

UNIVERSITAT DE BARCELONA

EXERCICIS

SEGON SEMESTRE

Aritmètica (ARI)

Autor:

Mario VILAR

Professor:

Dr. Luis DIEULEFAIT

7 de juny de 2021



UNIVERSITAT DE
BARCELONA

Aquesta obra està subjecta a una llicència de Creative Commons “Reconeixement-NoComercial-SenseObraDerivada 4.0 International”.



1
LABORATORI

1.1 Bases

Exercici 1.1.

- En quina base el nombre 136 s'escriu 2 5 3?
- En quina base el nombre 621 s'escriu 2 5 1 3?

Resolució. Primerament, resoldrem el primer apartat. Hem de trobar una base b_1 tal que

$$2 \cdot b_1^2 + 5 \cdot b_1 + 3 = 1 \cdot 10^2 + 3 \cdot 10^1 + 6 \iff 2 \cdot b_1^2 + 5 \cdot b_1 + 3 = 136. \quad (1.1.1)$$

resolent l'equació per Ruffini:

$$\begin{array}{c|ccc} & 2 & 5 & -133 \\ \hline 7 & & 14 & 133 \\ \hline & 2 & 19 & 0 \end{array} \implies \begin{cases} b_1 = 7, \\ b_1 = \frac{-19}{2}, \end{cases} \quad (1.1.2)$$

de les quals descartem la segona. Així, $b_1 = 7$.

Pel que fa a la segona expressió, es resol de manera anàloga: hem de trobar una base b_2 tal que

$$2 \cdot b_2^3 + 5 \cdot b_2^2 + b_2 + 3 = 621. \quad (1.1.3)$$

Per Ruffini:

$$\begin{array}{c|cccc} & 2 & 5 & 1 & -618 \\ \hline 6 & & 12 & 102 & 618 \\ \hline & 2 & 17 & 103 & 0 \end{array} \implies \begin{cases} b_1 = 6, \\ b_1 = \frac{1}{6}, \end{cases} \quad (1.1.4)$$

així doncs, la solució és $b_2 = 6$. ■

Exercici 1.2.

- Escriviu el nombre $(235\ 678\ 943\ 215)_{1000}$ en base 10 i en base 100.
- Escriviu el nombre $(ABCDEF01234)_{16}$ en les bases 2, 4 i 8.

Resolució. resolem els dos apartats separadament. En primer lloc, tenim:

$$(235\ 678\ 943\ 215)_{1000} = (23\ 56\ 78\ 94\ 32\ 15)_{100} = (2\ 3\ 5\ 6\ 7\ 8\ 9\ 4\ 3\ 2\ 1\ 5)_{10}. \quad (1.2.1)$$

Això és així perquè $1000 = 10^3$, és a dir,

Proposició 1.2.1. *Les xifres de l'expressió en base b^k de qualsevol nombre són els nombres naturals les expressions dels quals en base b s'obtenen en agrupar de k en k les xifres de l'expressió de x en base b .*

En segon lloc, veiem que:

$$\left\{ \begin{array}{l} (A)_{16} = (10)_{10} = (1010)_2 \\ (B)_{16} = (11)_{10} = (1011)_2 \\ (C)_{16} = (12)_{10} = (1100)_2 \\ (D)_{16} = (13)_{10} = (1101)_2 \\ (E)_{16} = (14)_{10} = (1110)_2 \\ (F)_{16} = (15)_{10} = (1111)_2 \\ (0)_{16} = (0)_{10} = 0000_2 \\ (1)_{16} = (1)_{10} = 0001_2 \\ (2)_{16} = (2)_{10} = 0010_2 \\ (3)_{16} = (3)_{10} = 0011_2 \\ (4)_{16} = (4)_{10} = 0100_2 \end{array} \right. \implies (10101011110011011110111100000001001000110100)_2 \quad (1.2.2)$$

Ara, per 1.2.1 tenim:

$$(10\ 10\ 10\ 11\ 11\ 00\ 11\ 01\ 11\ 10\ 11\ 11\ 00\ 00\ 00\ 01\ 00\ 10\ 00\ 11\ 01\ 00)_4, \quad (1.2.3)$$

i si apliquem la conversió:

$$(2223303132330001020310)_4 \quad (1.2.4)$$

Aplicant anàlogament 1.2.1 per $2^3 = 8$:

$$(010\ 101\ 011\ 110\ 011\ 011\ 110\ 111\ 100\ 000\ 001\ 001\ 000\ 110\ 100)_8 \implies (253633674011064)_8. \quad (1.2.5)$$

Notem que això és un pas intermig per passar de binari a base 4. En cap cas això podria ser el resultat final. ■

1.2 Euclides i primers

Exercici 1.3.

- Trobeu el màxim comú divisor i el mínim comú múltiple dels nombres enters 2047 i 2225.
- Trobeu el màxim comú divisor i el mínim comú múltiple dels nombres enters 2200 i 2816.

Resolució. Utilitzarem l'algorisme d'Euclides, que diu:

Algorithm 1 Euclid's algorithm

```

1: procedure EUCLID( $a, b$ ) ▷ El m.c.d. d' $a$  i  $b$ 
2:    $r \leftarrow a \bmod b$ 
3:   while  $r \neq 0$  do ▷ Si  $r$  és 0 ja hem acabat
4:      $a \leftarrow b$ 
5:      $b \leftarrow r$ 
6:      $r \leftarrow a \bmod b$ 
7:   return  $b$  ▷ El m.c.d. és  $b$ 

```

Aleshores,

$$\begin{array}{r} 2225 \end{array} \left| \begin{array}{r} 2047 \\ -2047 \\ \hline 178 \end{array} \right. \implies \begin{array}{r} 2047 \end{array} \left| \begin{array}{r} 178 \\ -1958 \\ \hline 89 \end{array} \right. \implies \begin{array}{r} 178 \end{array} \left| \begin{array}{r} 89 \\ -178 \\ \hline 0 \end{array} \right. \implies \text{mcd}(2047, 2225) = 89 \quad (1.3.1)$$

$$\text{mcm}(2225, 2047) = \frac{2047 \cdot 2225}{\text{mcd}(2225, 2047)} = 51175. \quad (1.3.2)$$

Anàlogament,

$$\begin{array}{r} 2816 \mid 2200 \\ -2200 \\ \hline 616 \end{array} \implies \begin{array}{r} 2200 \mid 616 \\ -1848 \\ \hline 352 \end{array} \implies \begin{array}{r} 616 \mid 352 \\ -352 \\ \hline 1 \end{array} \implies \begin{array}{r} 352 \mid 264 \\ -264 \\ \hline 88 \end{array} \implies \begin{array}{r} 264 \mid 88 \\ -264 \\ \hline 0 \end{array}$$

$$\implies \text{mcd}(2816, 2200) = 88 \implies \text{mcm}(2816, 2200) = \frac{2816 \cdot 2200}{\text{mcd}(2816, 2200)} = 70400 \quad (1.3.3)$$

■

Exercici 1.4.

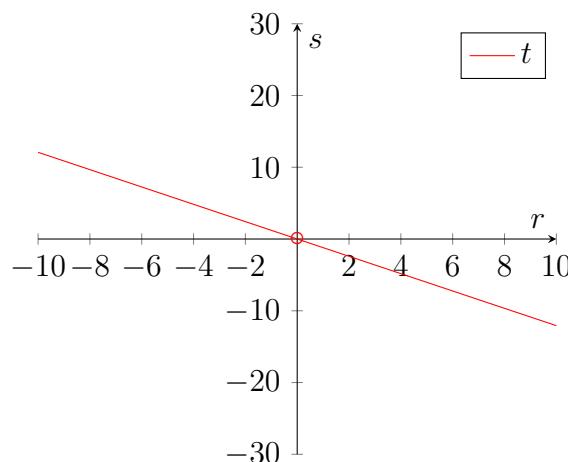
- Trobeu el màxim comú divisor $d > 0$ de la parella de nombres enters $a = 2795$ i $b = 2314$.
- Trobeu nombres enters r, s tals que $d = ra + sb$.
- Feu el mateix per a la parella $a = 2842$, $b = 3567$.

Resolució. Apliquem un procediment totalment anàleg a l'exercici anterior:

$$\begin{array}{r} 2795 \mid 2314 \\ -2314 \\ \hline 481 \end{array} \implies \begin{array}{r} 2314 \mid 481 \\ -1924 \\ \hline 390 \end{array} \implies \begin{array}{r} 481 \mid 390 \\ -390 \\ \hline 91 \end{array} \implies \begin{array}{r} 390 \mid 91 \\ -360 \\ \hline 26 \end{array} \implies \begin{array}{r} 91 \mid 26 \\ -78 \\ \hline 13 \end{array}$$

$$\implies \begin{array}{r} 26 \mid 13 \\ -26 \\ \hline 0 \end{array} \implies d = \text{mcd}(2795, 2314) = 13 > 0. \quad (1.4.1)$$

resolem l'apartat (b). Tenim que $2795r + 2314s = 13$, és a dir, una equació lineal de dues incògnites. La seva solució, doncs, és una recta t de \mathbb{R}^2 i volem trobar $(x, y) \in t \mid (x, y) \in (\mathbb{Z} \times \mathbb{Z} \setminus (0, 0))$. Aïllant s , tenim:



Amb la identitat de Bézout podem, doncs, trobar aquests $x, y \in \mathbb{Z}$. Recordem que és el que se'ns demana a l'enunciat:

Proposició 1.4.1 (Identitat de Bézout). *Si $d = (a, b)$, llavors $\exists x_0, y_0 \in \mathbb{Z} \mid d = ax_0 + by_0$. d és combinació lineal entera d'a, b.*

$$13 = 91 - 26 \cdot 3 \xrightarrow{26=390-91 \cdot 4} -390 \cdot 3 + 91 \cdot 13 \xrightarrow[390=2314-481 \cdot 4]{91=481-390} -2314 \cdot 16 + 481 \cdot 77 \xrightarrow{481=2795-2314} \\ 2795 \cdot 77 + 2314 \cdot -93 \implies r = 77, s = -93. \quad (1.4.2)$$

resolem (c) directament. Calculem $\text{mcd}(2842, 3567)$ amb l'algorisme d'Euclides. Com a resultat, tenim $\text{mcd}(2842, 3567) = 29$.

$$29 = 667 - 58 \cdot 11 \xrightarrow{58=725-667} -725 \cdot 11 + 667 \cdot 12 \xrightarrow{667=2842-723 \cdot 3} -725 \cdot 46 + 2842 \cdot 12 \xrightarrow{725=3567-2842} \\ 3567 \cdot (-47) + 2842 \cdot 59 \implies r = -47, s = 59. \quad (1.4.3)$$

Exercici 1.5. Calculeu, per a tot nombre enter n , $\text{mcd}(28n - 5, 35n - 8)$

Resolució. Simplement, tornem a utilitzar l'algorisme d'Euclides per calcular el màxim comú divisor:

$$\begin{array}{r}
 35n - 8 \quad | \quad 28n - 5 \\
 -28n + 5 \quad | \quad 1 \\
 \hline
 7n - 3
 \end{array} \implies
 \begin{array}{r}
 28n - 5 \quad | \quad 7n - 3 \\
 -28n + 12 \quad | \quad 4 \\
 \hline
 7
 \end{array} \implies
 \begin{array}{r}
 7n - 3 \quad | \quad 7 \\
 -7n \quad | \quad n \\
 \hline
 -3
 \end{array} \implies
 \begin{array}{r}
 7 \quad | \quad -3 \\
 -6 \quad | \quad 2 \\
 \hline
 1
 \end{array}$$

$\implies \begin{array}{r} -3 \quad | \quad 1 \\ +3 \quad | \quad -3 \\ \hline 0 \end{array} \implies \text{mcd}(28n - 5, 35n - 8) = 1, \forall n \in \mathbb{Z}$ (1.5.1)

Exercici 1.6. Siguin $a, b \in \mathbb{Z}$ nombres enters tals que $a > 0, b > 0$ i $\text{mcd}(a, b) = 1$.

1. Demostreu que si $ab = c^2$, per a algun nombre enter c , llavors existeixen $x, y \in \mathbb{Z}$ tals que $a = x^2$, $b = y^2$, i $\text{mcd}(x, y) = 1$.
 2. Doneu un exemple que ensenyi que en el cas en què no sigui $\text{mcd}(a, b) = 1$ es pot tenir una igualtat de la forma $ab = c^2$, amb $c \in \mathbb{Z}$, però a i b no quadrats.

Resolució. En (1) se'ns demana, en essència, que provem:

$$ab = c^2 \implies \exists x, y \in \mathbb{Z} \mid a = x^2, b = y^2 \wedge \text{mcd}(x, y) = 1. \quad (1.6.1)$$

Considerem $c = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n} \implies c^2 = p_1^{2c_1} p_2^{2c_2} \cdots p_n^{2c_n} = ab$. Siguin p_1, \dots, p_k els primers $\in \{p_1, \dots, p_n\}$ tals que $p_1, \dots, p_k | a$ i siguin p_{k+1}, \dots, p_n els primers $\in \{p_{k+1}, \dots, p_n\}$ tals que $p_{k+1}, \dots, p_n | a$. Definim el següent lemma

Lema 1.6.1. Si $p_i | a \Rightarrow p_i \nmid b$, ja que $\text{mcd}(a, b) = 1$.

$$\begin{aligned} a = p_1^{2c_1} \cdots p_k^{2c_k} \\ b = p_{k+1}^{2c_{k+1}} \cdots p_n^{2c_n} \end{aligned} \implies \text{Si } \begin{cases} x = p_1^{c_1} \cdots p_k^{c_k} \in \mathbb{Z} \\ y = p_{k+1}^{c_{k+1}} \cdots p_n^{c_n} \end{cases} \implies a = x^2 \\ b = y^2. \quad (1.6.2)$$

Exercici 1.7. Siquin $a, b \in \mathbb{Z}$ nombres enters.

- Proveu que si $\text{mcd}(a, b) = 1$, llavors $\text{mcd}(a^n, b^n) = 1$, per a tot nombre natural n .

- Proveu que si $\text{mcd}(a, b) = d$, llavors $\text{mcd}(a^n, b^n) = d^n$, per a tot nombre natural n .

Resolució. resolem, primerament, (a). Descomposant tant a com b en factors primers, i tenint en compte que no tenen factors comuns, tenim:

$$\mathbf{a} = a_1 a_2 a_3 \dots a_k; \quad \mathbf{b} = b_1 b_2 \dots b_\ell, \quad a_i \neq b_i, \forall i \mid 1 \leq i \leq k, \quad 1 \leq i \leq \ell. \quad (1.7.1)$$

Si elevem ambdós termes a n , tenim:

$$\mathbf{a}^n = (a_1 a_2 a_3 \dots a_k)^n = a_1^n a_2^n \dots a_k^n; \quad \mathbf{b}^n = (b_1 b_2 \dots b_\ell)^n = b_1^n b_2^n \dots b_\ell^n. \quad (1.7.2)$$

Com a i b no tenien factors comuns, aleshores a^n i b^n tampoc en tindran. Així, $\text{mcd}(a^n, b^n) = 1$.

Ara provem (b). Per l'enunciat, a i b tenen un factor en comú, d . Suposem que a i b esdevenen de la multiplicació de k i ℓ factors, respectivament. Reordenant si cal, per la commutativitat de la multiplicació en \mathbb{R} , suposem d l'últim factor:

$$\mathbf{a} = a_1 a_2 a_3 \dots a_{k-1} \cdot d; \quad \mathbf{b} = b_1 b_2 \dots b_{\ell-1} \cdot d, \quad a_i \neq b_i, \forall i \mid 1 \leq i \leq k-1, \quad 1 \leq i \leq \ell-1. \quad (1.7.3)$$

Per tant,

$$\mathbf{a}^n = a_1^n a_2^n a_3^n \dots a_{k-1}^n \cdot d^n; \quad \mathbf{b}^n = b_1^n b_2^n \dots b_{\ell-1}^n \cdot d^n. \quad (1.7.4)$$

Per l'apartat anterior, sabem que $\text{mcd}(\frac{a^n}{d^n}, \frac{b^n}{d^n}) = 1$. Aleshores, $\text{mcd}(a^n, b^n) = d^n$. ■

Exercici 1.8.

- Proveu que, per a tot nombre enter n , és $\text{mcd}(n, n+1) = 1$.
- Sigui $k \in \mathbb{Z}$ un nombre enter tal que, per a tot $t \in \mathbb{N}$, és $\text{mcd}(t, t+k) = 1$. Demostreu que $k = \pm 1$.
- Esbrineu per a quins valors de $k \in \mathbb{Z}$ es té que, per a tot $s \in \mathbb{N}$, és $\text{mcd}(s, s+k) = 2$.

Resolució. Provem el primer apartat. Suposem que $\text{mcd}(n, n+1) \neq 1$, $\forall n \in \mathbb{Z}$. Podem dir, doncs, que tenen un factor en comú $d \neq 1$. En altres paraules,

$$\begin{aligned} \mathbf{n} &= \alpha_1 \alpha_2 \dots \alpha_{k-1} \cdot d; \quad \mathbf{n+1} = \beta_1 \beta_2 \dots \beta_{\ell-1} \cdot d, \quad \alpha_i, \beta_i \in \mathbb{Z}, \quad 1 \leq i \leq k, \quad 1 \leq i \leq \ell \\ n+1 &= (\alpha_1 \alpha_2 \dots \alpha_{k-1} \cdot d) + 1 \implies \beta_1 \beta_2 \dots \beta_{\ell-1} = (\alpha_1 \alpha_2 \dots \alpha_{k-1} + \frac{1}{d}) \notin \mathbb{Z} \iff \frac{1}{d} \notin \mathbb{Z}, \end{aligned} \quad (1.8.1)$$

però $\beta_1 \beta_2 \dots \beta_{\ell-1} \in \mathbb{Z}$ per hipòtesi. Aquesta contradicció ve de suposar $\text{mcd}(n, n+1) \neq 1$. Així doncs, $\text{mcd}(n, n+1) = 1$.

Pel que fa al segon apartat, hem de tenir en compte el següent lema:

Lema 1.8.1.

$$\text{mcd}(a, b) = \text{mcd}(\pm a, \pm b) = \text{mcd}(a, b \pm a). \quad (1.8.2)$$

Així doncs,

$$\text{mcd}(t, t+k) = \text{mcd}(t, k) = \text{mcd}(t, -k) = 1 \quad (1.8.3)$$

D'aquesta manera, és fàcil veure que $\text{mcd}(t, 1) = 1, \forall t \in \mathbb{N}$. Anàlogament, $\text{mcd}(t, -1) = 1, \forall t \in \mathbb{N}$. Per tant, $k = \pm 1$.

Per últim, volem trobar un $k \in \mathbb{Z}$ tal que $\forall s \in \mathbb{N}$ es doni que $\text{mcd}(s, s+k) = 2$. Podem refutar aquest enunciat trobant un valor de s pel qual no es compleix per a cap valor de k . Sigui $k = 1 \in \mathbb{N}$:

$$\text{mcd}(1, 1+k) \neq 2, \quad \forall k \in \mathbb{Z}. \quad (1.8.4)$$

1.3 Complexos

Exercici 1.9. Escriviu en forma binòmica els nombres complexos $3e^{\frac{3\pi}{4}i}$, $12e^{-\frac{22\pi}{3}i}$, $19e^{\frac{14\pi}{2}i}$, $i(-\sqrt{3} + i)^8$

Resolució. $z = 3e^{\frac{3\pi}{4}i} = 3 \cos(\frac{3\pi}{4}) + i \sin(\frac{3\pi}{4}) = 3(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) = \frac{3\sqrt{2}}{2} - \frac{3\sqrt{2}}{2}i$. La resta els deixem com a exercici. Farem l'últim, ja que és el més difícil. Ens queda:

$$\begin{aligned} z &= (((-\sqrt{3} + i)^2)^2)^2, \\ |z| &= \sqrt{(-\sqrt{3})^2 + 1^2} = \sqrt{4} = 2 \\ \alpha &= \arctan(-\frac{1}{\sqrt{3}}) \implies \alpha_1 = -\frac{\pi}{6}, \alpha_2 = \frac{5\pi}{6}. \\ (2^{\frac{5\pi}{6}})^8 &\iff (2^{\frac{5\pi}{6}})^8 \iff 256^{\frac{2\pi}{3}} \\ 256^{\frac{2\pi}{3}} &= 256 \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) = -128 + 128\sqrt{3}i. \end{aligned} \quad (1.9.1)$$



Observació 1.9.1. Quan donem l'angle ens quedem amb el menor positiu, és a dir, farem una espècie de mòdul. Per conveni, intentarem donar el menor angle entre 0 i 2π .

Exercici 1.10. Escriviu en forma polar els complexos $\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, $5\sqrt{2} - 5i\sqrt{2}$, $\frac{i}{2}$.

Resolució. Per no estendre'ns molt, escriurem la del primer nombre, ja que és la més farragosa.

$$\begin{aligned} \sqrt{(5\sqrt{2})^2 + (-5\sqrt{2})^2} &= \sqrt{100} = 10 \\ \alpha &= \arctan(-1) = -\frac{\pi}{4} \\ 10^{\frac{7\pi}{4}} &= 10e^{\frac{7\pi}{4}i}. \end{aligned} \quad (1.10.1)$$



Exercici 1.11. Trobeu quatre nombres complexos diferents z_1, z_2, z_3, z_4 tals que $z_j^4 = 1$, per a $j = 1, 2, 3, 4$.

Resolució. Tenim que $(z)^4 = (r_\alpha)^4 = 1_{2\pi k}, \forall k \in \mathbb{Z} \implies r = 1, a = \frac{2\pi k}{4}$, amb $k \in \{0, 1, 2, 3\}$. Així doncs,

$$\begin{aligned} z_1 &= 1_0 = \cos(0) + i \sin(0) = 1, \\ z_2 &= 1_{\frac{\pi}{2}} = \cos\left(\frac{\pi}{2}\right) + i \sin\left(\frac{\pi}{2}\right) = i, \\ z_3 &= 1_\pi = \cos(\pi) + i \sin(\pi) = -1, \\ z_4 &= 1_{\frac{3\pi}{2}} = \cos\left(\frac{3\pi}{2}\right) + i \sin\left(\frac{3\pi}{2}\right) = -i. \end{aligned} \quad (1.11.1)$$



1.4 Mersenne, Fermat, perfectes

Exercici 1.12. Comproveu que els nombres de Mersenne M_2, M_3, M_5, M_7 són primers, però que el nombre de Mersenne M_{11} no ho és. Sabeu trobar algun altre nombre de Mersenne que sigui primer? I algun altre que sigui compost?

Resolució. Recordem que un nombre de Mersenne es defineix de la següent manera: $M_n = 2^n - 1$. Aleshores, $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, però $M_{11} = 2^{11} - 1 = 23 \cdot 89$.

Observació 1.12.1. De fet, M_{11} és el nombre de Mersenne compost d'exponent primer més petit.

Per trobar un nombre de Mersenne compost solament cal fixar-se en la proposició que vam demostrar a *Problemes* en el seu moment, el contrarrecíproc de la qual ens diu que per a una n composta tenim un M_n compost. Aleshores, $M_4 = 15 = 3 \cdot 5$ i ja hauríem acabat. Per trobar un nombre de Mersenne primer no tenim més alternativa que usar una metodologia basada en força bruta. A partir de 1.12.1 veiem que agafant $M_{13} = 2^{13} - 1 = 8191$, el qual és primer. ■

Exercici 1.13. El nombre $p := 57885161$ és primer. Demostreu-ho. Podem pensar en el nombre de Mersenne M_p . Quantes xifres té l'expressió decimal de M_p ?

Resolució. La comprovació que p és primer és rutinària a partir de PTFermat. Es pot veure immediatament que en forma binària té 2^p xifres. Aleshores, $\log_{10}(2^p) = p \log_{10}(2) = 17425170$ xifres. ■

Exercici 1.14. Comproveu que els nombres de Fermat F_0, \dots, F_4 són primers i que 641 és un divisor propi de F_5 , de manera que F_5 és compost. Sabeu trobar algun altre nombre de Fermat que sigui primer? I algun altre que sigui compost?

Resolució. $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$. Ara, $F_5 = 4294967297$ i $\frac{F_5}{641} = 6700417 \in \mathbb{Z}$. Fins a dia d'avui no s'ha pogut trobar un primer de Fermat més gran que F_4 . Tenim, en canvi, que F_6 és compost, ja que $F_6 = 641 \cdot 6700417$. ■

Exercici 1.15. Un nombre enter positiu es diu que és perfecte quan és igual a la suma de tots els seus divisors, llevat d'ell mateix. És a dir, quan $\rho_1(n) = 2n$.

1. Comproveu que $6, 28, 496, 8128$ són els quatre primers nombres perfectes.
2. Cerqueu informació sobre nombres perfectes parells.
3. Cerqueu informació sobre nombres perfectes senars.

Resolució. Tenim que $6 = 2+3+1$, $28 = 1+2+4+7+14$, $496 = 1+2+4+8+16+31+62+124+248$, $8128 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064$. Primer de tot, no està demostrada l'existència de nombres senars perfectes. A més, segons [Hag80], un nombre perfecte senar ha de tenir, com a mínim, 8 factors primers i, per [BCR91], no existeix tal nombre per sota de 10^{300} .

Euler va provar que tots els nombres parells perfectes són de la forma $2^{p-1}(2^p - 1)$, on p i $2^p - 1$ són primers ([Coh81], [Jia18]), en particular essent $2^p - 1$ un nombre primer de Mersenne. ■

Exercici 1.16. Demostreu que $2^{p-1}(2^p - 1)$ és un nombre perfecte quan $M_p = 2^p - 1$ és un nombre primer de Mersenne.

Demostració. La demostració és directa quan tenim en compte que els dos nombres han de ser primers per la resolució anterior. Amb més detall, $\sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\sigma(2^p - 1)$. Usant que

$$\sigma_1(n) = \prod_{i=1}^r \frac{p_i^{a_i+1} + 1}{p_i - 1}, \quad (1.16.1)$$

amb $n = p_1^{a_1} \cdots p_r^{a_r}$, ens queda:

$$\sigma(2^{p-1}(2^p - 1)) = \frac{2^p - 1}{2 - 1} \frac{(2^p - 1)^2 - 1}{2^p - 1 - 1} = (2^p - 1)(2^p - 1 + 1) = 2^p(2^p - 1). \quad (1.16.2)$$

Exercici 1.17. Demostreu que per a tot parell m, n de nombres enters diferents no negatius, els nombres de Fermat, F_m, F_n són relativament primers. Deduiu una demostració alternativa a la donada per Euclides sobre l'existència d'una infinitat de nombres primers.

Resolució. Hem de demostrar que un nombre parell és perfecte si, i només si, $n = 2^{p-1}(2^p - 1)$, $p > 1$. Suposem $n = 2^{p-1}m$, amb m imparell. Per hipòtesi tenim que $\sigma_1(n) = 2n$. Substituint i operant, $\sigma_1(2^{p-1}m) = \sigma_1(2^{p-1})\sigma_1(m) = \frac{2^p-1}{2-1}\sigma_1(m) = (2^p - 1)\sigma_1(m)$. Aleshores, ■

Exercici 1.18. Exercici 35

Resolució. La solució a aquest exercici es podria fer a mà o al *Mathematica*. Optarem per fer-ho a mà. Ens ajudarem del teorema següent:

Teorema 1.18.1. Existeixen arrels primitives mòdul N si, i només si, $N = 1, 2, 4, p^r, 2p^r$ amb p primer senar.

$N = 5$: $\varphi(5) = 4$. Hem de buscar elements $a \in (\frac{\mathbb{Z}}{5\mathbb{Z}})^*$ tal que $\text{ord}(a) = 4$.

Observació 1.18.1. $a^4 \equiv 1 \pmod{5}$. L'ordre d' $a \in (\frac{\mathbb{Z}}{5\mathbb{Z}})^*$ divideix $\varphi(5)$.

Per buscar les arrels primitives hauríem d'anar recorrent els elements invertibles. Aleshores:

1. $a = 2$: $2^2 \equiv 4 \pmod{5} \implies 2$ és arrel primitiva mòdul 5. $2^4 \equiv 1 \pmod{5}$ també, tot i que no és necessari ja que ja hem trobat l'ordre.
2. $a = 3$: $3^2 \equiv 9 \equiv 4 \pmod{5} \implies 3$ és arrel primitiva mòdul 5.
3. $a = 18$. Notem primerament que segueixen la fórmula del teorema anterior, ja que és de la forma $2 \cdot 3^r$. Calcularem $\varphi(18) = \varphi(2)\varphi(3^2) = 6$. Els possibles ordres d' $a \in (\frac{\mathbb{Z}}{18\mathbb{Z}})^*$ són 1, 2, 3, 6. Tenim que $a = 2$ no és a p ja que 2 no pertany als elements invertibles mòdul 18. Provem $a = 5$: ens queda $5^2 \equiv 25 \equiv 7 \pmod{18}$ i $5^3 \equiv 35 \equiv 17 \pmod{18}$

Exercici 1.19. Calculeu totes les solucions de les congruències

1. $x^2 + x + 1 \equiv 0 \pmod{7}$,
2. $x^2 + 5x + 1 \equiv 0 \pmod{7}$,
3. $x^2 + 3x + 1 \equiv 0 \pmod{7}$.

Resolució. Notem que totes aquestes equacions varien pel coeficient del terme de primer grau.

1. Tenim que $x^2 + x + 1 \equiv x^2 + x - 6 \equiv (x - 2)(x + 3) \equiv 0 \pmod{7}$ i, per tant, tenim dues solucions: $x \equiv 2 \pmod{7}$ o bé $x \equiv -3 \equiv 4 \pmod{7}$.
2. Tenim que $x^2 + 5x + 1 \equiv x^2 + 5x - 6 \equiv (x - 1)(x + 6) \pmod{7}$ i, per tant, ens queden un altre cop dues solucions: $x \equiv 1 \pmod{7}$ i $x \equiv -6 \equiv 1 \pmod{7}$. Aquesta última, si ens hi fixem, és equivalent a $x \equiv 1 \pmod{7}$; realment ens queda que aquesta congruència té una única solució.
3. Tenim que $x^2 + 3x + 1 \equiv 0 \pmod{7}$. Aquest polinomi és irreductible en l'anell dels enters. De totes maneres, podríem proposar solucions possibles en altres anells i cossos. Generalitzant-les totes, les trobaríem en el cos dels complexos.

Exercici 1.20. Trobeu totes les solucions de la congruència $x^2 + 6x - 31 \equiv 0 \pmod{72}$.

Resolució. Fixem-nos que aquesta congruència té solució si, i només si, les congruències $x^2 + 6x - 31 \equiv 0 \pmod{8}$ i $x^2 + 6x - 31 \equiv 0 \pmod{9}$ tenen solució. Tal raonament ha sorgit d'aplicar el TXResidu. Aleshores,

$$\begin{aligned} x^2 + 6x - 7 &\equiv (x-1)(x+7) \equiv 0 \pmod{8} \\ x^2 + 6x + 5 &\equiv (x+1)(x+5) \equiv 0 \pmod{9} \end{aligned} \quad (1.20.1)$$

amb la qual cosa ens queda que $x = 1 + 8\lambda$, $\lambda \in \mathbb{Z}$, ja que $x \equiv 1 \pmod{8}$ i $x \equiv -7 \pmod{8}$ són equivalents. I, per tant, $2(4\lambda+1)2(4\lambda+3) \equiv 0 \pmod{9}$. Així,

$$4(4\lambda+1)(4\lambda+3) \xrightarrow{\text{mcd}(4,9)=1} (4\lambda+1)(4\lambda+3) \equiv 0 \pmod{9}. \quad (1.20.2)$$

Tenim que $4\lambda \equiv 8 \pmod{9}$ o bé $4\lambda \equiv 6 \pmod{9}$. Ens queda que $\lambda \equiv -16 \pmod{9}$ o bé $\lambda \equiv -12 \pmod{9}$. Finalment, veiem que

$$\begin{aligned} x &\equiv 17 \pmod{72} \\ x &\equiv 49 \pmod{72}. \end{aligned} \quad (1.20.3)$$

Ara ens quedaria resoldre $x^2 + 6x - 31 \equiv 0 \pmod{8} \iff x \equiv 5 \pmod{8}$. Fixem-nos que $(x^2 + 6x + 9) - 40 \equiv (x+3)^2 \equiv 0 \pmod{8}$. Per tant, $x+3 \equiv 0 \pmod{8}$ i, per tant, $x \equiv 5 \pmod{8}$. Ens queda, doncs:

$$\begin{aligned} x &\equiv 5 \pmod{8} \iff x = 5 + 8\gamma, \gamma \in \mathbb{Z}, \\ x^2 + 6x + 5 &\equiv (x+1)(x+5) \equiv 0 \pmod{9}. \end{aligned} \quad (1.20.4)$$

Aleshores, $4(3+4\gamma)(5+4\gamma) \equiv 0 \pmod{9}$. Com que $\text{mcd}(4,9) = 1$, és equivalent a considerar $(3+4\gamma)(5+4\gamma) \equiv 0 \pmod{9}$. Per tant, ens queda que $\gamma \equiv -6 \equiv 2 \pmod{9}$ o bé $\gamma \equiv -10 \equiv 6 \pmod{9}$. En definitiva,

$$\begin{aligned} x &\equiv 13 \pmod{72} \\ x &\equiv 53 \pmod{72}. \end{aligned} \quad (1.20.5)$$

Ens queden, doncs, aquestes quatre solucions:

$$\begin{aligned} x &\equiv 17 \pmod{72} \\ x &\equiv 49 \pmod{72} \\ x &\equiv 13 \pmod{72} \\ x &\equiv 53 \pmod{72}. \end{aligned} \quad (1.20.6)$$



Exercici 1.21. Calculeu els símbols de Jacobi següents:

1. $\left(\frac{3}{53}\right),$
2. $\left(\frac{31}{641}\right),$
3. $\left(\frac{7}{79}\right),$
4. $\left(\frac{111}{991}\right),$
5. $\left(\frac{15}{101}\right),$
6. $\left(\frac{105}{1109}\right),$
7. $\left(\frac{5}{21}\right),$
8. $\left(\frac{1009}{2307}\right),$
9. $\left(\frac{27}{101}\right),$
10. $\left(\frac{2663}{3299}\right),$

11. $\left(\frac{111}{1001}\right)$,
 12. $\left(\frac{10001}{20003}\right)$.

Resolució.

1. $\left(\frac{3}{53}\right)$: com que 53 és un nombre primer, és el mateix que considerar el símbol de Legendre $\left(\frac{3}{p}\right)$. Recordant que

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{si } p \equiv 1, -1 \pmod{12}, \\ -1, & \text{si } p \equiv 5, -5 \pmod{12}, \end{cases} \quad (1.21.1)$$

ens queda que $\left(\frac{3}{53}\right) = -1$, ja que $53 \equiv 5 \pmod{12}$ i, per tant, $\left(\frac{3}{53}\right) = -1$.

2. $\left(\frac{31}{641}\right)$: anàlogament amb l'apartat anterior, ens queda que $\left(\frac{31}{641}\right)$ és equivalent a $\left(\frac{31}{31}\right)$, ja que ambdós nombres són primers. Com que $641 \equiv 1 \pmod{4}$, ens queda que $\left(\frac{31}{641}\right) = \left(\frac{641}{31}\right) = \left(\frac{21}{31}\right) = \left(\frac{3}{31}\right)\left(\frac{7}{31}\right)$, on la segona igualtat ve de reduir 641 mòdul 31 i la tercera, d'aplicar les propietats del símbol. Aplicant que $31 \equiv 3 \equiv -1 \pmod{4}$, i que $31 \equiv 7 \equiv -1 \pmod{4}$, ens queda que

$$\left(\frac{3}{31}\right)\left(\frac{7}{31}\right) = \left(\frac{1}{3}\right)\left(\frac{3}{7}\right) = -1, \quad (1.21.2)$$

on la primera igualtat ve d'aplicar la llei de reciprocitat quadràtica per a ambdós símbols i reduir 31 mòdul 3 en el primer cas, i aplicar el criteri d'Euler en el segon. Notem que la reducció mòdul p es pot aplicar gràcies a la primera propietat del símbol de Legendre (consultar els apunts de l'assignatura [Vil21]).

A partir d'ara, els resoldrem amb menys detall ja que hem aprofundit molt en aquests dos primers.

3. $\left(\frac{7}{79}\right) \equiv \left(\frac{7}{79}\right)$, amb $79 \equiv 2 \pmod{7}$ i $79 \equiv 7 \equiv -1 \pmod{4}$, ens queda que

$$\left(\frac{7}{79}\right) = \left(\frac{79}{7}\right) = \left(\frac{2}{7}\right) = (-1)^{\frac{7^2-1}{8}} = 1. \quad (1.21.3)$$

4. $\left(\frac{111}{991}\right) \equiv \left(\frac{111}{991}\right)$, amb $111 \equiv 991 \equiv -1 \pmod{4}$, $111 \equiv -1 \pmod{8}$, $111 \equiv 3 \pmod{4}$. Aleshores,

$$\left(\frac{111}{991}\right) = -\left(\frac{991}{111}\right) = -\left(\frac{-8}{111}\right) = -\left(\frac{-1}{111}\right)\left(\frac{2}{111}\right)^3 - (-1)(1)^3 = 1 \quad (1.21.4)$$

5. $\left(\frac{15}{101}\right) \equiv \left(\frac{3}{101}\right)\left(\frac{5}{101}\right)$, amb $101 \equiv 1 \pmod{4}$, $101 \equiv -1 \pmod{3}$ i $101 \equiv 1 \pmod{5}$.

$$\left(\frac{3}{101}\right)\left(\frac{5}{101}\right) = \left(\frac{101}{3}\right)\left(\frac{101}{5}\right) = \left(\frac{-1}{3}\right)\left(\frac{1}{5}\right) = (-1)(1) = -1. \quad (1.21.5)$$

6. $\left(\frac{105}{1109}\right) \equiv \left(\frac{105}{1109}\right) \equiv \left(\frac{3}{1109}\right)\left(\frac{5}{1109}\right)\left(\frac{7}{1109}\right)$, amb $1109 \equiv 1000 + 100 + 1 \equiv 0 + 0 + 1 \pmod{4}$ i $1109 \equiv 2 \equiv -1 \pmod{3}$, $1109 \equiv 9 \equiv -1 \pmod{5}$, $1109 \equiv 3 \pmod{7}$:

$$\left(\frac{3}{1109}\right)\left(\frac{5}{1109}\right)\left(\frac{7}{1109}\right) = \left(\frac{1109}{3}\right)\left(\frac{1109}{5}\right)\left(\frac{1109}{7}\right) = \left(\frac{-1}{3}\right)\left(\frac{-1}{5}\right)\left(\frac{3}{7}\right) = (-1)(1)(-1) = 1, \quad (1.21.6)$$

on hem usat les propietats del símbol de Legendre per a $a = -1$ en els dos primers símbols i el criteri d'Euler per al tercer.

7. $\left(\frac{5}{21}\right) \equiv \left(\frac{5}{3}\right)\left(\frac{5}{7}\right)$, on $5 \equiv 1 \pmod{4}$ i $5 \equiv -1 \pmod{3}$, $5 \equiv -2 \pmod{7}$:

$$\left(\frac{5}{3}\right)\left(\frac{5}{7}\right) = \left(\frac{-1}{3}\right)\left(\frac{-1}{7}\right)\left(\frac{2}{7}\right) \xrightarrow[3 \equiv 3 \pmod{4}, 7 \equiv 3 \pmod{4}]{7 \equiv -1 \pmod{8}} (-1)(-1)(1) = 1 \quad (1.21.7)$$

8. $\left(\frac{1009}{2307}\right) \equiv \left(\frac{1009}{3}\right)\left(\frac{1009}{769}\right)$, $1009 \equiv 1 \pmod{3}$, $1009 \equiv -409 \pmod{709}$, $409 \equiv 1 \pmod{4}$, $709 \equiv 1 \pmod{4}$:

$$\begin{aligned} \left(\frac{1009}{3}\right)\left(\frac{1009}{709}\right) &= \left(\frac{1}{3}\right)\left(\frac{-1}{709}\right)\left(\frac{409}{709}\right) = -\left(\frac{709}{409}\right) = -\left(\frac{-1}{409}\right)\left(\frac{11}{409}\right)\left(\frac{19}{409}\right) \\ &= -\left(\frac{2}{11}\right)\left(\frac{-1}{19}\right)\left(\frac{3^2}{19}\right) = -(-1)(-1)(1) = -1. \end{aligned} \quad (1.21.8)$$

9. $\left(\frac{27}{101}\right) \equiv \left(\frac{3}{101}\right)^3$, que resolem ràpidament donada la resolució de $\left(\frac{3}{p}\right)$, en el primer apartat. Ens queda que $\left(\frac{27}{101}\right) = -1$, ja que $101 \equiv -19 \equiv 5 \pmod{12}$.

10. $\left(\frac{2663}{3299}\right) \equiv \left(\frac{2663}{3299}\right)$, $2663 \equiv 3299 \equiv -1 \pmod{4}$. A més, $2663 \equiv 1 \pmod{4}$, $2663 \equiv -1 \pmod{8}$, $2663 \equiv -1 \pmod{12}$, $2663 \equiv -37 \equiv -1 \pmod{3}$, $53 \equiv 1 \pmod{4}$.

$$\left(\frac{2663}{3299}\right) = -\left(\frac{636}{2663}\right) = -\left(\frac{2}{2663}\right)\left(\frac{3}{2663}\right)\left(\frac{53}{2663}\right) = -(1)(1)\left(\frac{-1}{53}\right) = -1. \quad (1.21.9)$$

11. $\left(\frac{111}{1001}\right) \equiv \left(\frac{111}{7}\right)\left(\frac{111}{11}\right)\left(\frac{111}{13}\right)$.

$$\left(\frac{-1}{7}\right)\left(\frac{1}{11}\right)\left(\frac{7}{13}\right) = (-1)(-1)\left(\frac{13}{7}\right) = \left(\frac{-1}{7}\right) = -1. \quad (1.21.10)$$

12. $\left(\frac{10001}{20003}\right) \equiv \left(\frac{10001}{83}\right)\left(\frac{10001}{241}\right)$. Al seu torn, $10001 \equiv 41 \pmod{83}$, $10001 \equiv 120 \pmod{241}$, $41 \equiv 1 \pmod{4}$, $241 \equiv 1 \pmod{4}$, $83 \equiv 1 \pmod{41}$, $241 \equiv 1 \pmod{120}$.

$$\left(\frac{10001}{83}\right)\left(\frac{10001}{241}\right) = \left(\frac{41}{83}\right)\left(\frac{120}{241}\right) = \left(\frac{1}{41}\right)\left(\frac{1}{120}\right) = 1. \quad (1.21.11)$$

Observació 1.21.1. La llei de reciprocitat quadràtica es pot expressar en la forma equivalent següent: si algun dels dos nombres p, q és congru a 1 mòdul 4, els dos símbols de Legendre $\left(\frac{p}{q}\right)$ i $\left(\frac{q}{p}\right)$ coincideixen; mentre que si $p \equiv q \equiv -1 \pmod{4}$, aleshores $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

Comprovacions diverses amb el Mathematica

```
In[1]:= FactorInteger[641]
FactorInteger[79]
FactorInteger[991]
FactorInteger[111]
FactorInteger[101]
FactorInteger[1009]
FactorInteger[2307]
FactorInteger[409]
FactorInteger[709]
FactorInteger[209]
```

```
Out[1]= {{641, 1}}
```

```
Out[2]= {{79, 1}}
```

```
Out[3]= {{991, 1}}
```

Out[4]= $\{\{3, 1\}, \{37, 1\}\}$

Out[5]= $\{\{101, 1\}\}$

Out[6]= $\{\{1009, 1\}\}$

Out[7]= $\{\{3, 1\}, \{769, 1\}\}$

Out[8]= $\{\{409, 1\}\}$

Out[9]= $\{\{709, 1\}\}$

Out[10]= $\{\{11, 1\}, \{19, 1\}\}$



Exercici 1.22. En general, fixat un nombre enter a , sigui p un nombre enter primer per al qual a no sigui un quadrat en $\mathbb{Z}/p\mathbb{Z}$. Demostreu que si n és un nombre enter divisible per p , llavors a no és un quadrat en $\mathbb{Z}/p\mathbb{Z}$.

Resolució. Sigui $a \not\equiv x^2 \pmod{p}$, $\forall x \in \mathbb{Z}/p\mathbb{Z} \implies a \not\equiv x^2 \pmod{n}$, $\forall x \in \mathbb{Z}/p\mathbb{Z}$. Així doncs, ho demostrem per contrarrecíproc. Tenim que $\exists x \in \mathbb{Z}/p\mathbb{Z}$ tal que $a \equiv x^2 \pmod{n}$. Com que $n \mid x^2 - a$ i $p \mid x^2 - a$, ens queda $x^2 \equiv a \pmod{p}$ tal i com volíem. ■

2
PROBLEMES

Exercici 2.1. Siguin $a, b \in \mathbb{Z}$ nombres enters tals que $\text{mcd}(a, b) = 1$. Calculeu $\text{mcd}(a+b, a-b)$ en funció d'a i b.

Resolució. Podem afirmar que $\text{mcd}(a+b, a-b) = d$, $d \in \mathbb{Z}$, qualsevol. Aleshores, $d|a+b, d|a-b$, és a dir, si considerem dos nombres α, β tals que

$$\begin{aligned} \frac{a+b}{d} &= \alpha, \\ \frac{a-b}{d} &= \beta, \end{aligned} \tag{2.1.1}$$

aquests pertanyen als enters. Al seu torn,

$$\alpha + \beta \in \mathbb{Z} \implies \frac{(a+b) + (a-b)}{d} = \frac{2a}{d} \in \mathbb{Z}, \quad \alpha - \beta \in \mathbb{Z} \implies \frac{(a+b) - (a-b)}{d} = \frac{2b}{d} \in \mathbb{Z}. \tag{2.1.2}$$

Hem vist que $d|2a$ i $d|2b$. Tenint en compte que $\text{mcd}(a, b) = 1$, els únics valors de d pels quals $d|2a$ i $d|2b$ són $d = 1$ i $d = 2$. Cal caracteritzar les possibilitats:

- a és parell i b és imparell $\implies a = 2s$ i $b = 2t+1$, per algun $t, s \in \mathbb{Z}$. Operant:

$$\left. \begin{aligned} a+b &= 2(s+t) + 1 \in \mathbb{Z}, \\ a-b &= 2(s-t) - 1 \in \mathbb{Z}. \end{aligned} \right\} \implies \left. \begin{aligned} (a+b) + (a-b) &= 2a = 4s \in \mathbb{Z}, \\ (a+b) - (a-b) &= 2b = 2(2t+1) \in \mathbb{Z}. \end{aligned} \right\}, \tag{2.1.3}$$

és a dir,

$$\begin{aligned} \text{mcd}(a+b, a-b) &= \text{mcd}(a+b, 2a) = \text{mcd}(a+b, 2b) \xrightarrow[a \text{ parell}]{b \text{ senar}} \text{mcd}(2(s+t)+1, 4s) \\ &= \text{mcd}(2(s+t)+1, 2t). \end{aligned} \tag{2.1.4}$$

Suposant $s+t = 0$, $\text{mcd}(1, -2s) = \text{mcd}(1, 2s) = \text{mcd}(1, 2t) = \text{mcd}(1, a) = \text{mcd}(1, b-1) = 1$.

- a és imparell i b és parell. El procediment és anàleg a l'anterior cas, solament que .
- a i b són imparells. La suma de dos imparells és sempre parella. Aleshores, $\text{mcd}(a+b, a-b) = d = 2$.

Exercici 2.2. Demostreu que si $n, n+2$ i $n+4$ són nombres naturals primers, aleshores $n = 3$.

Resolució. Pel contrarrecíproc, tenim:

$$n \neq 3 \implies n, n+2, n+4 \text{ no són primers.} \tag{2.2.1}$$

Hem de diferenciar entre dos casos principals. Si cal, farem subcasos.

1. **Cas 1:** n parell. $n = 2k, k \in \mathbb{N}$. Aleshores, $2k, 2(k+1), 2(k+2)$ no són primers $\forall k \in \mathbb{N}$.
2. **Cas 2:** n imparell. Hem descartat directament $n = 1$ perquè no és primer, $n = 2$ és parell, $n \neq 3$ per hipòtesi. A partir d'aquí, $n > 3$, és a dir, escriurem els naturals > 3 tal que $n = 3q+r$, on $q \in \mathbb{N}_{\geq 1}$ i $0 \leq r < 3$.
 - **Subcàs 1:** $r = 0 \implies n = 3q$. Hem de considerar $q > 1$. Si no fos així, $n \geq 3$, però $n \neq 3$. Fixem-nos que $3|n$. Aleshores, aquest subcàs conté tot múltiple de 3 més gran que 3 (nombres no primers).

- *Subcàs 2:* $r = 1 \implies n = 3q + 1 \implies n + 2 = 3(q + 1) \implies 3|n + 2$. Per tant, tot $n + 2$ és múltiple de 3 i, en conseqüència, no primer.
- *Subcàs 3:* $r = 2 \implies n + 4 = 3(q + 2) \implies 3|n + 4$. Per tant, tot $n + 3$ és múltiple de 3 i, en conseqüència, no primer.

■

Exercici 2.3.

1. *Siguin a, m, n nombres naturals, $m \neq n$. Calculeu $\text{mcd}(a^{2^m} + 1, a^{2^n} + 1)$.*
2. *Siguin m, n nombres naturals i $d := \text{mcd}(m, n)$. Demostreu que $\text{mcd}(2^m - 1, 2^n - 1) = 2^d - 1$.*

Resolució.

1. **1r apartat:** Sense pèrdua de generalitat, suposarem que $m > n$ en tota la resolució de l'exercici.

$$\text{mcd}(a^{2^n} + 1, a^{2^m} + 1) = \text{mcd}(a^{2^n} + 1, a^{2^m} - a^{2^n}) = d. \quad (2.3.1)$$

Doncs, per definició,

$$\begin{aligned} \alpha &= \frac{a^{2^n} + 1}{d} \in \mathbb{N}, \beta = \frac{a^{2^m} + 1}{d} \in \mathbb{N}; \\ \alpha + \beta &= \left(\frac{a^{2^n} + a^{2^m}}{d} + \frac{2}{d} \right) \in \mathbb{N} \implies \frac{2}{d} \in \mathbb{N} \implies d = 1 \vee d = 2. \\ \hline \beta - \alpha &= \frac{a^{2^m} - a^{2^n}}{d} = \frac{a^{2^n}(2^{2^m-2^n} - 1)}{d}. \end{aligned} \quad (2.3.2)$$

Notem que podem dividir-ho en dos casos:

- a és parell $\implies a = 2k, k \in \mathbb{N}$:

$$\frac{2^{2^n}(k^{2^n}(2^{2^m-2^n} - 1))}{d} \implies 2^{2^n-1}(k^{2^n}(2^{2^m-2^n} - 1)) \implies \text{mcd}(a^{2^n} + 1, a^{2^m} + 1) = 2. \quad (2.3.3)$$

- a és senar $\implies a = 2k + 1, k \in \mathbb{N}$. A partir del cas anterior, és immediat veure que $\text{mcd}(a^{2^n} + 1, a^{2^m} + 1) = 2$.

2. **2n apartat:** El resultat és clar si $m = n$. Suposem, doncs, que és $m > n$.

Ara, tenim que

$$2^m - 1 - (2^n - 1) = 2^m - 2^n = 2^n(2^{m-n} - 1)$$

i, com que $\text{mcd}(2^n, 2^n - 1) = 1$, és

$$\text{mcd}(2^m - 1, 2^n - 1) = \text{mcd}(2^n(2^{m-n} - 1), 2^n - 1) = \text{mcd}(2^{m-n} - 1, 2^n - 1);$$

és a dir, podem restar n de m en l'exponent del primer dels dos nombres i el màxim comú divisor no canvia.

Sigui $m = nq + r$, amb $0 \leq r \leq n$, la divisió entera de m entre n . Com que $m > n$, resulta que és $q \geq 1$, i podem iterar q vegades el càlcul anterior; obtenim que

$$\text{mcd}(2^m - 1, 2^n - 1) = \text{mcd}(2^{m-nq} - 1, 2^n - 1) = \text{mcd}(2^r - 1, 2^n - 1) = \text{mcd}(2^n - 1, 2^r - 1).$$

Apliquem successivament aquest fet d'acord amb l'algoritme d'Euclides per al càlcul del màxim comú divisor de m i n . Obtenim exactament allò que hi ha enunciat:

$$\text{mcd}(2^m - 1, 2^n - 1) = \text{mcd}(2^d - 1, 2^0 - 1) = \text{mcd}(2^d - 1, 0) = 2^d - 1.$$



Solució de l'exercici 8, apartat a. Provarem que

$$\operatorname{mcd}(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1, & \text{si } a \text{ és parell i } m \neq n, \\ 2, & \text{si } a \text{ és senar i } m \neq n, \\ a^{2^m} + 1, & \text{si } m = n. \end{cases}$$

Clarament, si $m = n$, llavors $\operatorname{mcd}(a^{2^m} + 1, a^{2^n} + 1) = a^{2^m} + 1$ i ja hem acabat. Per tant, podem suposar, i ho fem, que $m > n$.

Notem que, en general, per a $r > 2^n$, tenim que

$$a^r + 1 - (a^{2^n} + 1) = a^r - a^{2^n} = a^{2^n}(a^{r-2^n} - 1)$$

i, com que $\operatorname{mcd}(a^{2^n}, a^{2^n} + 1) = 1$, és

$$\begin{aligned} \operatorname{mcd}(a^r + 1, a^{2^n} + 1) &= \operatorname{mcd}(a^r + 1 - (a^{2^n} + 1), a^{2^n} + 1) \\ &= \operatorname{mcd}(a^{2^n}(a^{r-2^n} - 1), a^{2^n} + 1) \\ &= \operatorname{mcd}(a^{r-2^n} - 1, a^{2^n} + 1). \end{aligned}$$

Anàlogament, i també per a $s > 2^n$, tenim que

$$a^s - 1 + (a^{2^n} + 1) = a^s + a^{2^n} = a^{2^n}(a^{s-2^n} + 1)$$

i, com que $\operatorname{mcd}(a^{2^n}, a^{2^n} + 1) = 1$, és

$$\begin{aligned} \operatorname{mcd}(a^s - 1, a^{2^n} + 1) &= \operatorname{mcd}(a^s - 1 + (a^{2^n} + 1), a^{2^n} + 1) \\ &= \operatorname{mcd}(a^{2^n}(a^{s-2^n} + 1), a^{2^n} + 1) \\ &= \operatorname{mcd}(a^{s-2^n} + 1, a^{2^n} + 1). \end{aligned}$$

Ara, notem que $2^m = 2^{m-n}2^n$, de manera que, per a $m > n$, podem restar 2^n de 2^m una quantitat parella de vegades (2^{m-n} és parell, perquè $m > n$). Així, obtenim que

$$\operatorname{mcd}(a^{2^m} + 1, a^{2^n} + 1) = \operatorname{mcd}(a^0 + 1, a^{2^n} + 1) = \operatorname{mcd}(2, a^{2^n} + 1),$$

que proporciona el càlcul desitjat,

$$\operatorname{mcd}(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1, & \text{si } a \text{ és parell,} \\ 2, & \text{si } a \text{ és senar.} \end{cases}$$



Exercici 2.4. Siguin $a, b \in \mathbb{Z}$ nombres enters tals que $\operatorname{mcd}(a, b) = 1$. Calculeu $\operatorname{mcd}(a^2 + b^2, a^2 - b^2, 2ab)$ en funció d'a i b.

Resolució. Podem posar d com a $\operatorname{mcd}(a^2 + b^2, a^2 - b^2, 2ab)$. Tenim que $d \mid a^2 + b^2, d \mid a^2 - b^2, d \mid 2ab$. Per la linealitat de la divisibilitat extraiem que $d \mid 2a^2$ i $d \mid 2b^2$. Com que $\operatorname{mcd}(a, b) = 1$, deduïm que $d \mid 2$. Ara, distingim una sèrie de casos:

1. a parell, b senar; o bé, a senar, b parell. D'aquí, tant $a^2 + b^2$ com $a^2 - b^2$ ens donen nombres senars. $\boxed{d = 1}$.
2. a, b senars. Ens donen $a^2 + b^2$ com $a^2 - b^2$ ens donen nombres parells. $\boxed{d = 2}$.
3. En ambdós casos, $2ab$ serà sempre parell. a, b no poden ser els dos parells donat que $\text{mcd}(a, b) = 1$. ■

Exercici 2.5. *Demostreu que no hi ha cap nombre primer de la forma $n = a^4 - b^4$, $a, b \in \mathbb{Z}$.*

Resolució. Sense pèrdua de generalitat, podem suposar $a > b$. Per tant, $a > b > 0$. Podem reescriure n de la següent manera:

$$a^4 - b^4 = (a^2 + b^2)(a + b)(a - b). \quad (2.5.1)$$

Fixem-nos, a més, que $a > b \iff a + b > 2b \geq 2 \implies a^2 + b^2 \geq a + b < 2$. Per tant, n té com, a mínim, dos factors més grans que 1, i tots més grans que 0. Concloem que n no és primer. ■

Exercici 2.6. *Trobeu totes les solucions (x, y) amb $x, y \in \mathbb{Z}_{>0}$, del sistema d'equacions*

$$\begin{cases} xy = 51840 \\ \text{mcd}(x, y) = 24 \end{cases} \quad (2.6.1)$$

Resolució. Per la segona equació, tenim que $x = 24a$ i $y = 24b$, així que $xy = 24^2 ab = 51840 \iff ab = 90$. Considerant $\text{mcd}(a, b) = 1$, reduïm el conjunt de solucions a $S = \{(1, 90), (2, 45), (5, 18), (9, 10)\}$. ■

Exercici 2.7. *Siguin $n > 1$ un nombre natural i p el menor nombre natural que divideix n . Demostreu que si $p^3 > n$, aleshores n és primer (i $p = n$) o bé $\frac{n}{p}$ és primer.*

Resolució. Si n és primer, ja hem acabat i es dona que $p = n$. Suposem n compost i sabem que $n > 1$ es pot descompondre com a producte de factors. Aleshores, si dividim per p i $\frac{n}{p}$ fos primer ja hauríem acabat. Per últim, suposem que dividim per p i $\frac{n}{p}$ no és primer: immediatament, veiem que podríem descompondre un altre cop el nombre com a producte de factors, de tal manera que tindríem $n = pp_1p_2 > p^3$, la qual cosa ens porta a una contradicció. ■

Exercici 2.8. *Demostreu que, per a tot nombre enter k , els nombres $6k - 1, 6k + 1, 6k + 2, 6k + 3, 6k + 5$ són primers entre si dos a dos; és a dir, que per a $a, b \in \{6k - 1, 6k + 1, 6k + 2, 6k + 3, 6k + 5\}$, $a \neq b$, és $\text{mcd}(a, b) = 1$.*

Resolució. Sigui $k \in \mathbb{Z}$. Aleshores, posem $\text{mcd}(6k + 5, 6k - 1)$. Operant:

$$\text{mcd}(6k - 5, 6k - 1) = \text{mcd}(6k - 1, 6k + 5) = \text{mcd}(6, 6k - 1) = \text{mcd}(6, (6k - 1) - 6k) = \text{mcd}(6, -1) = 1. \quad (2.8.1)$$

Aplicaríem un procediment anàleg amb cada parella de nombres. ■

Notem que l'algorisme d'Euclides es resol amb un nombre finit de passos, és proporcional al nombre de xifres binàries:

$$\begin{aligned} \text{mcd}(a, b) &= \text{mcd}(b, r), \quad 0 \leq r < b, \\ \text{mcd}(b, r) &= \text{mcd}(b, r - b), \quad -\frac{b}{2} \leq r' \leq \frac{b}{2}. \end{aligned} \quad (2.8.2)$$

Així, aniríem reduint el nombre en base binària en una xifra (com a mínim).

Exercici 2.9. Demostreu que no existeix cap polinomi no constant $f(x) \in \mathbb{Z}[x]$ tal que $f(a)$ sigui primer per a tot $a \in \mathbb{Z}$.

Resolució. Procedim per reducció a l'absurd. La negació de la propietat, aplicant correctament la lògica matemàtica, seria la següent:

$$\neg(\nexists f(x) \in \mathbb{Z}[x], \text{gr}(f) \geq 1, f(a) = p, \forall a \in \mathbb{Z}) \iff (\forall f(x) \in \mathbb{Z}[x], \text{gr}(f) = 0, f(a) \neq p \forall a \in \mathbb{Z}), \quad (2.9.1)$$

notant per p un nombre primer i, per tant, $f(a) \neq p$ un nombre compost. Podem provar la contradicció que volem amb un contraexemple: agafant $f(x) = 11$, tenim que $f(a) = 11 = p$ per tot $a \in \mathbb{Z}$. \perp

Hem trobat la contradicció que volíem i l'enunciat ha quedat provat. ■

Exercici 2.10. La masovera se'n va al mercat. En tornar cap a casa, es dedica a comptar-les. Si les compta de 2 en 2, n'hi sobra 1; si les compta de 3 en 3, n'hi sobren 2; i així, fins que les compta de 7 en 7, i no n'hi sobra cap. Quantes nous ha comprat?

Resolució. Per resoldre aquest problema ens val amb interpretar les dades que se'ns donen en forma de sistema de congruències lineals:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{6} \\ x \equiv 0 \pmod{7} \end{cases} \iff \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 3 \pmod{2} \\ x \equiv 5 \pmod{2} \\ x \equiv 5 \pmod{3} \\ x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 0 \pmod{7} \end{cases} \iff \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 0 \pmod{7} \end{cases} \quad (2.10.1)$$

Ens queda, resolent-lo, $x \equiv 119 \pmod{410}$, així que s'ha comprat 119 nous. ■

Observació 2.10.1. Notem, davant l'error que havia fet, la següent observació: Efectivament, els sistemes no són equivalents: m'hauria d'haver quedat amb $x \equiv 3 \equiv 7 \pmod{4}$ en lloc de $x \equiv 1 \equiv 7 \pmod{2}$, donat que la congruència mòdul 4 implica la congruència mòdul 2, però no a l'inrevés. Igualment, podríem simplificar $x \equiv 5 \pmod{6}$ per TXRes. Així doncs, el sistema estaria format per $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{4}$, $x \equiv 4 \pmod{5}$ i $x \equiv 0 \pmod{7}$. En la solució ara obtinguda, x també seria congru amb 119, però aquesta vegada mòdul 410. He fet unes quantes comprovacions ràpides per assegurar-me que, ara sí, es poden agafar $119 + 410 \cdot 0, 119 + 410 \cdot 1 = 529, \dots$ i es compleixen les directrius de l'enunciat.

Exercici 2.11 (Teorema de Wilson). Sigui $n \geq 2$ un nombre enter. Demostreu que n és primer si, i només si, n divideix $(n-1)! + 1$.

Resolució. \Rightarrow n és un primer p . Si $p = 2$, la congruència $1 \equiv -1 \pmod{2}$ prova el teorema. Sigui p un primer senar. Com p és un nombre primer, tenint en compte que les classes invertibles mòdul p són totes les classes diferents de les del 0: hem d'agafar representants en l'interval $[1, p]$ per a les classes i obtenim els representants de les classes invertibles: $1, 2, \dots, p-1$. Precisament pel fet de ser invertibles, això implica que per a tot $i \in \{1, 2, \dots, p-1\}$ existeix j en el mateix conjunt tal que $ij \equiv 1 \pmod{p}$.

Abans de procedir a emparellar a cada element amb el seu invers, hem d'aïllar el cas $i = j$: hem de trobar aquells i tals que $i^2 \equiv 1 \pmod{p}$. Notem que aquesta equació té dues solucions triviales: $1^2 \equiv 1 \pmod{p} \equiv (-1)^2 \equiv 1 \pmod{p}$. Vegem que no posseeix més solucions.

Sigui x tal que $x^2 \equiv 1 \pmod{p}$. Aleshores, $x^2 - 1 \equiv 0 \pmod{p} \implies (x+1)(x-1) \equiv 0 \pmod{p}$. Equivalentment, p divideix el producte $(x+1)(x-1)$. Per LFA (Lema Fonamental de l'Aritmètica), deduïm que $p \mid x+1$ o bé $p \mid x-1$. Per tant, $x \equiv -1 \equiv p-1 \pmod{p}$ o bé $x \equiv 1 \pmod{p}$. Tenim que les úniques $i \in \{1, 2, \dots, p-1\}$ que compleixen $i^2 \equiv 1 \pmod{p}$ són 1 i $p-1$.

Sabem, per tant, que els elements de $\{1, 2, \dots, p-1\}$ posseeixen un invers mòdul p en aquest mateix conjunt, i que solament 1 i $p-1$ són inversos de sí mateixos. Per tant, al fer el producte $1 \cdot 2 \cdot \dots \cdot (p-1) = (p-1)!$ en mòdul p , tots els elements s'emparellen en parelles d'inversos $ij \equiv 1 \pmod{p}$, d'on $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$.

Si n fos compost, existiria $k \mid n$, tal que $1 < k < n$. Aleshores, $k \mid (n-1)!$. En particular, per la nostra hipòtesi, $k \mid ((n-1)! + 1)$. Operant, es veu fàcilment que $k \mid 1$, però $k > 1$. Així que n ha de ser necessàriament primer. ■

Exercici 2.12. Calculeu a mà les potències següents:

$$\begin{aligned} 5^{2010} &\pmod{11} \\ 6^{40} &\pmod{33} \\ 7^{135} &\pmod{10} \\ 30^{45} &\pmod{15} \end{aligned} \tag{2.12.1}$$

Resolució. resoldrem les potències per ordre, usant sobretot la funció φ d'Euler. Tenim que $a^{\varphi(n)} \equiv 1 \pmod{n}$. En particular, com que n en el nostre cas és primer, tenim que $a^{p-1} \equiv 1 \pmod{p}$, i automàticament es compleix que $\text{mcd}(a, p) = 1$. Aleshores, $5^{10} \equiv 1 \pmod{11}$.

$$5^{2010} \iff (5^{10})^{201} \equiv 1^{201} \equiv 1 \pmod{11}. \tag{2.12.2}$$

resolem anàlogament la resta. Ara ens saltarem els detalls específics, ja que s'han vist clars en l'anterior resolució. Notem, per exemple, que hem hagut d'utilitzar el teorema de la divisió entera en l'exponent de l'expressió de l'última línia.

$$\begin{aligned} \varphi(2) &= 1, \varphi(3) = 2, \varphi(5) = 4, \varphi(11) = 10, \\ \varphi(33) &= \varphi(3)\varphi(11) = 20, \varphi(15) = \varphi(3)\varphi(5) = 8. \\ (6^{\varphi(33)})^2 &\equiv 1^2 \equiv 1 \pmod{33} \\ 7^{33 \cdot \varphi(10)+3} \pmod{10} &\iff 7^3 \pmod{10} \iff 7^{135} \equiv 3 \pmod{10}. \end{aligned} \tag{2.12.3}$$

Amb $30^{45} \pmod{15}$ el problema s'ha d'enfocar de manera diferent, ja que $\text{mcd}(15, 30) \neq 1$. Amb la qual cosa, per les propietats dels exponents i de les congruències, tenim equivalentment

$$\begin{aligned} 2^{45} \pmod{15} &\iff 2^{8 \cdot 4 + 5} \pmod{15} \iff 2^5 \pmod{15} \iff 2^{45} \equiv 2 \pmod{15}, \\ 15^{45} &\equiv 0 \pmod{15}. \end{aligned} \tag{2.12.4}$$

Si ens adonem, no era necessari fer el càcul $2^{45} \pmod{15}$ ja que $15^{45} \pmod{15}$ era, directament, congru amb 0. ■

Exercici 2.13. Siguin p, q dos nombres naturals primers diferents. Demostreu que $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Resolució. Per una banda, és evident que $\text{mcd}(p, q) = 1$. Així doncs, podem dir que els termes p^{q-1}, q^{p-1} no tenen factors en comú. D'altra banda, notem que per Fermat i Euler tenim $p^{q-1} \equiv 1 \pmod{q}$ i $q^{p-1} \equiv 1 \pmod{p}$, ja que $\varphi(p) = p-1, \varphi(q) = q-1$.

Podem posar $p^q \equiv p \pmod{pq}$ i $q^p \equiv q \pmod{pq}$, tot i que no ens servirà de molt. Cal fixar-nos que

$$\left. \begin{array}{l} p \mid q^{p-1} - 1 \wedge p \mid p^{q-1} \\ q \mid p^{q-1} - 1 \wedge q \mid q^{p-1} \end{array} \right\} \iff \left. \begin{array}{l} p \mid p^{q-1} + q^{p-1} - 1 \\ q \mid q^{p-1} + p^{q-1} - 1 \end{array} \right\} \xrightarrow{\text{mcd}(p,q)=1} pq \mid q^{p-1} + p^{q-1} - 1 \quad (2.13.1)$$

De la última implicació extraiem $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$, tal i com volíem demostrar. ■

Resolució alternativa. Per Fermat i Euler tenim $p^{q-1} \equiv 1 \pmod{q}$ i $q^{p-1} \equiv 0 \pmod{q}$. Aleshores,

$$\left. \begin{array}{l} p^{q-1} \equiv 1 \pmod{q} \\ q^{p-1} \equiv 0 \pmod{q} \end{array} \right\} \iff p^{q-1} + q^{p-1} \equiv 1 \pmod{q}. \quad (2.13.2)$$

Es podria fer anàlogament intercanviant els papers de p i q i s'arribaria al mateix resultat, però mòdul p . Aleshores, tindríem

$$\left. \begin{array}{l} p^{q-1} + p^{q-1} \equiv 1 \pmod{p} \\ q^{p-1} + p^{q-1} \equiv 1 \pmod{q} \end{array} \right\} \iff p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}. \quad (2.13.3)$$

Exercici 2.14. Demostreu que per a tot nombre natural primer p se satisfà que

$$a^p \equiv b^p \pmod{p} \implies a^p \equiv b^p \pmod{p^2}. \quad (2.14.1)$$

Resolució. Sense pèrdua de generalitat, suposem que $\text{mcd}(a,p) = \text{mcd}(b,p) = 1$. A l'enunciat se'n recomana que utilitzem la propietat del problema 15 de la llista. Suposant-la demostrada, tenim que $p \mid \frac{p!}{k!(p-k)!}$ o, equivalentment, $p \mid \binom{p}{k}$.

Cal suposar $a^p \equiv b^p \pmod{p}$. Per PTFermat, tenim que $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p}$, pel que $a^p \equiv b^p \equiv a \equiv b \pmod{p}$. Com que $a \equiv b \pmod{p}$, podem dir que $a = b + mp$. Aleshores,

$$a^p \equiv (b + mp)^p \equiv \sum_{k=0}^p \binom{p}{k} a^{p-k} (mp)^k \equiv \sum_{k=0,1} \equiv a^p + pmp \equiv a^p \pmod{p}. \quad (2.14.2)$$

Ens hem fixat que tots els termes són divisibles per p i, en particular, per p^2 . ■

Resolució alternativa. $f(x) = x^p - b^p$ té una doble arrel (apliquem el teorema de la doble arrel $(x - c)^2 \mid p(x)$) tal que $x \equiv b$, ja que $f'(b) \equiv pb^{p-1} \equiv 0$. Aleshores, $f(x) \equiv (x - b)^2 g(x)$ i $p^2 \mid f(a) = a^p - b^p \equiv (a - b)^2 g(a)$ donat per $p \mid a - b \equiv a^p - b^p$. ■

Exercici 2.15. Els enters de la forma $M_n := 2^n - 1$, amb n primer, s'anomenen nombres de Mersenne. Un primer de Mersenne és un nombre de Mersenne que, a més, és primer. Demostreu que

$$M_p \text{ és primer} \implies p \text{ és primer.} \quad (2.15.1)$$

Observació 2.15.1. Per començar, algunes consideracions prèvies. Veiem que $2^n - 1$ serà un nombre senar $\forall n \in (\mathbb{Z} \setminus \{0\})$. Fixem-nos que els nombres de la sèrie de Mersenne segueixen una sèrie geomètrica de raó $a - 1$:

$$a^n - 1 = (a - 1) \cdot (a^{n-1} + a^{n-2} + \dots + a + 1), \quad (2.15.2)$$

per la qual cosa $a - 1 \mid a^n - 1$ i $a^n - 1$ seria sempre compost si $a \neq 2$; considerem nombres de la forma $2^n - 1$.

Resolució. Procedint per contrarrecíproc, suposarem que p és compost, és a dir, és $p = \alpha\beta$ tal que $\alpha, \beta > 1$. Aleshores, $2^p = (2^\alpha)^\beta$ i podem, anàlogament a (2.15.2), considerar:

$$(2^\alpha)^\beta - 1 = (2^\alpha - 1)((2^\alpha)^{\beta-1} + (2^\alpha)^{\beta-2} + \cdots + 2^\alpha + 1). \quad (2.15.3)$$

En altres paraules, sempre podrem aïllar un factor $2^\alpha - 1$, així que el nombre solament és primer si $2^\alpha - 1 = 1 \iff 2^\alpha = 2 \iff \alpha = 1$, la qual cosa no es donarà per hipòtesi, ja que $\alpha, \beta > 1$ i, en conseqüència, $2^p - 1$ és compost. Per tant, p és compost implica que $2^p - 1$ és compost, tal i com volíem. ■

Exercici 2.16. Sigui $k \geq 2$ un nombre natural. Demostreu que si $2^k + 1$ és un nombre primer, llavors existeix $n \geq 1$ tal que $k = 2^n$. Els nombres $F_n := 2^{2^n} + 1$ per a $n \geq 0$ s'anomenen nombres de Fermat.

Resolució. Per a tot nombre enter $a > 1$ i tot nombre senar $k' > 1$ la igualtat

$$a^{k'} + 1 = (a+1) \cdot (a^{k'-1} - a^{k'-2} + \cdots + a^2 - a + 1) \quad (2.16.1)$$

proporciona una descomposició no trivial del nombre $a^{k'} + 1$, ja que $2 < a+1 < a^{k'} + 1$. En conseqüència, si $a > 1$ i $k' > 1$ el nombre $a^{k'} + 1$ és compost. Es pot veure que la recíproca d'aquest exercici serà, efectivament, falsa. Sigui $k = 2^n k'$, on $n \geq 0$ és un nombre enter i k' un nombre natural senar, i posem $a := 2^{2^n}$. Llavors, se satisfà la igualtat

$$2^k + 1 = 2^{2^n k'} + 1 = (2^{2^n})^{k'} + 1 = a^{k'} + 1. \quad (2.16.2)$$

Ara, com que $n \geq 0$, és $2^n \geq 1$, de manera que $a := 2^{2^n} > 1$ i, en conseqüència, pel problema anterior, si $2^k + 1$ és primer $k' = 1$, però això ens diu que $k = 2^n$, tal i com volíem demostrar. ■

Exercici 2.17. És cert que $a^k + 1$ primer implica que $a = 2$ i $k = 2^n$?

Resolució. Evidentment no, ja que si agafem a senar $\implies a^k + 1$ parell més gran que 2 i, per tant, compost. Aleshores, a és parell. ■

Exercici 2.18. Sigui $F_n = 2^{2^n} + 1$ l' n -èsim nombre de Fermat, on n és un enter no negatiu. Demostreu que

$$F_0 F_1 \cdots F_{n-1} = F_n - 2, \quad (2.18.1)$$

per a tot $n \geq 1$.

Resolució. Tenim que $F_0 F_1 \cdots F_{n-1} = F_{n-2}$ i procedim per inducció.

1. *Cas inicial:* Agafem $n = 1$. Hem de provar si $F_0 = F_1 - 2$. Efectivament és correcte, ja que $3 = 5 - 2$.
2. *Hipòtesi d'inducció:* $F_0 F_1 \cdots F_{n-1} = F_n - 2$.
3. *resolució:* $(F_0 F_1 \cdots F_{n-1}) F_n = (F_{n-2}) F_n = (F_n^2 - 2F_n + 1) - 1 = (F_n - 1)^2 - 1 = (2^{2^n})^2 - 1 = 2^{2^{n+1}} - 1 = F_{n+1} - 2$.

Corol·lari 2.18.1. Com a conseqüència directa de l'exercici anterior, $\text{mcd}(F_n, F_m) = 1$, amb $n \neq m$.

Exercici 2.19. Demostreu que per a tot parell m, n de nombres enters no negatius, els nombres de Fermat F_m, F_n són relativament primers. Deduïu una demostració alternativa a la donada per Euclides sobre l'existència d'una infinitat de nombres primers.

Resolució. Hem de veure que $\text{mcd}(F_m, F_n) = 1$. Suposarem que $m > n$, i es resoldria anàlogament en un altre cas. També suposarem que $\text{mcd}(F_m, F_n) \neq 1 = d$. Aleshores, $d \mid F_m$ i $d \mid F_n$, amb d impari (tant F_m com F_n són senars). Així doncs, tenim que $d \mid F_m - 2$, ja que $F_m - 2 = F_0 F_1 \cdots F_n \cdots F_{m-1}$ i $d \mid F_n$. Per tant, com per hipòtesi $d \mid F_m$, és necessari que $d \mid 2$. Notem, però, que arribem a una contradicció i s'ha de donar que $d = 1$, perquè abans hem dit que d ha de ser senar.

Per resoldre la segona part solament cal afegir que la sèrie infinita dels nombres de Fermat està formada per elements coprimers dos a dos, és a dir, els factors primers són sempre diferents. Així doncs, es té una quantitat infinita de nombres primers. ■

Exercici 2.20. *Determineu totes les congruències de grau 2 mòdul 2 i totes les seves solucions.*

Resolució. Notem que $0 \leq r < 2$. La solució ve donada directament per la proposició següent.

Proposició 2.20.1. *Considerant un polinomi tal que $f(X) := aX^2 + bX + c$, amb $a, b, c \in \mathbb{Z}$, $a \neq 0$ i p primer. Si $p \mid a$, la congruència $f(x) \equiv 0 \pmod{p}$ no és més que la congruència lineal $bx + c \equiv 0 \pmod{p}$. Per tant, hem de suposar $p \nmid a$. En particular, per al cas $p = 2$. Les solucions de les congruències quadràtiques $f(X) \equiv 0 \pmod{2}$ són*

$$f(X) = \begin{cases} X^2, & \text{solucions: } x \equiv 0 \pmod{2}, \\ X^2 + 1, & \text{solucions: } x \equiv 1 \pmod{2}, \\ X^2 + X, & \text{solucions: } x \equiv 0, 1 \pmod{2}, \\ X^2 + X + 1, & \text{no té solucions mòdul 2.} \end{cases} \quad (2.20.1)$$

Exercici 2.21. *Sigui p un nombre natural primer senar. Demostreu que a $\mathbb{Z}/p\mathbb{Z}$ hi ha exactament $\frac{p+1}{2}$ elements que són quadrats i $\frac{p-1}{2}$ elements que no ho són. Succeeix el mateix si p no és primer?*

Resolució. Considerem el conjunt dels invertibles mòdul p tal que

$$\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \xrightarrow{f} \left(\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*\right)^2 \subseteq \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*, \quad (2.21.1)$$

essent f un morfisme de grups commutatius. Tenim que $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*/\ker f \simeq \text{im } f$. Considerem l'equació $x^2 = y^2$ en $\mathbb{Z}/p\mathbb{Z}$, que podem escriure en la forma equivalent $(x+y)(x-y) = 0$; com que en $\mathbb{Z}/p\mathbb{Z}$ no hi ha divisors de zero, això vol dir que $x-y=0$, o que si $x+y=0$; és a dir, que $y=x$ o bé $y=-x$. Dit d'una altra manera, si a és el quadrat de x , aleshores només ho és dels dos elements x i $-x$.

Per tant, els quadrats diferents de $\mathbb{Z}/p\mathbb{Z}$ són els quadrats dels nombres $1, 2, \dots, \frac{p-1}{2}$, que també són els quadrats de $p-1, p-2, \dots, \frac{p+1}{2} = p - \frac{p-1}{2}$. Per tant, hi ha exactament $\frac{p-1}{2}$ elements no nuls que són quadrats i, en conseqüència, $\frac{p-1}{2}$ elements que no són quadrats.

No succeiria el mateix si p no fos primer. ■

Exercici 2.22. *Trobeu totes les solucions de les congruències següents:*

1. $X^2 \equiv 4 \pmod{p}$, per a tots els nombres primers p ;
2. $X^2 \equiv 31 \pmod{75}$;
3. $X^2 \equiv 46 \pmod{231}$;
4. $X^2 \equiv 16 \pmod{105}$;

$$5. X^2 \equiv 1156 \pmod{3^2 \cdot 5^4 \cdot 7^5 \cdot 11^6}.$$

Resolució.

1. $X^2 \equiv 4 \pmod{p}$: per a tots els nombres primers p . Ens queda que $(x+2)(x-2) \equiv 0 \pmod{p}$. Aleshores, $x \pm 2 \equiv 0 \pmod{p} \iff x \equiv \mp 2 \pmod{p}$.
2. $X^2 \equiv 31 \pmod{75}$, aplicant TXResidu ens queda que $x^2 \equiv 1 \pmod{3}$ i $x^2 \equiv 6 \pmod{25}$, així que $x \equiv \pm 1 \pmod{3}$ i $x \equiv \pm 9 \pmod{25}$. Vegem que forçosament $x^2 \equiv 6 \equiv 1 \pmod{5} \iff x \equiv \pm 1 \pmod{5}$. Usant que $x \equiv 1 + 5\lambda$ trobem que $\lambda \equiv 3 \pmod{5}$ i, per tant, que $x \equiv 16 \pmod{25}$. Aplicant que $x \equiv -1 + 5\lambda$ trobem $x \equiv -16 \pmod{25}$. Per l'altra congruència, ens queden finalment $x \equiv \pm 16$ i.
3. $X^2 \equiv 46 \pmod{231}$, aplicant que $231 = 3 \cdot 7 \cdot 11$ tenim que $x^2 \equiv 46 \equiv 2 \pmod{11}$, però $(\pm 3)^2 = 9 \equiv -2 \pmod{11}$. Com que no té solució mòdul 11 no tindrà solució mòdul 231.
4. $X^2 \equiv 16 \pmod{105}$;
5. $X^2 \equiv 1156 \pmod{3^2 \cdot 5^4 \cdot 7^5 \cdot 11^6}$: després de veure la resolució de l'Artur vegem que es fa a partir del *Mathematica*.



Exercici 2.23.

1. Demostreu que -2 és un quadrat mòdul un nombre primer $p > 2$ i, si només si, $p \equiv 1 \pmod{8}$ o bé $p \equiv 3 \pmod{8}$.
2. Sigui n un nombre enter, i posem $N := (2n+1)^2 + 2$. Demostreu que N és divisible per un nombre natural primer p tal que $p \equiv 3 \pmod{8}$.
3. Demostreu que hi ha una infinitat de nombres primers de la forma $8k+3$, $k \in \mathbb{N}$.

Resolució.

1. Podem demostrar les dues implicacions o fer una cadena d'equivalències. Aplicarem la proposició següent:

Proposició 2.23.1. Sigui p un nombre primer senar. Aleshores,

$$\begin{pmatrix} 2 \\ p \end{pmatrix} = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{si } p \equiv \pm 1 \pmod{8}, \\ -1, & \text{si } p \equiv \pm 3 \pmod{8}. \end{cases} \quad (2.23.1)$$

Demostració. Considerem les $\frac{p-1}{2}$ congruències següents:

$$\begin{aligned} p-1 &\equiv 1 \cdot (-1)^1 \pmod{p}, \\ 2 &\equiv 2 \cdot (-1)^2 \pmod{p}, \\ p-3 &\equiv 3 \cdot (-1)^3 \pmod{p}, \\ 4 &\equiv 4 \cdot (-1)^4 \pmod{p}, \\ &\vdots \\ a &\equiv \frac{p-1}{2} \cdot (-1)^{\frac{p-1}{2}} \pmod{p}, \end{aligned} \quad (2.23.2)$$

on a és $\frac{p-1}{2}$ o bé $p - \frac{p-1}{2}$, segons si $\frac{p-1}{2}$ és parell o senar. Si multipliquem totes aquestes congruències i tenim en compte que a l'esquerra apareixen els $\frac{p-1}{2}$ nombres parells positius i menors que p obtindrem la nova congruència

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! = 2 \cdot 4 \cdots (p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^r \pmod{p}, \quad (2.23.3)$$

on r és la suma dels exponents de -1 : $r = \sum_{j=1}^{\frac{p-1}{2}} j = \frac{1}{2} \frac{p-1}{2} \frac{p+1}{2} = \frac{p^2-1}{8}$. Per tant, podem simplificar el factor $\left(\frac{p-1}{2}\right)!$ i obtenim la congruència $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$. Així, en virtut del criteri d'Euler, se satisfà la relació $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$. De nou, com en el càlcul de $\left(\frac{-1}{p}\right)$, en tenir en compte que els dos factors són ± 1 , obtenim la primera igualtat. La segona és una simple comprovació: si $p \equiv \pm 1 \pmod{8}$, aleshores $\frac{p^2-1}{8} \equiv 0 \pmod{2}$, de manera que el nombre enter $\frac{p^2-1}{8}$ és parell, mentre que si $p \equiv \pm 3 \pmod{8}$, aleshores $\frac{p^2-1}{8} \equiv 1 \pmod{2}$ i $\frac{p^2-1}{8}$ és un nombre enter senar. ■

Ara, ja sabem que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, i també que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Aplicant les seves propietats, ens queda que $\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)(p+5)}{8}}$. Aleshores, $p \equiv 1 \pmod{8}$ o bé $p \equiv 3 \pmod{8}$, en particular $p \equiv 3 \pmod{8}$, ja que $\exists p \not\equiv 1 \pmod{8}$ tal que $p | N$, així que forçosament $p \equiv 3 \pmod{8}$.

2. Solament fa falta suposar que $p | (2n+1)^2$ i veure que $p \equiv 3 \pmod{8}$, la qual cosa és directa si ens adonem que -2 és residu quadràtic mòdul p i, per l'apartat anterior, deduïm que, efectivament, és cert.

3. El teorema de Dirichlet diu que per $a, b \in \mathbb{Z}$, $\text{mcd}(a, b) = 1$ i una seqüència no nula d'elements $an + b$ aquesta és infinita i conté infinitis nombres primers.

També podem fer una demostració per reducció a l'absurd [Arr]. Com sempre, suposem que p_1, \dots, p_r són tots els nombres primers de la forma $8k+3$. Considerem el nombre $a = (p_1 p_2 \cdots p_r)^2 + 2$. Aleshores, si p és un divisor primer d' a (necessàriament senar) es tindrà que $(p_1 p_2 \cdots p_r)^2 \equiv -2 \pmod{p}$ i, sabent que

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & \text{si } p \equiv 1 \pmod{8} \text{ o bé } p \equiv 3 \pmod{8}, \\ -1 & \text{si } p \equiv 5 \pmod{8} \text{ o bé } p \equiv 7 \pmod{8}, \end{cases} \quad (2.23.4)$$

es tindrà que $p \equiv 1 \pmod{8}$ o bé $p \equiv 3 \pmod{8}$. Com a és de la forma $8k+3$ (ja que el quadrat de cada p_i és de la forma $8k+1$), no tots els divisors d' a són de la forma $8k+1$. Per tant, a és divisible per algun nombre primer de la forma $8k+3$, és a dir, per algun p_i , la qual cosa és la contradicció que volíem trobar. ■

Exercici 2.24. Siguin a, n nombres naturals relativament primers. Estudieu quan l'equació congruencial $x^2 \equiv a \pmod{n}$ té solució.

Resolució. a ha de ser residu quadràtic mòdul n . El símbol de Legendre val $\left(\frac{a}{p}\right) = 1$ si, i només si, la congruència $x^2 \equiv a \pmod{p}$ té solució.

Considerem $n \geq 2$. Sabem que n es pot descompondre com a producte finit de factors primers $n = p_1^{v_1} \cdots p_r^{v_r}$, amb p_i primers diferents dos a dos, $v_i \geq 1$. Sabem també que $\text{mcd}(a, n) = 1$ si, i només si, $\text{mcd}(a, p_i) = 1, \forall i$. Aleshores, $\exists x \in \mathbb{Z} \mid x^2 \equiv a \pmod{n} \iff \forall i \exists x \in \mathbb{Z} \mid x^2 \equiv a \pmod{p_i^{v_i}}$. Aleshores, segons TXResidu,

$$\#\{\text{solucions de } x^2 \equiv a \pmod{n}\} = \prod_{i=1}^r \#\{\text{solucions de } x^2 \equiv a \pmod{p_i^{v_i}}\}. \quad (2.24.1)$$

Suposant $p_i > 2$, ens queda que $x^2 \equiv a \pmod{n}$ té solució si, i només si, $x^2 \equiv a \pmod{p_i^{v_i}}$ té solució si, i només si $x^2 \equiv a \pmod{p_i}$ té solució. Agafem un primer $p \in \{p_1, \dots, p_i, \dots, p_r\} > 2, p \nmid a$.

$$x^2 \equiv a \pmod{p^{v+1}} \implies x^2 \equiv a \pmod{p^v}, 1 \leq x < p^v. \quad (2.24.2)$$

Aleshores, $y = x + \lambda p^v, 1 \leq y < p^{v+1}$. Elevant al quadrat, $y^2 = x^2 + 2\lambda x p^v + \lambda^2 p^{2v}$, i

$$a \equiv x^2 + 2\lambda x p^v \pmod{p^{v+1}}. \quad (2.24.3)$$

Considerant que $x^2 = a + \mu p^v$, ens queda que $a \equiv a + \mu p^v + 2\lambda x p^v \pmod{p^{v+1}} \iff (2\lambda x + \mu)p^v \equiv 0 \pmod{p^{v+1}}$ i per tant, $2\lambda x + \mu \equiv 0 \pmod{p}$, la qual cosa ens diu que existeix una única λ que compleix aquesta congruència, tal i com volíem provar. (Resolució completa a [Gra98].) ■

Exercici 2.25. Demostreu que hi ha una infinitat de nombres naturals primers de la forma $4k + 1$.

Resolució. Suposem que $p \mid x^2 + 1$. En altres paraules, estem dient que $x^2 \equiv -1 \pmod{p}$. Aleshores, $p = 2$ o bé $p \equiv 1 \pmod{4}$. Considerem $p_0, \dots, p_r \equiv 1 \pmod{4}, p \neq p_0, \dots, p_r$. ■

Exercici 2.26. Per a quins nombres naturals primers p el nombre tres és residu quadràtic mòdul p ? $I - 3?$

Resolució. Volem trobar els nombres naturals p de la forma $\left(\frac{3}{p}\right) = 1$, ja que 3 ha de ser residu quadràtic mòdul p . En el cas de $\left(\frac{-3}{p}\right)$, hem de calcular $\left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = 1$. Tenim $\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right)$, i

$$\left(\frac{p}{3}\right) \equiv \begin{cases} 0, & \text{si } p = 3, \\ 1, & \text{si } p \equiv 1 \pmod{3}, \\ -1, & \text{si } p \equiv -1 \pmod{3} \end{cases} \quad (2.26.1)$$

Exercici 2.27. Sigui $N > 6$ un nombre enter per al qual existeix alguna arrel primitiva mòdul N . Demostreu que el producte de totes les arrels primitives mòdul N és $1 \in (\mathbb{Z}/n\mathbb{Z})^*$.

Resolució. Tenim que una arrel primitiva mòdul N és de la forma $\zeta^{\varphi(N)} \equiv 1 \pmod{N}$. Sabem que, donat que $\text{mcd}(a, N) = 1$, ζ , qualsevol, posseeix invers. A més, aquest invers resulta ser també una arrel primitiva: es pot comprovar fàcilment que l'ordre de ζ^{-1} també és $\varphi(N)$. Aleshores, considerant que podem organitzar les ζ_1, \dots, ζ_r arrels primitives mòdul N en parells (ja que la inversa d'una arrel ζ és única i $a \neq a^{-1}$ ja que $a^2 = 1$ i $\text{ord}(a) = \varphi(N) \mid 2$, però $\varphi(N) > 2$) $\{\zeta_i, \zeta_j\} \mid \zeta_i \zeta_j \equiv 1 \pmod{N}$. Per tant, al fer $\zeta_1 \cdots \zeta_r$ les arrels s'anirien cancel·lant automàticament, així que ens quedaria $\zeta_1 \cdots \zeta_r \equiv 1 \pmod{N}$, tal i com volíem. ■

Exercici 2.28. Sigui p un nombre natural primer i $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Demostreu que per a tot nombre enter n tal que $\text{mcd}(n, p-1) = 1$ la congruència $X^n \equiv a \pmod{p}$ té solament una solució.

Resolució. Comencem amb una sèrie d'observacions: primer de tot, com que $\text{mcd}(n, p-1) = 1$ és evident que $n \nmid \varphi(p) \implies a \neq 1$. I, de fet, per aquesta raó podem dir que n és invertible mòdul $\varphi(p)$: $n\ell \equiv 1 \pmod{\varphi(p)}$ per a un $\ell \in (\mathbb{Z}/\varphi(p)\mathbb{Z})^*$.

Sigui g una arrel primitiva mòdul p , i sigui i l'índex d' a respecte g . Al seu torn, tota solució x ha de ser $\text{mcd}(x, p) = 1$, i per tant sigui u l'índex d' x . Aleshores, la congruència $x^n \equiv a$ es converteix en la congruència $g^{nu} \equiv g^i \pmod{p} \iff nu \equiv i \pmod{p-1}$. Com que

$\text{mcd}(n, p - 1) = 1$, podem considerar $u \equiv in^{-1} \pmod{p - 1}$. Com que l'invers és únic i i està fixat, tenim que la congruència $g^{nu} \equiv g^i \pmod{p}$ té solució única i, per tant, $x^n \equiv a \pmod{p}$ té solució única. ■

Exercici 2.29. Sigui p un nombre natural primer, $a \in (\mathbb{Z}/p\mathbb{Z})^*$ i m l'ordre d' a en $(\mathbb{Z}/p\mathbb{Z})^*$. Demostreu que la congruència $X^n \equiv a \pmod{p}$ té solució si, i només si, $\text{mcd}(p - 1, n)$ divideix $\frac{p-1}{m}$ i que, en aquest cas, el nombre de solucions de la congruència és $\text{mcd}(p - 1, n)$.

Resolució. Sigui g una arrel primitiva mòdul p , i sigui i l'índex d' a respecte g . Al seu torn, tota solució x ha de ser $\text{mcd}(x, p) = 1$, i per tant sigui u l'índex d' x . Aleshores, la congruència $x^n \equiv a \pmod{p}$ es converteix en la congruència $g^{nu} \equiv g^i \pmod{p} \iff nu \equiv i \pmod{p - 1}$. Sigui $k = \text{mcd}(n, p - 1)$. Tenim que $m = \text{ord}(a) = \text{ord}(g^s) = \frac{\text{ord}(g)}{\text{mcd}(s, \text{ord}(g))} = \frac{p-1}{\text{mcd}(s, p-1)}$. Existeix solució de l'equació si, i només si, $\text{mcd}(n, p - 1) \mid i$. Tenint en compte que $\text{mcd}(s, p - 1) = \frac{p-1}{m}$, és evident que $\frac{p-1}{m} \mid s$. ■

Proposició 2.29.1. Considerem $(\frac{\mathbb{Z}}{N\mathbb{Z}})^*$. És un grup cíclic si, i només si, existeix una arrel primitiva mòdul N .

Exercici 2.30. Sigui $p \in \mathbb{N}$, senar, i $g \in \mathbb{Z}, p \nmid g$. Demostreu que p és una arrel primitiva mòdul p si, i només si, per a tot divisor primer ℓ de $p - 1$ és $g^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p}$.

Resolució. Una arrel primitiva té ordre $\varphi(p) = p - 1$. Podem reescriure $p - 1$ com $\ell_1^{v_1(\ell)} \ell_2^{v_2(\ell)} \dots \ell_n^{v_n(\ell)}$, tal que $\ell \leq p - 1$. Pel Teorema Fonamental de l'Aritmètica. Aleshores, ens queda que $g^{\frac{\ell_1^{v_1(\ell)} \dots \ell_n^{v_n(\ell)}}{\ell}}$. Operant, tenim que $g^{\ell_1^{v_1(\ell)} \dots \ell_{i-1}^{v_{i-1}(\ell)} \ell_i^{v_i(\ell)-1} \ell_{i+1}^{v_{i+1}(\ell)} \dots \ell_n^{v_n(\ell)}}$, amb $\lambda = \ell_1^{v_1(\ell)} \dots \ell_{i-1}^{v_{i-1}(\ell)} \ell_i^{v_i(\ell)-1} \ell_{i+1}^{v_{i+1}(\ell)} \dots \ell_n^{v_n(\ell)} < p - 1$. Així doncs, ens queda un últim argument per enllistar aquesta demostració. Podríem raonar les dues implicacions de manera directa, així que es farà tot de manera encara més compacta.

Si aquesta quantitat fos congruent amb 1, tindríem que $\lambda < p - 1$ seria l'ordre de g , per la qual cosa no seria arrel primitiva, ja que una arrel primitiva g^k mòdul n té ordre $\varphi(n)$. Davant d'aquesta contradicció, que ve de suposar $g^{\frac{p-1}{\ell}} \equiv 1 \pmod{p}$, hem demostrat el que volíem. ■

Observació 2.30.1. Compte! No sé si estaria bé. [Gra98, pàg. 191] ens dona un corol·lari que diu: *Sigui $N \geq 2$ un nombre enter. Suposem que existeix una arrel primitiva, g , mòdul N . Les altres arrels primitives mòdul N són els elements g^k tals que $1 \leq k \leq \varphi(N)$ i $\text{mcd}(k, \varphi(N)) = 1$.*

Resolució, corregida.

\Rightarrow Si N és primer, sigui g una arrel primitiva mòdul N ; la proposició anterior ens permet assegurar que g satisfà que $g^{N-1} \equiv 1 \pmod{N}$ i que per a tot divisor primer ℓ de $N - 1$, tenim que $g^{\frac{N-1}{\ell}} \not\equiv 1 \pmod{N}$. [Gra98, pàg. 241]

\Leftarrow Suposem que existeix un nombre enter g , $2 \leq g \leq N - 2$ que satisfà que $g^{N-1} \equiv 1 \pmod{N}$. En virtut d'això, és $g \in G(N)$ i, si m és l'ordre de g en $G(N)$, també obtenim que $m \mid N - 1$. Però si, a més, suposem que per a tot divisor primer ℓ de $N - 1$ tenim que $g^{\frac{N-1}{\ell}} \not\equiv 1 \pmod{N}$, m no pot ser un divisor estricte de $N - 1$, ja que no divideix cap dels nombres $\frac{N-1}{p}$, per als divisors primers de p de $N - 1$. En conseqüència, g és d'ordre $N - 1 \leq \varphi(N)$, d'on $N - 1 = \varphi(N)$ i N és primer. [Gra98, pàg. 241] ■

Exercici 2.31. Sigui $p \in \mathbb{N}$ primer i senar, tal que $q := 2p - 1$, amb q també un nombre primer. Posem $N := pq$. Demostreu que N és un nombre pseudoprimer respecte de tota base $b \in (\mathbb{Z}/N\mathbb{Z})^*$ que sigui un quadrat en $(\mathbb{Z}/q\mathbb{Z})^*$. En particular, N és pseudoprimer, com a mínim, per la meitat de les bases possibles.

Resolució. Veiem clarament que $p > 2$. Primerament, notem que N és pseudoprimer si, i només si, $b^{N-1} \equiv 1 \pmod{N}$. Tenim $q := 2p - 1$ primer i $N = pq$, així com $b \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$, donat que $p \nmid b$. A més, tenim que b és quadrat mòdul p , així que $\left(\frac{b}{q}\right) = 1$. Per tant,

$$\left(\frac{b}{q}\right) \equiv b^{\frac{q-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{q}, \quad b^{p-1} \equiv 1 \pmod{p}. \quad (2.31.1)$$

Per TXResidu, obtenim que $b^{p-1} \equiv 1 \pmod{N} \implies B^{N-1} \equiv 1 \pmod{N}$. Ara, $N - 1 = pq - 1 = (p - 1)(2p + 1) = p(2p - 1) - 1 = 2p^2 - p - 1 = (p - 1)(2p + 1)$. De fet,

$$\begin{cases} b^{(p-1)(2p+1)} \equiv b^{p-1} \equiv 1 \pmod{p} \\ b^{(p-1)(2p+1)} \equiv (b^{p-1})^2 \equiv 1 \pmod{2p-1} \end{cases} \quad (2.31.2)$$

Per a demostrar que N és pseudoprimer per a la meitat de les bases com a mínim (és a dir, en pot ser per a més), solament cal tenir en compte que

$$\# \left(\left(\frac{\mathbb{Z}}{q\mathbb{Z}} \right)^* \right)^2 = \frac{q-1}{2}. \quad (2.31.3)$$

Com que b és un quadrat invertible mòdul q , tenim que $b^{\frac{q-1}{2}} \equiv 1 \pmod{q}$. O sigui, ja que $\frac{q-1}{2} = p - 1$, tenim que $b^{p-1} \equiv 1 \pmod{q}$. D'altra banda, pel petit teorema de Fermat, tenim que $b^{p-1} \equiv 1 \pmod{p}$. I, en conseqüència, per ser $p \neq q$ i tots dos primers, $b^{p-1} \equiv 1 \pmod{pq}$. Així, és suficient veure que $p - 1$ divideix $N - 1$ (de manera que tindrem que $b^{N-1} \equiv 1 \pmod{N}$, com volem). Però un càlcul senzill demostra que $N - 1 = pq - 1 = (p - 1)(2p + 1)$. Per tant, hem vist que N és pseudoprimer per a la base b .

La resta de l'exercici també és senzilla. Tenim la meitat de quadrats mòdul q , i cap condició mòdul p . Per tant, la propietat se satisfà, com a mínim, per a aquesta quantitat d'elements, com cal veure. ■

Exercici 2.32.

1. Sigui $N := pq$ el producte de dos nombres naturals primers senars p i q . Demostreu que si N és pseudoprimer respecte d'una base $b > 1$, aleshores $p \mid (b^{q-1} - 1)$ i $q \mid (b^{p-1} - 1)$.
2. Deduïu de l'apartat anterior que, fixats un nombre primer p i una base $b > 1$, el conjunt dels nombres primers q per als quals $N := pq$ és pseudoprimer respecte de la base b és finit.

Resolució.

1. Tenim que N és pseudoprimer si, i només si, $b^{pq-1} \equiv 1 \pmod{pq}$. Aleshores, per TXResidu, considerant també que $b^{p-1} \equiv 1 \pmod{p}$ i $b^{q-1} \equiv 1 \pmod{q}$, ens queda:

$$\begin{aligned} \begin{cases} b^{pq-1} \equiv 1 \pmod{p}, \\ b^{pq-1} \equiv 1 \pmod{q}. \end{cases} &\implies \begin{cases} pq \equiv p \pmod{p-1}, \\ pq \equiv q \pmod{q-1}. \end{cases} \\ \implies \begin{cases} q \equiv 1 + (p-1) \equiv p \pmod{p-1}, \\ p \equiv 1 + (q-1) \equiv q \pmod{q-1}. \end{cases} &\implies \begin{cases} b^{p-1} \equiv b^{q-1} \equiv 1 \pmod{p}, \\ b^{q-1} \equiv b^{p-1} \equiv 1 \pmod{q}. \end{cases} \end{aligned} \quad (2.32.1)$$

D'altra banda, també podem raonar que $b^{pq-1} = b^{pq}b^{-1}$. Si tenim en compte que $b^p \equiv b \pmod{p}$, aleshores ens queda $b^{q-1} \pmod{p}$. Podríem raonar anàlogament en l'altre cas. Hem usat que $b \in (\frac{\mathbb{Z}}{N\mathbb{Z}})^*$ i, per tant, $b \in (\frac{\mathbb{Z}}{p\mathbb{Z}})^*$ i $b \in (\frac{\mathbb{Z}}{q\mathbb{Z}})^*$.

2. Pel que fa al segon apartat. Tenim el teorema següent [CP06]:

Teorema 2.32.1. *Per a cada enter $b \geq 2$ el nombre de pseudoprimeres amb base b és infinit.*

Ara, si suposem p i b constants, tenim directament a causa de la fixació de p que el conjunt de q primers per als quals N és pseudoprimer ha de ser finit.

Correcció de l'Artur: $b^{p-1} - 1$.



RESULTATS BÀSICS

1. Teorema Xinès del Residu
2. Teorema d'Euler, Petit Teorema de Fermat.
3. $\text{ord}(g^k) = \frac{\text{ord}(g)}{\text{mcd}(k, \text{ord}(g))}$.
4. $a^k \equiv 1 \pmod{n} \implies \text{mcd}(a, n) = 1$.
5. $a^{k-1} \equiv a^{-1} \pmod{n}$.
6. $\text{ord}_n(a) \mid k$.
7. Criteri d'Euler en el càlcul del símbol de Legendre: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Compte amb aplicar-lo directament al símbol de Jacobi directament, no es pot.

Exemple 3.1. Tenim que $\left(\frac{2}{3}\right) \neq \left(\frac{2}{9}\right)$. De fet, tenim que $\left(\frac{a}{3}\right)^2$ és 0 o 1, següent les seves propietats.

$$\begin{aligned}
 20) \quad & \left. \begin{array}{l} x \equiv 1 \pmod{5} \\ x \equiv 3 \pmod{8} \\ x \equiv 3 \pmod{12} \end{array} \right\} \iff \left. \begin{array}{l} x \equiv 1 \pmod{5} \\ x \equiv 3 \pmod{2} \\ x \equiv 3 \pmod{4} \\ x \equiv 3 \pmod{3} \\ x \equiv 3 \pmod{4} \end{array} \right\} \iff \left. \begin{array}{l} x \equiv 1 \pmod{5} \\ x \equiv 3 \pmod{4} \\ x \equiv 3 \pmod{3} \\ x \equiv 0 \pmod{3} \end{array} \right\} \\
 & \text{mcd}(3, 4, 5) = 1 \quad || \\
 & x = \sum_{i=0}^3 n_i M_i c_i \quad || \\
 & \iff x = 0 \cdot n_1 + 45n_2 + 12n_3 = 171 \\
 \begin{array}{|c|c|c|c|} \hline 19) & n_1 & 20 & 0 \\ \hline 20) & n_2 & 15 & 3 \\ \hline 21) & n_3 & 12 & 1 \\ \hline \end{array} & \iff 20n_1 \equiv 1 \pmod{3} \iff n_1 = -1 + 3k > 0 \iff n_1 = 2 \\
 & \iff 15n_2 \equiv 1 \pmod{4} \iff n_2 = -1 + 4k > 0 \iff n_2 = 3 \\
 & \iff 12n_3 \equiv 1 \pmod{5} \iff n_3 = -2 + 5k > 0 \iff n_3 = 3 \\
 & x \equiv 171 \pmod{60} \iff x \equiv 51 \pmod{60}
 \end{aligned}$$

Figura 1: A tall d'observació, adjunto com resolia TXResidu

 4
RESOLUCIONS D'EXAMEN

4.1 Examen 2020

Exercici 4.1. Sigui c un nombre enter positiu $10 \leq c \leq 10^3$. Determina el més petit valor tal que l'equació diofantina $84x + 990y = c$ té solució entera. Resol l'equació en tal cas.

Ara, donat el sistema

$$\begin{aligned} x &\equiv 4 \pmod{8} \\ x &\equiv a \pmod{6} \\ 14x &\equiv 1 \pmod{15} \end{aligned} \tag{4.1.1}$$

Resolució. Notem que $\text{mcd}(84, 990) = 6$. Així doncs, ens queda que

$$14x + 165y = 1 \iff x = 59, y = -5. \tag{4.1.2}$$

Per tal que tingui solució entera, $6 \mid c$. El nombre més petit que compleix aquest cas, adaptant-nos a les directrius de l'enunciat, és $c = 6$. Resolent l'equació en aquest cas:

$$14x + 165y = 1 \iff x = 59, y = -5. \tag{4.1.3}$$

Procedim a resoldre l'apartat b .

Exercici 4.2.

1. Demostra que per a tot $a, b, m \in \mathbb{Z}$ és $\text{mcd}(ab, m) \mid \text{mcd}(a, m)\text{mcd}(b, m)$. Al seu torn, demostra que per a tot $a, b \in \mathbb{Z}$, si $\text{mcd}(a, b) = 1$, aleshores $\text{mcd}(a, m)\text{mcd}(b, m) = \text{mcd}(ab, m)$.
2. Sigui n el teu NIUB. Calcula les potències següents: $n^7 \pmod{42}$ i $6^n \pmod{33}$.

Resolució. Aplicant la definició de mcd, volem trobar que $d \mid ef$. Aleshores, podem fer diverses afirmacions:

1. $\text{mcd}(ab, m) = d \implies d \mid ab \wedge d \mid m \implies d \mid ab \pm m$.
2. $\text{mcd}(a, m) = e \implies e \mid a \wedge e \mid m \implies e \mid a \pm m$.
3. $\text{mcd}(b, m) = f \implies f \mid b \wedge f \mid m \implies f \mid b \pm m$.

D'una banda podem dir que $ef \mid ab$, però no podem inferir directament que, aleshores, $d \mid ef$ i resoldre el problema, ja que la justificació aportada és nul·la. Es pot provar a partir de la linealitat de la divisibilitat: tenim $d = \alpha_1 ab + \beta_1 m$, $ef = \alpha_2 \alpha_3 ab + am\alpha_1\beta_2 + bm\beta_1\alpha_2 + m^2\beta_1\beta_2$. Per tant, recordant $d \mid ab \wedge d \mid m$, ens queda:

$$d \mid \alpha_2 \alpha_3 ab + am\alpha_1\beta_2 + bm\beta_1\alpha_2 + m^2\beta_1\beta_2, \tag{4.2.1}$$

ja que d divideix qualsevol dels termes. La igualtat que se'ns demana a l'enunciat és immediata quan considerem el cas $\text{mcd}(a, m)\text{mcd}(b, m) \mid \text{mcd}(ab, m)$ amb $\text{mcd}(a, b) = 1$.

Pel que fa a l'últim apartat, tenim el NIUB generat aleatoriament 20392724 i, per tant, l'equació $6^{20392724} \pmod{33}$. Notem per començar que $\text{mcd}(6, 33) \neq 1$, així que cal descompondre el nombre en $2^{20392724}3^{20392724} \pmod{33}$, la qual cosa podem fer per les propietats dels exponents. Dividim el problema:

1. $2^{20392724} \pmod{33}$. Aplicant la funció φ d'Euler, tenim que $\varphi(33) = 20$:

$$2^{\varphi(33) \cdot 1019636 + 4} \pmod{33} \iff (2^{\varphi(33)})^{1019636} 2^4 \pmod{33} \iff 2^{20392724} \equiv 16 \pmod{33}. \tag{4.2.2}$$

2. $3^{20392724} \pmod{33}$. Seguim tenint que $\text{mcd}(3, 33) \neq 1$, així que caldrà aplicar TXR:

$$3^{20392724} \equiv 0 \pmod{3} \quad (4.2.3)$$

$$3^{20392724} \pmod{11} \iff 3^4 \equiv 4 \pmod{11} \iff 3^{20392724} \equiv 15 \pmod{33}.$$

Per tant, ens queda $6^{20392724} \equiv 16 \cdot 15 \equiv 9 \pmod{33}$. Si ho passem pel *Mathematica*, veiem que els resultats coincideixen.

Ara ens queda resoldre $20392724^7 \pmod{42}$. La intenció seria aplicar el petit teorema de Fermat, així que hauríem de transformar l'expressió:

$$\begin{aligned} 20392724^7 &\equiv 20392724^6 \pmod{2} \\ 20392724^7 &\equiv 20392724^5 \pmod{3} \\ 20392724^7 &\equiv 20392724 \equiv 2 \pmod{7} \end{aligned} \quad (4.2.4)$$

Com que s'han de complir les tres congruències, en particular s'ha de complir la tercera, per tant $20392724^7 \equiv 2 \pmod{42}$. ■

Exercici 4.3. Calcula el màxim comú divisor i una identitat de Bézout dels següents polinomis de $\mathbb{Q}[x]$:

$$\begin{aligned} A(x) &= x^8 - 3x^4 - 4, \\ B(x) &= x^7 + x^4 - 4x^3 - 4. \end{aligned} \quad (4.3.1)$$

Determina les arrels del polinomi $A(x)$ pensat com a polinomi de $\mathbb{K}[x]$, on \mathbb{K} és cadascun dels següents cossos: $\mathbb{R}, \mathbb{C}, \mathbb{Z}/(7\mathbb{Z})$.

Resolució. Per trobar el màxim comú divisor ens cal resoldre iterativament els polinomis fins a trobar-ne un d'irreductible. Resolem l'equació en 2 i, per tant, el nostre $\text{mcd}(x^8 - 3x^4 - 4, x^7 + x^4 - 4x^3 - 4) = x^4 - 4$.

Ara fem arrels del polinomi $A(x)$.

Figura 2: Equació resolta

Exercici 4.4. Siguin a, b nombres enters positius tals que $a > b + 1$. Determina si el nombre $m = a^2 - b^2$ pot ser un nombre primer. Justifica la resposta.

Resolució. Podem posar m de la següent manera:

$$a^2 - b^2 = (a + b)(a - b). \quad (4.4.1)$$

D'aquesta manera, acotant inferiorment la restricció en els positius de \mathbb{Z} , tenim que $b = 1 \iff a > 2$. D'aquesta manera, ambdós termes $(a + b), (a - b) > 1$, amb la qual cosa m no s'escriu de forma única com a producte d'1 per ell mateix, així que no és primer. ■

4.2 Examen P-2018

Exercici 4.5.

1. *Dona la definició de màxim comú divisor de dos polinomis en un cos. Demostra que existeix i és únic tret d'un factor constant no nul.*
2. *Dona la definició de nombre primer i una demostració de la infinitud del conjunt de nombres primers.*

Resolució. El màxim comú divisor de dos polinomis $p(x), q(x)$ és un polinomi $d(x)$ tal que és aquell amb grau més gran que compleix $d(x) \mid p(x) \wedge d(x) \mid q(x)$. En altres paraules, $d(x)$ també compleix que si $s(x) \mid p(x) \wedge s(x) \mid q(x) \iff s(x) \mid d(x)$.

Un nombre primer és aquell nombre enter positiu més gran que 1 que es pot escriure de forma única com a producte d'ell mateix per 1. Per tal de demostrar la infinitud del conjunt dels nombres primers, ens podem ajudar del teorema i del lema d'Euclides. A continuació, la seva enunciació i demostració.

Teorema 4.5.1 (Teorema d'Euclides). *El conjunt dels nombres primers és infinit.*

Lema 4.5.1. *Per tot nombre primer P existeix un altre nombre primer P' tal que $P < P'$.*

Demostració del lema 4.5.1. Considerem un nombre primer P . Sigui $R = P! + 1$. Com $P \leq P!$, tenim que $P < R$. Demostrem per reducció a l'absurd que R és primer. *Suposem llavors que R és compost.* Sigui Q un factor primer de R . *Un factor primer és un nombre primer que apareix en la descomposició en factors primers de R .* Com Q és un factor primer de R , tenim que $Q \leq R$, però, com que Q és primer i R és compost, deduïm que $Q < R$. Per tant, $Q \leq P!$. Doncs, Q és un factor primer de $P!$.

Però com Q és un factor primer de R , tenim que Q és un divisor de $R = P! + 1$.

Així doncs, com Q és un divisor de $P!$ i és també un divisor de $P! + 1$, deduïm que Q és divisor de 1 i, per tant, que $Q = 1$, la qual cosa és impossible donat que Q és primer (i per tant, $Q \geq 2$). ■

Demostració del teorema d'Euclides. Demostrem el teorema d'Euclides per reducció a l'absurd. Suposem que el conjunt A dels nombres primers és finit. Sigui, doncs, P l'últim nombre primer, el qual existeix perquè estem suposant que A és finit. Aplicant llavors el lema 4.5.1, obtenim que existeix un nombre primer R tal que $P < R$. Però llavors, P no és l'últim nombre primer, amb la qual cosa arribem a una contradicció. ■

Exercici 4.6.

1. *Dona la descomposició en polinomis irreductibles en $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ del polinomi*

$$x^5 - 3x^4 + x^3 - 3x^2 - 6x + 18. \quad (4.6.1)$$

2. *Completa la multiplicació següent, en base 16:*

$$\begin{array}{r}
 & c & 7 & e \\
 \times & 2 & f & 7 \\
 \hline
 & 5 & 7 & 7 & 2 \\
 ? & ? & 6 & 2 \\
 \hline
 1 & 8 & f & c \\
 \hline
 ? & ? & ? & 9 & 9 & 2
 \end{array} \quad (4.6.2)$$

3. Calcula totes les solucions enteres de l'equació diofantina

$$12x + 10y + 15z = 7. \quad (4.6.3)$$

Determina'n les solucions (x, y, z) per a les quals també és $x + y + z = 1$.

Resolució. En primer lloc, se'ns demana reduir a polinomis irreductibles el $x^5 - 3x^4 + x^3 - 3x^2 - 6x + 18$. Per Ruffini, obtenim primer $(x - 3)(x^4 + x^2 - 6)$ i, aplicant un canvi de variable i Ruffini un altre cop, obtenim $(x - 3)(x^2 + 3)(x^2 - 2)$. Classificant-les en funció del cos que se'ns demana:

- en $\mathbb{Q}[x]$: $(x - 3)$;
- en $\mathbb{R}[x]$: $(x - 3)(x \pm \sqrt{2})$;
- en $\mathbb{C}[x]$: $(x - 3)(x \pm \sqrt{2})(x \pm 3i)$

Per últim, resolent-ho amb el sistema que hem fet a classe de laboratori, ens queda que

$$\begin{cases} x = 11 + 15k_1 + 10k_2, \\ y = -(11 + 15k_1 + 12k_2), \\ z = 1 - 2k_1. \end{cases} \quad (4.6.4)$$

De fet, aplicant la condició $x + y + z = 1$ ens queda que $1 - 2(k_1 + k_2) = 1$. Així doncs, les dues k són oposades entre elles: $k_1 = -k_2$. ■

Exercici 4.7.

1. Determina el residu de la divisió entera de $2018^{1304} + 1304^{2018} \pmod{7}$.
2. Escriu les comandes de Mathematica que faries servir per a calcular el residu de l'apartat anterior.
3. Calcula les solucions del sistema de congruències

$$\begin{cases} x \equiv 1 \pmod{9} \\ x \equiv 1 \pmod{12} \\ 3x \equiv 7 \pmod{10} \end{cases} \quad (4.7.1)$$

Quin és el menor enter positiu que n'és solució?

Resolució. Primer de tot, notem que $2018 \equiv 2 \pmod{7}$ i $1304 \equiv 2 \pmod{7}$. Així doncs, aplicant que $a \equiv b \pmod{m} \implies a^2 \equiv b^2 \pmod{m}$, tenim que $(2018^6)^{336} 2018^2 \pmod{7}$ i $(1304^6)^{217} 2018^2 \pmod{7}$. Per tant:

$$\begin{aligned} 2018^2 &\equiv 4 \pmod{7}, \\ 1304^2 &\equiv 4 \pmod{7}, \end{aligned} \iff 4 + 4 \equiv 1 \pmod{7}. \quad (4.7.2)$$

4.3 Examen T-2018

Exercici 4.8.

1. Siguin p, q nombres primers diferents i senars tals que $p - 1 \mid q - 1$, i sigui $n \in \mathbb{Z}$ tal que $\text{mcd}(n, pq) = 1$. Demostra que $n^{q-1} \equiv 1 \pmod{pq}$.
2. Demostra que si a, b, c són enters no nuls, aleshores

$$a \mid bc \iff \frac{a}{\text{mcd}(a, b)} \mid c. \quad (4.8.1)$$

Resolució. Primerament, tenim que $\text{mcd}(n, pq) = 1 \iff \text{mcd}(n, p) = 1 \iff \text{mcd}(n, q) = 1$. Considerem aquestes dues congruències, fruit d'haver aplicat el teorema petit de Fermat dues vegades:

$$\begin{aligned} n^{q-1} &\equiv 1 \pmod{q}, \\ n^{p-1} &\equiv 1 \pmod{p}. \end{aligned} \quad (4.8.2)$$

Ara, aplicant que $q - 1 \equiv 0 \pmod{p - 1}$, ens queda que

$$n^{q-1} \equiv 1 \pmod{p} \implies \begin{cases} n^{q-1} \equiv 1 \pmod{q} \\ n^{q-1} \equiv 1 \pmod{p} \end{cases} \iff n^{q-1} \equiv 1 \pmod{pq}. \quad (4.8.3)$$

Pel que fa al segon apartat, suposarem $a \mid bc$ i trobarem una cadena d'equivalències que ens permetrà provar $\frac{a}{\text{mcd}(a, b)} \mid c$ d'una tirada. Primerament, vegem que és equivalent a $a \mid \text{mcd}(a, b)c$. A partir d'aquí, notem per Bézout que $\text{mcd}(a, b) = d = \alpha a + \beta b$. Per tant:

$$a \mid ((\alpha a + \beta b)c) \iff a \mid (\alpha ac + \beta bc) \xrightarrow[a \mid ac]{a \mid bc} a \mid \text{mcd}(a, b)c. \quad (4.8.4)$$

En altres paraules, ens adonem que $a \mid ac$ i, per tant, a ha de dividir forçosament una combinació lineal de bc i ac . Amb això, quedaria demostrat l'enunciat. ■

4.4 Examen F-2020

Exercici 4.9. Calcula el màxim comú divisor dels polinomis

$$\begin{aligned} A(X) &= X^5 - 3X^4 + 27X^2 - 81X, \\ B(X) &= X^6 + X^4 + 27X^3 + 27X. \end{aligned} \quad (4.9.1)$$

Resolució. Per a trobar el màxim comú divisor entre aquests dos polinomis optarem per factoritzar ambdós polinomis. Abans, però, farem una petita modificació:

$$\begin{aligned} A'(X) &= X^4 - 3X^3 + 27X - 81, \\ B'(X) &= X^5 + X^3 + 27X^2 + 27, \end{aligned} \quad (4.9.2)$$

de tal manera que $\text{mcd}(A(X), B(X)) = X \text{mcd}(A'(X), B'(X))$. Aleshores, podem calcular directament el resultat d' $A'(X)$ amb la calculadora i ens dona que $A'(X) = (x+3)(x-3)(x^2-3x+9)$. Ara, si intentem, aplicant Ruffini, dividir $B'(X)$ entre $(x+3)$ ens surt un residu nul. Seguint, doncs, ens queda que $B'(X) = (x+3)(x^2-3x+9)(x^2+1)$. Per tant, ens queda que $\text{mcd}(A(X), B(X)) = X \text{mcd}(A'(X), B'(X)) = X(x+3)(x^2-3x+9)$.

Sabent, doncs, la factorització d' $A(X) = X A'(X) = X(X+3)(X^2 - 3X + 9)(X^2 + 1)$, podem determinar les arrels d' $A(X)$ en $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

$$\begin{aligned} \text{En } \mathbb{Z} : & X(X+3) \\ \text{En } \mathbb{R} : & X(X+3)(X^2 - 3X + 9)(X^2 + 1) \\ \text{En } \mathbb{C} : & X(X+3)(X^2 - 3X + 9)(X^2 + 1) = \\ & = X(X+3)(X^2 - 3X + 9)(X+i)(X-i)(X + \frac{3+3\sqrt{3}i}{2})(X - \frac{3+3\sqrt{3}i}{2}) \end{aligned} \quad (4.9.3)$$

■

Exercici 4.10. Sigui $q = 4^n + 1$ per a un cert $n \in \mathbb{Z}, n > 0$. Demostra que q és primer si, i només si, $3^{\frac{q-1}{2}} \equiv -1 \pmod{q}$.

Resolució. Hem de provar ambdues implicacions. Per tant,

⇒ Si q és primer podem aplicar el criteri de Gauss, de tal manera que

$$\begin{array}{ccc} q \text{ primer} & \xrightarrow{\hspace{3cm}} & 3^{\frac{q-1}{2}} \equiv -1 \pmod{q} \\ \Downarrow & \searrow & \nearrow ? \\ 3^{q-1} \equiv 1 \pmod{q} & 3^{\frac{q-1}{2}} \equiv \left(\frac{3}{q}\right) \pmod{q} & \end{array}$$

Pel que hem vist a teoria, hem de provar que $q \equiv \pm 5 \pmod{12}$ per tal que el símbol de Legendre equivalgui a -1 . Per tant, tenim que $2^{2n} + 1 \pmod{12}$.

Lema 4.10.1. $2^{2n} + 1 \equiv 4 \pmod{12}$, $\forall n > 0$.

Demostració del lemma. La demostració és fàcil per inducció. Per al cas inicial $n = 1$ és directe. Aleshores, suposant $2^{2n} \equiv 4 \pmod{16}$ ens queda que $2^{2(n+1)} \equiv 2^{2n+2} \equiv 4 \cdot 2^{2n} \equiv 16 \equiv 4 \pmod{12}$. Així doncs, queda provat $\forall n > 0$. ■

Per aquesta raó, tenim que $2^{2n} + 1 \equiv 5 \pmod{12}$, tal i com volíem. Conseguentment, $3^{\frac{q-1}{2}} \equiv -1 \pmod{p}$.

⇐ Si $p \mid 3^{\frac{q-1}{2}} + 1$, aleshores $p \mid (3^{\frac{q-1}{2}} + 1)^2$. Operant, i aplicant que

$$3^{2 \cdot \frac{q-1}{2}} \equiv (-1)^2 \pmod{q}. \quad (4.10.1)$$

Ens queda que $3^{q-1} \equiv 1 \pmod{q}$. No podem implicar que q sigui primer directament donat que el recíproc del teorema de Fermat no és cert. Per fer tal cosa, ens fa falta demostrar que $q-1 = \text{ord}_3(q) = \varphi(q)$, i ho farem pensant q compost (reducció a l'absurd). Recordem el teorema d'Euler, que deia:

Teorema 4.10.1 (Teorema d'Euler). Sigui $n > 1$ i $a \in \mathbb{Z}$ amb $\text{mcd}(a, n) = 1$. Aleshores, es compleix que $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Provem que $\text{mcd}(3, q) = 1$. Per reducció a l'absurd, raonem que si $\text{mcd}(3, q) > 1$, aleshores $q = 3p_1 \cdots p_r$. D'aquesta manera, tenim per TXResidu que $3^{q-1} \equiv 1 \pmod{q}$ es divideix en

$$\begin{aligned} 3^{q-1} &\equiv 1 \pmod{p_1}, \\ &\vdots \\ 3^{q-1} &\equiv 1 \pmod{p_r}, \\ 3^{q-1} &\equiv 1 \pmod{3}, \end{aligned} \quad (4.10.2)$$

però $3^{q-1} \equiv 0 \not\equiv 1 \pmod{3}$. En altres paraules, no existeix cap valor de $q \in \mathbb{Z}$ pel qual l'última congruència del sistema tingui sentit. Com no es compleix tal cosa, el sistema no té solució i $\text{mcd}(3, q) = 1$. Així doncs, pel Teorema d'Euler $\varphi(q) = q - 1$, però un nombre compost ha de tenir $\varphi(q) \neq q - 1$. Concloem, davant la contradicció que ve de suposar q compost, que q és primer.



Observació 4.10.1 (Nota a la resolució). D'una banda, si suposes que q és primer, pots aplicar el criteri d'Euler per al càlcul del símbol de Legendre, i obtens que $\left(\frac{3}{q}\right) \equiv 3^{\frac{q-1}{2}} \pmod{q}$.

Ara bé, com que $q \equiv 1 \pmod{4}$, la llei de reiprocedibilitat quadràtica et diu que $\left(\frac{3}{q}\right) = \left(\frac{q}{3}\right) = \left(\frac{2}{3}\right) = -1$, com volies veure.

A l'inrevés, si $3^{\frac{q-1}{2}} \equiv -1 \pmod{q}$ (nota que q és un nombre senar), llavors és $3^{q-1} \equiv 1 \pmod{q}$, i l'ordre de 3 és un divisor de $q - 1 = 4^n$; o sigui, és una potència de 2, que no pot ser menor que $q - 1$, perquè $3^{\frac{q-1}{2}} \equiv -1 \not\equiv 1 \pmod{q}$. Per tant, 3 és d'ordre $q - 1$ i això implica que q és primer (per exemple, perquè l'ordre divideix $\varphi(q)$, de manera que $q - 1$ divideix $\varphi(q) \leq q - 1$).

Exercici 4.11. *Diges si les equacions congruencials següents tenen o no solucions i en cas afirmatiu calcula-les totes.*

$$\begin{aligned} x^2 + 7 &\equiv 0 \pmod{247} \\ x^2 - 36 &\equiv 0 \pmod{323} \\ x^2 - 137 &\equiv 0 \pmod{401}. \end{aligned} \tag{4.11.1}$$

Resolució. Pel que fa a la primera, tenim que $247 = 13 \cdot 19$. Podem dir que directament no té solucions, ja que aplicant el criteri d'Euler en $x^2 + 7 \equiv 0 \pmod{13}$ ens dona -1 , així que 7 és un no-residu quadràtic mòdul 13.

Pel que fa a la segona, $x^2 \equiv 36 \pmod{323}$. Tenim que $323 = 17 \cdot 19$ i apliquem TXResidu. Ens queda que

$$\begin{aligned} x^2 &\equiv 36 \pmod{17} \\ x^2 &\equiv 36 \pmod{19} \end{aligned} \tag{4.11.2}$$

Tenim quatre casos diferents, dos d'immediats i uns altres dos que ens faran treballar força més.

1. $x \equiv 6 \pmod{17}$ i $x \equiv 6 \pmod{19}$. És immediat que $x \equiv 6 \pmod{323}$.
2. Totalment anàleg al cas anterior. $x \equiv -6 \pmod{17}$ i $x \equiv -6 \pmod{19}$. És immediat que $x \equiv -6 \equiv 317 \pmod{323}$.
3. $x \equiv 6 \pmod{17}$ i $x \equiv -6 \pmod{19}$. x és de la forma $x = 6 + 17\lambda$, $\lambda \in \mathbb{Z}$. Aleshores, $6 + 17\lambda \equiv -6 \pmod{19} \iff 17\lambda \equiv -12 \pmod{19}$. Trobant $17^{-1} \pmod{19}$ trobem λ , la qual substituirem a l'expressió d' x i reduirem mòdul 323. Finalment, obtenim $x \equiv 108 \pmod{323}$.
4. $x \equiv -6 \pmod{17}$ i $x \equiv 6 \pmod{19}$. Es resoldria d'una manera similar i en aquest cas s'obtindria $x \equiv 215 \pmod{323}$.

Per últim, tenim $x^2 - 137 \equiv 0 \pmod{401}$. 401 és un nombre primer, així que no caldria usar TXResidu. De fet, fixem-nos que x no té arrels enteres mòdul 401: solament cal intentar fer l'arrel quadrada de 137. De totes maneres, podríem resoldre el símbol de Legendre següent:

$$\left(\frac{137}{401}\right) = (-1)^{\frac{401-1}{2} \frac{137-1}{2}} \left(\frac{401}{137}\right) = \left(\frac{127}{137}\right) = (-1)^{\frac{137-1}{2} \frac{127-1}{2}} \left(\frac{137}{127}\right) = \left(\frac{2}{127}\right) \left(\frac{5}{127}\right) = -1. \tag{4.11.3}$$



Exercici 4.12.

1. La següent progressió aritmètica té cinc termes, diferència 6 i tots els seus termes són nombres primers: 5, 11, 17, 23, 29. Demostra que és l'única progressió aritmètica amb aquestes propietats.
2. Sigui $n > 1$ enter. Determina la suma de tots els enters positius més petits que n i relativament primers amb n .
3. Prova que $3^{2n+5} + 2^{4n+1} \equiv 0 \pmod{7}$, $\forall n \geq 1$.
4. Determina les dues darreres xifres de 103^{1243} .

Resolució, primer apartat. Hem de demostrar la unicitat d'aquesta progressió. Per demostrar aquest resultat, intentem escriure'l en forma de condicional. Ens quedaria la següent proposició:

Proposició 4.12.1. Si $a, a+6, a+12, a+18, a+24$ són primers, se segueix que $a = 5$.

Resolució de la proposició. Sabem que $a \geq 0$. Estudiem l'anell $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.

1. Si $a \equiv 1 \pmod{5} \implies a+24 \equiv 0 \pmod{5} \implies 5 | a+24 \implies a+24$ no és primer.
2. Si $a \equiv 2 \pmod{5} \implies a+18 \equiv 0 \pmod{5} \implies 5 | a+18 \implies a+18$ no és primer.
3. Si $a \equiv 3 \pmod{5} \implies a+12 \equiv 0 \pmod{5} \implies 5 | a+12 \implies a+12$ no és primer.
4. Si $a \equiv 4 \pmod{5} \implies a+6 \equiv 0 \pmod{5} \implies 5 | a+6 \implies a+6$ no és primer.

Aleshores, l'únic cas possible és $a \equiv 0 \pmod{5}$ i, en aquest cas, $a \equiv 0 \pmod{5} \implies 5 | a \implies a = 5$. ■

Tal i com volíem veure, $a = 5$. Això ens dona la unicitat d' a i, per tant, la unicitat de la progressió aritmètica. ■

Resolució, segon apartat.

Resolució, tercer apartat. Reduïm l'expressió mòdul 7. Tenim que $3^{2n+5} + 2^{4n+1} \equiv (3^n)^2 3^5 + (2^n)^4 2^1 \equiv (3^n)^2 3^{-1} + (-5)(2^n)^4 \equiv 5((3^n)^2 - (2^n)^4) \pmod{7}$.

Lema 4.12.1. $(3^n)^2 \equiv (2^n)^4 \pmod{7}$.

Demostració del lema. És fàcil per inducció. Per al cas inicial $n = 1$ ens queda que $3^2 \equiv 9 \equiv 2^4 \equiv 16 \pmod{7}$. Agafem com a hipòtesi d'inducció que $(3^n)^2 \equiv (2^n)^4 \pmod{7}$ i veiem que es compleix per a $n+1$:

$$3^{2n+2} \equiv 2^{4n+4} \pmod{7} \iff 3^{2n} 9 \equiv 2^{4n} 16 \pmod{7}. \quad (4.12.1)$$

De tal manera que es compleix el que volíem, ja que $9 \equiv 16 \pmod{7}$ pel que hem vist en el cas inicial i $(3^n)^2 \equiv (2^n)^4 \pmod{7}$ es compleix per hipòtesi d'inducció. ■

Com que $(3^n)^2 \equiv (2^n)^4 \pmod{7}$, ens queda que $3^{2n+5} + 2^{4n+1} \equiv 5(0) \equiv 0 \pmod{7}$, acabant així la demostració. ■

Resolució, quart apartat. Les dues darreres xifres d'un nombre coincideixen amb el seu residu mòdul 100. Per calcular el residu 103^{1243} necessitem reduir aquest exponent mòdul $\varphi(100) = 40$. Ara, podem reduir 1243 mòdul $\varphi(100) = 40$, de tal manera que $1243 \equiv 3 \pmod{40} \implies 103^{1243} \equiv 103^3 \pmod{100}$. Aleshores, $103^{1243} \equiv 103^3 \equiv 3^3 \equiv 27 \pmod{100}$. Les dues darreres xifres de 103^{1243} són 2 i 7. ■

Exercici 4.13.

1. Prova que per a $x, y \in \mathbb{Z}$ l'expressió $2x + 3y$ és divisible per 17 si, i només si, l'expressió $9x + 5y$ és divisible per 17.

2. Considera l'última xifra k del teu NIUB. Resol, si és possible, $x^6 \equiv k+1 \pmod{11}$.
3. Tenim $n \in \mathbb{Z}$ i $3 \mid \varphi(m)$. Si $x^3 \equiv 1 \pmod{m}$ té més de 3 solucions, aleshores no existeixen arrels primitives mòdul m .

Resolució, primer apartat. Aquest exercici és fàcil de resoldre si considerem la cadena d'equivalències de la següent figura. ■

$$\begin{array}{ccc} 2x + 3y \equiv 0 \pmod{17} & \xleftarrow{\quad\quad\quad} & 9x + 5y \equiv 0 \pmod{17} \\ \Downarrow \Updownarrow & & \Downarrow \Updownarrow \\ x \equiv -27y \pmod{17} & \xleftarrow{\quad\quad\quad} & x \equiv -10y \pmod{17} \end{array}$$

Figura 3: Resolució bàsica

Resolució, segon apartat. La última xifra del meu NIUB és 4. Per tant, hem de resoldre $x^6 \equiv 5 \pmod{11}$. Fem el canvi de variable següent $t = x^3$, de tal manera que $t^2 \equiv 5 \pmod{11}$. Per tant, $t = x^3 \equiv \pm 4 \pmod{11}$. Així doncs,

1. $x^3 \equiv 4 \pmod{11}$: la manera més ràpida és anar provant els representants de les classes residuals mòdul 11. Així, trobem que $x \equiv 5 \pmod{11}$. Fixem-nos que $4 + 11 \cdot 11 = 125$.
2. $x^3 \equiv -4 \equiv 7 \pmod{11}$: de la mateixa manera que a l'apartat anterior, provant iterativament tals valors trobem que $x \equiv 6 \pmod{11}$.

Així doncs, $x \equiv 5, 6 \pmod{11}$. ■

Resolució, tercer apartat. Ens hem d'adonar que la solució més còmoda passa per utilitzar reducció a l'absurd. Aleshores, suposem que existeix una arrel primitiva g mòdul m tal que $g \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$. Notem que

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* = \{g, g^2, \dots, g^{\varphi(m)}\}. \quad (4.13.1)$$

Aleshores, $x^3 \equiv 1 \pmod{m} \iff (g^3)^3 \equiv 1 \pmod{m} \iff g^{3i} \equiv g^0 \pmod{m}$. Per PTFermat, tenim que $3i \equiv 0 \pmod{\varphi(m)}$. Podem dividir per 3 a tot arreu i ens queda que $i \equiv 0 \pmod{\frac{\varphi(m)}{3}}$. Per tant, totes les solucions de $x^3 \equiv 1 \pmod{n}$ són de la forma g^i tal que $i \equiv 0 \pmod{\frac{\varphi(m)}{3}}$. Així, tenim que i és múltiple de $\frac{\varphi(m)}{3}$: $i = \frac{\varphi(m)}{3}k, k \in \mathbb{Z}$.

1. Si $k \equiv 0 \pmod{3}$, ens queda que $g^i \equiv g^{\frac{\varphi(m)}{3}3\ell} \equiv g^{\varphi(m)\ell} \equiv 1 \pmod{m}$.
2. Si $k \equiv 1 \pmod{3}$, ens queda que $g^i \equiv g^{\frac{\varphi(m)}{3}(3\ell+1)} \equiv g^{\varphi(\frac{\varphi(m)}{3})} \pmod{m}$.
3. Si $k \equiv 2 \pmod{3}$, aleshores $g^i \equiv g^{\frac{\varphi(m)}{3}(3\ell+2)} \equiv g^{\frac{2\varphi(m)}{3}} \pmod{m}$.

Observem que en tots els casos, la solució que obtenim és una de les tres que havíem trobat anteriorment. Per tant, queda demostrat que l'equació $x^3 \equiv 1 \pmod{m}$ té exactament 3 solucions. ■

4.5 Examen R-2020

Exercici 4.14.

1. Prova que si $n, m \in \mathbb{Z}_{>0}$ tenen els mateixos divisors primers, aleshores $n\varphi(m) = m\varphi(n)$.
2. Prova que $(n+1)|(2^{n!}-1)$, per a tot $n \in \mathbb{Z}_{>0}$ parell.
3. Prova que si n és pseudoprimer en base 2, aleshores $2^n - 1$ també és pseudoprimer en base 2.
2. Prova que hi ha infinitos pseudoprimeres en base 2.

Resolució, 4.14.1. Ho provarem directament, seguint les propietats de la funció ϕ d'Euler.

$$\begin{aligned} n &= \prod_i p_i^{v_{p_i}(n)}, \\ m &= \prod_i p_i^{v_{p_i}(m)}. \end{aligned} \quad (4.14.1)$$

Veiem, doncs, que els nombres poden canviar o no simplement per les valoracions p -àdiques dels factors. Distingim dos casos:

1. $v_{p_i}(n) = v_{p_i}(m), \forall i$. En aquest cas, $n = m$ i el resultat es dedueix de manera trivial.
2. $\exists i \mid v_{p_i}(n) \neq v_{p_i}(m)$ (poden ser tots diferents o bé només un, no ho sabem). Escrivint $n\varphi(m)$ arribarem a $m\varphi(n)$ mitjançant igualtats.

$$\begin{aligned} n\varphi(m) &= \prod_i p_i^{v_{p_i}(n)} \varphi \left(\prod_i p_i^{v_{p_i}(m)} \right) = \prod_i p_i^{v_{p_i}(n)} \varphi \left(p_i^{v_{p_i}(m)} \right) = \prod_i p_i^{v_{p_i}(n)} p_i^{v_{p_i}(m)-1} (p_i - 1) \\ &= \prod_i p_i^{v_{p_i}(m)} p_i^{v_{p_i}(n)-1} (p_i - 1) = m\varphi(n) \end{aligned} \quad (4.14.2)$$

Resolució, 4.14.2.

Resolució, 4.14.3. Notem que $M_n = 2^n - 1$ té la forma d'un nombre de Mersenne.

Exercici 4.15.

1. Sigui $A(x) = x^6 + 10x^5 + 24x^4 - 10x^3 - 24x^2 + 10x + 25$. Troba les arrels d' $A(x)$ a $\mathbb{C}, \mathbb{R}, \mathbb{Z}/5\mathbb{Z}$.
2. Sigui $n > 100$ un nombre enter que és un quadrat perfecte i tal que les seves dues darreres xifres en base 10 són iguals. Prova que aquestes dues xifres són 0 o 4.
3. Demostra que per a tot enter n , la darrera xifra d' n és la mateixa que la darrera xifra d' n^5 .

Resolució, 4.15.1. Suposarem que hi ha una solució entera, i si no ja arribarem a contradicció. De tal manera, intentarem descompondre aquest polinomi per Ruffini. Hem de provar els valors $\pm 1, \pm 5$. Trobem que, efectivament, $x = -5$ és arrel doble i el polinomi restant és irreductible en \mathbb{R} .

- En \mathbb{R} : $(x + 5)^2(x^4 - x^2 + 1)$.
- En \mathbb{C} podríem descompondre el segon factor una mica més. Ens quedaría tal que $(x + 5)^2(x - \frac{\sqrt{3}-i}{2})(x - \frac{\sqrt{3}+i}{2})(x + \frac{\sqrt{3}+i}{2})(x + \frac{\sqrt{3}-i}{2})$ (*consell*: aplicar un canvi de variable $t = x^2$).
- En $\mathbb{Z}/5\mathbb{Z}$: hem de resoldre $(x + 5)^2(x^4 - x^2 + 1) \equiv 0 \pmod{5}$. Tenim, aleshores, que $(x + 5)^2 \equiv 0 \pmod{5}$ o bé $x^4 - x^2 + 1 \equiv 0 \pmod{5}$. Pel que fa a la primera, obtenim que la classe residual del 0 és solució en $\mathbb{Z}/5\mathbb{Z}$; en canvi, si provem tots els representants de les 5 classes residuals mòdul 5 no obtenim una solució addicional. En conclusió, $\bar{0}$ és arrel en $\mathbb{Z}/5\mathbb{Z}$.

Resolució, 4.15.2. Notem que el nombre s'ha de reduir el nombre n mòdul 100 i, a més, podem escriure'l d'una determinada manera ja que se'ns demana específicament que sigui sobre base 10. Sobre això, notar que $\lambda_0, \lambda_1, \lambda_2 \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} = \{0, 2, 4, 6, 8\} \cup \{1, 3, 5, 7, 9\}$. Notem que $\lambda_2 \neq 0$.

$$\begin{aligned} \sqrt{n} = 100\lambda_2 + 10\lambda_1 + \lambda_0 &\iff n = 10000\lambda_2^2 + 2000\lambda_2\lambda_1 + 200\lambda_0\lambda_2 + 100\lambda_1^2 + 20\lambda_1\lambda_0 + \lambda_0^2 \pmod{100} \\ &\iff 20\lambda_1\lambda_0 + \lambda_0^2 \pmod{100} \iff \pmod{100}. \end{aligned} \quad (4.15.1)$$

Resolució, 4.15.3. Notem que aquesta proposició és equivalent a la següent:

Proposició 4.15.1. $n^5 \equiv n \pmod{10}$, $\forall n$.

Ho provarem per inducció. Per a $n = 0$ la comprovació és trivial. Suposem cert per a n i vegem que es compleix

$$(n+1)^5 - (n+1) = n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 - n - 1 = n^4 - n + 10(n^3 + n^2) + 5n(n^3 + 1). \quad (4.15.2)$$

Ara, d'una banda tenim que $n^5 - n$ és divisible per 10 gràcies a la hipòtesi d'inducció, així com $10(n^4 + n^2)$ és clarament divisible per aquest nombre. D'altra banda, solament ens faltarà demostrar que $5n(n^3 + 1)$ és divisible per 10, que és equivalent a provar que $n(n^3 + 1)$ és divisible per 2, la qual cosa podem fer immediatament: si n és parell ja hem acabat; en canvi, si n és imparell ens queda que $n^3 + 1$ és parell i $n(n^3 + 1)$ és divisible per 2. ■

Exercici 4.16. Sigui n el teu NIUB, $m = 6000$ i $d = \text{mcd}(n, m)$. Escriu, també $n' = da$ i $m' = db$, amb $a, b \in \mathbb{Z}$.

1. Calcula d i justifica, sense calcular-les, que l'equació diofantina $mx + ny = 2020d$ té solucions enteres.
2. Calcula totes les solucions enteres de l'equació anterior.
3. Donat el sistema

$$\begin{aligned} x &\equiv 3c \pmod{22} \\ x &\equiv 1 \pmod{10} \\ x &\equiv c \pmod{18} \end{aligned} \quad (4.16.1)$$

determina tots els possibles valors de $c \in \mathbb{Z}$ tals que el sistema té solució. Resol el sistema per a cadascun d'aquests valors de c .

Resolució, 4.16.1. De primeres, tenim que $\text{mcd}(da, db) = d\text{mcd}(a, b) = d$, ja que $\text{mcd}(a, b) = 1$ per hipòtesi dels nombres n, m . Per la qual cosa, quan traiem factor comú i cancel·lem a banda i banda de l'equació ens queda

$$bx + ay = 2020 \quad (4.16.2)$$

i com que $\text{mcd}(a, b) \mid 2020$, (4.16.2) té solució. ■

Resolució, 4.16.2. Podem fer servir el sistema dels meus apunts, [Vil21], de tal manera que ens guardem els quocients de cada divisió i ens queda

$$\begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -6 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3398 \end{pmatrix} \begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} 221 & -751132 \\ * & * \end{pmatrix}, \quad (4.16.3)$$

Així que $s = 221$ i $t = -751132$, i els hem de multiplicar per 2020. De tal manera que $s = 446420$ i $t = -1517286640$. ■

Resolució, 4.16.3.

Exercici 4.17.

1. Sigui $p > 5$ un nombre primer. Prova que $p^8 \equiv 1 \pmod{240}$. És cert que $p^4 \equiv 1 \pmod{240}$?
2. Per a quins nombres primers p , -15 és un residu quadràtic mòdul p ?

3. Siguin $m > 2, m \in \mathbb{Z}$ i $a \in \mathbb{Z} \mid \text{mcd}(a, m) = 1$. Demostra que si a és un residu quadràtic mòdul m , aleshores $a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$.

Resolució, 4.17.1. Hem de resoldre $p^8 \pmod{240}$ i hem de demostrar que p^8 és congru amb 1. Apliquem TXResidu i veiem que podem resoldre diversos casos. En tots, haurem de trobar que p^8 és, efectivament, congru amb 1:

- $p^8 \pmod{3}$. Tenim que $\varphi(3) = 2$, així que $p^2 \equiv 1 \pmod{3}$. Aleshores, $(p^2)^4 \equiv p^8 \equiv 1^4 \equiv 1 \pmod{3}$. Així, $p^8 \equiv 1 \pmod{3}$. Notem que si $p = 3$, $p^8 \equiv 0 \not\equiv 1 \pmod{3}$.
 - $p^8 \pmod{5}$. La resolució és anàloga a la del cas anterior, ja que $\varphi(5) = 4 = 2^2$. De tal manera, obtenim que $p^8 \equiv 1 \pmod{5}$. Notem que si $p = 5$, $p^8 \equiv 0 \not\equiv 1 \pmod{5}$.
 - $p^8 \pmod{16}$. Aquest apartat és una mica més complicat. Ja sabem que p és senar, ja que $p > 5$ i és primer. Per definició podem dir, per tant, que $p \equiv 1 \pmod{2}$. Per tant, $p^8 \equiv p^4 \equiv 1 \pmod{2}$. Aleshores, com que $\text{mcd}(p, 16) = 1$, $p^{\varphi(16)} \equiv p^8 \equiv 1 \pmod{16}$.

Mathematica.

```
In[11]:= F[n_] := Table[Mod[i^8, 4], {i, 7, n, 2}]
F[100]
```

```
In[12]:= F[n_] := Table[Mod[i^8, 8], {i, 7, n, 2}]\nF[100]
```

```
In[13]:= F[n_] := Table[Mod[i^8, 16], {i, 7, n, 2}]
F[100]
```

Per acabar, hem de veure que $p^4 \equiv 1 \pmod{16}$. Fem el canvi $t = p^4$ i ens queda $p^4 \equiv \pm 1 \pmod{16}$. Com que no em queden més idees, he agafat el *Mathematica* i he aplicat força bruta per a $p \in \{7, 11, 13\}$. Efectivament, $p^4 \equiv 1 \pmod{16}$. ■

Resolució, 4.17.2. En primer lloc, directament $p \notin \{3, 5\}$, ja que, en cas contrari, tindríem que el símbol de Legendre corresponent seria igual a 0 i, per tant, -15 no seria un residu quadràtic. ■

Resolució, 4.17.3. Completament automàtic per analogia al criteri d'Euler, aplicant també el teorema d'Euler. Com que $m > 2$ tenim que $\varphi(m)$ és parell $\implies 2 \mid \varphi(m)$. Aleshores, se satisfà la congruència

$$(a^{\frac{\varphi(m)}{2}})^2 \equiv a^{\varphi(N)} \equiv 1 \pmod{m}. \quad (4.17.1)$$

de tal manera que $a^{\frac{\varphi(m)}{2}} \equiv \pm 1$. En particular, com que a és residu quadràtic, ens queda que $a^{\frac{\varphi(m)}{2}} \equiv 1$.

4.6 Examen F-2019

Exercici 4.18.

1. Enuncia i demostra el teorema d'Euler.
2. Siguin p, q nombres naturals primers i senars i $N := 2^q - 1$. Demostra que si $p \mid N$, aleshores, $p \equiv 1 \pmod{2q}$.
3. Amb les mateixes notacions per a p, q, N , demostra que si $p^2 \mid N$, aleshores $2^{\frac{p-1}{2}} \equiv 1 \pmod{p^2}$.

Resolució, 4.18.1. El teorema d'Euler diu així:

Teorema 4.18.1. Siguin $a, m \in \mathbb{Z}_{>0} \mid a \in (\mathbb{Z}/m\mathbb{Z})^*$, no necessàriament primers. Aleshores, $a^{\varphi(m)} \equiv 1 \pmod{m}$.

La seva demostració és la següent:

Demostració. Sigui $S = \{x_1, x_2, \dots, x_r\}$, format per un representant de cada classe invertible mòdul n , amb $|S| = r = \varphi(n)$.

Sigui $x \in S$. Com $\text{mcd}(x, n) = 1$ i $\text{mcd}(a, n) = 1 \implies \text{mcd}(ax, n) = 1$. Per tant, si multipliquem a tots els elements de S per a obtenim $aS = \{ax_1, \dots, ax_r\}$ i veiem que tots els elements d'aquest conjunt són, de nou, coprimers amb n . A més, $|aS| = r = \varphi(n)$.

Volem veure que aquests elements representen totes les $\varphi(n)$ classes invertibles mòdul n , per a la qual cosa solament fa falta veure que cada parell d'aquests no són congruents mòdul n . Per a això, apliquem la propietat cancel·lativa, que ens diu que si $ax_i \equiv ax_j$, com $\text{mcd}(a, n) = 1 \implies x_i \equiv x_j \implies i = j$.

Per tant, tant s com aS estan format per un representant de cada classe invertible mòdul n . D'aquí se segueix que si multipliquem tots els seus elements obtenim la congruència

$$x_1 \cdots x_r \equiv ax_1 \cdots ax_r \pmod{n}, \quad (4.18.1)$$

on $r = \varphi(n)$. Si anomenem x al producte dels x_i , amb $i \in \{0, 1, \dots, r\}$: $x \equiv a^{\varphi(n)} \cdot x \pmod{n}$. Com els x_i són coprimers amb n , també x és coprimer amb n , amb la qual cosa podem cancel·lar-lo i obtenim que $1 \equiv a^{\varphi(n)} \pmod{n}$. ■■

Resolució, 4.18.2. Com que $2^q \equiv 1 \pmod{N}$ i $p \equiv 0 \pmod{N}$ tenim que, aplicant el TXResidu, $2^q \equiv 1 \pmod{p}$: ens queda que $q = \text{ord}(p)$ donat que q és primer. D'altra banda, pel PTFermat $2^{p-1} \equiv 1 \pmod{p}$. Aleshores, $q \equiv p-1 \pmod{\varphi(p)}$. D'aquesta manera, $q \mid \varphi(p)$ i $q \mid (p-1)$. Ens queda un últim pas: notem que q és senar i $p-1$ és parell: $2q \mid p-1$ com calia veure. ■■

Resolució, 4.18.3. Si $p^2 \mid N$, aleshores $2^{q-1} \equiv 2^{(p+1)(p-1)} \equiv 1 \pmod{p^2}$. De fet, $q-1 \equiv (p+1)(p-1) \equiv p-1 \pmod{p(p-1)}$. Per tant, ens queda, tal i com volíem, $2^{\frac{p-1}{2}} \equiv 1 \pmod{p^2}$. ■■

Exercici 4.19.

1. Calcula totes les arrels quadrades del nombre complex $\frac{1+\sqrt{3}i}{2}$.
2. Sigui $a := 436$. Sabem que $a^{333} \equiv 436 \pmod{667}$ i que $a^{666} \equiv 1 \pmod{667}$. A partir d'aquesta única informació, podem concloure que el nombre natural 667 és compost? Per què?
3. Sigui $b := 212$. Sabem que $b^{1146} \equiv 1 \pmod{1147}$ i que $b^{573} \equiv 1146 \pmod{1147}$. A partir d'aquesta única informació, podem concloure que el nombre natural 1147 és compost? Per què?

3. Sigui $p > 2$ un nombre primer i g, h arrels primitives mòdul p . Demostra que el producte gh no és una arrel primitiva mòdul p .

Resolució, 4.19.1. Si posem $r := \frac{\sqrt{3}+i}{2}$, resulta que $r^2 = \frac{3-1+2\sqrt{3}i}{4} = \frac{1+\sqrt{3}i}{2}$. Per tant, les dues arrels demandades són $\pm r$. ■

Resolució, 4.19.2. En el primer cas, tenim que per $a^{333} \equiv 436 \pmod{667}$ i $a^{666} \equiv 1 \pmod{667}$ podem implicar $a^2 \equiv 1 \pmod{667}$. D'altra banda, tenim que $a \equiv 436 \not\equiv \pm 1 \pmod{667}$. Per tant, mòdul $n := 667$ hi ha més de dues arrels quadrades d' a , però això ens implica que no hi ha arrels primitives mòdul n . Per tant, n és compost. ■

El segon cas no és cert. ■

Resolució, 4.19.3. g, h són no-quadrats mòdul p i, per tant, gh és un quadrat mòdul p ; per tant, no pot ser arrel primitiva. ■

Exercici 4.20. Sigui $p > 2$, un nombre primer tal que $p = a^2 + b^2$, per a certs nombres $a, b \in \mathbb{Z}$ i a senar. Demostra que $\left(\frac{a}{p}\right) = 1$.

Resolució. Per començar, com que $p > 2$, aleshores p és senar. A l'haver fixat a com a senar, b ha de ser parell per força. A més, $\text{mcd}(a, b) = 1$, ja que si fos $\text{mcd}(a, b) > 1$, tindrien un factor d compartit tal que $d^2((a')^2 + (b')^2) = p$ i $d^2 \mid p$. Ja com a última observació, $p \equiv 1 \pmod{4}$ ja que b és parell: $a^2 + b^2 \equiv b^2 \equiv (2k+1)^2 \equiv 1 \pmod{4}$. Aleshores:

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{a^2 + b^2}{a}\right) = \left(\frac{b^2}{a}\right) = \left(\frac{b}{a}\right)^2 = 1. \quad (4.20.1)$$

Exercici 4.21. Demostra que si p és un primer tal que $p \mid \varphi(m)$ i $p \nmid m$, aleshores existeix almenys un factors primer q de m tal que $q \equiv 1 \pmod{p}$.

Resolució. Considerem $n = \prod_i q_i$ i tenim per hipòtesi que $\varphi(m) \equiv 0 \pmod{p}$. Com que p és primer, i per la multiplicitat de la funció φ d'Euler, podem dividir aquesta congruència en les següents:

$$\begin{aligned} \varphi(q_1) &\equiv 0 \pmod{p} \\ &\vdots \\ \varphi(q_r) &\equiv 0 \pmod{p} \end{aligned} \quad (4.21.1)$$

És fàcil veure que agafant $q \in \{q_1, \dots, q_r\}$ ens queda que $\varphi(q) \equiv q-1 \equiv 0 \pmod{p} \iff q \equiv 1 \pmod{p}$. ■

Exercici 4.22. Sigui p un primer tal que $p \equiv 2 \pmod{3}$ i sigui a un enter amb $p \nmid a$. Demostra que la congruència $x^3 \equiv a \pmod{p}$ té com a única solució $x \equiv a^{\frac{2p-1}{3}} \pmod{p}$.

Resolució. ■

Exercici 4.23. Demostra que $x^2 \equiv -1 \pmod{p}$ no té solucions si, i només si, $p \equiv 3 \pmod{4}$.

Resolució. $x^2 \equiv -1 \pmod{p} \iff x^4 \equiv 1 \pmod{p}$. Considerem $x^{p-1} \pmod{p}$: $x^{p-1} \equiv x^{2+4k} \equiv x^2 x^{4k} \equiv -(x^4)^k \equiv -1 \pmod{p}$, contradient PTFermat. ■

4.7 Examen R-2019

Exercici 4.24.

1. Digues quins són els tres nombres naturals més petits que, en dividir-los per 12, 17, 45 o 70 el seu residu és 4.
2. Calcula el mínim nombre enter tal que $\sqrt[5]{\frac{n}{5}}$ i $\sqrt[7]{\frac{n}{7}}$ són, simultàniament, nombres enters.

Resolució. Resoldrem els dos apartats aquí, seguits. En primer lloc, hem de plantejar el següent sistema de congruències:

$$\begin{aligned} x &\equiv 4 \pmod{12} \\ x &\equiv 4 \pmod{17} \\ x &\equiv 4 \pmod{45}, \\ x &\equiv 4 \pmod{70} \end{aligned} \tag{4.24.1}$$

de tal manera que el podem simplificar així:

$$\begin{aligned} x &\equiv 4 \pmod{4} \\ x &\equiv 4 \pmod{17} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 4 \pmod{9} \\ x &\equiv 4 \pmod{7} \end{aligned} \tag{4.24.2}$$

i, finalment, el podem resoldre i ens dona que $x = 4 + 21420\lambda$ i

$$\begin{aligned} n_1 &= 4 \\ n_2 &= 21424 \\ n_3 &= 42844 \\ n_4 &= 64264 \end{aligned} \tag{4.24.3}$$

En segon lloc, podem veure que $n = 5^m 7^\ell$. Així:

$$\begin{aligned} \sqrt[5]{\frac{n}{5}} &= 5^{\frac{m-1}{5}} 7^{\frac{\ell}{5}} \\ \sqrt[7]{\frac{n}{7}} &= 5^{\frac{\ell-1}{7}} 7^{\frac{\ell}{7}} \end{aligned} \tag{4.24.4}$$

Ara, podem plantejar dos sistemes de congruències, mirant els diferents exponents que haurien de tenir ambdós nombres (5 i 7).

$$\begin{aligned} m &\equiv 1 \pmod{5} & \ell &\equiv 0 \pmod{5} \\ m &\equiv 0 \pmod{7} & \ell &\equiv 1 \pmod{7} \end{aligned} \tag{4.24.5}$$

Resolent-los, ens queda que $m \equiv 21 \pmod{35}$ i $\ell \equiv 15 \pmod{35}$, respectivament. Aleshores, $n = 5^{21} 7^{15}$.

Exercici 4.25. Sigui N un nombre pseudoprimer respecte d'una base b i sigui $N - 1 = kq^r$, on $k > 0, r > 0$ i q és un nombre primer. Prova que per a tot factor primer p de N es té que o bé $p \mid (b^{\frac{N-1}{q}} - 1)$ o bé $p \equiv 1 \pmod{q^r}$.

Resolució. Per hipòtesi sabem que n és pseudoprimer. Aleshores, $b^{N-1} \equiv 1 \pmod{N}$ es compleix si, i només si, $b^{N-1} \equiv 1 \pmod{p}$ per a algun primer $p \mid N$. Aleshores, l'ordre de b mòdul p és un divisor d' $N - 1 = kq^r$. Per tant:

- si $q^r \mid \text{ord}_b(p)$, i com que $\text{ord}_b(p) \mid \varphi(p)$, és evident que $q^r \mid \varphi(p) = p - 1$ amb la qual cosa $p \equiv 1 \pmod{q^r}$;
- si $\text{ord}_b(p) \mid \frac{N-1}{q}$, de tal manera que $b^{\frac{N-1}{q}} \equiv 1 \pmod{p}$.

4.8 Examen P-2021

Exercici 4.26. Siguin $a, b \mid \text{mcd}(a, b) = 1$. Determina, en funció d' a, b el valor de $\text{mcd}(a^2b^2, a^2 + ab + b^2)$. Determina, en funció d' a, b el valor de $\text{mcd}(a^2b^2, a^2 + ab)$.

Resolució, 4.26. Suposem que un nombre primer p divideix $\text{mcd}(a^2b^2, a^2 + ab + b^2)$. Com que divideix a^2b^2 i és primer, ha de dividir a o b , però no tots dos. Si divideix a , també divideix $a^2 + ab$, però no divideix b^2 ; i si divideix b , també divideix $ab + b^2$, però no divideix a^2 ; per tant, no divideix $a^2 + ab + b^2$. Així, no hi ha cap nombre primer que divideixi $\text{mcd}(a^2b^2, a^2 + ab + b^2)$ i $\text{mcd}(a^2b^2 + a^2 + ab + b^2) = 1$.

Notem, primerament, que $\text{mcd}(a^2b^2, a^2 + ab) = a \text{mcd}(ab^2, a + b)$. Si p fos un nombre primer que dividís $\text{mcd}(ab^2, a + b)$, com que divideix ab^2 , hauria de dividir a o b , però no tots dos; llavors no dividiria $a + b$. Per tant, $\text{mcd}(ab^2, a + b)$ no és divisible per cap nombre primer, de manera que $\text{mcd}(ab^2, a + b) = 1$ i, finalment, $\text{mcd}(a^2b^2, a^2 + ab) = a$. ■

REFERÈNCIES

- [Hag80] Peter HAGIS JR. “Outline of a proof that every odd perfect number has at least eight prime factors”. A: *Mathematics of Computation* (1980), pàg. 1027 - 1032.
- [Coh81] Graeme L COHEN. “65.1 Even perfect numbers”. A: *The Mathematical Gazette* 65.431 (1981), pàg. 28 - 30.
- [BCR91] Richard P BRENT, Graeme Laurence COHEN i Herman JJ te RIELE. “Improved techniques for lower bounds for odd perfect numbers”. A: *Mathematics of Computation* 57.196 (1991), pàg. 857 - 868.
- [Hea94] DR HEATH-BROWN. “Odd perfect numbers”. A: (1994).
- [Gra98] Artur Travesa i GRAU. *Aritmètica*. Vol. 25. Edicions Universitat Barcelona, 1998.
- [CP06] Richard CRANDALL i Carl B POMERANCE. *Prime numbers: a computational perspective*. Vol. 182. Springer Science & Business Media, 2006.
- [Jia18] Xing-Wang JIANG. “On even perfect numbers”. A: *Colloquium Mathematicum*. Vol. 154. Instytut Matematyczny Polskiej Akademii Nauk. 2018, pàg. 131 - 136.
- [Vil21] Mario VILAR. *Aritmètica*. Febr. de 2021.
- [Arr] Enrique ARRONDO. *Teoría Elemental de Números*. URL: <http://www.mat.ucm.es/~arrondo/ten.pdf>.