligned}
z &= \frac{1+\sqrt{3}i}{1-i}\cdot\frac{1+i}{1+i}\\
z &= \frac{1+i+\sqrt{3}i-\sqrt{3}}{2}\\
z &= \frac{1-\sqrt{3}}{2} + i\frac{1+\sqrt{3}}{2}
\end{aligned}$$

$$\begin{aligned}
Arg(z) &= \mathrm{tg}^{-1}\left(\frac{\frac{1+\sqrt{3}}{2}}{\frac{1-\sqrt{3}}{2}}\right)\\
Arg(z) &= -75\\
Arg(z) &= -\frac{5\pi}{12} + \pi = \frac{7\pi}{12}\\
|z| &= \sqrt{\frac{(1-\sqrt{3})^2}{4} + \frac{(1+\sqrt{3})^2}{4}}\\
|z| &= \sqrt{2}
\end{aligned}$$



Luego, se tiene que

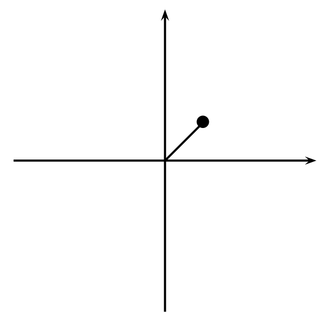
$$z = \left(2^{\frac{1}{2}}\cdot cis\left(\frac{7\pi}{12}\right)\right)$$

$$\begin{aligned}
z^{40} &= 2^{\frac{40}{2}} \cdot cis\left(\frac{40 \cdot 7\pi}{12}\right) = 2^{20} \cdot cis\left(\frac{70\pi}{3}\right) \\
z^{40} &= 2^{20} \cdot \left(\cos\left(\frac{70\pi}{3}\right) + \operatorname{sen}\left(\frac{70\pi}{3}\right)\right) \\
z^{40} &= 2^{20} \cdot \left(-\frac{1}{2} - \frac{\sqrt{3}i}{2}\right) \\
z^{40} &= -2^{19} \cdot (1 + \sqrt{3}i)
\end{aligned}$$

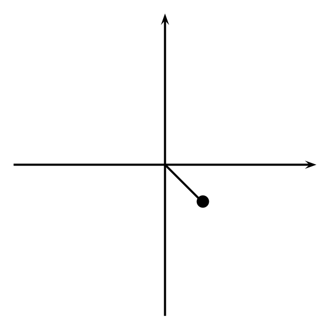
III) $(1+i)^n + (1-i)^n$

Sea $z_1 = 1 + i, \quad z_2 = 1 - i$

$$\begin{aligned}
Arg(z_1) &= \operatorname{tg}^{-1}\left(\frac{1}{1}\right) \\
Arg(z_1) &= 45 \\
Arg(z_1) &= \frac{\pi}{4} \\
|z_1| &= \sqrt{1^2 + 1^2} = \sqrt{2} \\
z_1 &= 2^{\frac{1}{2}} \cdot cis\left(\frac{\pi}{4}\right)
\end{aligned}$$



$$\begin{aligned}
Arg(z_2) &= \operatorname{tg}^{-1}\left(\frac{1}{-1}\right) \\
Arg(z_2) &= -45 \\
Arg(z_2) &= \frac{-\pi}{4} \\
|z_2| &= \sqrt{2} \\
z_2 &= 2^{\frac{1}{2}} \cdot cis\left(\frac{-\pi}{4}\right)
\end{aligned}$$



$$\begin{aligned}
z_1^n + z_2^n &= 2^{\frac{n}{2}} \cdot \left(cis\left(\frac{n\pi}{4}\right) + cis\left(\frac{-n\pi}{4}\right)\right) \\
z_1^n + z_2^n &= 2^{\frac{n}{2}} \cdot \left(\cos\left(\frac{n\pi}{4}\right) + i \operatorname{sen}\left(\frac{n\pi}{4}\right) + \cos\left(\frac{-n\pi}{4}\right) + i\left(\frac{-n\pi}{4}\right)\right) \\
\cos(-x) &= \cos(x) \\
\operatorname{sen}(-x) &= -\operatorname{sen}(x) \\
z_1^n + z_2^n &= 2^{\frac{n}{2}} \cdot \left(\cos\left(\frac{n\pi}{4}\right) + i \operatorname{sen}\left(\frac{n\pi}{4}\right) + \cos\left(\frac{n\pi}{4}\right) - i\left(\frac{n\pi}{4}\right)\right) \\
z_1^n + z_2^n &= 2^{\frac{n}{2}} \cdot 2 \cdot \cos\left(\frac{n\pi}{4}\right)
\end{aligned}$$

Solución 46.

$$\left(\frac{1-z}{z+i}\right)^3 = 1 = cis(0)$$

Las raíces cubica de uno son:

$$cis\left(\frac{2k\pi}{3}\right) \quad k = 0, 1, 2$$

- $k = 0: \quad cis(0) = 1$

$$\begin{aligned} \frac{1-z}{z+i} &= 1 \\ 1-z &= z+i \\ 2z &= 1-i \\ z &= \frac{1}{2} - \frac{1}{2}i \end{aligned}$$

- $k = 1: \quad cis(\frac{2\pi}{3}) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$$\begin{aligned} \frac{1-z}{z+i} &= -\frac{1}{2} + \frac{\sqrt{3}}{2}i \quad / \cdot 2(z+i) \\ 2(1-z) &= (z+i)\cdot\left(-1+\sqrt{3}i\right) \\ 2-2z &= -i - z - \sqrt{3} + z\sqrt{3}i \\ z\cdot(1+\sqrt{3}i) &= 2+\sqrt{3}+i \\ z &= (2+\sqrt{3}+i)\cdot(1+\sqrt{3}i)^{-1} \\ z &= (2+\sqrt{3}+i)\cdot\left(\frac{1}{4} - \frac{\sqrt{3}}{4}i\right) \\ z &= \frac{1}{2} - \frac{\sqrt{3}}{2}i + \frac{\sqrt{3}}{4} - \frac{3}{4}i + \frac{1}{4}i + \frac{\sqrt{3}}{4} \\ z &= \frac{1}{2} + \frac{\sqrt{3}}{2} - \left(\frac{1}{2} + \frac{\sqrt{3}}{2}\right) i \end{aligned}$$

- $k = 2: \quad cis(\frac{4\pi}{3}) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$

$$\begin{aligned} \frac{1-z}{z+i} &= -\frac{1}{2} - \frac{\sqrt{3}}{2}i \quad / \cdot 2(z+i) \\ 2(1-z) &= (z+i)\cdot\left(-1-\sqrt{3}i\right) \\ 1-z &= -i - z + \sqrt{3} - z\sqrt{3}i \\ z\cdot(1-\sqrt{3}i) &= 2-\sqrt{3}+i \\ z &= (2-\sqrt{3}+i)\cdot(1-\sqrt{3}i)^{-1} \end{aligned}$$

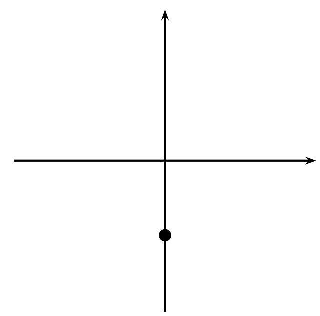
$$\begin{aligned}
z &= (2-\sqrt{3}+i)\cdot\left(\frac{1}{4}+\frac{\sqrt{3}}{4}i\right)\\
z &= \frac{1}{2}+\frac{\sqrt{3}}{2}i-\frac{\sqrt{3}}{4}-\frac{3}{4}+\frac{1}{4}i-\frac{\sqrt{3}}{4}i\\
z &= \frac{1}{2}-\frac{\sqrt{3}}{2}-\left(\frac{1}{2}-\frac{\sqrt{3}}{2}\right)i
\end{aligned}$$

Por lo tanto $z \in \left\{\frac{1}{2}-\frac{1}{2}i,\quad \frac{1}{2}+\frac{\sqrt{3}}{2}-\left(\frac{1}{2}+\frac{\sqrt{3}}{2}\right)i,\quad \frac{1}{2}-\frac{\sqrt{3}}{2}-\left(\frac{1}{2}-\frac{\sqrt{3}}{2}\right)i\right\}$ ♡

Solución 47.

a) Las raíces cúbicas de $-i$. Si $z=-i$, entonces la forma polar es:

$$\begin{aligned}
Arg(z) &= \frac{3\pi}{2}\\
|z| &= \sqrt{1}\\
z &= 1cis\left(\frac{3\pi}{2}\right)
\end{aligned}$$



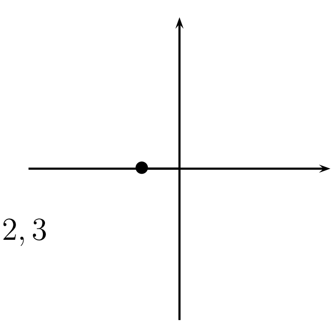
Las raíces cúbicas son

$$z_k = 1\cdot cis\left(\frac{\frac{3\pi}{2}+2k\pi}{3}\right);\quad k=0,1,2$$

- $k=0\quad 1\cdot cis\left(\frac{\pi}{2}\right)=i$
- $k=1\quad 1\cdot cis\left(\frac{7\pi}{6}\right)=1\cdot\left(-\frac{\sqrt{3}}{\sqrt{2}}-\frac{1}{\sqrt{2}}i\right)=-\frac{\sqrt{3}}{2}-\frac{1}{2}i$
- $k=2\quad 1\cdot cis\left(\frac{11\pi}{6}\right)=1\cdot\left(\frac{\sqrt{3}}{\sqrt{2}}-\frac{1}{\sqrt{2}}i\right)=\frac{\sqrt{3}}{2}-\frac{1}{2}i$

b) Las raíces cuárticas de -1. Si $z=-1$, entonces la forma polar:

$$\begin{aligned}
Arg(z) &= \pi\\
|z| &= \sqrt{1}\\
z &= 1cis(\pi)
\end{aligned}$$



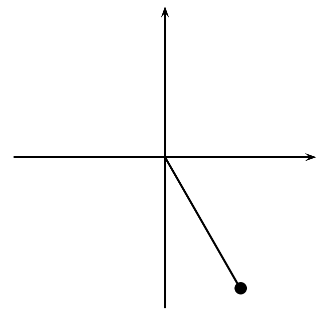
$$z_k = 1\cdot cis\left(\frac{\pi+2k\pi}{4}\right);\quad k=0,1,2,3$$

- $k=0\quad 1\cdot cis\left(\frac{\pi}{4}\right)=1\cdot\left(\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i\right)=\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i$
- $k=1\quad 1\cdot cis\left(\frac{3\pi}{4}\right)=1\cdot\left(-\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i\right)=-\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i$
- $k=2\quad 1\cdot cis\left(\frac{5\pi}{4}\right)=1\cdot\left(-\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i\right)=-\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i$

- $k=3 \quad 1\cdot cis\left(\frac{7\pi}{4}\right)=1\cdot\left(\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i\right)=\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i$

c) Las raíces cuadradas de $2-2\sqrt{3}i$, si $z=2-2\sqrt{3}i$, entonces la forma polar

$$\begin{aligned}Arg(z) &= \operatorname{tg}^{-1}\left(\frac{-2\sqrt{3}}{2}\right)\\ Arg(z) &= -60\\ Arg(z) &= \frac{-\pi}{3}+2\pi=\frac{5\pi}{3}\\ |z| &= \sqrt{4+4\cdot 3}=2\\ z &= 2cis\left(\frac{5\pi}{3}\right)\end{aligned}$$

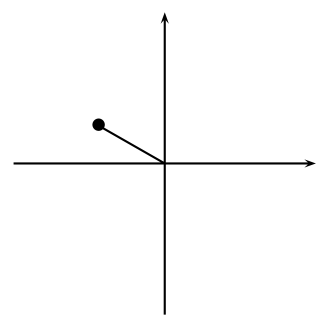


$$z_k=2\cdot cis\left(\frac{\frac{5\pi}{3}+2k\pi}{2}\right);\quad k=0,1$$

- $k=0 \quad 2\cdot cis\left(\frac{5\pi}{6}\right)=2\cdot\left(-\frac{\sqrt{3}}{2}+\frac{1}{2}i\right)=-\sqrt{3}+i$
- $k=1 \quad 2\cdot cis\left(\frac{11\pi}{6}\right)=2\cdot\left(\frac{\sqrt{3}}{2}-\frac{1}{2}i\right)=-\sqrt{3}-i$

d) Las raíces cúbicas de $-\frac{\sqrt{3}}{2}+\frac{1}{2}i$, si $z=-\frac{\sqrt{3}}{2}+\frac{1}{2}i$ entonces la forma polar es:

$$\begin{aligned}Arg(z) &= \operatorname{tg}^{-1}\left(\frac{\frac{1}{2}}{-\frac{\sqrt{3}}{2}}\right)\\ Arg(z) &= -30\\ Arg(z) &= -\frac{\pi}{6}+\pi=\frac{5\pi}{6}\\ |z| &= \sqrt{\frac{3}{4}+\frac{1}{4}}=1\\ |z|^{\frac{1}{3}} &= 1cis\left(\frac{5\pi}{6}\right)\end{aligned}$$



Luego

$$z_k=1\cdot cis\left(\frac{\frac{5\pi}{6}+2k\pi}{3}\right);\quad k=0,1,2$$

- $k=0 \quad 1\cdot cis\left(\frac{5\pi}{18}\right)$
- $k=1 \quad 1\cdot cis\left(\frac{17\pi}{18}\right)$
- $k=2 \quad 1\cdot cis\left(\frac{29\pi}{18}\right)$

♡

Solución 48.

Supongamos que $2+3i$ divide $4+8i$, entonces existen $a, b \in \mathbb{Z}$ tal que:

$$4+8i = (2+3i)\cdot(a+bi)$$

Calculando norma tenemos

$$80 = 13t$$

Lo cual es una contradicción

Por lo tanto $2+3i$ no divide a $4+8i \quad \in \mathbb{Z}[i]$. ♡

Solución: 49 Supongamos que $7+5i$, no es primo, luego existen $z_1 = a_1+b_1i, \quad z_2 = a_2+b_2i$, no invertibles en $\mathbb{Z}[i]$ tales que

$$\begin{aligned} z_1\cdot z_2 &= 7+5i \quad /\|\ \| \\ \|z_1\|\cdot\|z_2\| &= \|7+5i\| \\ \|z_1\|\cdot\|z_2\| &= 74 \\ \|z_1\|\cdot\|z_2\| &= 2\cdot 37 \end{aligned}$$

Una posible solución es:

$$\begin{aligned} \|z_1\| = 2 \quad \wedge \quad \|z_2\| = 37 \\ \|z_1\| &= a_1^2+b_1^2 = 2 \\ \|z_2\| &= a_2^2+b_2^2 = 37 \end{aligned}$$

De la cual se obtiene

$$7+5i = (1-i)\cdot(1+6i)$$

Por lo tanto $7+5i$ no es primo en $\mathbb{Z}[i]$

Solución: 50 Supongamos que 7, no es primo, luego existen $z_1 = a_1+b_1i, \quad z_2 = a_2+b_2i$, no invertibles en $\mathbb{Z}[i]$ tales que

$$\begin{aligned} z_1\cdot z_2 &= 7 \quad /\|\ \| \\ \|z_1\|\cdot\|z_2\| &= \|7\| \\ \|z_1\|\cdot\|z_2\| &= 7^2 \\ \|z_1\| = 7 \quad &\wedge \quad \|z_2\| = 7 \end{aligned}$$

Veremos si es posible que un elemento tenga norma 7, primero notemos que a_1, b_1, no pueden ser múltiplo de 7.

$$\begin{aligned} \|z_1\| = a_1^2+b_1^2 &= 7 \\ a_1^2+b_1^2 &\equiv 0(\texttt{mod } 7) \\ a_1^2 &\equiv -b_1^2(\texttt{mod } 7) \quad /\cdot b_1^{-2}, b_1\neq 0 \\ a_1^2\cdot b_1^{-2} &\equiv -1(\texttt{mod } 7) \\ (a_1\cdot b_1^{-1})^2 &\equiv -1(\texttt{mod } 7) \\ \left(\frac{-1}{7}\right) &= (-1)^{\frac{7-1}{2}} = -1 \end{aligned}$$

Por lo tanto $-1 \not\square_7$, de lo cual se obtiene que 7 es primo en $\mathbb{Z}[i]$. ♡

A.2.4. Polinomios

Solución 51. Si $p(x) = x^4 + ax^2 + bx + 5$, como 1 es raíz de $p(x)$, luego $p(1) = 0$, análogamente $p(-2) = 0$.

$$\begin{array}{rcl} p(1) = 0 & \Leftrightarrow & 1 + a + b + 5 = 0 \\ p(-2) = 0 & \Leftrightarrow & 16 + 4a - 2b + 5 = 0 \end{array}$$

Luego tenemos el sistema

$$\left.\begin{array}{rcl} a + b & = & -6 \\ 4a - 2b & = & 21 \end{array}\right|$$

Amplificando por 2 y sumando obtenemos

$$\begin{array}{rcl} 6a & = & 9 \\ a & = & \dfrac{9}{6} = \dfrac{3}{2} \end{array}$$

Reemplazando

$$b = -6 - a = -6 - \frac{3}{2} = -\frac{15}{2}$$

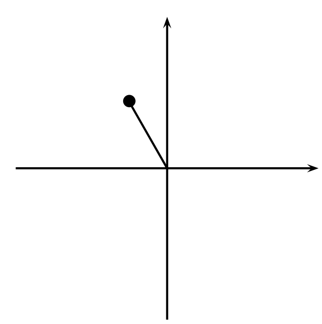
Luego tenemos que $p(x) == x^4 + \frac{3}{2}x^2 - \frac{15}{2}x + 5.$ ♡

Solución 52. Determinar todas las raíces de $x^8 + x^4 + 1$. Sea $u = x^4$, luego $u^2 = x^8$ reemplazando obtenemos

$$\begin{array}{rcl} u^2 + u + 1 & = & 0 \\ u & = & \dfrac{-1 \pm \sqrt{1-4}}{2} = \dfrac{-1 \pm \sqrt{3}i}{2} \\ x^4 & = & \dfrac{-1 \pm \sqrt{3}i}{2} \end{array}$$

Sea $z = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, su forma polar

$$\begin{array}{rcl} Arg(z) & = & \operatorname{tg}^{-1}\left(\dfrac{\frac{\sqrt{3}}{2}}{-\frac{\sqrt{1}}{2}}\right) = -60 \\ Arg(z) & = & -\dfrac{\pi}{3} + \pi = \dfrac{2\pi}{3} \\ |z| & = & \sqrt{\dfrac{1}{4} + \dfrac{3}{4}} = 1 \end{array}$$



Por lo tanto

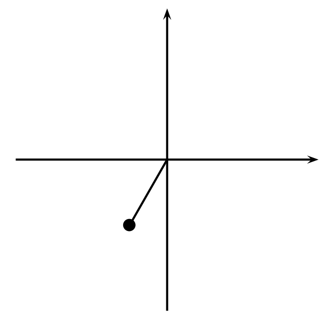
$$z_k = 1 \cdot cis\left(\frac{\frac{2\pi}{3} + 2k\pi}{4}\right); \quad k = 0, 1, 2, 3$$

- $k = 0 \quad z_0 = cis\left(\frac{\pi}{6}\right) = \frac{\sqrt{3}}{2} + \frac{1}{2}i$
- $k = 1 \quad z_1 = cis\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

- $k=2 \quad z_2 = cis\left(\frac{7\pi}{6}\right) = -\frac{\sqrt{3}}{2} - \frac{1}{2}i$
- $k=3 \quad z_3 = cis\left(\frac{5\pi}{3}\right) = \frac{1}{2} - \frac{\sqrt{3}}{2}i$

Ahora sea $w = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$, su forma polar

$$\begin{array}{rcl} Arg(w) & = & \operatorname{tg}^{-1}\left(\frac{\frac{-\sqrt{3}}{2}}{-\frac{\sqrt{1}}{2}}\right) = 60 \\ Arg(w) & = & \frac{\pi}{3} + \pi = \frac{4\pi}{3} \\ |w| & = & \sqrt{\frac{1}{4} + \frac{3}{4}} = 1 \end{array}$$



Luego

$$w = 1 \cdot cis\left(\frac{\frac{4\pi}{3} + 2k\pi}{4}\right); \quad k = 0,1,2,3$$

- $k=0 \quad z_0 = cis\left(\frac{\pi}{3}\right) = \frac{1}{2} + \frac{\sqrt{3}}{2}i$
- $k=1 \quad z_1 = cis\left(\frac{5\pi}{6}\right) = -\frac{\sqrt{3}}{2} + \frac{1}{2}i$
- $k=2 \quad z_2 = cis\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$
- $k=3 \quad z_3 = cis\left(\frac{11\pi}{6}\right) = \frac{\sqrt{3}}{2} - \frac{1}{2}i$

Por lo tanto las raíces de $x^8 + x^4 + 1$ son:

$$\left\{\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{\sqrt{3}}{2} + \frac{1}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i, \frac{\sqrt{3}}{2} - \frac{1}{2}i, \frac{\sqrt{3}}{2} + \frac{1}{2}i, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{\sqrt{3}}{2} - \frac{1}{2}i, \frac{1}{2} - \frac{\sqrt{3}}{2}i\right\}$$

♡

Solución 53. Sea $p(x) = 3x^3 + 2x^2 + cx - k$.

$$\left.\begin{array}{rcl} p(-2) & = & 37 \\ p(1) & = & -2 \end{array}\right|; \qquad \left.\begin{array}{rcl} -24 + 8 - 2c - k & = & 37 \\ 3 + 2 + c - k & = & -2 \end{array}\right|$$

$$\left.\begin{array}{rcl} 2c + k & = & -53 \\ c - k & = & -7 \end{array}\right|$$

Sumando obtenemos

$$\begin{array}{ll} 3c = -60; & c = -20. \\ k = c + 7; & k = -20 + 7 = -13. \end{array}$$

por lo tanto, Sea $p(x) = 3x^3 + 2x^2 - 20x + 13$. ♡

Solución 54. Sea $p(x) = 2x^3 + bx^2 + cx + d$, tal que

- El resto al dividir $p(x)$ por x es $2+b$, es decir, $p(0)=2+b$
- El resto al dividir $p(x)$ por $x+1$ es $b+d$, de otro modo, $p(-1)=b+d$
- 1 es raíz de $p(x)$, por lo tanto $p(1)=0$

$$\left.\begin{array}{rll} 2+b= & p(0) & =d \\ b+d= & p(-1) & =-2+b-c+d \\ 0= & p(0) & =2+b+c+d \end{array}\right|; \qquad \text{simplificando} \qquad \left.\begin{array}{rcr} -b+d & = & 2 \\ c & = & -2 \\ b+d & = & 0 \end{array}\right|$$

De lo cual

$$b=-1 \quad c=-2 \quad d=1$$

Por lo tanto $p(x)=2x^3-x^2-2x+1$. ♡

Solución 55. Como se tiene que $gr((x-2)(x-3)(x-4))=3$, luego el resto debe ser $r(x)=ax^2+bx+c$, sea $p(x)$ tal que,

$$\left.\begin{array}{rcl} p(x) & = & q_1(x)\cdot(x-3)+2 \\ p(x) & = & q_2(x)\cdot(x-2)+0 \\ p(x) & = & q_3(x)\cdot(x-4)+6 \\ p(x) & = & q(x)\cdot(x-3)\cdot(x-2)\cdot(x-4)+ax^2+bx+c \end{array}\right|;$$

Evaluando en 3,2 4, obtenemos

$$\left.\begin{array}{rll} 2= & p(3) & =9a+2b+c \\ 0= & p(2) & =4a+2b+c \\ 6= & p(4) & =16a+4b+c \end{array}\right|; \quad \text{simplificando} \quad \left.\begin{array}{rcr} 9a+2b+c & = & 2 \\ 4a+2b+c & = & 0 \\ 16a+4b+c & = & 6 \end{array}\right|;$$

Despejemos c de la primera ecuación, $c=2-3b-9a$ y lo reemplazamos en la segunda ecuación

$$\begin{array}{rcl} 4a+2b+2-3b-9a & = & 0 \\ b & = & -5a+2 \end{array}$$

Reemplazando en el valor de b obtenemos

$$\begin{array}{rcl} c & = & 2-3\cdot(-5a+2)-9a \\ c & = & 6a-4 \end{array}$$

de este modo tenemos $b=-5a+2;\ c=6a-4$, reemplacemos en la tercera ecuación del sistema

$$\begin{array}{rcl} 16a+4\cdot(-5a+2)+6a-4 & = & 6 \\ 16a-20a+8+6a-7 & = & 6 \\ a & = & 1 \end{array}$$

$$\begin{array}{rcl} b & = & -5a+2=-5+2=-3 \\ c & = & 6a-4=6-4=2 \end{array}$$

Por lo tanto $r(x)=x^2-3x+2$. ♡

Solución 56. Apliquemos división sintética en $p(x)=x^4+ax^3+(a-b)x^2+bx+1$

-1	1	a	$a-b$	b	1
		-1	$-a+1$	$-1+b$	$1-2b$
-1	1	$a-1$	$1-b$	$-1+2b$	$2-2b=0$
		-1	$2-a$	$-3+a+b$	
	1	$a-2$	$3-a-b$	$-4+a+3b=0$	

De lo cual obtenemos el siguientes sistema

$$\left.\begin{array}{rcl} 2-2b & = & 0 \\ -4+a+3b & = & 0 \end{array}\right|$$

Resolviendo el sistema obtenemos

$$b=1; \quad a=1$$

Luego $p(x)=x^4+x^3+x+1$. ♡

Solución 57. Sea $p(x)=6x^3+tx^2+kx-3t$, el enunciados se traduce en el siguiente sistema

$$\left.\begin{array}{rcl} p(2) & = & 21 \\ p(1) & = & 0 \end{array}\right|$$

Reemplazando obtenemos

$$\left.\begin{array}{rcl} 48+4t+2k-3t & = & 21 \\ 6+t+k-3t & = & 0 \end{array}\right|; \quad \text{Simplificando} \quad \left.\begin{array}{rcl} t+2k & = & -27 \\ -2t+k & = & -6 \end{array}\right|$$

Amplificando por 2 y sumando las ecuaciones

$$\begin{array}{rl} 5k=-60; & k=-12 \\ t=-27-2k; & t=-27+24=-3 \end{array}$$

Por lo tanto $k=-12$ y $t=-3$ y $p(x)=6x^3-3x^2-12x+9$. ♡

Solución 58. Sea $p(x)=2x^4+ax^3+28x^2+bx+6$, tal que

$$\left.\begin{array}{rcl} p(1) & = & 0 \\ p(\frac{1}{2}) & = & 0 \end{array}\right|; \quad \text{Evaluando} \quad \left.\begin{array}{rcl} 2+a+28+b+6 & = & 0 \\ \frac{1}{8}+\frac{a}{8}+7+\frac{b}{2}+6 & = & 0 \end{array}\right|$$

Simplificando

$$\left.\begin{array}{rcl} a+b & = & -36 \\ -a-4b & = & 105 \end{array}\right|;$$

Sumando obtenemos

$$\begin{aligned} -3b = 69; &\qquad b = -23 \\ a = -36 - b; &\qquad a = -36 + 23 = -13 \end{aligned}$$

Luego Sea $p(x) = 2x^4 - 13x^3 + 28x^2 - 23x + 6$. ♡

Solución 59. Ya que el $gr((x+1)\cdot(x-1)) = 2$, luego el resto debe ser $r(x) = ax + b$. Sea $p(x) \in \mathbb{R}[x]$ tal que

$$\left.\begin{array}{rcl} p(x) & = & q_1(x)\cdot(x+1) + 2 \\ p(x) & = & q_2(x)\cdot(x-1) + 3 \\ p(x) & = & q(x)\cdot(x+1)\cdot(x-1) + ax + b \end{array}\right|;$$

Evaluando y simplificando obtenemos

$$\left.\begin{array}{rcl} 3 & = & a + b \\ 2 & = & -a + b \end{array}\right|;$$

Luego

$$\begin{aligned} 5 = 2b; &\qquad b = \frac{5}{2} \\ a = -b + 3; &\qquad a = 3 - \frac{5}{2} = \frac{1}{2} \end{aligned}$$

Por lo tanto $r(x) = \frac{1}{2}x + \frac{5}{2}$. ♡

Solución 60. La factorización esta dada por

a) En $\mathbb{Q}[x]$:
$x^6 - 1 = (x^3 - 1)\cdot(x^3 + 1) = (x-1)\cdot(x^2 + x + 1)\cdot(x+1)\cdot(x^2 - x + 1)$

b) En $\mathbb{R}[x]$:
$x^6 - 1 = (x-1)\cdot(x^2 + x + 1)\cdot(x+1)\cdot(x^2 - x + 1)$

c) En $\mathbb{C}[x]$:

$$x^6 - 1 = (x-1)\left(x - \frac{-1+\sqrt{3}i}{2}\right)\left(x - \frac{-1-\sqrt{3}i}{2}\right)(x+1)\left(x - \frac{1+\sqrt{3}i}{2}\right)\left(x - \frac{1-\sqrt{3}i}{2}\right)$$

♡

Solución 61. Sea $p(x) = 2x^4 + ax^3 + 28x^2 + bx + 6$, apliquemos división sintética

1	2	a	28	b	6
		2	$2+a$	$30+a$	$30+a+b$
$\frac{1}{2}$	2	$2+a$	$30+a$	$30+a+b$	$36+a+b=0$
		1	$\frac{3+a}{2}$	$\frac{63+3a}{4}$	
	2	$3+a$	$\frac{63+3a}{2}$	$\frac{183+7a+4b}{4} = 0$	

$$\left.\begin{array}{rcll} a+b & = & -36 & /\cdot -4 \\ 7a+4b & = & -183 & \end{array}\right|; \quad \text{Amplificando} \quad \left.\begin{array}{rcl} -4a-4b & = & 144 \\ 7a+4b & = & -183 \end{array}\right|;$$

Sumando obtenemos

$$\begin{array}{rl} 3a=-39; & a=-13 \\ b=-36-a; & b=-36+13=-23 \end{array}$$

Luego el polinomio es $p(x)=2x^4+-13x^3+28x^2-23x+6$, y se factoriza $p(x)=(x-1)(x-\frac{1}{2})(2x^2-10x+12)$. Veamos ahora el factor cuadrático $2x^2-10x+12$, cuyo discriminante es $\Delta=10^2-4\cdot 2\cdot 12=4$, luego las raíces son

$$x_1=\frac{10+2}{4}=3; \qquad x_2=\frac{10-2}{4}=2$$

Luego el polinomio es

$$p(x)=2\cdot(x-1)\cdot\left(x-\frac{1}{2}\right)\cdot(x-2)\cdot(x-3)$$

♡

Solución 62. Sea $p(x)=x^6-x^5-5x^4+5x^3-36x^2+36x$

a) Determine las raíces racionales de $p(x)$

$p(x)=x\cdot(x^5-x^4-5x^3+5x^2-36x+36)$

1	1	-1	-5	5	-36	36
		1	0	-5	0	-36
	1	0	-5	0	-36	0

$$\begin{array}{rcl} p(x) & = & x\cdot(x-1)\cdot(x^4-5x-36) \\ p(x) & = & x\cdot(x-1)\cdot(x^2-9)\cdot(x^2+4) \\ p(x) & = & x\cdot(x-1)\cdot(x+3)\cdot(x-3)\cdot(x^2+4) \end{array}$$

Raíces racionales $0,1,\pm 3$

b) La factorización de $p(x)$ como producto de polinomios irreducibles en $\mathbb{R}[x]$ es

$$p(x)=x\cdot(x-1)\cdot(x+3)\cdot(x-3)\cdot(x^2+4)$$

c) La factorización de $p(x)$ como producto de polinomios irreducibles en $\mathbb{C}[x]$

$$p(x)=x\cdot(x-1)\cdot(x+3)\cdot(x-3)\cdot(x+2i)\cdot(x-2i)$$

♡

Solución 63. Para factorizar $x^8+x^4+\overline{1}\in\mathbb{Z}_7[x]$, note que 0 no es raíz de $p(x)$, además

$$\begin{array}{rcl} x^7 & \equiv & x(\texttt{mod}\ 7) \quad / \cdot x \\ x^8 & \equiv & x^2(\texttt{mod}\ 7) \end{array}$$

Luego

$$x^4+x^2+\overline{1}=0$$

Realizando el cambio de variable $u=x^2,\ u^2=x^4$ tenemos

$$\begin{array}{rcl} u^2+u+\overline{1} & = & 0 \quad 1\equiv -6(\texttt{mod}\ 7) \\ u^2+u-\overline{6} & = & 0 \\ (u+\overline{3})\cdot(u-\overline{2}) & = & 0 \\ (x^2+\overline{3})\cdot(x^2-\overline{2}) & = & 0 \quad 3\equiv -4(\texttt{mod}\ 7), \quad -2\equiv -9(\texttt{mod}\ 7) \\ (x^2-\overline{4})\cdot(x^2-\overline{9}) & = & 0 \\ (x-\overline{2})\cdot(x+\overline{2})\cdot(x+\overline{3})\cdot(x-\overline{3}) & = & 0 \end{array}$$

Por lo tanto

$$x^8+x^4+\overline{1}=(x-\overline{2})\cdot(x+\overline{2})\cdot(x+\overline{3})\cdot(x-\overline{3})$$

♡

Solución 64. Factorizar $x^4+\overline{4}\in\mathbb{Z}_5[x]$.

$$\begin{array}{rcl} x^4+\overline{4} & = & x^4-\overline{1} \quad 4\equiv -1(\texttt{mod}\ 5) \\ x^4+\overline{4} & = & (x^2-\overline{1})\cdot(x^2+\overline{1}) \quad 1\equiv -4(\texttt{mod}\ 5) \\ x^4+\overline{4} & = & (x-\overline{1})\cdot(x+\overline{1})\cdot(x^2-\overline{4}) \\ x^4+\overline{4} & = & (x-\overline{1})\cdot(x+\overline{1})\cdot(x+\overline{2})\cdot(x-\overline{2}) \end{array}$$

♡

Solución 65 Descomponer $p(x)=x^4+x^3+x^2+x+\overline{1}\in\mathbb{Z}_5[x]$ en factores irreducibles.

1	1	1	1	1	1
		1	2	3	4
1	1	2	3	4	$5=0$
		1	3	6	
1	1	3	6	$10=0$	
		1	4		
1	1	4	$10=0$		
		$5=0$			

Por lo tanto $x^4+x^3+x^2+x+\overline{1}=(x-\overline{1})^4$ ♡

Solución 66. Dado el polinomio $x^3+x^2+x+1=(x-a)\cdot(x-b)\cdot(x-c)$

$$x^3+x^2+x+1 \quad = \quad x^3+x^2\cdot(-a-b-c)+x\cdot(ab+bc+ac)-abc$$

de lo cual obtenemos el siguiente sistema

$$\left.\begin{array}{lcl} -a-b-c & = & 1 \\ ab+bc+ac & = & 1 \\ -abc & = & 1 \end{array}\right|$$

Además, se tiene que

$$(x-a^2)\cdot(x-b^2)\cdot(x-c^2) = x^3 + x^2\cdot(-a^2-b^2-c^2) + x\cdot(a^2b^2+b^2c^2+a^2c^2) - a^2b^2c^2$$

Luego debemos calcular el valor de $a^2b^2c^2$, $(a^2b^2+b^2c^2+a^2c^2)$, $(-a^2-b^2-c^2)$, veamos el primer valor, de la tercera ecuación tenemos

$$\begin{array}{rcl} -abc & = & 1 \quad /()^2 \\ a^2b^2c^2 & = & 1 \quad /\cdot -1 \\ -a^2b^2c^2 & = & -1 \end{array}$$

De la segunda ecuación tenemos

$$\begin{array}{rcl} -a-b-c & = & 1 \quad /()^2 \\ a^2+b^2+c^2+2ab+2bc+2ac & = & 1 \\ a^2+b^2+c^2+2\cdot(ab+bc+ac) & = & 1 \end{array}$$

Reemplazando el valor de la segunda ecuación

$$\begin{array}{rcl} a^2+b^2+c^2+2 & = & 1 \\ a^2+b^2+c^2 & = & -1 \end{array}$$

El último coeficiente lo obtenemos de

$$\begin{array}{rcl} ab+bc+ac & = & 1 \quad /()^2 \\ a^2b^2+b^2c^2+a^2c^2+2aabc+2babc+2cabc & = & 1 \\ a^2b^2+b^2c^2+a^2c^2+2abc\cdot(a+b+c) & = & 1 \end{array}$$

Reemplazando tenemos

$$a^2b^2+b^2c^2+a^2c^2 = -1$$

Por lo tanto el polinomio pedido es $x^3+x^2-x-1 = (x-a^2)\cdot(x-b^2)\cdot(x-c^2)$. ♡

Solución 67. De forma similar obtenemos

$$x^3+2x^2+3x+1 = x^3+x^2\cdot(-a-b-c)+x\cdot(ab+bc+ac)-abc,$$

igualando coeficiente obtenemos

$$\left.\begin{array}{rcl} -a-b-c & = & 2 \\ ab+bc+ac & = & 3 \\ -abc & = & 1 \end{array}\right|$$

Por otro lado necesitamos los valores de

$$(x-a^2)\cdot(x-b^2)\cdot(x-c^2) \quad = \quad x^3 + x^2\cdot(-a^2-b^2-c^2) + x\cdot(a^2b^2+b^2c^2+a^2c^2) - a^2b^2c^2$$

$$-a^2b^2c^2 = (abc)^2 = -1$$

El segundo se obtiene de

$$a^2+b^2+c^2 = (-a-b-c)^2 - 2\cdot(ab+bc+ac) = -2$$

Y el tercero

$$a^2b^2+b^2c^2+a^2c^2 = (ab+bc+ac)^2 - 2abc\cdot(a+b+c) = 5$$

Por lo tanto el polinomio pedido es $x^3+2x^2+5x-1 = (x-a^2)\cdot(x-b^2)\cdot(x-c^2)$. ♡

Solución: 68 Sea $x^3-x^2-1 = (x-a)\cdot(x-b)\cdot(x-c)$, luego

$$x^3-x^2-1 \quad = \quad x^3 - x^2\cdot(a+b+c) + x\cdot(ab+bc+ac) - abc$$

De lo cual se obtiene

$$\left.\begin{array}{rcl} a+b+c & = & 1 \\ ab+bc+ac & = & 0 \\ abc & = & 1 \end{array}\right|$$

Por otro lado

$$\begin{aligned}
& (x-(a+b))\cdot(x-(a+c))\cdot(x-(b+c)) \\
= \; & (x^2-(a+c)x-(a+b)x+(a+b)\cdot(a+c))\cdot(x-(b+c)) \\
= \; & (x^2-x(2a+b+c)+(a+b)\cdot(a+c))\cdot(x-(b+c)) \\
= \; & x^3-x^2(2a+b+c)+x(a+b)(a+c)- \\
& \quad x^2(b+c)+x(2a+b+c)(b+c)-(a+b)(a+c)(b+c) \\
= \; & x^3-x^2(2a+2b+2c)+x(a^2+b^2+c^2+3ab+3bc+3ac)- \\
& \quad (a^2b+a^2c+b^2c+b^2a+ac^2+bc^2+2abc)
\end{aligned}$$

Los coeficientes buscados

$$\begin{aligned}
2a+2b+2c & = 2(a+b+c) = 2 \\
a^2+b^2+c^2+3ab+3bc+3ac & = (a+b+c)^2+(ab+bc+ac) = 1
\end{aligned}$$

Además

$$\begin{aligned}
& a^2b+a^2c+b^2c+b^2a+ac^2+bc^2+2abc \\
= \; & (a+b+c)(ac+ab+bc)-abc = -1
\end{aligned}$$

Por lo tanto el polinomio pedido es x^3-2x^2+x+1. ♡

Solución 69. Factorizar $x^8+\overline{4}\in\mathbb{Z}_5[x]$

$$\begin{aligned}
x^8+\overline{4} &= x^8-\overline{1} \quad 4\equiv -1(\texttt{mod}\ 5)\\
x^8+\overline{4} &= (x^4-\overline{1})\cdot(x^4+\overline{1}) \quad 1\equiv -4(\texttt{mod}\ 5)\\
x^8+\overline{4} &= (x^2-\overline{1})\cdot(x^2+\overline{1})\cdot(x^4-\overline{4})\\
x^8+\overline{4} &= (x-\overline{1})\cdot(x+\overline{1})\cdot(x^2-\overline{4})\cdot(x^2-\overline{2})\cdot(x^2+\overline{2})\\
x^8+\overline{4} &= (x-\overline{1})\cdot(x+\overline{1})\cdot(x-\overline{2})\cdot(x+\overline{2})\cdot(x^2-\overline{2})\cdot(x^2+\overline{2})
\end{aligned}$$

Veremos los polinomios cuadráticos

$$\begin{aligned}
x^2-\overline{2} &\equiv 0(\texttt{mod}\ 5)\\
x^2 &\equiv \overline{2}(\texttt{mod}\ 5)\\
\left(\frac{2}{5}\right) &= (-1)^{\frac{5^2-1}{8}}=-1
\end{aligned}$$

Por lo tanto $2\notin\mathbb{Z}_5$, es decir, $x^2-\overline{2}$ es irreducible en $\mathbb{Z}_5[x]$

$$\begin{aligned}
x^2+\overline{2} &\equiv 0(\texttt{mod}\ 5)\\
x^2 &\equiv -\overline{2}(\texttt{mod}\ 5)
\end{aligned}$$

Veamos si -2 es un cuadrado, para ello calculemos

$$\left(\frac{-2}{5}\right)=\left(\frac{-1}{5}\right)\cdot\left(\frac{2}{5}\right)=(-1)^{\frac{5-1}{2}}(-1)^{\frac{5^2-1}{8}}=1\cdot -1=-1$$

Por lo tanto $-2\notin\mathbb{Z}_5$, es decir, $x^2+\overline{2}$ es irreducible en $\mathbb{Z}_5[x]$, de este modo tenemos que

$$x^8+\overline{4}=(x-\overline{1})\cdot(x+\overline{1})\cdot(x-\overline{2})\cdot(x+\overline{2})\cdot(x^2-\overline{2})\cdot(x^2+\overline{2})$$

♡

Solución 70. El anillo

$$\begin{aligned}
\mathbb{Z}_3[x]/<x^2-\overline{1}> &= \{\overline{ax+b}\mid a,b\in\mathbb{Z}_2\wedge\overline{x^2-1}=\overline{0}\}\\
\mathbb{Z}_3[x]/<x^2-\overline{1}> &= \{\overline{0},\overline{1},\overline{2},\overline{x},\overline{2x},\overline{x+1},\overline{x+2},\overline{2x+1},\overline{2x+2}\}
\end{aligned}$$

La aditiva

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x++2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$	$\overline{x+1}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{x}$	$\overline{2x+2}$	$\overline{2x}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$	$\overline{x+2}$	$\overline{2x+2}$	$\overline{x}$	$\overline{x+1}$	$\overline{2x}$	$\overline{2x+1}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{0}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{1}$	$\overline{2}$
$\overline{2x}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{0}$	$\overline{x}$	$\overline{1}$	$\overline{2}$	$\overline{x+1}$	$\overline{x+2}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{x}$	$\overline{2x+1}$	$\overline{1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2}$	$\overline{0}$
$\overline{x+2}$	$\overline{x+2}$	$\overline{x}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{0}$	$\overline{1}$
$\overline{2x+1}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{1}$	$\overline{x+1}$	$\overline{2}$	$\overline{0}$	$\overline{x+2}$	$\overline{x}$
$\overline{2x+2}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2}$	$\overline{x+2}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$

Ahora la multiplicativa

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{2}$	$\overline{2}$	$\overline{1}$	$\overline{2x}$	$\overline{x}$	$\overline{2x+2}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{x+1}$
$\overline{x}$	$\overline{x}$	$\overline{2x}$	$\overline{1}$	$\overline{2}$	$\overline{x+1}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{2x+1}$
$\overline{2x}$	$\overline{2x}$	$\overline{x}$	$\overline{2}$	$\overline{x}$	$\overline{2x+2}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{x+1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{2x+2}$	$\overline{0}$	$\overline{0}$	$\overline{x+1}$
$\overline{x+2}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{0}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{0}$
$\overline{2x+1}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{0}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{0}$
$\overline{2x+2}$	$\overline{2x+2}$	$\overline{x+1}$	$\overline{2x+1}$	$\overline{x+1}$	$\overline{x+1}$	$\overline{0}$	$\overline{0}$	$\overline{2x+2}$

♡

Solución 71. Dado el cuerpo

$$\mathbb{F}_{27} = \mathbb{Z}_3[x]/ < x^3 + 2x + 1 >= \{\overline{ax^2 + bx + c} \quad | \quad a, b, c \in \mathbb{Z}_3 \wedge \overline{x^3 + 2x + 1} = \overline{0}\}$$

Ya que,

$$x^3 = -2x - 1; \quad x^3 = x + 2; \quad x^4 = x^2 + 2x; \quad x^4 + 1 = x^2 + 2x + 1$$

Ahora busquemos el inverso de $\overline{x^4 + \overline{1}}$

$$\begin{array}{rcl} 1 & = & (x^2 + 2x + 1) \cdot (ax^2 + bx + c) \\ 1 & = & ax^4 + bx^3 + cx^2 + 2ax^3 + 2bx^2 + 2cx + ax^2 + bx + c \\ 1 & = & ax^4 + (b + 2a) \cdot x^3 + (a + c + 2b) \cdot x^2 + (b + 2c) \cdot x + c \\ 1 & = & a \cdot (x^2 + 2x) + (b + 2a) \cdot (x + 2) + (a + c + 2b) \cdot x^2 + (b + 2c) \cdot x + c \\ 1 & = & x^2 \cdot (2a + 2b + c) + x \cdot (4a + 2b + 2c) + 4a + 2b + c \end{array}$$

De lo cual tenemos, el siguiente sistema

$$\left.\begin{array}{rcl} 2a + 2b + c & = & 0 \\ a + 2b + 2c & = & 0 \\ a + 2b + c & = & 1 \end{array}\right|$$

Ahora resolveremos el sistema, los coeficiente esta módulo 3. Despejando de la primera ecuación obtenemos $c = -2a - 2b = a + b$, reemplazando el la segunda ecuación obtenemos $b = 0$, de lo cual $c = a$ reemplazando en la tercera ecuación $a+2b+c = 1$, obtenemos $2a = 1$, y finalmente $a = 2$. Por lo tanto

$$\overline{x^4 + \overline{1}}^{-1} = \overline{\overline{2}x^2 + \overline{2}}$$

♡

Solución 72.

$$\mathbb{F}_{25} \quad = \quad \{\overline{ax + b} \quad | \quad a, b \in \mathbb{Z}_5 \wedge \overline{x^2 + x + 1} = \overline{0}\}$$

Busquemos un representante de $x^7+x^5+x^4+4$, para ello

$$x^7+x^5+x^4+4=(x^2+x+1)(x^5-x^4+x^3+x^2-2x+1)+(x+3)$$

De este modo obtenemos $x^7+x^5+x^4+4=x+3$ en $\mathbb{F}_{25}$.

Ahora busquemos el inverso

$$\begin{array}{rcl}(x+3)\cdot(ax+b) & = & 1\\ (2a+b)\cdot x-a+3b & = & 0\cdot x+1\end{array}$$

de lo cual tenemos el siguiente sistema

$$\left.\begin{array}{rcl}2a+b & = & 0\\ -a+3b & = & 1\end{array}\right|$$

Amplificando por 2, y sumando las ecuaciones tenemos

$$\begin{array}{rl}7b=2; & b=1\\ 2a=-b; & a=2\end{array}$$

Por lo tanto $[x^7+x^5+x^4+4]^{-1}=[2x+1]$ ♡

Solución 73.

$$\begin{array}{rcl}\mathbb{F}_8 & = & \{\overline{ax^2+bx+c} \quad | \quad a,b,c\in\mathbb{Z}_2\wedge\overline{x^3+x+1}=\overline{0}\}\\ \mathbb{F}_8^* & = & \{\overline{1},\overline{x},\overline{x^2},\overline{x+1},\overline{x^2+1},\overline{x^2+x},\overline{x^2+x+1}\}\end{array}$$

Veremos el generado por $\overline{x}$

$$<\overline{x}> \;=\; \{\overline{x},\overline{x^2},\overline{x+1},\overline{x^2+x},\overline{x^2+x+1},\overline{x^2+1},\overline{1}\}$$

Por lo tanto $\mathbb{F}_8^*$ es cíclico, pues $\overline{x}$ es un generador. ♡

Solución 74. Los elementos invertibles son;

$$\begin{array}{rcl}\mathbb{F}_9 & = & \{\overline{ax+b} \quad | \quad a,b\in\mathbb{Z}_3\wedge\overline{x^2+1}=\overline{0}\}\\ \mathbb{F}_9^* & = & \{\overline{1},\overline{2},\overline{x},\overline{2x},\overline{x+1},\overline{x+2},\overline{2x+1},\overline{2x+2}\}\end{array}$$

Ahora veremos los ordenes, recuerde que debe ser un divisor de $9-1=8$

$$\begin{array}{rcl}<\overline{1}> & = & \{\overline{1}\}\\ <\overline{2}> & = & \{\overline{2},\overline{1}\}\\ <\overline{x}> & = & \{\overline{x},\overline{2},\overline{2x},\overline{1}\}\\ <\overline{2x}> & = & \{\overline{2x},\overline{2},\overline{x},\overline{1}\}\\ <\overline{x+1}> & = & \{\overline{x+1},\overline{2x},\overline{2x+1},\overline{2},\overline{2x+2},\overline{x},\overline{x+2},\overline{1}\}\\ <\overline{x+2}> & = & \{\overline{x+2},\overline{x},\overline{2x+2},\overline{2},\overline{2x+1},\overline{2x},\overline{x+1},\overline{1}\}\\ <\overline{2x+1}> & = & \{\overline{2x+1},\overline{x},\overline{x+1},\overline{2},\overline{x+2},\overline{2x},\overline{2x+2},\overline{1}\}\\ <\overline{2x+2}> & = & \{\overline{2x+2},\overline{2x},\overline{x+2},\overline{2},\overline{x+1},\overline{x},\overline{2x+1},\overline{1}\}\end{array}$$

elemento	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x+2}$
orden	1	2	4	4	8	8	8	8

♡

Solución 75. Necesitamos saber si x^2-8 es irreducible en $\mathbb{Z}_{19}$, lo cual depende si 8 es un cuadrado

$$\left(\frac{8}{19}\right) = \left(\frac{2^2}{19}\right)\cdot\left(\frac{2}{19}\right) = 1(-1)^{\frac{19^2-1}{8}} = -1$$

Por lo tanto, $8 \notin \square_{19}$, es decir, x^2-8 es irreducible, luego $\mathbb{Z}_{19}[x]/<x^2-8>$ es un cuerpo. ♡

Solución 76. El polinomio x^2+1 irreducible en $\mathbb{Z}_3$, luego

$$\begin{aligned}\mathbb{F}_9 &= \{\overline{ax+b} \quad | \quad a,b\in\mathbb{Z}_3 \wedge \overline{x^2+1}=\overline{0}\}\\ \mathbb{F}_9 &= \{\overline{1},\overline{2},\overline{x},\overline{2x},\overline{x+1},\overline{x+2},\overline{2x+1},\overline{2x+2}\}\end{aligned}$$

$$\begin{aligned}\overline{-1}^2=\overline{1}^2 &= \overline{1}\\ \overline{-x}^2=\overline{x}^2 &= \overline{2}\\ \overline{2x+2}^2=\overline{x+1}^2 &= \overline{x^2+2x+1}=\overline{-1+2x+1}=\overline{2x}\\ \overline{2x+1}^2=\overline{x+2}^2 &= \overline{x^2+4x+4}=\overline{-1+x+1}=\overline{x}\end{aligned}$$

Luego los cuadrados son

$$\square_{\mathbb{F}_9}=\{\overline{1},\overline{2},\overline{x},\overline{2x}\}$$

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$
$\overline{2}$	$\overline{2}$	$\overline{1}$	$\overline{2x}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{2x}$	$\overline{2}$	$\overline{1}$
$\overline{2x}$	$\overline{2x}$	$\overline{x}$	$\overline{1}$	$\overline{2}$

♡

Solución 77. Para que no se un cuerpo es necesario que $x^2-\alpha$ sea reducible, luego la ecuación

$$\begin{aligned}x^2-\alpha &\equiv 0(\texttt{mod}\ 7)\\ x^2 &\equiv \alpha(\texttt{mod}\ 7)\end{aligned}$$

Debe tener solución, luego $\alpha=0\vee\alpha\in\square_7$

Pero

$$\square_7=\{\overline{1},\overline{4},\overline{2}\}$$

Por lo tanto $\alpha\in\{\overline{0},\overline{1},\overline{2},\overline{4}\}$. ♡