ARITMÈTICA Curs 2010-11

Teresa Crespo

12 de maig de 2011

Índex

Capítol 1

Nombres complexos

1.1 Nombres naturals, enters, racionals, reals

Indiquem per $\mathbb{N}$ el conjunt dels enters naturals. Fem el conveni $0 \in \mathbb{N}$.

Indiquem per $\mathbb{Z}$ el conjunt dels enters.

Indiquem per $\mathbb{Q}$ el conjunt dels nombres racionals.

Indiquem per $\mathbb{R}$ el conjunt dels nombres reals.

Tenim $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Recordem que a $\mathbb{N}$ tenim definides dues operacions internes, la suma $(+)$ i el producte $(\cdot)$ complint les propietats següents.

- la suma és associativa, commutativa i 0 és element neutre per la suma,
- el producte és associatiu, commutatiu, 1 és element neutre pel producte i el producte és distributiu respecte de la suma.

A $\mathbb{Z}$ la suma i el producte compleixen les mateixes propietats que a $\mathbb{N}$ i a més tot element de $\mathbb{Z}$ té oposat. Diem que $\mathbb{Z}$ és un anell commutatiu amb unitat.
A $\mathbb{Q}$ la suma i el producte compleixen les mateixes propietats que a $\mathbb{Z}$ i a més tot element no nul de $\mathbb{Q}$ té invers. Diem que $\mathbb{Q}$ és un cos.
El conjunt $\mathbb{R}$ amb la suma i el producte també és un cos.

1.2 El cos dels nombres complexos

Considerem

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a, b) : a, b \in \mathbb{R}\}.$$

Sabem que a $\mathbb{R}^2$ tenim definida una suma per

$$(a, b) + (a', b') = (a + a', b + b')$$

i que $(\mathbb{R}^2, +)$ és un grup abelià. Volem definir a $\mathbb{R}^2$ un producte intern. Posem

$$(a, b) \cdot (a', b') = (aa' - bb', ab' + a'b).$$

A partir de les propietats de la suma i el producte de nombres reals, es pot provar que aquest producte és associatiu, commutatiu, distributiu respecte de la suma i $(1, 0)$ és element neutre per aquest producte.
Recordem que $\mathbb{R}^2$ és espai vectorial amb la suma i el producte extern definit per

$$\lambda(a, b) = (\lambda\, a, \lambda\, b), \text{ per a } \lambda \in \mathbb{R}, (a, b) \in \mathbb{R}^2.$$

Si $a \in \mathbb{R}$, tenim

$$a(a', b') = (aa', ab') = (a, 0) \cdot (a', b')$$

Identifiquem el nombre real a amb l'element $(a, 0)$ de $\mathbb{R}^2$. Fem servir la notació $i := (0, 1)$. Per la definició del producte, tenim $i^2 = -1$. A més, si $b \in \mathbb{R}$, tenim $bi = (0, b)$ i $a + bi = (a, b)$.
Si $a + bi \neq 0$, tenim $a \neq 0$ o $b \neq 0$, aleshores

$$(a + bi)(a - bi) = a^2 + b^2 \neq 0$$

i per tant

$$(a + bi)(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\, i) = 1.$$

Tenim doncs que tot element no nul té invers. Hem obtingut que $\mathbb{R}^2$ amb la suma i el producte intern que hem definit és un cos. S'escriu $\mathbb{C}$ i es diu cos dels nombres complexos. Escrivim els seus elements en la forma $a + bi$. Amb aquest notació, la suma i el producte s'escriuen en la forma

$(a+bi)+(a'+b'i) = (a+a')+(b+b')i\,,\ (a+bi)\cdot(a'+b'i) = (aa'-bb')+(ab'+a'b)i.$

Per a $z = a+bi \in \mathbb{C}$, a és diu *part real* de z, b és diu *part imaginària* de z. Posem $a = \operatorname{Re} z, b = \operatorname{Im} z$. Diem que $a+bi$ és la *forma binòmica* del nombre complex z. Si $z = a+bi$, posem $\overline{z} = a-bi$ i diem que $\overline{z}$ és el nombre complex *conjugat* de z.

Proposició 1.2.1. *Si $z_1, z_2 \in \mathbb{C}$, es compleix*

1. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
2. $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

Demostració. Posem $z_1 = a_1 + b_1 i, z_2 = a_2 + b_2 i$, amb $a_1, a_2, b_1, b_2 \in \mathbb{R}$. Tenim $\overline{z_1} = a_1 - b_1 i, \overline{z_2} = a_2 - b_2 i$. Ara

$$z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)i \Rightarrow \overline{z_1 + z_2} = (a_1 + a_2) - (b_1 + b_2)i = \overline{z_1} + \overline{z_2}$$

$z_1 \cdot z_2 = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)i \Rightarrow \overline{z_1 \cdot z_2} = (a_1a_2 - b_1b_2) - (a_1b_2 + a_2b_1)i = \overline{z_1} \cdot \overline{z_2}.$

□

1.3 Arrels quadrades en forma binòmica.

Sabem que tot nombre real $a > 0$ té dues arrels quadrades a $\mathbb{R}$. Escrivim $\sqrt{a}$ l'arrel quadrada positiva de a. Com $i^2 = -1$, tot nombre real $a < 0$ té dues arrels quadrades a $\mathbb{C}$: $\pm\sqrt{|a|}\, i$. Veiem ara com calcular les arrels quadrades d'un nombre complex, no real.
Volem calcular les arrels quadrades del nombre complex $z = a + bi$, amb $b \neq 0$. Volem doncs resoldre l'equació

$$(x + yi)^2 = a + bi.$$

Com $(x+yi)^2 = x^2 - y^2 + 2xyi$, igualant part real i part imaginària, tenim les dues equacions

$$\begin{cases} x^2 - y^2 &= a \\ 2xy &= b. \end{cases}$$

Si $x = 0$, $(yi)^2 = -y^2$ és un nombre real, per tant ha de ser $x \neq 0$ i de la segona equació, obtenim

$$y = \frac{b}{2x}$$

i, substituint a la primera,

$$x^2 - \frac{b^2}{4x^2} = a$$

que, multiplicant per x^2, dóna

$$x^4 - ax^2 - \frac{b^2}{4} = 0,$$

equació biquadràtica en x. Posant $X = x^2$, obtenim l'equació quadràtica en X

$$X^2 - aX - \frac{b^2}{4} = 0, \tag{1.1}$$

de la qual busquem arrels positives, ja que x ha de ser real i per tant $X = x^2$ ha de ser positiu. Les dues arrels de (1.1) són

$$X = \frac{a \pm \sqrt{a^2 + b^2}}{2}.$$

Com $a^2 + b^2 > 0$, tenim dues arrels reals diferents. Ara, $b \neq 0 \Rightarrow a^2 + b^2 > a^2$. Per tant, l'arrel amb + davant de l'arrel quadrada és positiva i l'arrel amb - negativa. Obtenim doncs dues solucions.

$$x = \pm\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}},\ y = \frac{b}{2x}.$$

Exercici. *Calculeu les arrels quadrades del nombre complex* $3 + 4i$.

Tenim les equacions

$$\begin{cases} x^2 - y^2 &= 3 \\ 2xy &= 4. \end{cases}$$

De la segona obtenim $y = 2/x$ i, substituint a la primera, $x^2 - 4/x^2 = 3$. Multiplicant per x^2, obtenim $x^4 - 3x^2 - 4 = 0$. Posant $X = x^2$, tenim l'equació quadràtica $X^2 - 3X - 4 = 0$, de la qual l'arrel positiva és 4. Obtenim doncs $x = \pm 2, y = \pm 1$. Les arrel quadrades de $3 + 4i$ són $\pm(2 + i)$.

1.4 Pla complex

Podem representar el nombre complex $a + bi$ pel punt (a, b) del pla. És a dir, en el pla $\mathbb{R}^2$, agafem 1 com a vector unitat de les abscisses i i com a vector unitat de les ordenades. Direm eix real l'eix de les abscisses i eix imaginari l'eix de les ordenades. Diem *mòdul* del nombre complex $z = a + bi$ el mòdul del vector (a, b). Posem $|z|$ el mòdul de z. Si $z = a + bi$, tenim $|z| = \sqrt{a^2 + b^2}$. Diem *argument* del nombre complex no nul $z = a+bi$ l'angle que fa el vector (a, b) amb l'eix real. Posem $\operatorname{Arg} z$ l'argument de z. L'argument d'un nombre complex està determinat tret d'un múltiple enter de 2π, si el donem en radians, i tret d'un múltiple enter de 360, si el donem en graus. Si $r = |z|, \alpha = \operatorname{Arg} z$, tenim $\operatorname{Re} z = r\cos\alpha, \operatorname{Im} z = r\sin\alpha$. El nombre complex z queda doncs determinat pel seu mòdul i el seu argument. Posem $z = r_\alpha$ i diem aquesta expressió la *forma polar* del nombre complex z.

Exemples.

1) Si $a \in \mathbb{R}, a > 0$, $\operatorname{Arg} a = 0$. Si $a \in \mathbb{R}, a < 0$, $\operatorname{Arg} a = \pi$.

2) Si $b \in \mathbb{R}, b > 0$, $\operatorname{Arg}(b\,i) = \pi/2$. Si $b \in \mathbb{R}, b < 0$, $\operatorname{Arg}(b\,i) = 3\pi/2$.

3) Si $z = 1 + i$, $|z| = \sqrt{2}, \operatorname{Arg} z = \pi/4$.

4) Si $a > 0, \operatorname{Arg}(a + bi) = \arctan(b/a)$, si $a < 0, \operatorname{Arg}(a + bi) = \arctan(b/a) + \pi$

1.5 Arrels n-èsimes de nombres complexos

Veiem ara com s'expressa el producte de dos nombres complexos en forma polar. Si $z = r_\alpha, z' = r'_{\alpha'}$, tenim

$$\begin{aligned} zz' &= r(\cos\alpha + i\sin\alpha)\cdot r'(\cos\alpha' + i\sin\alpha') \\ &= rr'(\cos\alpha + i\sin\alpha)\cdot(\cos\alpha' + i\sin\alpha') \\ &= rr'\left((\cos\alpha\cos\alpha' - \sin\alpha\sin\alpha') + (\cos\alpha\sin\alpha' + \cos\alpha'\sin\alpha)\,i\right) \\ &= rr'(\cos(\alpha+\alpha') + i\sin(\alpha+\alpha')). \end{aligned}$$

Hem obtingut doncs

$$|zz'| = |z||z'|,\ \mathrm{Arg}(zz') = \mathrm{Arg}\, z + \mathrm{Arg}\, z'.$$

Per tant l'expressió del producte de dos nombres complexos en forma polar és

$$r_\alpha r'_{\alpha'} = (rr')_{\alpha+\alpha'}.$$

Com a cas particular, obtenim

$$|z^2| = |z|^2,\ \mathrm{Arg}(z^2) = 2\,\mathrm{Arg}\, z.$$

Per inducció, es demostra

$$|z^n| = |z|^n,\ \mathrm{Arg}(z^n) = n\,\mathrm{Arg}\, z, \tag{1.2}$$

per a tot enter $n > 1$.
A partir de (1.2), podem veure com calcular les arrels n-èsimes d'un nombre complex, per a qualsevol enter $n > 1$. Si ω és una arrel n-èsima del nombre complex z, ha de complir

$$|\omega|^n = |z|,\ n\,\mathrm{Arg}\,\omega = \mathrm{Arg}\, z.$$

Com $|z|$ és un nombre real positiu, existeix exactament un nombre real positiu que aixecat a n dóna $|z|$ i que escrivim $\sqrt[n]{|z|}$. Ara, com $\mathrm{Arg}\, z$ està determinat tret d'un múltiple enter de 2π, l'equació $n\,\mathrm{Arg}\,\omega = \mathrm{Arg}\, z$ té n solucions que són

$$\frac{\mathrm{Arg}\, z}{n}, \frac{\mathrm{Arg}\, z + 2\pi}{n}, \ldots, \frac{\mathrm{Arg}\, z + 2(n-1)\pi}{n}.$$

Obtenim doncs n arrels n-èsimes del nombre complex z que s'escriuen

$$(\sqrt[n]{|z|})_{\frac{\mathrm{Arg}\, z + 2k\pi}{n}},\ 0 \le k \le n-1$$

en forma polar.

Exercici. *Calculeu les arrels cúbiques de -1.*

El mòdul de -1 és 1 i el seu argument és π. Les tres arrels cúbiques de -1, escrites en forma polar, són doncs

$$1_{\pi/3}, 1_\pi, 1_{5\pi/3}.$$

Tenint en compte $\cos(\pi/3) = 1/2, \sin(\pi/3) = \sqrt{3}/2, \cos\pi = -1, \sin\pi = 0$, $\cos(5\pi/3) = 1/2, \sin(5\pi/3) = -\sqrt{3}/2$, obtenim que les arrels cúbiques de -1 en forma binòmica són

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

Exercici. *Calculeu les arrels vuitenes de 25.*

El mòdul de 25 és 25 i el seu argument és 0. Les 8 arrels vuitenes de 25, escrites en forma polar, són doncs

$$(\sqrt[4]{5})_0, (\sqrt[4]{5})_{\pi/4}, (\sqrt[4]{5})_{\pi/2}, (\sqrt[4]{5})_{3\pi/4}, (\sqrt[4]{5})_{\pi}, (\sqrt[4]{5})_{5\pi/4}, (\sqrt[4]{5})_{3\pi/2}, (\sqrt[4]{5})_{7\pi/4}.$$

Tenint en compte els valors de sinus i cosinus dels arguments, obtenim que les arrels vuitenes de 25 en forma binòmica són

$$\begin{array}{cccc} \sqrt[4]{5}, & \sqrt[4]{5}\sqrt{2}(1+i)/2, & \sqrt[4]{5}i, & \sqrt[4]{5}\sqrt{2}(-1+i)/2, \\ -\sqrt[4]{5}, & \sqrt[4]{5}\sqrt{2}(-1-i)/2, & -\sqrt[4]{5}i, & \sqrt[4]{5}\sqrt{2}(1-i)/2. \end{array}$$

1.6 Arrels de la unitat.

En particular, les arrels n-èsimes complexes de 1 per a n enter > 1 són $(1)_{2k\pi/n}$, $0 \leq k \leq n-1$.

Exercici. *Calculeu les arrels sisenes de 1.*

Les arrels sisenes de 1 són, en forma polar,

$$(1)_0, (1)_{\pi/3}, (1)_{2\pi/3}, (1)_{\pi}, (1)_{4\pi/3}, (1)_{5\pi/3}.$$

I en forma trigonomètrica

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

Capítol 2

Divisibilitat a l'anell dels enters

2.1 Divisió entera

Proposició 2.1.1 (Divisió de nombres enters)**.** *Donats $a, b \in \mathbb{Z}$, $b \neq 0$, existeixen $q, r \in \mathbb{Z}$ únics tals que*

$$a = bq + r, \quad 0 \leq r < |b|.$$

Diem que q és el quocient *i r la* resta *(o el* residu*) de la divisió de a entre b.*

Demostració. Provem primer l'existència. Distingim quatre casos segons el signe de a i b.

1. Primer cas. $a \geq 0, b > 0$.

   Si $a < b$, clarament $q = 0, r = a$ compleixen les condicions de l'enunciat.

   Si $a \geq b$, considerem el conjunt

   $$\{n \in \mathbb{N} : b(n+1) > a\}.$$

   Per la propietat del primer element de $\mathbb{N}$, existeix q tal que $bq \leq a$ i $b(q+1) > a$. Posem $r = a - bq$ i tenim $r \geq 0, r < b$.

2. Segon cas. $a \geq 0, b < 0$.

   Com $-b > 0$, pel primer cas, tenim q, r tals que

   $$a = (-b)q + r, 0 \leq r < |b|.$$

Per tant $-q$ i r compleixen

$$a = b(-q) + r, 0 \leq r < |b|$$

tal com volíem.

3. Tercer cas. $a < 0, b > 0$.

   Com $-a > 0$, pel primer cas, tenim q, r tals que

   $$-a = bq + r, 0 \leq r < |b|.$$

   Si $r = 0$, tenim $a = b(-q)$.

   Si $r > 0$, $a = b(-q) - r = b(-q - 1) + (b - r)$ amb $0 < b - r < b$.

   Per tant $-q - 1$ i $b - r$ compleixen les condicions per ser quocient i resta de la divisió de a entre b.

4. Quart cas. $a < 0, b < 0$.

   Com $-b > 0$, pel tercer cas, tenim q, r tals que

   $$a = (-b)q + r, 0 \leq r < |b|.$$

   Per tant $-q$ i r compleixen

   $$a = b(-q) + r, 0 \leq r < |b|$$

   tal com volíem.

Provem ara l'unicitat. Suposem que, donats enters a, b, tenim dues parelles d'enters $(q_1, r_1), (q_2, r_2)$ tals que

$$\begin{array}{lll} a = bq_1 + r_1 & , & 0 \leq r_1 < |b|, \\ a = bq_2 + r_2 & , & 0 \leq r_2 < |b|. \end{array}$$

Restant les dues igualtats, obtenim $b(q_2 - q_1) = r_1 - r_2$. Ara la desigualtat $0 \leq r_2 < |b|$ implica $-|b| < -r_2 \leq 0$ i sumant aquesta amb la desigualtat que compleix r_1, obtenim $-|b| < r_1 - r_2 < |b|$ i, per tant $-|b| < b(q_2 - q_1) < |b|$. Com $q_2 - q_1$ és enter, ha de ser $q_2 - q_1 = 0$, és a dir $q_2 = q_1$ i també $r_2 = r_1$. □

Exemple.
2 i 1 són el quocient i la resta de la divisió entera de 7 entre 3.
-2 i 1 són el quocient i la resta de la divisió entera de 7 entre -3.
-3 i 2 són el quocient i la resta de la divisió entera de -7 entre 3.
3 i 2 són el quocient i la resta de la divisió entera de -7 entre -3.

Observació. De vegades interessa tenir una resta de la divisió que sigui el més petita possible en valor absolut. Proveu com a exercici, a partir de 2.1.1, el resultat següent.
Donats $a, b \in \mathbb{Z}$, $b \neq 0$, existeixen $q, r \in \mathbb{Z}$ únics tals que

$$a = bq + r, \quad -|b|/2 < r \leq |b|/2.$$

2.2 Bases de numeració

Habitualment escrivim els enters naturals en base 10. Aleshores, començant per la dreta, la primera xifra és la de les unitats, la segona la de les desenes, la tercera la de les centenes, etc. Per exemple, 7543 representa l'enter $7 \times 10^3 + 5 \times 10^2 + 4 \times 10 + 3$. Podem escriure els enters naturals utilitzant com a base qualsevol enter $b > 1$. Concretament, tenim el resultat següent, que es pot provar per inducció a partir de la divisió entera.

Proposició 2.2.1. *Sigui b un enter > 1. Si n és un enter > 0, existeixen enters $k \geq 0$ i $a_0, a_1, \ldots, a_k \in \{0, 1, 2, \ldots, b-1\}$ únics tals que $a_k \neq 0$ i*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0.$$

Posem $n = (a_k a_{k-1} \ldots a_1 a_0)_b$ i diem que $a_k, a_{k-1}, \ldots, a_1, a_0$ són les xifres de n en base b.

Habitualment, fem servir les xifres $0, 1, \ldots, b-1$ si $b \leq 10$. Si $b > 10$, afegim lletres majúscules en ordre alfabètic. Per exemple, $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, A, B, C, D són les xifres en base 14. Per trobar les xifres en base b d'un nombre escrit en base 10, fem divisions successives.

Exercici. *Escriviu 6695 en base 12 i 545 en base 2. Quin és l'enter $(1CAFE)_{16}$?*

1. Volem escriure 6695 en base 12. Escrivim les xifres en base 12 com $0, 1, \ldots, 9, A, B$. Fent les divisions corresponents, obtenim

$$6695 = 12 \times 557 + 11; 557 = 12 \times 46 + 5; 46 = 12 \times 3 + 10.$$

I per tant $6695 = 12\times557+11 = 12\times(12\times46+5)+11 = 46\times12^2+5\times12+11 = (12 \times 3 + 10) \times 12^2 + 5 \times 12 + 11 = 3 \times 12^3 + 10 \times 12^2 + 5 \times 12 + 11$ que dóna $6695 = (3A5B)_{12}$.

2. Escrivim 545 en base 2. Tenim

$$545 = 2 \times 272 + 1; 272 = 2 \times 136; 136 = 2 \times 68; 68 = 2 \times 34;$$
$$34 = 2 \times 17; 17 = 2 \times 8 + 1; 8 = 2 \times 4; 4 = 2 \times 2; 2 = 2 \times 1.$$

Obtenim doncs $545 = (1000100001)_2$.

3. Per escriure en base 10 un enter escrit en una altra base, simplement operem tenint en compte la magnitud que indica cada xifra.

$$(1CAFE)_{16} = 14 + 15 \times 16 + 10 \times 16^2 + 12 \times 16^3 + 16^4 = 117502,$$

ja que A representa 10, B representa 11, C representa 12, D representa 13, E representa 14 i F representa 15.

Definició 2.2.2. Donats $a, b \in \mathbb{Z}$, si existeix $q \in \mathbb{Z}$ tal que $a = bq$, diem que a és *múltiple* de b o que b és *divisor* de a o que b divideix a o que a és divisible per b. Posem $b \mid a$. Si b no divideix a, posem $b \nmid a$.

Exemples. $4 \mid 12, 5 \nmid 12$, 1 divideix qualsevol enter, 0 és divisible per qualsevol enter. Si n és qualsevol enter, n és divisible per $1, -1, n, -n$.

Observació. Si a i b són enters no nuls, $b \mid a \Rightarrow |b| \leq |a|$.

Proposició 2.2.3 (Propietats de la relació de divisibilitat a $\mathbb{Z}$)**.** *Si $a, b, c, m, n \in \mathbb{Z}$, es compleix*

a) $a \mid a$ *(*reflexivitat*)*

b) $\left.\begin{array}{l} c \mid b \\ b \mid a \end{array}\right\} \Rightarrow c \mid a$ *(*transitivitat*)*

c) $\left.\begin{array}{l} a \mid b \\ b \mid a \end{array}\right\} \Rightarrow b = \pm a$ *(*antisimetria*)*

d) $\left.\begin{array}{l} b \mid a \\ b \mid c \end{array}\right\} \Rightarrow b \mid am + cn$ *(*linealitat*)*

e) $b \mid a \Rightarrow cb \mid ca$ *(*multiplicativitat*)*

f) $\left.\begin{array}{l} cb \mid ca \\ c \neq 0 \end{array}\right\} \Rightarrow b \mid a$ *(*llei de simplificació*)*

Demostració.

a) Clarament $a = a \cdot 1$

b) $\left.\begin{array}{l} c \mid b \Rightarrow b = qc \text{ amb } \ q \text{ enter} \\ b \mid a \Rightarrow a = q'b \text{ amb } \ q' \text{ enter} \end{array}\right\} \Rightarrow$

$a = q'b = q'(qc) = (q'q)c$ i qq' és enter $\Rightarrow c \mid a$.

c) Si $a = 0$, tenim $b = 0$, ja que $b = aq$, per a algun enter q i per tant es compleix $b = a$.

Suposem ara $a \neq 0$.

$\left.\begin{array}{l} a \mid b \Rightarrow b = qa \text{ amb } \ q \text{ enter} \\ b \mid a \Rightarrow a = q'b \text{ amb } \ q' \text{ enter} \end{array}\right\} \Rightarrow$

$a = (qq')a \overset{a \neq 0}{\Rightarrow} qq' = 1 \Rightarrow q = q' = \pm 1 \Rightarrow b = \pm a.$

d) $\left.\begin{array}{l} b \mid a \Rightarrow a = bq \text{ amb } \ q \text{ enter} \\ b \mid c \Rightarrow c = bq' \text{ amb } \ q' \text{ enter} \end{array}\right\} \Rightarrow am + cn = (bq)m + (bq')n$

$= b(qm + q'n),$ on $qm + q'n$ és enter $\Rightarrow b \mid am + cn.$

e) $b \mid a \Rightarrow a = bq$ amb $\ q$ *enter* $\Rightarrow ca = (cq)b$ on cq és enter $\Rightarrow cb \mid ca.$

f) $\left.\begin{array}{l} cb \mid ca \Rightarrow ca = cbq \text{ amb } \ q \text{ enter} \\ c \neq 0 \end{array}\right\} \Rightarrow a = bq \Rightarrow b \mid a$

□

Observació. Les propietats a),b),c) de la relació de divisibilitat indiquen que aquesta relació és relació d'ordre a $\mathbb{N}$. No és relació d'ordre total.

2.3 Màxim comú divisor de dos enters

Un *divisor comú* de dos enters a i b és un enter d tal que $d \mid a$ i $d \mid b$.

Definició 2.3.1. Donats dos enters a, b direm que un enter d és màxim comú divisor de a i b si compleix les dues propietats següents.

1. $d \mid a$ i $d \mid b$
2. Si d_1 és un enter tal que $d_1 \mid a$ i $d_1 \mid b$, aleshores $d_1 \mid d$.

Observació. Si d és màxim comú divisor de a i b, $-d$ també ho és.

Proposició 2.3.2. *Si d_1 i d_2 són màxims comuns divisors de a i b, tenim $d_1 = \pm d_2$.*

Demostració. Com d_1 és màxim comú divisor de a i b i d_2 n'és un divisor comú, obtenim de la definició, $d_2 \mid d_1$. Anàlogament, obtenim $d_1 \mid d_2$. Aleshores, per la propietat antisimètrica de la relació de divisibilitat, obtenim $d_1 = \pm d_2$. □

Tenim doncs que el màxim comú divisor de dos enters queda determinat tret del signe. Podem escriure, per exemple, $2 = \mathrm{mcd}(4, 6)$ i també $-2 = \mathrm{mcd}(4, 6)$. Qualsevol igualtat amb màxims comuns divisors serà també tret del signe.

Exemple. Per a tot enter a, tenim $\mathrm{mcd}(a, 0) = a$ ja que qualsevol enter divideix 0.

2.4 Algoritme d'Euclides.

Veiem ara un algoritme per a calcular el màxim comú divisor de dos nombres enters. En particular, tindrem que, donats dos nombres enters, existeix el seu màxim comú divisor. Abans provem un resultat previ.

Lema 2.4.1. *Si a, b, q són nombres enters, tenim*

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(a - bq, b).$$

Demostració. Veiem que les parelles (a, b) i $(a - bq, b)$ tenen els mateixos conjunts de divisors comuns. D'aquí es dedueix clarament la igualtat dels màxims comuns divisors. Ara, per la propietat de linealitat de la relació de divisibilitat, tenim les implicacions següents.

$$d \mid a \text{ i } d \mid b \Rightarrow d \mid a - bq$$
$$d \mid a - bq \text{ i } d \mid b \Rightarrow d \mid (a - bq) + qb = a.$$

□

Proposició 2.4.2 (Algoritme d'Euclides)**.** *Siguin a, b dos enters, $b \neq 0$. Fem successivament les divisions enteres*

$$\begin{aligned} a &= bq_1 + r_1, & 0 \leq r_1 < |b| \\ b &= r_1q_2 + r_2, & 0 \leq r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, & 0 \leq r_3 < r_2 \\ r_2 &= r_3q_4 + r_4, & 0 \leq r_4 < r_3 \\ &\vdots \end{aligned}$$

Aleshores, existeix $n \in \mathbb{N}$ tal que $r_n = 0$ i es compleix $\mathrm{mcd}(a, b) = r_{n-1}$.

Demostració. Volem veure que arribem a una resta igual a 0 en un nombre finit de passos. En efecte, si considerem la successió de restes, tenim $r_1 > r_2 > r_3 > \ldots$ per tant formen una successió estrictament decreixent d'enters naturals i tenim doncs $r_n = 0$ per a algun $n \in \mathbb{N}$. Ara, pel lema, es compleix $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r_1) = \mathrm{mcd}(r_1, r_2) = \mathrm{mcd}(r_2, r_3) = \cdots = \mathrm{mcd}(r_{n-1}, r_n) = \mathrm{mcd}(r_{n-1}, 0) = r_{n-1}$. □

Exercici. *Calculeu el màxim comú divisor de les següents parelles d'enters amb l'algoritme d'Euclides.*

$$\{4347, 235\},\ \{5957, 994\},\ \{2874, 999\}.$$

1. $\mathrm{mcd}(4347, 235)$

$$\begin{aligned} 4347 &= 235 \times 18 + 117 \\ 235 &= 117 \times 2 + 1 \end{aligned}$$

   Obtenim $\mathrm{mcd}(4347, 235) = 1$.

2. $\mathrm{mcd}(5957, 994)$

$$\begin{aligned} 5957 &= 994 \times 5 + 987 \\ 994 &= 987 \times 1 + 7 \\ 987 &= 7 \times 28 + 0 \end{aligned}$$

Obtenim $\mathrm{mcd}(5957, 994) = 7$.

3. $\mathrm{mcd}(2874, 999)$

$$\begin{aligned} 2874 &= 999 \times 2 + 876 \\ 999 &= 876 \times 1 + 123 \\ 876 &= 123 \times 7 + 15 \\ 123 &= 15 \times 8 + 3 \\ 15 &= 3 \times 5 + 0 \end{aligned}$$

Obtenim $\mathrm{mcd}(2874, 999) = 3$.

Proposició 2.4.3 (Identitat de Bézout)**.** *Si $d = \mathrm{mcd}(a, b)$, aleshores existeixen enters s, t tals que*

$$d = sa + tb.$$

Demostració. Veiem com es poden calcular s, t complint $d = sa + tb$ a partir de les divisions que hem fet en aplicar l'algoritme d'Euclides. Si $a = bq_1 + r_1$, tenim $r_1 = a - bq_1$ i podem escriure la igualtat de matrius

$$\begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Anàlogament, $b = r_1 q_2 + r_2 \Rightarrow r_2 = b - r_1 q_2$ que dóna la igualtat de matrius

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} b \\ r_1 \end{pmatrix}$$

i, per a cada i, $r_i = r_{i+1} q_{i+2} + r_{i+2} \Rightarrow r_{i+2} = r_i - r_{i+1} q_{i+2}$ que dóna

$$\begin{pmatrix} r_{i+1} \\ r_{i+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+2} \end{pmatrix} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}.$$

Si r_n és la primera resta nul·la, obtenim

$$\begin{aligned}
\begin{pmatrix} r_{n-1} \\ 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \begin{pmatrix} r_{n-3} \\ r_{n-2} \end{pmatrix} \\
&= \dots \\
&= \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}}_{\begin{pmatrix} s & t \\ * & * \end{pmatrix}} \begin{pmatrix} a \\ b \end{pmatrix}.
\end{aligned}$$

Com s i t s'obtenen fent sumes i productes d'enters, són enters i per la igualtat de matrius compleixen $\mathrm{mcd}(a,b) = r_{n-1} = sa + tb$. □

Exercici. *Calculeu els coeficients d'una identitat de Bézout per a 2874 i 999.*

Havíem calculat $\mathrm{mcd}(2874, 999) = 3$. Tenim

$$\begin{pmatrix} 3 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -7 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

Fent el producte de matrius

$$\begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -7 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} -65 & 187 \\ * & * \end{pmatrix}.$$

Per tant $3 = -65 \times 2874 + 187 \times 999$.

Observació. També podem calcular els coeficients de la identitat de Bézout aïllant successivament les restes de cada divisió començant per l'última. En l'exemple anterior, tenim

$$\begin{aligned}
3 &= 123 - 15 \times 8 = 123 - (876 - 123 \times 7) \times 8 = 123 \times 57 - 876 \times 8 \\
&= (999 - 876 \times 1) \times 57 - 876 \times 8 = 999 \times 57 - 876 \times 65 \\
&= 999 \times 57 - (2874 - 999 \times 2) \times 65 = 999 \times 187 - 2874 \times 65.
\end{aligned}$$

Podem definir també el màxim comú divisor de més de dos enters.

Definició 2.4.4. Donats enters $a_1, a_2, \ldots, a_n$ direm que un enter d és màxim comú divisor de $a_1, a_2, \ldots, a_n$ si compleix les dues propietats següents.

1. $d \mid a_i$ per a tot $i = 1, \ldots, n$,
2. Si d_1 és un enter tal que $d_1 \mid a_i$ per a tot $i = 1, \ldots, n$, aleshores $d_1 \mid d$.

Es compleix la igualtat següent entre màxims comuns divisors

$$\mathrm{mcd}(a_1, a_2, \ldots, a_n) = \mathrm{mcd}(\mathrm{mcd}(a_1, a_2, \ldots, a_{n-1}), a_n)$$

per tant el càlcul del màxim comú divisor de més de dos enters es redueix al càlcul del màxim comú divisor de dos enters.

Exercici. *Calculeu* $\mathrm{mcd}(750, 1110, 780, 474)$.

Aplicant l'algoritme d'Euclides, obtenim $\mathrm{mcd}(750, 1110) = 30, \mathrm{mcd}(30, 780) = 30, \mathrm{mcd}(30, 474) = 6$. Tenim doncs $\mathrm{mcd}(750, 1110, 780, 474) = 6$.

2.5 Mínim comú múltiple

Un múltiple comú de dos enters a, b és un enter m tal que $a \mid m$ i $b \mid m$.

Definició 2.5.1. Donats dos enters a, b direm que un enter m és mínim comú múltiple de a i b si compleix les dues propietats següents.

1. $a \mid m$ i $b \mid m$
2. Si m_1 és un enter tal que $a \mid m_1$ i $b \mid m_1$, aleshores $m \mid m_1$.

Observació. Si m és mínim comú múltiple de a i b, $-m$ també ho és.

Proposició 2.5.2. *Si m_1 i m_2 són mínims comuns múltiples de a i b, tenim $m_1 = \pm m_2$.*

Demostració. És anàlega a la de 2.3.2. □

Dos enters a i b es diuen *coprimers* si $\mathrm{mcd}(a, b) = 1$.

Exemple. 4337 i 235 són coprimers.

Proposició 2.5.3. *Siguin $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ i $\mathrm{mcd}(a, b) = 1$, aleshores $a \mid c$.*

Demostració. Com $\mathrm{mcd}(a, b) = 1$, existeixen enters s, t tals que $1 = sa + tb$. Multiplicant aquesta igualtat per c, obtenim $c = sac + tbc$. Com per hipòtesi $a \mid bc$, obtenim $a \mid c$. □

Observació. En general, si un enter divideix un producte de dos altres enters, no necessàriament divideix un dels factors. Per exemple, $4 \mid 6 \times 10$ però $4 \nmid 6$ i $4 \nmid 10$.

Proposició 2.5.4. *Si a, b són enters no nuls, tenim*

$$\mathrm{mcd}(a, b) = 1 \Leftrightarrow \text{ existeixen enters } s, t \text{ tals que } sa + tb = 1.$$

Demostració. L'implicació $\Rightarrow$ ja està vista.
Suposem ara que existeixen enters s, t tals que $sa + tb = 1$. Si $d \mid a$ i $d \mid b$, per la propietat de linealitat de la divisibilitat, tenim $d \mid sa + tb = 1$, per tant ha de ser $d = \pm 1$. Com els únics divisors comuns de a i b són 1 i -1, tenim $\mathrm{mcd}(a, b) = 1$. □

Corol·lari 2.5.5. *Si a, b són enters, $d = \mathrm{mcd}(a, b)$, posem $a = da_1$, $b = db_1$. Aleshores $\mathrm{mcd}(a_1, b_1) = 1$.*

Demostració. Tenim $d = sa + tb$ per certs enters s, t i per tant $1 = sa_1 + tb_1$ que implica $\mathrm{mcd}(a_1, b_1) = 1$ per la proposició anterior. □

Proposició 2.5.6. *Si a, b són enters, $d = \mathrm{mcd}(a, b), m = \mathrm{mcm}(a, b)$, es compleix $dm = \pm ab$.*

Demostració. Posant $a = da_1$, $b = db_1$, tenim que $ab/d = ab_1$ és enter. Veiem que ab/d és mínim comú múltiple de a i b. Com $ab/d = ab_1 = a_1 b$, és múltiple de a i de b.
Sigui ara m_1 un múltiple comú de a i b. Tenim $m_1 = pa, m_1 = qb$ per certs enters p i q. Per tant $m_1 = pa = pda_1$ i $m_1 = qb = qdb_1$. Tenim doncs $pda_1 = qdb_1 \Rightarrow pa_1 = qb_1$. Com $b_1 \mid pa_1$ i $\mathrm{mcd}(a_1, b_1) = 1$, obtenim $b_1 \mid p$. Podem escriure $p = b_1 s$, per un cert enter s. Aleshores $m_1 = pda_1 = s(b_1 da_1) = s(ab/d)$, és a dir m_1 és múltiple de ab/d i hem provat que ab/d compleix la segona propietat de mínim comú múltiple. □

A partir d'aquesta proposició i del càlcul del màxim comú divisor, podem calcular el mínim comú múltiple de dos enters.

Exercici. *Calculeu el mínim comú múltiple de 5957 i 994.*

Havíem calculat $\mathrm{mcd}(5957, 994) = 7$. Tenim doncs

$$\mathrm{mcm}(5957, 994) = \frac{5957 \times 994}{7} = 845894.$$

Definició 2.5.7. Un *nombre primer* és un enter p, diferent de $0, 1$ i -1, que només és divisible per $1, -1, p, -p$.

Observació. Si p és primer, $-p$ també ho és.

Proposició 2.5.8. *Siguin a, b nombres enters i sigui p un nombre primer. Si $p \mid ab$ i $p \nmid a$, aleshores $p \mid b$.*

Demostració. Si p és primer i $p \nmid a$, tenim $\mathrm{mcd}(a, p) = 1$. Per tant, per 2.5.3, $p \mid b$. □

Lema 2.5.9. *Si n és un enter que no és primer, és divisible per un primer p positiu tal que $p \leq \sqrt{|n|}$.*

Demostració. Com n i $-n$ tenen els mateixos divisors, podem suposar $n > 0$. Per la definició de nombre primer, si n no ho és, tenim $n = m_1 m_2$ amb m_1, m_2 enters positius diferents de $1, n$. Podem suposar $m_1 \leq m_2$ i tenim $m_1 \leq \sqrt{n}$. Si m_1 és primer, ja estem. Si no, podem escriure $m_1 = q_1 q_2$, amb q_1, q_2 enters positius diferents de $1, m_1$. Si q_1 és primer, ja estem. Si no, reiterem el procès. Com $m_1 > q_1 > \ldots$, en un nombre finit de passos trobem un divisor primer de n, més petit o igual que $\sqrt{|n|}$. □

Garbell d'Eratòstenes. Suposem que volem trobar tots els nombres primers positius fins a una fita M. Ho podem fer amb el mètode del garbell d'Eratòstenes que data del segle III a. C. Posem M=100. Escrivim tots els enters naturals fins a M excepte 0 i 1.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

El 2 és primer ja que l'únic enter positiu més petit que ell és l'1. Treiem tots els seus múltiples:

	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49
51		53	55	57	59
61		63	65	67	69
71		73	75	77	79
81		83	85	87	89
91		93	95	97	99

El primer enter, més gran que 2, que no hem tret és el 3. És primer, ja que l'únic enter positiu diferent de 1 més petit que ell és el 2, que no el divideix, ja que si 2 dividís 3, hauríem tret el 3. Treiem ara els múltiples de 3 que queden (és a dir els que no són també múltiples de 2).

	2	3	5	7	
11		13		17	19
		23	25		29
31			35	37	
41		43		47	49
		53	55		59
61			65	67	
71		73		77	79
		83	85		89
91			95	97	

El primer enter, més gran que 3, que no hem tret és el 5. És primer ja que 2 i 3 no el divideixen. Treiem els seus múltiples.

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	49
		53			59
61				67	
71		73		77	79
		83			89
91				97	

Com abans, 7 és primer, treiem els seus múltiples.

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	
		53			59
61				67	
71		73			79
		83			89
				97	

El primer enter, més gran que 7, que no hem tret és l'11. Com $11 > \sqrt{100}$, tenint

en compte el lema 2.5.9, podem afirmar que els enters que queden a la taula són tots primers.
Amb el mateix mètode, podem obtenir la taula dels nombres primers positius més petits o iguals que un enter positiu M donat. Observem que, quan treiem de la taula els múltiples d'un primer p, comencem per p^2 ja que els anteriors són divisibles per algun primer més petit i que, quan arribem a un primer més gran que $\sqrt{M}$ ja hem acabat, és a dir els nombres que queden a la taula són tots primers.

Teorema 2.5.10 (Teorema d'Euclides)**.** *El conjunt dels nombres primers és infinit.*

Demostració. Es poden donar diferents proves d'aquest resultat. Aquí en veurem dues.
Primera prova. Veiem que, per a tot nombre natural n, existeix un nombre primer més gran que n. Com $\mathbb{N}$ és infinit, això implicarà que el conjunt dels nombres primers també ho és. Considerem l'enter $n! + 1$. Si aquest nombre és primer, ja hem acabat, ja que $n! + 1 > n$. Si no, existeix un primer p que el divideix. Si $p \leq n$, p és un dels factors de $n!$. Tenim doncs $p \mid n! + 1$ i $p \mid n!$ que implica $p \mid 1$ per tant arribem a contradicció i ha de ser $p > n$.
Segona prova. Suposem que el nombre de primers positius és finit i arribarem a contradicció. Sigui $\{p_1, p_2, \ldots, p_n\}$ el conjunt dels nombres primers positius. Considerem l'enter $N = p_1 p_2 \ldots p_n + 1$. L'enter N no pot ser primer, ja que és estrictament més gran que tots els p_i. Per tant és divisible per un primer, és a dir per un dels p_i. Tenim doncs $p_i \mid N$ i $p_i \mid p_1 p_2 \ldots p_n$ que implica $p_i \mid 1$ i per tant arribem a contradicció. Hem provat doncs que el conjunt de primers és infinit. □

2.6 El teorema fonamental de l'aritmètica

Teorema 2.6.1 (Teorema fonamental de l'aritmètica)**.** *Sigui a un nombre enter, $a \neq 0, 1, -1$. Aleshores existeixen nombres primers positius $p_1, \ldots, p_n$, $(n \geq 1)$ tals que*

$$a = \varepsilon p_1 \ldots p_n$$

on ε és igual a 1 o -1. A més, $p_1, \ldots, p_n$ són únics trets de l'ordre.

Demostració. Podem suposar $a > 0$, ja que, si és cert per a, només cal canviar el signe per tenir el resultat per $-a$.

Si a és primer, tenim el resultat amb $n = 1, p_1 = a$. Si a no és primer, és divisible per un primer positiu p_1 i $a_2 = a/p_1$ és estrictament més petit que a. Ara, si a_2 és primer, posem $p_2 = a_2$ i tenim $a = p_1p_2$, producte de dos primers. Si a_2 no és primer, és divisible per un primer positiu p_2 i $a_3 = a_2/p_2$ és estrictament més petit que a_2. Repetim el procès. Com $a, a_2, a_3, \ldots$ és una successió decreixent d'enters positius, arribem a a_n primer en un nombre finit de passos. Obtenim doncs $a = p_1p_2 \ldots p_n$, amb $p_1, p_2, \ldots, p_n$ primers.
Veiem ara l'unicitat. Clarament ε és únic, ja que és 1 si $a > 0$ i -1 si $a < 0$. Ara suposem que tenim una igualtat $p_1p_2 \ldots p_n = q_1q_2 \ldots q_m$ amb $p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_m$ primers positius. Podem suposar $n \leq m$. Aleshores $q_1 \mid p_1p_2 \ldots p_n$ que implica que q_1 divideix algun p_i per 2.5.8. Reordenant els $p's$ podem suposar $q_1 \mid p_1$ i, com tots dos són primers positius, tenim $p_1 = q_1$. Simplificant la igualtat, tenim $p_2 \ldots p_n = q_2 \ldots q_m$. Repetint el procès, obtenim successivament $p_2 = q_2$, $\ldots$, $p_n = q_n$ i ens queda la igualtat $1 = q_{n+1} \ldots q_m$. Però 1 no és divisible per cap primer, per tant ha de ser $n = m$. □

Observació. Podem associar els factors iguals en la descomposició de l'enter a en producte de primers i escriure

$$a = \varepsilon p_1^{r_1} \ldots p_k^{r_k}, \text{ amb } r_i \geq 1; p_1, \ldots, p_k \text{ primers diferents.}$$

2.7 Equacions diofantines lineals

Una *equació diofantina lineal amb dues incògnites* és una equació de la forma

$$ax + by = c$$

amb a, b, c enters. Les solucions de l'equació són les parelles (x, y) d'enters que la compleixen.

El teorema següent dóna la resolució de les equacions diofantines lineals amb dues incògnites.

Teorema 2.7.1. *L'equació diofantina*

$$ax + by = c$$

té solució si i només si $\text{mcd}(a, b) \mid c$. *Si* (x, y) *és una solució, totes les solucions són*

$$(x+\lambda\frac{b}{\mathrm{mcd}(a,b)}, y-\lambda\frac{a}{\mathrm{mcd}(a,b)},\ \ amb\ \ \lambda\in\mathbb{Z}.$$

Demostració. Posem $d=\mathrm{mcd}(a,b)$. Si (x,y) és una solució de l'equació, tenim $d \mid ax+by=c$. Suposem ara $d \mid c$. Posem $c=dc_1$, amb c_1 enter. Sabem, per 2.4.3, que existeixen enters s,t tals que $d=as+bt$. Multiplicant aquesta igualtat per c_1, obtenim $c=dc_1=asc_1+btc_1$, per tant (sc_1,tc_1) és una solució de l'equació. Veiem ara la forma de totes les solucions. Suposem que (x,y) és una solució de l'equació i (x_1,y_1) n'és una altra. Tenim

$$\left.\begin{array}{rcl} ax+by & = & c \\ ax_1+by_1 & = & c \end{array}\right\} \Rightarrow a(x_1-x)+b(y_1-y)=0.$$

Si $d=\mathrm{mcd}(a,b)$, podem posar $a=da_1, b=db_1$. Dividint la igualtat obtinguda per d, tenim $a_1(x_1-x)+b_1(y_1-y)=0$, que implica $a_1(x_1-x)=-b_1(y_1-y)$. Tenim doncs $b_1 \mid a_1(x_1-x)$ i, com a_1,b_1 són primers entre ells (veure 2.5.5), $b_1 \mid (x_1-x)$ (per 2.5.3). Podem posar doncs, $x_1-x=b_1\lambda$, amb λ enter. Ara, substituint a $a_1(x_1-x)=-b_1(y_1-y)$, tenim $a_1b_1\lambda=-b_1(y_1-y)$ i, per tant, $y_1-y=-a_1\lambda$. Hem obtingut $(x_1,y_1)=(x+b_1\lambda, y-a_1\lambda)$, amb λ enter. Només queda veure que, si (x,y) és solució de l'equació, aleshores $(x+b_1\lambda, y-a_1\lambda)$ també ho és per a qualsevol enter λ. Substituint a l'equació, tenim

$$a(x+b_1\lambda)+b(y-a_1\lambda)=ax+by+(ab_1-ba_1)\lambda=ax+by=c,$$

ja que $ab_1=da_1b_1=ba_1$ i (x,y) és solució de l'equació. □

Exercici. *Resoleu les equacions diofantines següents.*

$$91x+112y=14,\ 221x+273y=3,\ 105x-176y=2.$$

a) $91x+112y=14$

Tenim $\mathrm{mcd}(91,112)=7$ i $7 \mid 14$, per tant l'equació té solucions. Una identitat de Bézout és

$$5\times 91-4\times 112=7,$$

per tant $(10,-8)$ és una solució de l'equació. Totes les solucions són:

$$\begin{cases} x = 10 + 16\lambda \\ y = -8 - 13\lambda \end{cases}$$

b) $221x + 273y = 3$

Tenim $\text{mcd}(221, 273) = 13 \nmid 3$, per tant l'equació no té solucions.

c) $105x - 176y = 2$

Tenim $\text{mcd}(105, 176) = 1$ i $1 \mid 2$, per tant l'equació té solucions. Una identitat de Bézout és

$$57 \times 105 - 34 \times 176 = 1,$$

per tant $(114, 68)$ és una solució de l'equació. Totes les solucions són:

$$\begin{cases} x = 114 + 176\lambda \\ y = 68 + 105\lambda \end{cases}$$

Capítol 3

Polinomis amb coeficients en un cos

3.1 L'anell $K[X]$

Sigui K un cos (per exemple, $K = \mathbb{Q}$, $K = \mathbb{R}$ o $K = \mathbb{C}$). Una successió d'elements de K és una aplicació de $\mathbb{N}$ en K. Si indiquem per a_n l'imatge de n, la successió està determinada per $(a_0, a_1, a_2, \dots)$ i l'indiquem per $(a_n)_{n\in\mathbb{N}}$ o simplement (a_n). Un *polinomi amb coeficients a* K és una successió (a_n) d'elements de K tal que $a_n = 0$ excepte per un nombre finit de valors de n. Definim la suma i el producte de dos polinomis $(a_n), (b_n)$ per

$$(a_n) + (b_n) = (a_n + b_n),\ (a_n) \cdot (b_n) = (\sum_{i=0}^{n} a_i b_{n-i}).$$

Si $a_n = 0$, per a $n > N$, i $b_n = 0$, per a $n > M$, tenim $a_n + b_n = 0$ per a $n > \max\{N, M\}$ i $\sum_{i=1}^{n} a_i b_{n-i} = 0$ per a $n > N + M + 1$, per tant suma i producte són operacions internes en el conjunt de polinomis. A partir de les propietats de la suma i el producte del cos K, podem provar les següents propietats de la suma i el producte en el conjunt de polinomis amb coeficients a K.

- La suma és associativa i commutativa. El polinomi (a_n) amb $a_n = 0$ per a tot $n \in \mathbb{N}$ és element neutre per la suma. Tot polinomi (a_n) té oposat: $(-a_n)$.

- El producte és associatiu, commutatiu i distributiu respecte de la suma. El polinomi (a_n) amb $a_0 = 1, a_n = 0$ per a tot $n > 0$ és element neutre pel producte.

Per tant el conjunt de polinomis amb coeficients a K amb la suma i el producte que hem definit és un anell commutatiu i amb unitat.

Posem $X = (0, 1, 0, \dots)$. A partir de la definició del producte, tenim $X^2 = (0, 0, 1, 0, \dots), X^3 = (0, 0, 0, 1, 0, \dots)$ i, en general, $X^n = (\underbrace{0, \dots, 0}_{n}, 1, 0, \dots)$.

Definim un producte extern amb escalars a K en el conjunt de polinomis.

$$\lambda(a_n) = (\lambda a_n).$$

Si $b \in K$ i (a_n) és un polinomi amb coeficients a K, tenim

$$b(a_n) = (ba_n) = (b, 0, \dots)(a_n).$$

Identifiquem un element $b \in K$ amb el polinomi $(b, 0, \dots)$. Anomenem *constants* els polinomis d'aquesta forma. Obtenim

$$(a_n) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n + \dots.$$

Anomenem X *indeterminada* o *variable* i denotem per $K[X]$ l'anell de polinomis amb coeficients a K.
Diem que el polinomi no nul (a_n) té *grau* m si $a_m \neq 0$ i $a_n = 0$ per a tot $n > m$. El grau del polinomi 0 és $-\infty$. Si (a_n) té grau m i $a_m = 1$, diem que (a_n) és mònic.

Notació. A partir d'ara escriurem A, o $A(X)$, el polinomi amb coeficients a_n; B, o $B(X)$, el polinomi amb coeficients b_n, ...

Proposició 3.1.1. *Siguin $A, B \in K[X]$. Si $A \neq 0$ i $B \neq 0$, aleshores $AB \neq 0$.*

Demostració. Si $n = grA, m = grB$, el coeficient de X^{m+n} en $A + B$ és $a_nb_m \neq 0$, per tant $AB \neq 0$. □

Corol·lari 3.1.2 (Llei de simplificació)**.** *Siguin $A, B, C \in K[X]$. Si $C \neq 0$, aleshores $CA = CB \Rightarrow A = B$.*

Demostració. $CA = CB \Rightarrow C(A - B) = CA - CB = 0$. Per la proposició, un dels dos factors ha de ser 0. Com per hipòtesi, $C \neq 0$, tenim $A - B = 0$. □

Proposició 3.1.3 (Propietats del grau)**.** *Per a $A, B \in K[X]$, es compleix*

1. $gr(A + B) \leq \max\{grA, grB\}$

2. $gr(AB) = grA + grB$

Demostració. Observem primer que les dues fòrmules són vàlides en el cas que un dels polinomis és 0 si convenim que $-\infty$ és més petit que qualsevol enter i $-\infty + n = -\infty$ per a tot $n \in \mathbb{N} \cup \{-\infty\}$.
Suposem ara A i B no nuls. Sigui $n = grA, m = grB$. Podem suposar $n \leq m$. Aleshores, si $n < m$, el coeficient de X^m en $A+B$ és $b_m \neq 0$ i els de X^k, $k > m$, són tots nuls. Per tant, en aquest cas, tenim $gr(A+B) = \max\{grA, grB\}$. Si $n = m$, els coeficients en $A+B$ de X^k, $k > m$, són tots nuls però no podem assegurar que el coeficient en $A+B$ de X^m no sigui nul i tenim $gr(A+B) \leq \max\{grA, grB\}$.
Pel producte, si $n = grA, m = grB$, el coeficient de X^{m+n} en AB és $a_n b_m \neq 0$ i els de X^k, $k > m+n$ són tots nuls. Per tant, tenim $gr(AB) = grA + grB$. □

Corol·lari 3.1.4. *Els elements invertibles de $K[X]$ són exactament els de $K \setminus \{0\}$.*

Demostració. Per la proposició, si $A, B \in K[X] \setminus \{0\}$, $AB = 1$ implica $grA + grB = 0$ i com el grau ha de ser un nombre natural, tenim $grA = grB = 0$, per tant A i B constants. □

3.2 Divisió entera de polinomis.

Proposició 3.2.1 (Divisió de polinomis)**.** *Sigui K un cos. Donats $A, B \in K[X]$, $B \neq 0$, existeixen $Q, R \in K[X]$ únics tals que*

$$A = BQ + R, \quad grR < grB.$$

Diem que Q és el quocient *i R la* resta *(o el* residu*) de la divisió de A entre B.*

Demostració. Provem primer l'existència.
1) Si $grA < grB$, és clar que $Q = 0, R = A$ compleixen les dues relacions de l'enunciat.
2) Si $grA \geq grB$, fem inducció sobre grA. Suposem l'enunciat cert per a $grA < n$ i ho provem per a $grA = n$. Posem

$$A(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0, \text{ amb } a_n \neq 0$$
$$B(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_0, \text{ amb } b_m \neq 0$$

Considerem $A_1(X) = A(X) - \frac{a_n}{b_m}X^{n-m}B(X)$. El coeficient de X^n en A_1 és $a_n - \frac{a_n}{b_m}b_m = 0$, per tant $grA_1(X) < grA(X)$. Per hipòtesi d'inducció, existeixen $Q_1(X), R(X) \in K[X]$ tals que

$$A_1(X) = B(X)Q_1(X) + R(X),\ grR(X) < grB(X).$$

Tenim doncs

$$\begin{aligned} A(X) &= A_1(X) + \frac{a_n}{b_m}X^{n-m}B(X) \\ &= B(X)\underbrace{\left(\frac{a_n}{b_m}X^{n-m} + Q_1(X)\right)}_{Q(X)} + R(X). \end{aligned}$$

Per tant $Q(X) = \frac{a_n}{b_m}X^{n-m} + Q_1(X), R(X)$ compleixen les condicions per ser quocient i resta de la divisió de $A(X)$ entre $B(X)$.
Provem ara l'unicitat. Suposem que, donats polinomis $A, B \in K[X]$, tenim dues parelles $(Q_1, R_1), (Q_2, R_2)$ de polinomis de $K[X]$ tals que

$$\begin{aligned} A = BQ_1 + R_1 \quad &, \quad grR_1 < grB, \\ A = BQ_2 + R_2 \quad &, \quad grR_2 < grB. \end{aligned}$$

Restant les dues igualtats, obtenim

$$B(Q_2 - Q_1) = R_1 - R_2. \tag{3.1}$$

Ara tenim

$$gr(R_1 - R_2) \leq \max\{grR_1, grR_2\} < grB.$$

D'altra banda

$$gr(B(Q_2 - Q_1)) = grB + gr(Q_2 - Q_1),$$

per tant $Q_2 - Q_1 = 0$. Substituint a (3.1), obtenim $R_1 - R_2 = 0$. □

Exercici. *Considerem els polinomis* $A = X^4 + 3X^3 - 2X^2 + 5X - 3$, $B = 2X^2 - X + 4 \in \mathbb{Q}[X]$. *Feu la divisió de* A *entre* B.

$$
\begin{array}{rcrcrcrcr|l}
X^4 & + & 3X^3 & - & 2X^2 & + & 5X & - & 3 & 2X^2 - X + 4 \\
\cline{10-10}
- X^4 & + & \frac{1}{2}X^3 & - & 2X^2 & & & & & \frac{1}{2}X^2 + \frac{7}{4}X - \frac{9}{8} \\
\cline{1-5}
 & & \frac{7}{2}X^3 & - & 4X^2 & + & 5X & & & \\
 & - & \frac{7}{2}X^3 & + & \frac{7}{4}X^2 & - & 7X & & & \\
\cline{2-7}
 & & & - & \frac{9}{4}X^2 & - & 2X & - & 3 & \\
 & & & & \frac{9}{4}X^2 & - & \frac{9}{8}X & + & \frac{9}{2} & \\
\cline{5-9}
 & & & & & - & \frac{25}{8}X & + & \frac{3}{2} &
\end{array}
$$

Obtenim que el quocient és $\frac{1}{2}X^2 + \frac{7}{4}X - \frac{9}{8}$ i la resta $-\frac{25}{8}X + \frac{3}{2}$.

Donats $A, B \in K[X]$, si existeix $Q \in K[X]$ tal que $A = BQ$, direm que A és *múltiple* de B o que B és *divisor* de A. Posem $B \mid A$.

Exemples. $X + 1 \mid X^2 - 1, X \nmid X^2 + 1$; $\lambda \in K \setminus \{0\}$ divideix qualsevol polinomi; 0 és divisible per qualsevol polinomi. Si A és qualsevol polinomi de $K[X]$, A és divisible per $\lambda, \lambda A$, per a tot $\lambda \in K \setminus \{0\}$.

Proposició 3.2.2. *(Propietats de la relació de divisibilitat a $K[X]$)*
Si $A, B, C, M, N \in K[X]$, es compleix

a) $A \mid A$ *(*reflexivitat*)*

b) $\left.\begin{array}{c} C \mid B \\ B \mid A \end{array}\right\} \Rightarrow C \mid A$ *(*transitivitat*)*

c) $\left.\begin{array}{c} A \mid B \\ B \mid A \end{array}\right\} \Rightarrow B = \lambda A$, *amb* $\lambda \in K \setminus \{0\}$ *(*antisimetria*)*

d) $\left.\begin{array}{c} B \mid A \\ B \mid C \end{array}\right\} \Rightarrow B \mid AM + CN$ *(*linealitat*)*

e) $B \mid A \Rightarrow CB \mid CA$ *(*multiplicativitat*)*

f) $\left.\begin{array}{l} CB \mid CA \\ C \neq 0 \end{array}\right\} \Rightarrow B \mid A$ *(*llei de simplificació*)*

Demostració. Es proven igual que les propietats anàlegues dels enters.
Per c), tenim $A \mid B \Rightarrow B = AQ$, amb $Q \in K[X]$; $B \mid A \Rightarrow A = BP$, amb $P \in K[X]$. Si $A = 0$, tenim $B = AQ = 0$ i es compleix l'implicació. Si $A \neq 0$, la igualtat $A = BP = AQP$ implica $QP = 1$, és a dir Q és element invertible de $K[X]$ i per 3.1.4, $Q \in K \setminus \{0\}$.
Per f), fem servir 3.1.2. □

3.3 Màxim comú divisor de dos polinomis

Un *divisor comú* de dos polinomis A, B de $K[X]$ és un polinomi $D \in K[X]$ tal que $D \mid A$ i $D \mid B$.

Definició 3.3.1. Donats dos polinomis A, B de $K[X]$ direm que un polinomi D de $K[X]$ és màxim comú divisor de A i B si compleix les dues propietats següents.

1. $D \mid A$ i $D \mid B$

2. Si D_1 és un polinomi de $K[X]$ tal que $D_1 \mid A$ i $D_1 \mid B$, aleshores $D_1 \mid D$.

Observació. Si D és màxim comú divisor de A i B, λD, amb $\lambda \in K \setminus \{0\}$ també ho és.

Proposició 3.3.2. *Si D_1 i D_2 són màxims comuns divisors de A i B, tenim $D_1 = \lambda D_2$, amb $\lambda \in K \setminus \{0\}$.*

Demostració. Com D_1 és màxim comú divisor de A i B i D_2 n'és un divisor comú, obtenim de la definició, $D_2 \mid D_1$. Anàlogament, obtenim $D_1 \mid D_2$. Aleshores, per la propietat antisimètrica de la relació de divisibilitat, obtenim $D_1 = \lambda D_2$, amb $\lambda \in K \setminus \{0\}$. □

A $K[X]$, les igualtats entre màxims comuns divisors són tret d'un factor constant no nul.

3.4 Algoritme d'Euclides per a polinomis

Veiem ara que l'algoritme d'Euclides també és vàlid per calcular el màxim comú divisor de dos polinomis de $K[X]$. En particular, tindrem que, donats dos polinomis de $K[X]$, existeix el seu màxim comú divisor. Abans provem el lema anàleg de 2.4.1.

Lema 3.4.1. *Si A, B, Q són polinomis de $K[X]$, tenim*

$$\mathrm{mcd}(A, B) = \mathrm{mcd}(A - BQ, B).$$

Demostració. La demostració es fa igual que per 2.4.1, tenint en compte que la relació de divisibilitat entre polinomis també compleix la propietat de linealitat. □

Proposició 3.4.2 (Algoritme d'Euclides per polinomis)**.** *Siguin A, B dos polinomis de $K[X]$, $B \neq 0$. Fem successivament les divisions enteres*

$$\begin{array}{ll} A = BQ_1 + R_1, & grR_1 < grB \\ B = R_1Q_2 + R_2, & grR_2 < grR_1 \\ R_1 = R_2Q_3 + R_3, & grR_3 < grR_2 \\ R_2 = R_3Q_4 + R_4, & grR_4 < grR_3 \\ \vdots & \end{array}$$

Aleshores, existeix $n \in \mathbb{N}$ tal que $R_n = 0$ i es compleix $\mathrm{mcd}(A, B) = R_{n-1}$.

Demostració. La demostració és anàlega a la de 2.4.2. En aquest cas, veiem que arribem a una resta igual a 0 en un nombre finit de passos observant que, si considerem la successió de restes, tenim $grR_1 > grR_2 > grR_3 > \ldots$, és a dir una successió estrictament decreixent d'enters naturals, per tant arribem a $R_n = 0$ per a algun $n \in \mathbb{N}$. Ara, aplicant 3.4.1, es compleix $\mathrm{mcd}(A, B) = \mathrm{mcd}(B, R_1) = \mathrm{mcd}(R_1, R_2) = \mathrm{mcd}(R_2, R_3) = \cdots = \mathrm{mcd}(R_{n-1}, R_n) = \mathrm{mcd}(R_{n-1}, 0) = R_{n-1}$. □

Exercici. *Calculeu el màxim comú divisor dels polinomis $A = X^5 - X^3 - X^2 - 2X + 2, B = X^4 + 3X^3 - X^2 - 6X - 2$.*

Fent la divisió de A entre B, obtenim quotient $Q_1 = X - 3$ i resta $R_1 = 9X^3 + 2X^2 - 18X - 4$.
Fent la divisió de B entre R_1, obtenim quotient $Q_2 = \frac{1}{9}X + \frac{25}{81}$ i resta $R_2 = \frac{31}{81}X^2 - \frac{62}{81} = \frac{31}{81}(X^2 - 2)$.

Fent la divisió de R_1 entre R_2, obtenim quocient $Q_3 = \frac{81}{31}(9X+2)$ i resta 0.
Per tant hem obtingut $\mathrm{mcd}(A,B) = X^2-2$.
Feu les divisions com a exercici.

Com pels enters, tenim el resultat següent.

Proposició 3.4.3 (Identitat de Bézout)**.** *Si $A, B, D \in K[X]$ i $D = \mathrm{mcd}(A,B)$, aleshores existeixen polinomis S, T a $K[X]$ tals que*

$$D = SA + TB.$$

Demostració. Es demostra igual que 2.4.3. □

Exercici. *Calculeu una identitat de Bézout pels polinomis $A = X^5 - X^3 - X^2 - 2X + 2, B = X^4 + 3X^3 - X^2 - 6X - 2$ de l'exemple anterior.*

A partir de les divisions efectuades per calcular el màxim comú divisor, obtenim

$$\begin{pmatrix} \frac{31}{81}(X^2-2) \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -Q_3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -Q_2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -Q_1 \end{pmatrix}\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} -Q_2 & 1+Q_1Q_2 \\ * & * \end{pmatrix}\begin{pmatrix} A \\ B \end{pmatrix}.$$

Operem:

$$-Q_2 = -(\frac{1}{9}X + \frac{25}{81}) = -\frac{1}{81}(9X+25),$$

$$1 + Q_1Q_2 = 1 + (X-3)(\frac{1}{9}X + \frac{25}{81}) = \frac{1}{81}(9X^2 - 2X + 6).$$

Hem obtingut

$$\frac{31}{81}(X^2-2) = -\frac{1}{81}(9X+25)A + \frac{1}{81}(9X^2-2X+6)B$$

o, equivalentment

$$X^2 - 2 = -\frac{1}{31}(9X+25)A + \frac{1}{31}(9X^2-2X+6)B.$$

Donem ara la definició de mínim comú múltiple de dos polinomis.

Definició 3.4.4. Donats dos polinomis A, B de $K[X]$ direm que un polinomi M és *mínim comú múltiple* de A i B si compleix les dues propietats següents.

1. $A \mid M$ i $B \mid M$
2. Si M_1 és un polinomi de $K[X]$ tal que $A \mid M_1$ i $B \mid M_1$, aleshores $M \mid M_1$.

Observació. Si M és mínim comú múltiple de A i B, λM, amb $\lambda \in K \setminus \{0\}$ també ho és.

Proposició 3.4.5. *Si M_1 i M_2 són mínims comuns múltiples de A i B, tenim $M_1 = \lambda M_2$, amb $\lambda \in K \setminus \{0\}$.*

Demostració. És anàlega a la de 3.3.2. □

Els apartats de la proposició següent es proven igual que les propietats corresponents dels enters 2.5.3, 2.5.4, 2.5.5.

Proposició 3.4.6. *a) Siguin $A, B, C \in K[X]$. Si $A \mid BC$ i $\mathrm{mcd}(A, B) = 1$, aleshores $A \mid C$.*

b) Si A, B són polinomis de $K[X]$ no nuls, tenim

$$\mathrm{mcd}(A, B) = 1 \Leftrightarrow \text{ existeixen polinomis } S, T \text{ tals que } SA + TB = 1.$$

c) Si A, B són polinomis de $K[X]$, $D = \mathrm{mcd}(A, B)$, posem $A = DA_1$, $B = DB_1$. Aleshores $\mathrm{mcd}(A_1, B_1) = 1$.

Veiem ara la relació entre màxim comú divisor i mínim comú múltiple de dos polinomis.

Proposició 3.4.7. *Si A, B són polinomis de $K[X]$, $D = \mathrm{mcd}(A, B), M = \mathrm{mcm}(A, B)$, es compleix $DM = \lambda AB$, amb $\lambda \in K \setminus \{0\}$.*

Demostració. Igual que per 2.5.6, veiem que AB/D és mínim comú múltiple de A i B. Després utilitzem que el mínim comú múltiple de dos polinomis està determinat tret d'un factor constant no nul. □

3.5 Descomposició d'un polinomi en producte d'irreductibles

Definició 3.5.1. Un polinomi P de $K[X]$ de grau més gran o igual que 1 s'anomena *irreductible* si els seus únics divisors a $K[X]$ són $\lambda, \lambda P$, amb $\lambda \in K \setminus \{0\}$.

Exemple $X^4 + 2X^2 + 1$ no és irreductible ja que $X^4 + 2X^2 + 1 = (X^2 + 1)^2$; $X^4 - X^3 + X - 1$ no és irreductible ja que $X^4 - X^3 + X - 1 = (X - 1)(X^3 + 1)$.

Dos polinomis $P, Q \in K[X]$ es diuen *associats* si $Q = \lambda P$, amb $\lambda \in K \setminus \{0\}$.

Observació. Si P és irreductible, també ho són els seus associats.

Proposició 3.5.2. *Sigui P un polinomi irreductible de $K[X]$.*

a) Si $Q \in K[X]$, es compleix o bé $P \mid Q$ o bé $\operatorname{mcd}(P, Q) = 1$.

b) Si $A, B \in K[X]$, aleshores $P \mid AB$ i $P \nmid A \Rightarrow P \mid B$.

Demostració. a) Sigui $D = \operatorname{mcd}(P, Q)$. Com P és irreductible, ha de ser $D = 1$, o bé $D = P$. En el segon cas, P divideix Q.
b) Si $P \nmid A$, tenim $\operatorname{mcd}(P, A) = 1$ i, per 3.4.6 a), P ha de dividir B. □

Teorema 3.5.3 (Descomposició en producte d'irreductibles)**.** *Sigui $A \in K[X]$, $grA \geq 1$. Aleshores existeixen polinomis irreductibles $P_1, \ldots, P_n$ de $K[X]$, $(n \geq 1)$, tals que*

$$A = P_1 \ldots P_n. \tag{3.2}$$

A més, si $A = Q_1 \ldots Q_m$ és una altra descomposició de A en producte de polinomis irreductibles, tenim $n = m$ i existeix una bijecció σ de $\{1, \ldots, n\}$ en $\{1, \ldots, n\}$ tal que P_i és associat de $Q_{\sigma(i)}$ per a tot $i \in \{1, \ldots, n\}$.

Demostració. Veiem primer que per a $A \in K[X]$ de grau ≥ 1 existeix una descomposició en producte d'irreductibles.
Si A és irreductible, té una descomposició amb un únic factor.
Ara procedim per l'absurd. Suposem que hi ha algun polinomi de grau ≥ 1 que no descompon en producte d'irreductibles. En triem un, A, de grau mínim. Com no és irreductible, tenim $A = PQ$, amb $P, Q \in K[X]$, $1 \leq grP < grA, 1 \leq grQ < grA$.

Com hem escollit A de grau mínim entre els polinomis que no descomponen en producte d'irreductibles, P i Q si que ho fan i per tant A també. Hem arribat doncs a contradicció.
Veiem ara l'unicitat. Siguin $A = P_1 \dots P_n$, $A = Q_1 \dots Q_m$ dues descomposicions de A en producte de polinomis irreductibles. Podem suposar $n \geq m$. Tenim $P_1 \mid Q_1 \dots Q_m$. Com P_1 és irreductible, per 3.5.2 b) hem de tenir $P_1 \mid Q_{j_1}$, per a algun j_1. Com Q_{j_1} també és irreductible, $Q_{j_1} = \lambda_1 P_1$, amb $\lambda_1 \in K \setminus \{0\}$. Posem $\sigma(1) = j_1$. Simplificant el factor P_1 a les dues bandes de la igualtat $P_1 \dots P_n = Q_1 \dots Q_m$, obtenim $\prod_{i=2}^{n} P_i = \lambda_1 \prod_{j \neq j_1} Q_j$. Repetint el procès, trobem Q_{j_2} tal que $Q_{j_2} = \lambda_2 P_2$, amb $\lambda_2 \in K \setminus \{0\}$. Posem $\sigma(2) = j_2$ i tenim la igualtat $\prod_{i=3}^{n} P_i = \lambda_1 \lambda_2 \prod_{j \neq j_1, j_2} Q_j$. Podem repetir el procès fins a obtenir $P_{m+1} \dots P_n \in K$. Tenim doncs $n = m$ i hem establert una bijecció σ de $\{1, \dots, n\}$ en $\{1, \dots, n\}$ tal que P_i és associat de $Q_{\sigma(i)}$ per a tot $i \in \{1, \dots, n\}$. □

Cada polinomi A de grau $n \geq 1$ té un únic polinomi mònic associat: el polinomi $\frac{1}{a_n} A$. Agafant a (3.2), el polinomi mònic associat a cada factor P_i de la descomposició i associant els factors iguals, obtenim

Corol·lari 3.5.4. *Sigui $A \in K[X], A(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$, amb $n \geq 1, a_n \neq 0$. Aleshores*

$$A = a_n P_1^{r_1} \dots P_k^{r_k}$$

amb $r_1, \dots, r_k$ enters ≥ 1, $P_1, \dots, P_k$ polinomis mònics irreductibles diferents de $K[X]$. Aquesta descomposició és única tret de l'ordre dels factors.

3.6 Arrels de polinomis

Si $A(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in K[X], \alpha \in K$, diem *valor de A en α* l'element de K

$$A(\alpha) = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0.$$

Proposició 3.6.1. *Sigui $A(X) \in K[X], \alpha \in K$. Aleshores la resta de la divisió a $K[X]$ de A entre $X - \alpha$ és igual a $A(\alpha)$. En particular*

$$A(\alpha) = 0 \Leftrightarrow X - \alpha \text{ divideix } A(X).$$

Demostració. La divisió de $A(X)$ entre $X-\alpha$ és $A(X)=Q(X)(X-\alpha)+r$ amb $r\in K$, ja que la resta ha de tenir grau $< gr(X-\alpha)=1$. Substituint X per α, obtenim $A(\alpha)=Q(\alpha)(\alpha-\alpha)+r=r$. □

Definició 3.6.2. Sigui $A(X)\in K[X]\setminus\{0\}, \alpha\in K$. Diem que α és *arrel* de A si $A(\alpha)=0$.

Exemples

1. X^2+1 no té arrels a $\mathbb{R}$,
2. $i,-i$ són arrels de X^2+1 a $\mathbb{C}$,
3. un polinomi de grau 0 no té arrels. Un polinomi de grau 1 té una única arrel. Si $A(X)=a_1X+a_0$, amb $a_1\neq 0$, $\alpha=-\dfrac{a_0}{a_1}$ és l'arrel de A.

Corol·lari 3.6.3. *Sigui $A\in K[X]$. El nombre d'arrels de A a K és com a màxim igual al grau de A.*

Demostració. Per la proposició 3.6.1, si $\alpha\in K$ és arrel de A, tenim $A(X)=(X-\alpha)A_1(X)$, amb $A_1(X)\in K[X]$ i $grA_1=grA-1$. Si ara α_1 és arrel de A_1, i per tant de A, tindrem $A_1(X)=(X-\alpha_1)A_2(X)$, amb $A_2(X)\in K[X]$ i $grA_2=grA_1-1=grA-2$. Reiterant el procès, obtenim el resultat. □

Corol·lari 3.6.4. *Sigui $A\in K[X]$.*

(a) Si A té grau 1, aleshores és irreductible a $K[X]$ i té una arrel a K.

(b) Si $grA\geq 2$ i A té alguna arrel a K, aleshores no és irreductible a $K[X]$.

(c) Si $grA=2$ o 3, aleshores

$$A \text{ és irreductible a } K[X] \Leftrightarrow A \text{ no té arrels a } K.$$

Demostració. (a) Ja hem vist que, si A té grau 1, té una arrel a K. Si $A=PQ$, $grP+grQ=gr(PQ)=grA=1$, per tant un dels dos factors ha de ser constant i doncs l'altre associat de A.
(b) Si α és arrel de A, $X-\alpha$ divideix A, per 3.6.1, i per tant A no és irreductible.
(c) Per (b), passant al contrarecíproc, tenim $\Rightarrow$. Suposem ara que A no és irreductible. Tenim doncs $A=PQ$, amb $1\leq grP, grQ<grA$, $grP+grQ=grA$. Per tant A té un divisor de grau 1 i l'arrel d'aquest és arrel de A. □

Exemples

1. El polinomi X^2+1 és irreductible a $\mathbb{R}[X]$ perquè no té arrels a $\mathbb{R}$.
2. El polinomi X^2+1 no és irreductible a $\mathbb{C}[X]$ perquè té l'arrel i.
3. El polinomi X^4+2X^2+1 no té arrels a $\mathbb{R}$ ja que el seu valor és >0 en tot nombre real però no és irreductible, ja que X^2+1 el divideix.
4. A $\mathbb{R}[X]$ els polinomis de grau 2 irreductibles són els que no tenen arrels reals, és a dir, els de la forma aX^2+bX+c, amb $a\neq 0$, $b^2-4ac<0$.

Definició 3.6.5. Sigui $A\in K[X]$. Un polinomi irreductible P de $K[X]$ direm que és *factor de A de multiplicitat k* si $P^k \mid A$ i $P^{k+1}\nmid A$. Direm que P és *factor múltiple* de A si és factor amb multiplicitat més gran que 1. Direm que P és *factor simple* de A si és factor amb multiplicitat igual 1. Direm que α és arrel de A *de multiplicitat k* si $X-\alpha$ és factor de A de multiplicitat k. Direm que α és *arrel múltiple* de A si $X-\alpha$ és factor múltiple de A. Direm que α és *arrel simple* de A si $X-\alpha$ és factor simple de A.

Definició 3.6.6. Si $A(X)=a_nX^n+a_{n-1}X^{n-1}+\cdots+a_iX^i+\cdots+a_1X+a_0\in K[X]$, el polinomi derivat de $A(X)$ és

$$A'(X)=na_nX^{n-1}+(n-1)a_{n-1}X^{n-2}+\cdots+ia_iX^{i-1}+\cdots+a_1.$$

Proposició 3.6.7 (Propietats del polinomi derivat.)**.** *Siguin $A(X),B(X)\in K[X]$, $\lambda\in K, k\in\mathbb{N}\setminus\{0\}$. Es compleix*

a) $A(X)\in K\Rightarrow A'(X)=0$.

b) $(A(X)+B(X))'=A'(X)+B'(X)$.

c) $(\lambda A(X))'=\lambda A'(X)$.

d) $(A(X)B(X))'=A'(X)B(X)+A(X)B'(X)$.

e) $(A(X)^k)'=kA(X)^{k-1}A'(X)$.

Proposició 3.6.8. *Sigui $K=\mathbb{Q},\mathbb{R}$ o $\mathbb{C}$ i sigui $A(X)\in K[X]$. Si $A(X)$ té un factor $P(X)$ de multiplicitat k, aleshores $P(X)$ és factor de $A'(X)$ de multiplicitat $k-1$.*

Demostració. Tenim

$$A(X) = P(X)^k Q(X), \text{ amb } P(X) \nmid Q(X).$$

Derivant els dos membres de la igualtat, obtenim

$$\begin{aligned} A'(X) &= kP(X)^{k-1}P'(X)Q(X) + P(X)^k Q'(X) \\ &= P(X)^{k-1}(kP'(X)Q(X) + P(X)Q'(X)). \end{aligned}$$

Hem de veure $P(X) \nmid (kP'(X)Q(X) + P(X)Q'(X))$ que és equivalent a $P(X) \nmid kP'(X)Q(X)$. Tenim $P(X) \nmid Q(X)$ i, com $gr(kP'(X)) = grP(X) - 1$, $P(X)$ tampoc no el pot dividir. Per tant $P(X) \nmid kP'(X)Q(X)$. □

Corol·lari 3.6.9. *$A(X)$ té un factor irreductible múltiple $\Leftrightarrow$ $\mathrm{mcd}(A(X), A'(X)) \neq 1$.*

Demostració. $\Rightarrow$: si $P(X)$ és factor irreductible múltiple de $A(X)$, també divideix $A'(X)$ per la proposició.
$\Leftarrow$: sigui $P(X)$ un factor irreductible de $D(X) = \mathrm{mcd}(A(X), A'(X))$. Si divideix $A(X)$ amb multiplicitat k, divideix $A'(X)$ amb multiplicitat $k-1$. Per tant, ha de ser $k - 1 \geq 1$, és a dir $k \geq 2$. □

Exercici. *Considerem el polinomi*

$$A(X) = X^6 + 4X^4 + 5X^2 + 2 \in \mathbb{R}[X].$$

Proveu que té factors múltiples a $\mathbb{R}[X]$ i descomponeu-lo en factors irreductibles a $\mathbb{R}[X]$.

Calculem el polinomi derivat:

$$A'(X) = 6X^5 + 16X^3 + 10X = 2X(3X^4 + 8X^2 + 5).$$

Com clarament $X \nmid A(X)$, tenim

$$\mathrm{mcd}(A(X), A'(X)) = \mathrm{mcd}(A(X), 3X^4 + 8X^2 + 5).$$

Calculem aquest màxim comú divisor.
Dividint $A(X)$ entre $3X^4+8X^2+5$, obtenim quocient $\frac{1}{3}X^2+\frac{4}{9}$ i resta $-\frac{2}{9}X^2-\frac{2}{9} = -\frac{2}{9}(X^2+1)$;

dividint $3X^4 + 8X^2 + 5$ entre $X^2 + 1$, obtenim quocient $3X^2 + 5$ i resta $5X^2 + 5$. Tenim doncs $\mathrm{mcd}(A(X), 3X^4 + 8X^2 + 5) = X^2 + 1$. Pel corol·lari, $X^2 + 1$ és factor múltiple de $A(X)$. Dividint, obtenim

$$A(X) = (X^2 + 1)(X^4 + 3X^2 + 2), X^4 + 3X^2 + 2 = (X^2 + 1)(X^2 + 2)$$

i, per tant

$$A(X) = (X^2 + 1)^2(X^2 + 2).$$

Els dos polinomis $X^2 + 1, X^2 + 2$ són irreductibles a $\mathbb{R}[X]$ ja que tenen grau 2 i no tenen arrels a $\mathbb{R}$.

3.7 El teorema fonamental de l'àlgebra

Teorema 3.7.1 (Teorema fonamental de l'àlgebra)**.** *Tot polinomi $A(X) \in \mathbb{C}[X]$ de grau més gran o igual a 1 té alguna arrel a $\mathbb{C}$.*

La demostració d'aquest teorema excedeix el nivell d'aquest curs. El lector interessat pot consultar el llibre "Curso de Matemáticas" de J. Teixidor i J. Vaquer, Romargraf, 1976.

Corol·lari 3.7.2. *Si $A(X) \in \mathbb{C}[X]$ és un polinomi de grau $n \geq 1$, aleshores*

$$A(X) = a_n(X - \alpha_1) \dots (X - \alpha_n),$$

on a_n és el coeficient de grau n de $A(X)$ i $\alpha_1, \dots, \alpha_n \in \mathbb{C}$.

Demostració. Fem la prova per inducció sobre n.
Si $n = 1$, tenim $A(X) = a_1X + a_0$, amb $a_1 \neq 0$ i, per tant, $A(X) = a_1(X - a_0/a_1)$, amb $a_0/a_1 \in \mathbb{C}$.
Suposem que el resultat és cert per a polinomis de $\mathbb{C}[X]$ de grau $n - 1$ i sigui $A(X) \in \mathbb{C}[X]$ de grau n. Posem $A(X) = a_nX^n + \dots$. Pel teorema, $A(X)$ té una arrel α a $\mathbb{C}$. Per tant

$$A(X) = (X - \alpha)B(X),$$

on $B(X)$ és un polinomi de grau $n - 1$ i $B(X) = a_nX^{n-1} + \dots$. Per hipòtesi d'inducció, tenim

$$B(X) = a_n(X - \alpha_1)\dots(X - \alpha_{n-1})$$

i, per tant

$$A(X) = a_n(X - \alpha_1)\dots(X - \alpha_{n-1})(X - \alpha).$$

□

Corol·lari 3.7.3. *Els polinomis irreductibles de* $\mathbb{C}[X]$ *són exactament els de grau 1.*

Volem veure ara quins són els polinomis irreductibles de $\mathbb{R}[X]$.

Proposició 3.7.4. *Sigui* $A(X) \in \mathbb{R}[X]$ *amb* $grA(X) > 1$ *i* $\alpha \in \mathbb{C}$. *Aleshores*

$$A(\alpha) = 0 \Rightarrow A(\overline{\alpha}) = 0,$$

on $\overline{\alpha}$ *indica el conjugat de* α.

Demostració. Si $A(X) = a_nX^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$, tenim

$$0 = A(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0.$$

Prenent conjugats, obtenim

$$\begin{aligned} 0 &= \overline{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0} \\ &= \overline{a_n\alpha^n} + \overline{a_{n-1}\alpha^{n-1}} + \dots + \overline{a_1\alpha} + \overline{a_0} \\ &= a_n\overline{\alpha}^n + a_{n-1}\overline{\alpha}^{n-1} + \dots + a_1\overline{\alpha} + a_0 \\ &= A(\overline{\alpha}), \end{aligned}$$

tenint en compte 1.2.1 i que $\overline{a_i} = a_i, i = 0, \dots n$, ja que $a_i \in \mathbb{R}$. □

Proposició 3.7.5. *Sigui* $\alpha \in \mathbb{C}$. *Aleshores*

$$(X - \alpha)(X - \overline{\alpha}) = X^2 - 2\,\mathrm{Re}(\alpha)X + |\alpha|^2 \in \mathbb{R}[X].$$

En particular, si $A(X) \in \mathbb{R}[X]$ *té una arrel complexa no real, aleshores* $A(X)$ *és divisible per un polinomi irreductible de grau 2 a* $\mathbb{R}[X]$.

Demostració.

$$(X-\alpha)(X-\overline{\alpha}) = X^2 - (\alpha+\overline{\alpha})X + \alpha\overline{\alpha} = X^2 - 2\,\mathrm{Re}(\alpha)X + |\alpha|^2.$$

Si $A(X)$ té arrel α, també $\overline{\alpha}$ és arrel de $A(X)$, per la proposició anterior. Per tant, $A(X)$ és divisible per $X-\alpha$ i per $X-\overline{\alpha}$ i, com aquests dos són coprimers, també pel seu producte. Ara $(X-\alpha)(X-\overline{\alpha}) = X^2 - 2\,\mathrm{Re}(\alpha)X + |\alpha|^2$ és un polinomi irreductible a $\mathbb{R}[X]$ ja que no té arrels a $\mathbb{R}$. □

Teorema 3.7.6. *Els polinomis irreductibles de $\mathbb{R}[X]$ són exactament els polinomis de grau 1 i els polinomis de grau 2 amb discriminant estrictament negatiu.*

Demostració. Ja havíem vist

1. els polinomis de grau 1 són irreductibles.
2. un polinomi de grau 2 de $\mathbb{R}[X]$ és irreductible si i només si el seu discriminant és estrictament negatiu.

Només queda veure que el polinomis de $\mathbb{R}[X]$ de grau > 2 no són irreductibles. Sigui $A(X) \in \mathbb{R}[X]$, amb $grA(X) > 2$. Pel teorema fonamental de l'àlgebra, $A(X)$ té una arrel $\alpha \in \mathbb{C}$. Si $\alpha \in \mathbb{R}$, $A(X)$ és divisible per $X-\alpha \in \mathbb{R}[X]$, i per tant no és irreductible a $\mathbb{R}[X]$. Si $\alpha \notin \mathbb{R}$, per la proposició anterior, $A(X)$ és divisible per un polinomi de grau 2 a $\mathbb{R}[X]$ i tampoc no és irreductible. □

Corol·lari 3.7.7. *A $\mathbb{R}[X]$ tot polinomi de grau més gran o igual que 1 descompon en producte de polinomis irreductibles de graus 1 o 2.*

Exercici. *Feu la descomposició en producte d'irreductibles de X^8-1 a $\mathbb{R}[X]$ i a $\mathbb{Q}[X]$.*

Calculem les arrels complexes de X^8-1:

$$\begin{array}{rcrcl}
z_1 & = & 1_0 & = & 1 \\
z_2 & = & 1_{\pi/4} & = & \dfrac{\sqrt{2}}{2} + i\dfrac{\sqrt{2}}{2} \\
z_3 & = & 1_{\pi/2} & = & i \\
z_4 & = & 1_{3\pi/4} & = & -\dfrac{\sqrt{2}}{2} + i\dfrac{\sqrt{2}}{2} \\
z_5 & = & 1_{\pi} & = & -1 \\
z_6 & = & 1_{5\pi/4} & = & -\dfrac{\sqrt{2}}{2} - i\dfrac{\sqrt{2}}{2} \\
z_7 & = & 1_{3\pi/2} & = & -i \\
z_8 & = & 1_{7\pi/4} & = & \dfrac{\sqrt{2}}{2} - i\dfrac{\sqrt{2}}{2}
\end{array}$$

Les arrels 1 i -1 són reals. Per tant $X-1, X+1$ són factors irreductibles de X^8-1 a $\mathbb{R}[X]$. Associem les altres arrels en parelles de conjugats i fem el producte dels factors lineals corresponents:

$$\begin{aligned}(X-i)(X+i) &= X^2+1\\ (X-z_2)(X-z_8) &= X^2-\sqrt{2}X+1\\ (X-z_4)(X-z_6) &= X^2+\sqrt{2}X+1\end{aligned}$$

La descomposició de X^8-1 en producte de polinomis irreductibles a $\mathbb{R}[X]$ és doncs

$$X^8-1=(X-1)(X+1)(X^2+1)(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1).$$

Els dos últims factors no tenen coeficients a $\mathbb{Q}$. Per la unicitat de la descomposició d'un polinomi a coeficients en un cos en producte de polinomis irreductibles, tenim que la descomposició en producte de polinomis irreductibles a $\mathbb{Q}[X]$ s'obté agrupant convenientment els factors de la descomposició en producte de polinomis irreductibles a $\mathbb{R}[X]$. Tenim

$$\begin{aligned}(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1) &= (X^2+1)^2-2X^2\\ &= X^4+2X^2+1-2X^2\\ &= X^4+1\in\mathbb{Q}[X].\end{aligned}$$

La descomposició de X^8-1 en producte de polinomis irreductibles a $\mathbb{Q}[X]$ és doncs

$$X^8-1=(X-1)(X+1)(X^2+1)(X^4+1).$$

Observació. Per a cada enter $n\geq 1$, existeixen polinomis irreductibles a $\mathbb{Q}[X]$ de grau n. (cf. Antoine-Camps-Moncasi "Introducció a l'àlgebra abstracta").

Capítol 4

Congruències

4.1 Relació de congruència.

Fixat un enter $m > 1$, definim una relació binària a $\mathbb{Z}$ anomenada *relació de congruència* en la forma següent. Donats dos enters a, b diem que *a és congru amb b mòdul m* i escrivim $a \equiv b \pmod{m}$ si $a - b$ és múltiple de m.

Proposició 4.1.1. *La relació de congruència és relació d'equivalència.*

Demostració. Hem de veure que la relació és reflexiva, simètrica i transitiva.

1. Clarament tot enter a compleix $a \equiv a \pmod{m}$, ja que 0 és múltiple de m.

2. Si $a \equiv b \pmod{m}$, tenim $a - b$ múltiple de m i per tant també $b - a$ múltiple de m que dóna $b \equiv a \pmod{m}$.

3. Si $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$, tenim $a - b$ i $b - c$ múltiples de m i per tant $a - c = (a - b) + (b - c)$ també és múltiple de m i tenim $a \equiv c \pmod{m}$. □

A més la relació de congruència compleix les propietats següents.

Proposició 4.1.2. *Sigui m un enter, $m > 1$, $a, b, r_1, r_2 \in \mathbb{Z}$. Es compleix*

1. *Si r és la resta de la divisió entera de a entre m, aleshores $a \equiv r \pmod{m}$.*

2. *Si $r_1 \equiv r_2 \pmod{m}$ i $0 \leq r_1 < m$, $0 \leq r_2 < m$ aleshores $r_1 = r_2$.*

3. $a \equiv b \pmod{m}$ *si i només si la resta de la divisió entera de* a *entre* m *coincideix amb la resta de la divisió entera de* b *entre* m.

Demostració.

1. Si $a = mq + r$, tenim $a - r$ múltiple de m i per tant $a \equiv r \pmod{m}$.

2. $0 \leq r_1 < m$, $0 \leq r_2 < m \Rightarrow -m < r_1 - r_2 < m$. Com $r_1 - r_2$ és múltiple de m, tenim $r_1 - r_2 = 0$.

3. Tenim $a - b = mn$ per un cert enter n. Si la divisió entera de b entre m és $b = mq + r$, tenim $a = b + mn = m(q + n) + r$, amb $0 \leq r < m$. □

Si a és un enter, posem $\overline{a}$ la classe d'equivalència de a per la relació de congruència, és a dir

$$\overline{a} = \{b \in \mathbb{Z} : b \equiv a \pmod{m}\}.$$

La proposició anterior ens diu que tot enter a pertany a la classe d'equivalència per la relació de congruència mòdul m d'un enter r tal que $0 \leq r < m$ i que dos enters diferents r_1, r_2 tals que $0 \leq r_1, r_2 < m$ pertanyen a classes d'equivalència diferents. Per tant les classes d'equivalència mòdul m són

$$\overline{0}, \overline{1}, \ldots, \overline{m-1}.$$

Com cada una de les classes té com a representant un enter que és resta de divisió entre m, aquestes classes d'equivalència s'anomenen *classes de restes*. El conjunt quocient s'escriu $\mathbb{Z}/m$.
Recordem que, si A és un conjunt dotat d'una relació d'equivalència $\simeq$, un *sistema complet de representants* del conjunt quocient $A/\simeq$ és un subconjunt S de A complint les dues condicions següents.

1. Per a tot $a \in A$, existeix $s \in S$ tal que $a \simeq s$.

2. Si $s_1, s_2 \in S$, $s_1 \simeq s_2 \Rightarrow s_1 = s_2$

Per exemple, $\{0, 1, \ldots, m-1\}$ és un sistema complet de representants de $\mathbb{Z}/m$.

Observació. Es pot provar el següent resultat anàleg al punt 2. de 4.1.2.

Siguin $m, r_1, r_2 \in \mathbb{Z}, m > 1$. *Si* $r_1 \equiv r_2 \pmod{m}$ *i* $-m/2 < r_1 \leq m/2$, $-m/2 < r_2 \leq m/2$, *aleshores* $r_1 = r_2$.

Podem doncs també escriure
si m és senar, $m = 2n+1$, $\{-n, -(n-1), \ldots, 0, \ldots, n-1, n\}$ és un sistema complet de representants de $\mathbb{Z}/m$.
si m és parell, $m = 2n$, $\{-(n-1), \ldots, 0, \ldots, n-1, n\}$ és un sistema complet de representants de $\mathbb{Z}/m$.

4.2 Anells de classes de restes

Si m és un enter $m > 1$, volem veure que a l'anell $\mathbb{Z}/m$ de classes de restes podem definir una suma i un producte que li donen estructura d'anell.
Definim una suma a $\mathbb{Z}/m$ per

$$\overline{a} + \overline{b} = \overline{a+b},$$

on, en el terme de la dreta + indica la suma de $\mathbb{Z}$. Cal veure que la suma està ben definida, és a dir que no depen del representant de cada classe. En efecte, si tenim $\overline{a'} = \overline{a}, \overline{b'} = \overline{b}$, aleshores $a' = a + pm, b' = b + qm$, per certs enters p, q. Aleshores $a' + b' = (a + pm) + (b + qm) = a + b + (p + q)m \in \overline{a+b}$.
Clarament les propietats de la suma de $\mathbb{Z}$ passen a $\mathbb{Z}/m$ i per tant la suma que hem definit a $\mathbb{Z}/m$ és associativa, commutativa, té element neutre: $\overline{0}$, i cada element $\overline{a}$ té un oposat: $\overline{-a}$.

Exercici. *Feu la taula de la suma de* $\mathbb{Z}/5$.

$\mathbb{Z}/5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Per a cada suma $\overline{a}+\overline{b}$, busquem el representant de $\overline{a+b}$ entre 0 i 4, és a dir la resta de $a + b$ entre 5. Per exemple, $\overline{3} + \overline{4} = \overline{7} = \overline{2}$. Obtenim la taula donada en la figura 4.1.

Definim ara un producte a $\mathbb{Z}/m$ per

$$\overline{a}\,\overline{b} = \overline{ab},$$

on, en el terme de la dreta ab indica el producte de a i b a $\mathbb{Z}$. Cal veure que el producte està ben definit, és a dir que no depen del representant de cada classe. En efecte, si tenim $\overline{a'} = \overline{a}, \overline{b'} = \overline{b}$, aleshores $a' = a + pm, b' = b + qm$, per certs enters p, q. Aleshores $a'b' = (a + pm)(b + qm) = ab + (pb + qa + pq)m \in \overline{ab}$.
El producte de $\mathbb{Z}/m$ hereta les propietats del producte de $\mathbb{Z}$. Per tant, el producte a $\mathbb{Z}/m$ és associatiu, commutatiu, té element neutre: $\overline{1}$, i és distributiu respecte de la suma.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Figura 4.1

Tenint en compte les propietats del producte i les de la suma, tenim que, per a tot enter $m > 1$, $\mathbb{Z}/m$ és un anell commutatiu amb unitat.

Exercici. *Feu les taules del producte de* $\mathbb{Z}/5$ *i de* $\mathbb{Z}/6$.

1) $\mathbb{Z}/5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Com per la suma, per fer el producte $\overline{a}\overline{b}$, busquem el representant de ab comprès entre 0 i 4. Queda la taula donada en la figura 4.2.

2) $\mathbb{Z}/6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Fent els productes, queda la taula donada en la figura 4.3.

Observem que a $\mathbb{Z}/5$, tot element diferent de $\overline{0}$ té invers. A $\mathbb{Z}/6$ tenim que el producte de dos elements no nuls pot donar $\overline{0}$ i només $\overline{1}$ i $\overline{5}$ són invertibles.

Si A és un anell, un element no nul a de A es diu *divisor de zero* si existeix un element b de A no nul tal que $ab = 0$.

Exemple. $\overline{2}, \overline{3}, \overline{4}$ són divisors de zero a $\mathbb{Z}/6$.

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Figura 4.2

Si un anell no té divisors de zero, es diu *íntegre*.

Exemple. $\mathbb{Z}$ és anell íntegre, $\mathbb{Z}/5$ és anell íntegre. Tot cos és un anell íntegre (cf. 4.2.2).

Observació. Si A és un anell íntegre, $a, b \in A$, tenim

$$a \neq 0 \text{ i } \ ab = 0 \Rightarrow b = 0.$$

Per tant, es compleix també, per a a, b, c elements de A,

$$a \neq 0 \text{ i } \ ab = ac \Rightarrow b = c.$$

Si A és un anell commutatiu amb unitat, posem A^* el conjunt dels elements invertibles de A.

Exemples.

1. $\mathbb{Z}^* = \{1, -1\}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Figura 4.3

2. $(\mathbb{Z}/5)^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$
3. $(\mathbb{Z}/6)^* = \{\overline{1}, \overline{5}\}$
4. si K és cos, $K^* = K \setminus \{0\}$.
5. si K és cos, $(K[X])^* = K^* = K \setminus \{0\}$.

Proposició 4.2.1. *Si A és un anell commutatiu amb unitat, A^* és un grup commutatiu amb el producte de A.*

Demostració. Clarament, el producte és associatiu, commutatiu, té element neutre i tot element de A^* té invers, per definició. □

El grup A^* es diu *grup multiplicatiu* de l'anell A.

Proposició 4.2.2. *Sigui A un anell commutatiu amb unitat, $a \in A$. Si a és element invertible de A, aleshores a no és divisor de zero.*

Demostració. Sigui $b \in A$ tal que $ab = 0$, multiplicant les dues bandes de la igualtat per a^{-1}, obtenim $0 = a^{-1}(ab) = (a^{-1}a)b = b$. □

La següent proposició caracteritza els elements invertibles i els divisors de zero de $\mathbb{Z}/m$.

Proposició 4.2.3. *Sigui $\overline{a}$ un element no nul de $\mathbb{Z}/m$.*

1. *$\overline{a}$ és invertible a $\mathbb{Z}/m \Leftrightarrow \mathrm{mcd}(a, m) = 1$.*
2. *$\overline{a}$ és divisor de zero a $\mathbb{Z}/m \Leftrightarrow \mathrm{mcd}(a, m) = d > 1$.*

Demostració. Per definició, $\overline{a}$ és invertible a $\mathbb{Z}/m$ si i només si existeix un element $\overline{b}$ a $\mathbb{Z}/m$ tal que $\overline{a}\overline{b} = \overline{1}$ a $\mathbb{Z}/m$. Aquesta igualtat equival a $ab - 1 = mq$ per un cert enter q o, equivalentment $ab - mq = 1$. Per 2.5.4, l'última igualtat equival a $\mathrm{mcd}(a, m) = 1$.
Suposem ara $\overline{a}$ divisor de zero a $\mathbb{Z}/m$. Per definició, existeix $\overline{b} \neq \overline{0}$ tal que $\overline{a}\overline{b} = \overline{0}$ a $\mathbb{Z}/m$. Aquesta igualtat implica $ab = mq$, per un cert enter q. Si fos $\mathrm{mcd}(a, m) = 1$, tindriem, per 2.5.3, $m|b$ i per tant $\overline{b} = \overline{0}$, contradicció. Tenim doncs $\mathrm{mcd}(a, m) = d > 1$.
Recíprocament, suposem $\mathrm{mcd}(a, m) = d > 1$. Posem $a = da_1, m = dm_1$. Aleshores $\overline{m_1} \neq \overline{0}$ a $\mathbb{Z}/m$ i $\overline{am_1} = \overline{a_1 m} = \overline{0}$, per tant $\overline{a}$ és divisor de zero a $\mathbb{Z}/m$. □

A partir del punt 1. de la proposició anterior, veiem com calcular l'invers d'un element invertible de $\mathbb{Z}/m$. Si $\overline{a}$ és invertible a $\mathbb{Z}/m$, tenim $\mathrm{mcd}(a, m) = 1$. Per tant existeixen enters s, t (que sabem calcular) tals que $sa + tm = 1$. A partir d'aquesta igualtat, tenim $\overline{sa} = \overline{1}$ a $\mathbb{Z}/m$ i, per tant $\overline{a}^{-1} = \overline{s}$.

Exercici. *Calculeu l'invers de $\overline{16}$ a $\mathbb{Z}/27$.*

Fem les divisions enteres:

$$\begin{aligned} 27 &= 16 \times 1 + 11 \\ 16 &= 11 \times 1 + 5 \\ 11 &= 5 \times 2 + 1 \end{aligned}$$

Obtenim $1 = 11 - 5 \times 2 = 11 - (16 - 11) \times 2 = 3 \times 11 - 2 \times 16 = 3 \times (27 - 16) - 2 \times 16 = 3 \times 27 - 5 \times 16$. Tenim doncs $\overline{16}^{-1} = -\overline{5} = \overline{22}$ a $\mathbb{Z}/27$.

Si p és primer, tenim, a partir de 4.2.3, que tot element $\overline{a} \neq \overline{0}$ de $\mathbb{Z}/p$ és invertible, per tant $\mathbb{Z}/p$ és un cos. Si m no és primer, aleshores l'anell $\mathbb{Z}/m$ té divisors de

zero. En efecte, si m no és primer, tenim $m = m_1 m_2$, amb $1 < m_1, m_2 < m$. Per tant $\overline{m_1}, \overline{m_2}$ són elements no nuls de $\mathbb{Z}/m$ i $\overline{m_1}\overline{m_2} = \overline{m} = \overline{0}$.

Més en general, tenim

Proposició 4.2.4. *Tot anell commutatiu amb element unitat íntegre i finit és cos.*

Demostració. Sigui A un anell commutatiu, amb element unitat, íntegre, finit i sigui n el cardinal de A. Posem $A = \{a_1, a_2, \ldots, a_n\}$. Sigui $b \in A, b \neq 0$. Considerem els productes $ba_1, ba_2, \ldots, ba_n$. Com A és íntegre, tots aquests productes són diferents. En efecte, $ba_i = ba_j$ implica $a_i = a_j$ per ser $b \neq 0$. Com són n elements diferents de A, són exactament tots els elements de A. En particular, entre ells, hi és l'1. Tenim doncs ba_i=1, per a un cert i. Hem provat doncs que tot element no nul de A és invertible i tenim que A és cos. □

Observació. Com $\mathbb{Z}/p$ és cos, si p és primer, podem considerar l'anell de polinomis $(\mathbb{Z}/p)[X]$ i tots els resultats que hem vist per a l'anell de polinomis $K[X]$, amb K cos, són vàlids per a $(\mathbb{Z}/p)[X]$.
Veiem ara que 3.6.8 no es compleix per a $K = \mathbb{Z}/p$. Considerem $p = 2$ i el polinomi de $(\mathbb{Z}/2)[X]$, $P(X) = X^3 + X$. Tenim $P(X) = (X + \overline{1})^2 X$, per tant $\overline{1}$ és arrel de $P(X)$ amb multiplicitat 2. Ara $P'(X) = \overline{3}X^2 + \overline{1} = X^2 + \overline{1}$ té l'arrel $\overline{1}$ amb multiplicitat 2.

4.3 Congruències lineals

Considerem el problema següent.

Donats nombres enters a, b, m amb $m > 1$, calcular tots els nombres enters x tals que $ax \equiv b \pmod{m}$.

Observació. Si x és una solució al problema plantejat i y és un enter congru amb x, mòdul m, aleshores y també n'és solució. Per tant, considerarem que dues solucions són diferents si no són còngrues mòdul m. Resoldre el problema plantejat equival a resoldre l'equació $\overline{ax} = \overline{b}$ a $\mathbb{Z}/m$.

Exemples.

1. 1 i 3 són solucions de $3x \equiv 3 \pmod{6}$. Són solucions diferents ja que $1 \not\equiv 3 \pmod{6}$.

2. la congruència $2x \equiv 1 \pmod 6$ no té solució ja que $\overline{2}\overline{x} = \overline{0}, \overline{2}$ o $\overline{4}$ a $\mathbb{Z}/6$.

El següent teorema dóna la solució al problema plantejat.

Teorema 4.3.1. *Siguin $a, b, m \in \mathbb{Z}$, $m > 1$.*
La congruència $ax \equiv b \pmod m$ té solució $\Leftrightarrow$ b és múltiple de $\mathrm{mcd}(a, m)$.
Si $d = \mathrm{mcd}(a, m) > 0$ i $d|b$, el nombre de solucions diferents mòdul m és d. Si x és una solució, totes les solucions són $x + \lambda\frac{m}{d}$, amb $\lambda = 0, \ldots, d-1$.

Demostració. Si x és solució de la congruència, tenim $m \mid ax - b$. Per tant, si $d = \mathrm{mcd}(a, m)$, tenim $d \mid ax - b$ i $d \mid a$ que implica $d \mid b$.
Suposem ara que $d = \mathrm{mcd}(a, m)$ divideix b. Per la identitat de Bézout, podem trobar enters s, t tals que $sa + tm = d$. Si $b = db_1$, tenim $b = sb_1a + tb_1m$, per tant $a(sb_1) \equiv b \pmod m$, és a dir $x = sb_1$ és solució de la congruència. Ara, si x_1, x_2 són dues solucions, tenim

$$\left.\begin{array}{ll} ax_1 \equiv b & \pmod m \\ ax_2 \equiv b & \pmod m \end{array}\right\} \Rightarrow a(x_1 - x_2) \equiv 0 \pmod m.$$

Tenim doncs $a(x_1 - x_2) = mq$, per un cert enter q. Com $d = \mathrm{mcd}(a, m)$, tenim $a = da_1, m = dm_1$ amb a_1, m_1 primers entre ells. De $a(x_1 - x_2) = mq$, obtenim $a_1(x_1 - x_2) = m_1q$ i per tant $m_1 \mid a_1(x_1 - x_2)$ que implica $m_1 \mid x_1 - x_2$ per ser a_1, m_1 primers entre ells. Tenim doncs $x_1 - x_2 = \lambda\frac{m}{d}$, per algun enter λ.
Recíprocament, si x és solució, $x + \lambda\frac{m}{d}$ també ho és, ja que $a(x + \lambda m_1) = ax + a\lambda m_1 = ax + a_1 m\lambda \equiv ax \equiv b \pmod m$.
Ara hem de veure quan x i $x + \lambda\frac{m}{d}$ donen la mateixa solució. Tenim $x + \lambda\frac{m}{d} \equiv x \pmod m \Leftrightarrow \lambda\frac{m}{d} \equiv 0 \pmod m \Leftrightarrow \frac{\lambda}{d}$ és enter. Per tant $\lambda = 0, 1, \ldots, d-1$ donen exactament totes les solucions. □

Exercici. *Resoleu les congruències següents.*

$$201x \equiv 67 \pmod{1139},\ 1845x \equiv 90 \pmod{4545},\ 1122x \equiv 20 \pmod{2210}.$$

1) $201x \equiv 67 \pmod{1139}$

Calculant per l'algoritme d'Euclides, obtenim $\mathrm{mcd}(201, 1139) = 67$, per tant la congruència té solucions. Calculem una identitat de Bézout $67 = 6 \times 201 - 1139$.

Obtenim doncs la solució $x = 6$. Tenim $\frac{1139}{67} = 17$. Pel teorema, totes les solucions són

$$x = 6 + 17t, t = 0, \ldots, 66.$$

2) $1845x \equiv 90 \pmod{4545}$

Calculant per l'algoritme d'Euclides, obtenim $\mathrm{mcd}(4545, 1845) = 45$. Com $45 \mid 90$, la congruència té solucions. Calculem una identitat de Bézout $45 = 13 \times 4545 - 32 \times 1845$. Multiplicant per 2, tenim $90 = 26 \times 4545 - 64 \times 1845$. Obtenim doncs la solució $x = -64$. Tenim $\frac{4545}{45} = 101$. Pel teorema, totes les solucions són

$$x = -64 + 101t, t = 0, \ldots, 44.$$

3) $1122x \equiv 20 \pmod{2210}$

$\mathrm{mcd}(2210, 1122) = 34 \nmid 20$, per tant la congruència no té cap solució.

Veiem ara dos resultats de simplificació de congruències.

Proposició 4.3.2. *Siguin $a, b, c, m \in \mathbb{Z}$, $m > 1$, tals que $ac \equiv bc \pmod{m}$. Si $\mathrm{mcd}(c, m) = 1$, aleshores $a \equiv b \pmod{m}$.*

Demostració. Si $\mathrm{mcd}(c, m) = 1$, tenim que $\overline{c}$ és invertible a $\mathbb{Z}/m$; equivalentment, existeix un enter c' tal que $cc' \equiv 1 \pmod{m}$. Tenim doncs $a \equiv a(cc') = (ac)c' \equiv (bc)c' = b(cc') \equiv b \pmod{m}$. □

Proposició 4.3.3. *Siguin $a, b, c, m \in \mathbb{Z}$, $m > 1$, tals que $ac \equiv bc \pmod{m}$. Sigui $d = \mathrm{mcd}(c, m)$. Aleshores $a \equiv b \pmod{\frac{m}{d}}$.*

Demostració. Tenim $(a - b)c = ac - bc = mq$, per un cert enter q. Com $d = \mathrm{mcd}(c, m)$, posem $c = dc_1, m = dm_1$, amb c_1, m_1 enters. De $(a - b)c = mq$, obtenim $(a - b)c_1 = m_1 q$ i per tant $m_1 \mid (a - b)c_1$. Com m_1 i c_1 són primers entre ells, ha de ser $m_1 \mid a - b$, és a dir $a \equiv b \pmod{m_1}$. □

Exercici. *Resoleu les congruències següents utilitzant els resultats de simplificació.*

$$201x \equiv 67 \pmod{1139}, \quad 94x \equiv 15 \pmod{64},$$
$$255x \equiv 30 \pmod{195}, \quad 18x \equiv 36 \pmod{40}.$$

1) $201x \equiv 67 \pmod{1139}$

   $201x \equiv 67 \pmod{1139} \Leftrightarrow 3x \equiv 1 \pmod{17}$. Mòdul 17, la congruència té una única solució $x = 6$. Les solucions mòdul $1139 = 17 \times 67$ són $x = 6 + 17t, t = 0, \ldots, 66$.

2) $94x \equiv 15 \pmod{64}$.

   $94x \equiv 15 \pmod{64} \Leftrightarrow 30x \equiv 15 \pmod{64} \Leftrightarrow 2x \equiv 1 \pmod{64}$, ja que 15 és primer amb 64. Com 2 no és invertible mòdul 64, la congruència no té solució.

3) $255x \equiv 30 \pmod{195}$.

   $255x \equiv 30 \pmod{195} \Leftrightarrow 60x \equiv 30 \pmod{195} \Leftrightarrow 4x \equiv 2 \pmod{13}$. Módul 13, la congruència té una única solució $x = 7$. Les solucions mòdul $195 = 13 \times 15$ són $x = 7 + 13t, t = 0, \ldots, 14$.

4) $18x \equiv 36 \pmod{40}$.

   Com $\mathrm{mcd}(18, 40) = 2$, tenim $18x \equiv 36 \pmod{40} \Leftrightarrow x \equiv 2 \pmod{20}$. Mòdul 20, la congruència té una única solució $x = 2$. Les solucions mòdul 40 són $x = 2$ i $x = 22$.

4.4 Sistemes de congruències lineals

Teorema 4.4.1 (Teorema xinès dels residus)**.** *Si $m_1, \ldots, m_r$ són enters > 1, primers entre ells dos a dos, $a_1, \ldots, a_r$ són enters qualssevol, el sistema de congruències*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

té una solució, única mòdul $M = m_1 \ldots m_r$.

Demostració. Si x, x' són dues solucions, tenim $x \equiv x' \pmod{m_i}, 1 \leq i \leq r$. Com els m_i són dos a dos primers entre ells, tenim $x \equiv x' \pmod{M}$.
Sigui ara $M_i = \dfrac{M}{m_i}$. Tenim $\text{mcd}(m_i, M_i) = 1$ i, per tant, existeix un enter N_i, que es pot calcular amb l'algoritme d'Euclides, tal que $M_i N_i \equiv 1 \pmod{m_i}$. Posem

$$x = \sum_{i=1}^{r} a_i M_i N_i.$$

Tenim $x \equiv a_i \pmod{m_i}$, per a $i = 1, \ldots, r$, ja que $m_i \mid M_j$, per a $j \neq i$, $M_i N_i \equiv 1 \pmod{m_i}$. □

Exercici. *Resoleu el sistema de congruències*

$$\begin{array}{rcll} x & \equiv & 1 & \pmod 4 \\ x & \equiv & 2 & \pmod 7 \\ x & \equiv & 5 & \pmod{11} \end{array}$$

Doneu-ne la solució positiva més petita.

Clarament $4, 7$ i 11 són primers entre ells dos a dos. Sabem que la solució és única mòdul $4 \times 7 \times 11 = 308$. Tenim

$$\begin{array}{lll} m_1 = 4 & m_2 = 7 & m_3 = 11 \\ M_1 = 77 & M_2 = 44 & M_3 = 28 \end{array}$$

Calculem l'invers N_i de M_i mòdul m_i, $i = 1, 2, 3$.

$$\begin{array}{lllll} 77 = 4 \times 16 + 1 & \Rightarrow & 77 \equiv 1 \pmod 4 & \Rightarrow & N_1 = 1 \\ 44 = 7 \times 6 + 2 & \Rightarrow & 44 \equiv 2 \pmod 7 & \Rightarrow & N_2 = 4 \\ 28 = 11 \times 2 + 6 & \Rightarrow & 28 \equiv 6 \pmod{11} & \Rightarrow & N_3 = 2 \end{array}$$

Tenim doncs la solució $x = 1 \times 77 \times 1 + 2 \times 44 \times 4 + 5 \times 28 \times 2 = 709$. La solució positiva més petita és la resta de la divisió de 709 entre 308. Tenim $709 = 308 \times 2 + 93$. La solució positiva més petita del sistema de congruències és doncs 93.

Exercici. *Trobeu un enter comprès entre* 1000 *i* 1910 *tal que la seva última xifra sigui* 1 *quan s'escriu en base* 7*;* 5 *quan s'escriu en base* 10 *i* 10 *quan s'escriu en base* 13*.*

Busquem x tal que

$$\begin{array}{rcll} x & \equiv & 1 & (\text{mod } 7) \\ x & \equiv & 5 & (\text{mod } 10) \\ x & \equiv & 10 & (\text{mod } 13) \end{array}$$

Com $7, 10$ i 13 són primers entre ells dos a dos, aquest sistema té una solució única mòdul $7 \times 10 \times 13 = 910$. Tenim

$$\begin{array}{lll} m_1 = 7 & m_2 = 10 & m_3 = 13 \\ M_1 = 130 & M_2 = 91 & M_3 = 70 \end{array}$$

Busquem l'invers N_i de M_i mòdul m_i, $i = 1, 2, 3$.

$$\begin{array}{lll} 130 \equiv 4 \pmod 7 & \Rightarrow & N_1 = 2 \\ 91 \equiv 1 \pmod{10} & \Rightarrow & N_2 = 1 \\ 70 \equiv 5 \pmod{13} & \Rightarrow & N_3 = 8 \end{array}$$

Una solució és $2 \times 130 + 91 \times 5 + 70 \times 8 \times 10 = 6315$.
Com $(6315 - 1910)/910 \simeq 4,8$, la solució en l'interval demanat és $x = 6315 - 5 \times 910 = 1765$.

4.5 Propietats multiplicatives de les congruències

Teorema 4.5.1 (Petit teorema de Fermat)**.** *Sigui p un nombre primer positiu i sigui a un enter. Aleshores es compleix*

$$a^p \equiv a \pmod p.$$

Demostració. Si $p \mid a$, els dos membres son congrus a 0 mòdul p i per tant és compleix la congruència.
L'enunciat per a a no divisible per p és equivalent a

$$\overline{a}^{p-1} = \overline{1} \text{ a } \mathbb{Z}/p, \text{ per a tot } \overline{a} \in \mathbb{Z}/p, \overline{a} \neq \overline{0}.$$

Per a $\overline{a} \in \mathbb{Z}/p, \overline{a} \neq \overline{0}$, considerem l'aplicació

$$\begin{array}{rccc} f: & \mathbb{Z}/p & \to & \mathbb{Z}/p \\ & \overline{x} & \mapsto & \overline{ax} \end{array}$$

Tenim $f(\overline{0}) = \overline{0}$. L'aplicació f és bijectiva. En efecte

1. Com $\overline{a}$ és invertible, tenim $\overline{ax} = \overline{ay} \Rightarrow \overline{x} = (\overline{a}^{-1}(\overline{a})\overline{x} = \overline{a}^{-1}(\overline{ax}) = \overline{a}^{-1}(\overline{ay}) = (\overline{a}^{-1}\overline{a})\overline{y} = \overline{y}$, per tant f és injectiva.

2. Si $\overline{y} \in \mathbb{Z}/p$, tenim $\overline{y} = (\overline{a}\overline{a}^{-1})\overline{y} = \overline{a}(\overline{a}^{-1}\overline{y}) = f(\overline{a}^{-1}\overline{y})$, per tant f és exhaustiva.

Els dos conjunts

$$\{\overline{x} : \overline{x} \in \mathbb{Z}/p, \overline{x} \neq \overline{0}\} \text{ i } \{\overline{ax} : \overline{x} \in \mathbb{Z}/p, \overline{x} \neq \overline{0}\}$$

són doncs iguals i obtenim

$$\prod_{\overline{x}\in\mathbb{Z}/p\setminus\{\overline{0}\}} \overline{x} = \prod_{\overline{x}\in\mathbb{Z}/p\setminus\{\overline{0}\}} \overline{ax} = \overline{a}^{p-1} \prod_{\overline{x}\in\mathbb{Z}/p\setminus\{\overline{0}\}} \overline{x}$$

Com $\prod_{\overline{x}\in\mathbb{Z}/p\setminus\{\overline{0}\}} \overline{x}$ és invertible, tenim $\overline{a}^{p-1} = \overline{1}$ a $\mathbb{Z}/p$. □

Volem veure ara una generalització del petit teorema de Fermat. Per això definim una funció anomenada funció φ d'Euler.
Havíem vist

$$\overline{a} \text{ invertible a } \mathbb{Z}/m \Leftrightarrow \text{mcd}(a, m) = 1.$$

La funció φ d'Euler compta el nombre d'aquests elements invertibles, és a dir, per a m enter, $m \geq 1$, definim

$$\varphi(m) = |\{a \text{ enter } : 1 \leq a \leq m \text{ i } \text{mcd}(a, m) = 1\}|.$$

(on $|A|$ indica el cardinal del conjunt A.) Per definició de φ, tenim doncs que, per a $m > 1$, $(\mathbb{Z}/m)^*$ té $\varphi(m)$ elements.

Proposició 4.5.2. *1. Si p és primer $\varphi(p) = p - 1$.*

2. Si p és primer, r un enter ≥ 1, $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$.

Demostració. Si p és primer, tot enter a amb $1 \leq a < p$ és primer amb p, per tant $\varphi(p) = p - 1$.
Si p és primer, r un enter ≥ 1, tenim $\text{mcd}(a, p^r) > 1 \Leftrightarrow a$ és múltiple de p. Els múltiples de p entre 1 i p^r són $p, 2p, \ldots, p^r = p^{r-1} \cdot p$, per tant n'hi ha p^{r-1}. Tenim doncs $\varphi(p^r) = p^r - p^{r-1}$. □

Proposició 4.5.3. *Si m, n són enters ≥ 1, primers entre ells, tenim*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Exemple. Veiem amb un exemple que la condició "$\mathrm{mcd}(m,n) = 1$" és necessària en la proposició anterior. Posem $m = 4, n = 6$. Tenim

$\varphi(m) = 2$, ja que els enters entre 1 i 4, primers amb 4 són 1 i 3.

$\varphi(n) = 2$, ja que els enters entre 1 i 6, primers amb 6 són 1 i 5.

$\varphi(mn) = 8$, ja que els enters entre 1 i 24, primers amb 24 són 1, 5, 7, 11, 13, 17, 19, 23.

Tenim doncs en aquest cas $\varphi(mn) \neq \varphi(m)\varphi(n)$.

Demostració de la proposició 4.5.3. Siguin

$$\begin{aligned} A &= \{a \text{ enter} : 1 \leq a \leq mn \text{ i } \ \mathrm{mcd}(a, mn) = 1\}, \\ B &= \{b \text{ enter} : 1 \leq b \leq m \text{ i } \ \mathrm{mcd}(b, m) = 1\}, \\ C &= \{c \text{ enter} : 1 \leq c \leq n \text{ i } \ \mathrm{mcd}(c, n) = 1\}. \end{aligned}$$

Definim una aplicació

$$\begin{array}{rccc} f: & A & \to & B \times C \\ & a & \mapsto & (a_1, a_2) \end{array}$$

on a_1 és la resta de la divisió de a entre m i a_2 és la resta de la divisió de a entre n. Veiem que f està ben definida, és a dir $\mathrm{mcd}(a, mn) = 1 \Rightarrow \mathrm{mcd}(a_1, m) = 1$ i $\mathrm{mcd}(a_2, n) = 1$. En efecte, tenim $a = mq_1 + a_1, a = nq_2 + a_2$, per certs enters q_1, q_2. Per tant si d és divisor comú de a_1 i m (resp. de a_2 i n) també ho és de a i m (resp. de a i n) i per tant de a i mn.
Volem veure ara que f és bijectiva. Si tenim $(b, c) \in B \times C$, pel teorema xinès dels residus 4.4.1, existeix un únic enter a, amb $1 \leq a \leq mn$, tal que $a \equiv b \pmod{m}$ i $a \equiv c \pmod{n}$. Hem de veure $a \in A$, és a dir $\mathrm{mcd}(a, mn) = 1$. Si fos $\mathrm{mcd}(a, mn) \neq 1$, existiria un primer p dividint a i mn. Aleshores p hauria de dividir m o n. Si $p \mid m$, tindriem $\mathrm{mcd}(a, m) \neq 1$. Però, com $a \equiv b \pmod{m}$, per 2.4.1, $\mathrm{mcd}(b, m) = \mathrm{mcd}(a, m)$. Tindriem doncs $\mathrm{mcd}(b, m) \neq 1$, contradicció, ja que $b \in B$. Si $p \mid n$, arribem igualment a contradicció.
Hem establert doncs que els conjunts A i $B \times C$ estan en bijecció. Per definició de φ, el nombre d'elements de A és $\varphi(mn)$, el de B, $\varphi(m)$ i el de C, $\varphi(n)$. Tenim doncs $\varphi(mn) = \varphi(m)\varphi(n)$. □

Corol·lari 4.5.4. *Sigui n un enter,*

$$n = \prod_{i=1}^{s} p_i^{r_i}$$

la seva descomposició en producte de primers, amb $p_i \neq p_j$ si $i \neq j$. Aleshores

$$\varphi(n) = \prod_{i=1}^{s} p_i^{r_i-1}(p_i - 1) = n \prod_{p|n} (1 - \frac{1}{p}).$$

Demostració. Fem inducció sobre s. Per $s = 1$, és 4.5.2. Suposem que el resultat és cert per s i sigui $n = \prod_{i=1}^{s+1} p_i^{r_i}$. Tenim $\prod_{i=1}^{s} p_i^{r_i}$ i $p_{s+1}^{r_{s+1}}$ primers entre ells, per tant, per 4.5.3,

$$\varphi(n) = \varphi(\prod_{i=1}^{s} p_i^{r_i})\varphi(p_{s+1}^{r_{s+1}}).$$

Per hipòtesi d'inducció, tenim $\varphi(\prod_{i=1}^{s} p_i^{r_i}) = \prod_{i=1}^{s} p_i^{r_i-1}(p_i - 1)$, i, per 4.5.2, $\varphi(p_{s+1}^{r_{s+1}}) = p_{s+1}^{r_{s+1}-1}(p_{s+1} - 1)$. Per tant

$$\varphi(n) = \prod_{i=1}^{s+1} p_i^{r_i-1}(p_i - 1).$$

Per veure la segona igualtat, només cal tenir en compte $p_i^{r_i-1}(p_i - 1) = p_i^{r_i}(1 - \frac{1}{p_i})$.
□

Exemples. $\varphi(24) = \varphi(2^3)\varphi(3) = 4 \times 2 = 8$.
$\varphi(225) = \varphi(3^2 \cdot 5^2) = 6 \times 20 = 120$.

Teorema 4.5.5 (Teorema d'Euler)**.** *Sigui m un enter $m \geq 2$. Per a tot enter a tal que* $\text{mcd}(a, m)$*=1, tenim*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Demostració. La prova és anàlega a la del petit teorema de Fermat. Per a un enter a, amb $\text{mcd}(a, m)$=1, considerem l'aplicació

$$\begin{array}{rccc} f: & (\mathbb{Z}/m)^* & \to & (\mathbb{Z}/m)^* \\ & \overline{x} & \mapsto & \overline{ax} \end{array}$$

Com $\overline{a}$ és invertible a $\mathbb{Z}/m$, l'aplicació és bijectiva. Per tant

$$\prod_{\overline{x}\in(\mathbb{Z}/m)^*} \overline{x} = \prod_{\overline{x}\in(\mathbb{Z}/m)^*} \overline{ax} = \overline{a}^{\varphi(m)} \prod_{\overline{x}\in(\mathbb{Z}/m)^*} \overline{x}$$

i, com $\prod_{\overline{x}\in(\mathbb{Z}/m)^*} \overline{x}$ és invertible a $\mathbb{Z}/m$, obtenim

$$\overline{a}^{\varphi(m)} = \overline{1} \text{ a } \mathbb{Z}/m.$$

□

Exercici. *Calculeu el residu de dividir* 2^{5000} *entre 45.*

Tenim 2 i 45 coprimers, per tant $2^{\varphi(45)} \equiv 1 \pmod{45}$. Ara $45 = 3^2 \times 5$. Per tant $\varphi(45) = \varphi(3^2)\varphi(5) = (3^2-3)(5-1) = 6 \times 4 = 24$. Dividim 5000 entre 24: $5000 = 24 \times 208 + 8$. Tenim doncs $2^{5000} = 2^{24\times 208+8} = (2^{24})^{208} \times 2^8 \equiv 2^8 \pmod{45}$. Calculem ara $2^8 \pmod{45}$. Tenim $2^8 = 256 \equiv 31 \pmod{45}$.
El residu de dividir 2^{5000} entre 45 és doncs 31.

Definició 4.5.6. Sigui m un enter $m \geq 2$ i b un element de $(\mathbb{Z}/m)^*$. Anomenem *ordre* de b en $(\mathbb{Z}/m)^*$ l'enter $k \geq 1$ més petit tal que $b^k = 1$.

Exemple.
A $(\mathbb{Z}/7)^*$, $\overline{2}$ té ordre 3,
$\overline{3}$ té ordre 6,
$\overline{4}$ té ordre 3,
$\overline{5}$ té ordre 6,
$\overline{6}$ té ordre 2.

Proposició 4.5.7. *Sigui* m *un nombre enter,* $m \geq 2$*. L'ordre de qualsevol element de* $(\mathbb{Z}/m)^*$ *és un divisor de* $\varphi(m)$*.*

Demostració. Per a tot $b \in (\mathbb{Z}/m)^*$, tenim $b^{\varphi(m)} = 1$. Per tant, si k és l'ordre de b a $(\mathbb{Z}/m)^*$, tenim $k \leq \varphi(m)$. Fem la divisió entera de $\varphi(m)$ entre k: $\varphi(m) = kq + r$, amb $0 \leq r < k$. Tenim

$$1 = b^{\varphi(m)} = b^{kq+r} = (b^k)^q b^r = b^r$$

ja que $b^k = 1$. Ara k és l'enter positiu més petit tal que $b^k = 1$. Per tant ha de ser $r = 0$ i obtenim $k \mid \varphi(m)$. □

Definició 4.5.8. Sigui m un nombre enter ≥ 2. Un element $g \in (\mathbb{Z}/m)^*$ es diu *arrel primitiva* mòdul m si el seu ordre és $\varphi(m)$.

Exemple. $\overline{3}$ és arrel primitiva mòdul 7.

Observació. Si g és arrel primitiva mòdul m, aleshores $g, g^2, \ldots, g^{\varphi(m)} = \overline{1}$ són tots els elements de $(\mathbb{Z}/m)^*$.

Exemple. Els elements de $(\mathbb{Z}/7)^*$ són
$\overline{3}, \overline{3}^2 = \overline{2}, \overline{3}^3 = \overline{6}, \overline{3}^4 = \overline{4}, \overline{3}^5 = \overline{5}, \overline{3}^6 = \overline{1}$.

Exemple. Tenim $\varphi(8) = 4$ i $(\mathbb{Z}/8)^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. Ara $\overline{3}^2 = \overline{1}, \overline{5}^2 = \overline{1}, \overline{7}^2 = \overline{1}$. Per tant, no existeixen arrels primitives mòdul 8.

Lema 4.5.9. *Sigui $m \geq 2$ un enter, b un element de $(Z/m)^*$ i sigui k l'ordre de b en $(\mathbb{Z}/m)^*$. Si n és un enter ≥ 1, tenim $b^n = 1 \Rightarrow k \mid n$.*

Demostració. Fem la divisió entera de n entre k: $n = kq + r$, amb $0 \leq r < k$. Tenim

$$1 = b^n = b^{kq+r} = (b^k)^q b^r.$$

Com $r < k$, ha de ser $r = 0$. □

Proposició 4.5.10. *Sigui $m \geq 2$ un enter, b un element de $(Z/m)^*$ i sigui k l'ordre de b en $(\mathbb{Z}/m)^*$. Per a tot r enter $r \geq 1$, l'ordre de b^r en $(\mathbb{Z}/m)^*$ és*

$$\frac{k}{\operatorname{mcd}(k, r)}.$$

Demostració. Posem $d = \operatorname{mcd}(k, r), k = dk_1, r = dr_1$. Tenim

$$(b^r)^{k_1} = (b^k)^{r_1} = 1.$$

Suposem ara $(b^r)^l = 1$ per un enter $l \geq 1$. Tenim doncs $b^{rl} = 1$. Per 4.5.9, $k \mid rl$. Dividint per d, obtenim $k_1 \mid r_1 l$. Com k_1 i r_1 són primers entre ells, ha de ser $k_1 \mid l$. Per tant l'ordre de b^r és $k_1 = k/\operatorname{mcd}(k, r)$. □

Corol·lari 4.5.11. *Sigui $m \geq 2$ un enter tal que existeix una arrel primitiva mòdul m. Aleshores, el nombre d'arrel primitives mòdul m és $\varphi(\varphi(m))$. Més exactament, si g és una arrel primitiva mòdul m, totes les arrels primitives mòdul m són g^r, amb $1 \leq r \leq \varphi(m)$ i $\mathrm{mcd}(r, \varphi(m)) = 1$.*

Demostració. Sigui g una arrel primitiva mòdul m. Aleshores, g té ordre $\varphi(m)$ mòdul m i els elements de $(\mathbb{Z}/m)^*$ són els g^r, amb $1 \leq r \leq \varphi(m)$. Ara

$$g^r \text{ és arrel primitiva } \Leftrightarrow \text{ el seu ordre és } \varphi(m).$$

Per 4.5.10, l'ordre de g^r és $\dfrac{\varphi(m)}{\mathrm{mcd}(\varphi(m), r)}$. És doncs igual a $\varphi(m)$ si i només si $\mathrm{mcd}(\varphi(m), r) = 1$.
Per tant, el nombre d'arrels primitives mòdul m és

$$|\{r \in \mathbb{Z} : 1 \leq r \leq \varphi(m) \text{ i } \mathrm{mcd}(r, \varphi(m)) = 1\}| = \varphi(\varphi(m)).$$

□

Exercici. *Calculeu totes les arrels primitives mòdul 22.*

Tenim $(\mathbb{Z}/22)^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{13}, \overline{15}, \overline{17}, \overline{19}, \overline{21}\}$, $\varphi(22) = 10$.
Busquem una arrel primitiva, provant successivament amb els elements de $(\mathbb{Z}/22)^*$.
Calculem les potències de $\overline{3}$: $\overline{3}^2 = \overline{9}, \overline{3}^3 = \overline{5}, \overline{3}^4 = \overline{15}, \overline{3}^5 = \overline{1}$, per tant $\overline{3}$ no és arrel primitiva.
Calculem les potències de $\overline{5}$: $\overline{5}^2 = \overline{3}, \overline{5}^3 = \overline{15}, \overline{5}^4 = \overline{9}, \overline{5}^5 = \overline{1}$, per tant $\overline{5}$ tampoc no és arrel primitiva.
Calculem les potències de $\overline{7}$: $\overline{7}^2 = \overline{5}, \overline{7}^3 = \overline{13}, \overline{7}^4 = \overline{3}, \overline{7}^5 = \overline{21}, \overline{7}^6 = \overline{17}, \overline{7}^8 = \overline{9}, \overline{7}^9 = \overline{19}, \overline{7}^{10} = \overline{1}$ per tant $\overline{7}$ és arrel primitiva.
Sabem que tenim $\varphi(10) = 4$ arrels primitives mòdul 22. Són $\overline{7}^r$, amb r primer amb 10, per tant:
$\overline{7}, \overline{7}^3 = \overline{13}, \overline{7}^7 = \overline{17}, \overline{7}^9 = \overline{19}$.
Quan busquem una arrel primitiva, es pot fer més ràpid, tenint en compte 4.5.7. En aquest cas, l'ordre de qualsevol element de $(\mathbb{Z}/22)^*$ divideix 10. Per tant un element diferent de $\overline{1}$ que no sigui arrel primitiva té ordre 2 o bé 5. Si volem veure si $b \in (\mathbb{Z}/22)^*$ és arrel primitiva, calculem b^2 i b^5. Si cap dels dos no dóna $\overline{1}$, aleshores b és arrel primitiva mòdul 22.

Veiem ara per quins enters m existeixen arrels primitives mòdul m.

Proposició 4.5.12. *Els enters m tals que existeixen arrels primitives mòdul m són*

$$m = 2, 4, p^r, 2p^r, \text{ on } p \text{ és un primer senar, } r \geq 1.$$

Demostració. Veure A. Travesa, "Aritmètica".

4.6 Símbol de Legendre.

Volem estudiar el nombre de solucions de la congruència

$$x^2 \equiv a \pmod{p},$$

on p és un primer senar. Equivalentment, el nombre d'arrels del polinomi $X^2 - \overline{a} \in (\mathbb{Z}/p)[X]$. Sabem que un polinomi sobre un cos té com a màxim tantes arrels com el seu grau, per tant la congruència tindrà com a màxim dues solucions diferents mòdul p.

Definició. Sigui p un primer senar. Per a tot nombre enter a, posem

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a \\ 1 & \text{si } p \nmid a \text{ i } \overline{a} \text{ és quadrat a } (Z/p)^* \\ -1 & \text{si } p \nmid a \text{ i } \overline{a} \text{ no és quadrat a } (Z/p)^* \end{cases}$$

$\left(\frac{a}{p}\right)$ es diu *símbol de Legendre.*

Observació. Si p és un primer senar, el nombre de solucions de $x^2 \equiv a \pmod{p}$ és $\left(\frac{a}{p}\right) + 1$.

Proposició 4.6.1 (Propietats del símbol de Legendre.)**.** *1. Si $a \equiv b \pmod{p}$, aleshores $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

3. Si $p \nmid a$, aleshores $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$

Demostració. 1) és immediat a partir de la definició.
2) si $p \mid a$ o $p \mid b$, aleshores $p \mid ab$, per tant en aquest cas es compleix la igualtat. Suposem ara $p \nmid a$ i $p \nmid b$. Si tenim $\left(\frac{a}{p}\right) = 1$ i $\left(\frac{b}{p}\right) = 1$, per definició del símbol, $a \equiv x^2, b \equiv y^2 \pmod{p}$, per certs enters x, y. Tenim doncs $ab \equiv (xy)^2$, per tant $\left(\frac{ab}{p}\right) = 1$. Suposem ara $\left(\frac{a}{p}\right) = 1, \left(\frac{b}{p}\right) = -1$. Tenim doncs $a \equiv x^2$, per un cert enter x, no divisible per p. Aleshores existeixen a', x' tals que $aa' \equiv 1, xx' \equiv 1 \pmod{p}$ i per tant tenim $a' \equiv x'^2 \pmod{p}$. Si fos $ab \equiv z^2 \pmod{p}$, tindríem $b \equiv (a'a)b = a'(ab) \equiv (x'z)^2 \pmod{p}$, contradicció. Tenim doncs $\left(\frac{ab}{p}\right) = -1$. De fet hem provat que el producte d'un quadrat per un noquadrat a $(\mathbb{Z}/p)^*$ és no quadrat.
Si a i b no són quadrats mòdul p, tenim que ac és no quadrat per a tot quadrat c. Tenint en compte que a $(\mathbb{Z}/p)^*$ hi ha exactament $\frac{p-1}{2}$ elements que són quadrats, obtenim que, si c agafa tots els valors dels quadrats mòdul p, ac són tots els no quadrats. Per tant $b = ac$, per a algun c quadrat i $ab = a^2c$ és quadrat mòdul p.
3) Per 2), tenim

$$\left(\frac{a^2b}{p}\right) = \left(\frac{a^2}{p}\right)\left(\frac{b}{p}\right)$$

i

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)^2 = 1,$$

ja que $p \nmid a$ implica $\left(\frac{a}{p}\right)^2 = \pm 1$. □

Proposició 4.6.2 (Criteri d'Euler)**.** *Sigui p un nombre primer senar. Per a tot nombre enter a, se satisfà la congruència*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Demostració. Si $p \mid a$, els dos membres són iguals a zero.
Si $p \nmid a$, $\left(\frac{a}{p}\right) = \pm 1$, per definició. Pel petit teorema de Fermat,

$$(a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1 \pmod{p}$$

per tant

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

Només cal veure doncs

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Ara $\left(\frac{a}{p}\right) = 1$ si i només si $a \equiv b^2 \pmod{p}$ per a algun enter b i tenim aleshores $a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \pmod{p}$.
Si $\left(\frac{a}{p}\right) = -1$, a no és quadrat mòdul p. Com la congruència $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ té com a màxim $(p-1)/2$ solucions i els $(p-1)/2$ quadrats de $(\mathbb{Z}/p)^*$ ho són, a no n'és solució i per tant $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Corol·lari 4.6.3. *Sigui p un primer senar. Aleshores*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & si \quad p \equiv 1 \pmod{4} \\ -1 & si \quad p \equiv 3 \pmod{4} \end{cases}$$

Demostració. Pel criteri d'Euler

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Com els dos nombres són iguals a ± 1 i $p > 2$, tenim la igualtat.
Ara $(p-1)/2$ és parell (resp. senar) si i només si $p \equiv 1 \pmod{4}$ (resp. $p \equiv 3 \pmod{4}$). □

Proposició 4.6.4. *Sigui p un primer senar. Aleshores*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & si \quad p \equiv \pm 1 \pmod{8} \\ -1 & si \quad p \equiv \pm 3 \pmod{8} \end{cases}$$

Demostració. Com p és senar, $p-1$ és parell. Considerem els $(p-1)/2$ nombres enters parells entre 1 i $p-1$ i les congruències següents.

$$\begin{array}{rcrcll} p-1 & \equiv & -1 & = & 1\cdot(-1) & \pmod p \\ 2 & \equiv & 2 & = & 2\cdot(-1)^2 & \pmod p \\ p-3 & \equiv & -3 & = & 3\cdot(-1)^3 & \pmod p \\ 4 & \equiv & 4 & = & 4\cdot(-1)^4 & \pmod p \\ p-5 & \equiv & -5 & = & 5\cdot(-1)^5 & \pmod p \\ 6 & \equiv & 6 & = & 6\cdot(-1)^6 & \pmod p \\ \vdots & & \vdots & & \vdots & \\ a & & & \equiv & \dfrac{p-1}{2}\cdot(-1)^{\frac{p-1}{2}} & \pmod p \end{array}$$

on a és $\dfrac{p-1}{2}$, si $\dfrac{p-1}{2}$ és parell; $p-\dfrac{p-1}{2}$, si $\dfrac{p-1}{2}$ és senar.
Multiplicant totes les congruències, obtenim

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!(-1)^{\sum_{j=1}^{(p-1)/2}j}\pmod p. \tag{4.1}$$

Ara $\sum_{j=1}^{(p-1)/2}j=\dfrac{1}{2}(\dfrac{p-1}{2})(\dfrac{p-1}{2}+1)=\dfrac{(p-1)(p+1)}{8}=\dfrac{p^2-1}{8}$. Simplificant a (4.1) el factor $((p-1)/2)!$, obtenim

$$2^{\frac{p-1}{2}}\equiv(-1)^{\frac{p^2-1}{8}}\pmod p.$$

Aplicant el criteri d'Euler,

$$\left(\frac{2}{p}\right)\equiv 2^{\frac{p-1}{2}}\equiv(-1)^{\frac{p^2-1}{8}}\pmod p.$$

i, com les dues expressions són iguals a ±1, obtenim la igualtat. □

Si $a\neq -1,2$, el criteri d'Euler permet d'obtenir el valor de $\left(\dfrac{a}{p}\right)$ calculant $a^{\frac{p-1}{2}}$ (mod p). Aquest càlcul es pot fer amb l'algoritme binari d'exponenciació.

Algoritme binari d'exponenciació.
Donats enters $a,b,m\geq 2$, volem calcular $a^b \pmod m$. L'algoritme és el següent.

1. Posem $x=1$
2. si és $b=0$, escriure x i acabar

3. si b és senar, fer $x = x \cdot a \pmod{m}$

4. Fer $b = \left[\frac{b}{2}\right], a = a^2 \pmod{m}$ i tornar a 2.

Veiem que l'algoritme calcula efectivament $a^b \pmod{m}$. Sigui

$$b = b_k 2^k + b_{k-1} 2^{k-1} + \cdots + b_1 2 + b_0$$

l'expressió de b en base 2. Tenim $b_0 = 1$, si b és senar i $b_0 = 0$ si b és parell. Per tant, en començar a executar l'algoritme, el pas 3. calcula $a^{b_0} \pmod{m}$. Ara, en el pas 4., posa $b = \left[\frac{b}{2}\right] = b_k 2^{k-1} + b_{k-1} 2^{k-2} + \cdots + b_1$ i canvia a per a^2. En tornar a 3., calcula $a^{b_0} \cdot (a^2)^{b_1} = a^{b_0 + 2b_1}$ i en el pas 4., posa $b = b_k 2^{k-2} + b_{k-1} 2^{k-3} + \cdots + b_2$ i canvia a^2 per a^4 ...
Observem que l'algoritme redueix en cada pas mòdul m i per tant opera sempre amb enters $< m$.

Teorema 4.6.5 (Llei de reciprocitat quadràtica)**.** *Siguin p i q nombres naturals primers senars. Es compleix la igualtat*

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

És a dir,

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) \quad \textit{si} \;\; p \equiv 3 \pmod{4} \;\; \textit{i} \;\; q \equiv 3 \pmod{4}$$

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \quad \textit{en els altres casos.}$$

Exercici. *Calculeu els símbols de Legendre*

$$\left(\frac{46}{97}\right), \left(\frac{54}{101}\right), \left(\frac{61}{113}\right), \left(\frac{67}{107}\right).$$

1. $$\left(\frac{46}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{23}{97}\right) = \left(\frac{97}{23}\right) = \left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = -1,$$

   on, per la primera igualtat, hem usat 4.6.1 2), per la segona 4.6.4 i 4.6.5, per la tercera 4.6.1 1), per la quarta 4.6.5, per la cinquena 4.6.1 1) i finalment, com $\overline{3}$ no és quadrat a $\mathbb{Z}/5$, obtenim $\left(\frac{3}{5}\right) = -1$.

2. $$\left(\frac{54}{101}\right) = \left(\frac{6}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{3}{101}\right) = -\left(\frac{101}{3}\right) = -\left(\frac{2}{3}\right) = 1,$$

   on, per la primera igualtat, hem usat 4.6.1 3), per la segona 4.6.1 2), per la tercera 4.6.4 i 4.6.5, per la quarta 4.6.1 1) i finalment, com $\overline{2}$ no és quadrat a $\mathbb{Z}/3$, obtenim $\left(\frac{2}{3}\right) = -1$.

3. $$\left(\frac{61}{113}\right) = \left(\frac{113}{61}\right) = \left(\frac{52}{61}\right) = \left(\frac{13}{61}\right) = \left(\frac{61}{13}\right) = \left(\frac{9}{13}\right) = 1,$$

   on, per la primera igualtat, hem usat 4.6.5, per la segona 4.6.1 1), per la tercera 4.6.1 3), per la quarta 4.6.5, per la cinquena 4.6.1 1) i finalment, com 9 és quadrat, obtenim $\left(\frac{9}{13}\right) = 1$.

4. $$\left(\frac{67}{107}\right) = -\left(\frac{107}{67}\right) = -\left(\frac{40}{67}\right) = -\left(\frac{2}{67}\right)\left(\frac{5}{67}\right) = \left(\frac{67}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

   on, per la primera igualtat, hem usat 4.6.5, per la segona 4.6.1 1), per la tercera 4.6.1 3) i 2), per la quarta 4.6.4 i 4.6.5, per la cinquena 4.6.1 1) i finalment, com $\overline{2}$ no és quadrat a $\mathbb{Z}/5$, obtenim $\left(\frac{2}{5}\right) = -1$.

Exercici. *Considerem els dos primers* $p = 2784853, q = 505399$. *Calculeu* $\left(\frac{p}{q}\right)$.

Tenim

$$\left(\frac{p}{q}\right) = \left(\frac{2784853}{505399}\right) = \left(\frac{257858}{505399}\right) = \left(\frac{2}{505399}\right) \cdot \left(\frac{31}{505399}\right) \cdot \left(\frac{4159}{505399}\right)$$

Per la primera igualtat, hem calculat la resta de la divisió de p entre q i aplicat 4.6.1 1); per la segona, hem fet la descomposició en producte de primers $257858 = 2 \times 31 \times 4159$ i aplicat 4.6.1 2). Calculem ara cada factor.

$$\left(\frac{2}{505399}\right) = 1,$$

per 4.6.4, ja que $505399 \equiv -1 \pmod 8$.

$$\left(\frac{31}{505399}\right) = -\left(\frac{505399}{31}\right) = -\left(\frac{6}{31}\right) = -\left(\frac{2}{31}\right)\left(\frac{3}{31}\right),$$

on, en la primera igualtat, hem aplicat 4.6.5, en la segona hem calculat la resta de dividir 505399 entre 31 i aplicat 4.6.1 1), en la tercera, hem aplicat 4.6.1 2). Calculem ara cada factor.

$$\left(\frac{2}{31}\right) = 1,$$

per 4.6.4, ja que $31 \equiv -1 \pmod 8$,

$$\left(\frac{3}{31}\right) = -\left(\frac{31}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

aplicant 4.6.5. Per tant

$$\left(\frac{31}{505399}\right) = 1.$$

Finalment

$$\left(\frac{4159}{505399}\right) = -\left(\frac{505399}{4159}\right) = -\left(\frac{2160}{4159}\right) = -\left(\frac{3}{4159}\right)\left(\frac{5}{4159}\right),$$

on, en la primera igualtat, hem aplicat 4.6.5, en la segona 4.6.1 1) i que 2160 és la resta de dividir 505399 entre 4159. Ara la descomposició en producte de primers de 2160 és $2160 = 2^4 \times 3^3 \times 5$ i, de 4.6.1 2) i 3), obtenim la tercera igualtat. Calculem ara

$$\left(\frac{3}{4159}\right) = -\left(\frac{4159}{3}\right) = -1,$$

$$\left(\frac{5}{4159}\right) = \left(\frac{4159}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

Obtenim doncs

$$\left(\frac{4159}{505399}\right) = 1.$$

Com a resultat final

$$\left(\frac{2784853}{505399}\right) = 1,$$

és a dir 2784853 és residu quadràtic mòdul 505399.

Per provar la llei de reciprocitat quadràtica, fem primer el lema següent.

Lema 4.6.6 (Lema de Gauss)**.** *Sigui p un nombre natural primer senar i a un nombre enter no divisible per p. Per a cada enter k, $1 \leq k \leq \frac{p-1}{2}$, sigui r_k la resta de la divisió entera de ka entre p. Aleshores*

$$\left(\frac{a}{p}\right) = (-1)^m,$$

on $m = |\{r_k : r_k > \frac{p}{2}\}|$.

Demostració. Tenim $1 \leq r_k \leq p-1$, ja que són restes de divisions enteres entre p d'enters no divisibles per p. Siguin

$b_1, \ldots, b_m$ les restes r_k que són $> p/2$,

$c_1, \ldots, c_n$ les restes r_k que són $\leq p/2$.

Tenim $ka \equiv k'a \pmod{p} \Rightarrow k \equiv k' \pmod{p}$, ja que $p \nmid a$, i per tant, els r_k són tots diferents i tenim doncs $m+n = (p-1)/2$. Per a $1 \leq i \leq m$, tenim $1 \leq p - b_i < p/2$ i els $p - b_i$ són diferents. A més, per a tot $j = 1, \ldots, n$ és $p - b_i \neq c_j$, en efecte, si $b_i \equiv ka, c_j \equiv k'a \pmod{p}$, $p - b_i = c_j \Rightarrow -ka \equiv k'a \Rightarrow (k'+k)a \equiv 0 \pmod{p} \Rightarrow$

$(k'+k) \equiv 0 \pmod p$, ja que $p \nmid a$, però $1 \leq k, k' \leq (p-1)/2 \Rightarrow 1 \leq k+k' \leq p-1$. Tenim doncs que la reunió de $\{c_j : 1 \leq j \leq n\}$ i $\{p - b_i : 1 \leq i \leq m\}$ és el conjunt dels enters entre 1 i $(p-1)/2$. Multiplicant, obtenim la congruència

$$\begin{aligned}((p-1)/2)! &= \textstyle\prod_{i=1}^{m}(p-b_i)\prod_{j=1}^{n} c_j \\ &\equiv (-1)^m \textstyle\prod_{k=1}^{(p-1)/2} ka = (-1)^m a^{(p-1)/2}\,((p-1)/2)! \pmod p.\end{aligned}$$

Simplificant per $((p-1)/2)!$, obtenim $a^{(p-1)/2} \equiv (-1)^m \pmod p$. Ara, pel criteri d'Euler $\left(\dfrac{a}{p}\right) \equiv (-1)^m \pmod p$. Com tots dos valen ± 1, tenim igualtat. □

Notem que, per aplicar el lema de Gauss, només cal saber la paritat de m. Tenim el resultat següent.

Proposició 4.6.7. *Siguin p, a, m com en el lema de Gauss. Llavors*

$$m \equiv \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] + (a-1)\frac{p^2-1}{8} \pmod 2.$$

En particular, si a és senar, $m \equiv \sum_{k=1}^{(p-1)/2} \left[\dfrac{ka}{p}\right]$.

Demostració. Per a $1 \leq k \leq (p-1)/2$, tenim $ka = p\left[\dfrac{ka}{p}\right] + r_k$, ja que $\left[\dfrac{ka}{p}\right]$ és el quocient de la divisió entera de ka entre p. Havíem vist que el conjunt dels r_k era la reunió disjunta dels conjunts dels b_i i dels c_j. Tenim doncs

$$\sum_{i=1}^{m} b_i + \sum_{j=1}^{n} c_j = \sum_{k=1}^{(p-1)/2} r_k = a\sum_{k=1}^{(p-1)/2} k - p\sum_{k=1}^{(p-1)/2}\left[\frac{ka}{p}\right].$$

D'altra banda, el conjunt dels nombres $1, 2, \ldots, (p-1)/2$, és la reunió disjunta dels nombres c_j i $p - b_i$, tenim doncs també

$$\sum_{k=1}^{(p-1)/2} k = \sum_{i=1}^{m}(p-b_i) + \sum_{j=1}^{n} c_j = mp - \sum_{i=1}^{m} b_i + \sum_{j=1}^{n} c_j.$$

Sumant les dues igualtats de forma creuada, obtenim

$$(a+1)\sum_{k=1}^{(p-1)/2} k - p\sum_{k=1}^{(p-1)/2}\left[\frac{ka}{p}\right] = mp + 2\sum_{j=1}^{n} c_j.$$

I, reduint mòdul 2, tenint en compte $p \equiv -1, a+1 \equiv a-1 \pmod 2$, i $\sum_{k=1}^{(p-1)/2} k = (p^2-1)/8$,

$$m \equiv (a-1)\frac{p^2-1}{8} + \sum_{k=1}^{(p-1)/2}\left[\frac{ka}{p}\right].$$

□

Demostració de la llei de reciprocitat quadràtica.
Si $p = q$, es té $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = 0$ i es compleix trivialment.
Suposem doncs $p \neq q$. Tenim

$$\left(\frac{q}{p}\right) = (-1)^m, \left(\frac{p}{q}\right) = (-1)^n,$$

amb

$$m \equiv \sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right], n \equiv \sum_{k=1}^{(q-1)/2}\left[\frac{kp}{q}\right] \pmod 2.$$

Per tant $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{m+n}$. Volem provar la igualtat

$$\frac{p-1}{2}\frac{q-1}{2} = \sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right] + \sum_{k'=1}^{(q-1)/2}\left[\frac{k'p}{q}\right]. \tag{4.2}$$

Clarament, $\frac{p-1}{2}\frac{q-1}{2}$ és el nombre de parelles (k,k') de nombres enters amb $1 \leq k \leq (p-1)/2, 1 \leq k' \leq (q-1)/2$. Ara $\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]$ és el nombre de parelles (k,k') amb $1 \leq k \leq (p-1)/2, 1 \leq k' \leq (q-1)/2$ i $pk' < qk$, ja que $pk' < qk$ equival a $k' \leq \left[\frac{kq}{p}\right]$ per a k enter entre 1 i $(p-1)/2$. Anàlogament, $\sum_{k'=1}^{(q-1)/2}\left[\frac{k'p}{q}\right]$ és el nombre de parelles (k,k') amb $1 \leq k \leq (p-1)/2, 1 \leq k' \leq (q-1)/2$ i $pk' > qk$. Com no pot ser $pk' = qk$, obtenim la igualtat (4.2). □

4.7 Símbol de Jacobi.

Veiem ara una generalització del símbol de Legendre. Si P és un nombre enter positiu senar, $P = p_1^{r_1} \dots p_s^{r_s}$ la seva descomposició en producte de primers, definim el *símbol de Jacobi*

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)^{r_1} \dots \left(\frac{a}{p_s}\right)^{r_s}, \tag{4.3}$$

per a a enter qualsevol, on $\left(\frac{a}{p_i}\right)$, és el símbol de Legendre, $1 \leq i \leq s$.

Proposició 4.7.1. *Siguin P, P_1, P_2 nombres enters senars, a, a_1, a_2 nombres enters qualssevol*

a) si $\mathrm{mcd}(a, P) > 1$, *aleshores* $\left(\frac{a}{P}\right) = 0$,

b) si $\mathrm{mcd}(a, P) = 1$, *aleshores* $\left(\frac{a}{P}\right) = \pm 1$,

c) $a_1 \equiv a_2 \pmod{P} \Rightarrow \left(\frac{a_1}{P}\right) = \left(\frac{a_2}{P}\right)$,

d) $\left(\frac{a}{P_1 P_2}\right) = \left(\frac{a}{P_1}\right)\left(\frac{a}{P_2}\right)$ *i* $\left(\frac{a_1 a_2}{P}\right) = \left(\frac{a_1}{P}\right)\left(\frac{a_2}{P}\right)$.

Demostració. a) Si $\mathrm{mcd}(a, P) > 1$, a és divisible per un primer p_i dividint P i per tant $\left(\frac{a}{p_i}\right) = 0$ i $\left(\frac{a}{P}\right) = 0$, per (4.3).
b) Si $\mathrm{mcd}(a, P) = 1$, a no és divisible per cap dels primer p_i dividint P i per tant $\left(\frac{a}{p_i}\right) = \pm 1$, per a $i = 1, \dots s$ i $\left(\frac{a}{P}\right) = \pm 1$, per (4.3).
c) Si $a_1 \equiv a_2 \pmod{P}$, aleshores $a_1 \equiv a_2 \pmod{p_i}$ per a cada primer p_i dividint P i per tant $\left(\frac{a_1}{p_i}\right) = \left(\frac{a_2}{p_i}\right)$, per a $i = 1, \dots, s$ per 4.6.1 1), i $\left(\frac{a_1}{P}\right) = \left(\frac{a_2}{P}\right)$, per (4.3).
d) a partir de (4.3) i el fet que, el producte de les descomposicions en producte de primers de P_1 i P_2 dóna la del seu producte, obtenim la primera igualtat. La segona ve de la igualtat $\left(\frac{a_1 a_2}{p_i}\right) = \left(\frac{a_1}{p_i}\right)\left(\frac{a_2}{p_i}\right)$ per a $i = 1, \dots, s$ (4.6.1 2)) i (4.3). □

Volem veure ara que pel símbol de Jacobi el valor en -1 i 2 s'obté amb les mateixes fòrmules que pel de Legendre i que és vàlida la llei de reciprocitat quadràtica.

Lema 4.7.2. *Si P és un enter natural senar, posem*

$$\varepsilon(P) = \frac{P-1}{2},\ \omega(P) = \frac{P^2-1}{8}.$$

Si P_1, P_2 són enters naturals senars, tenim

$$\begin{aligned} \varepsilon(P_1P_2) &\equiv \varepsilon(P_1) + \varepsilon(P_2) \pmod 2 \\ \omega(P_1P_2) &\equiv \omega(P_1) + \omega(P_2) \pmod 2. \end{aligned}$$

Demostració. Si P_1 i P_2 són senars, tenim $(P_1-1)(P_2-1) \equiv 0 \pmod 4$. Efectuant $(P_1-1)(P_2-1) = P_1P_2 - P_2 - P_1 + 1 = (P_1P_2-1) - (P_2-1) - (P_1-1)$. Tenim doncs $(P_1P_2-1) - (P_2-1) - (P_1-1) \equiv 0 \pmod 4$ i, per tant,

$$\frac{P_1P_2-1}{2} - \frac{P_2-1}{2} - \frac{P_1-1}{2} \equiv 0 \pmod 2.$$

Ara P_1 senar $\Rightarrow P_1^2 \equiv 1 \pmod 8$. Per tant $(P_1^2-1)(P_2^2-1) \equiv 0 \pmod{64}$. Efectuant $(P_1^2-1)(P_2^2-1) = P_1^2P_2^2 - P_2^2 - P_1^2 + 1 = (P_1^2P_2^2-1) - (P_2^2-1) - (P_1^2-1)$. Per tant $(P_1^2P_2^2-1) - (P_2^2-1) - (P_1^2-1) \equiv 0 \pmod{64}$ que implica

$$\frac{P_1^2P_2^2-1}{8} - \frac{P_2^2-1}{8} - \frac{P_1^2-1}{8} \equiv 0 \pmod 8.$$

□

Corol·lari 4.7.3. *Si $P = p_1^{r_1} \dots p_s^{r_s}$ és la descomposició en producte de primers de l'enter positiu senar P, tenim*

$$\varepsilon(P) \equiv \sum_{i=1}^{s} r_i\varepsilon(p_i),\ \omega(P) \equiv \sum_{i=1}^{s} r_i\omega(p_i) \pmod 2.$$

Demostració. Es prova per inducció a partir del lema anterior.

Proposició 4.7.4. *a) (Llei de reciprocitat quadràtica) Siguin P, Q nombres enters, positius i senars. Es compleix*

$$\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}} \left(\frac{Q}{P}\right).$$

b) Si P és un nombre enter positiu senar

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}, \ \left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$$

Demostració. Si $P = \prod_{i=1}^{s} p_i^{r_i}, Q = \prod_{j=1}^{t} q_j^{v_j}$ són les descomposicions en producte de primers de P i Q, tenim

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{t} \left(\frac{P}{q_j}\right)^{v_j} = \prod_{j=1}^{t} \prod_{i=1}^{s} \left(\frac{p_i}{q_j}\right)^{r_i v_j},$$

aplicant (4.3) i 4.6.1 2). Ara

$$\left(\frac{p_i}{q_j}\right) = (-1)^{\varepsilon(p_i)\varepsilon(q_j)} \left(\frac{q_j}{p_i}\right),$$

per 4.6.5. Per tant

$$\begin{aligned}
\left(\frac{P}{Q}\right) &= \prod_{j=1}^{t} \prod_{i=1}^{s} \left((-1)^{\varepsilon(p_i)\varepsilon(q_j)} \left(\frac{q_j}{p_i}\right)\right)^{r_i v_j} \\
&= \prod_{j=1}^{t} \left(((-1)^{\sum_{i=1}^{s} r_i \varepsilon(p_i)})^{v_j \varepsilon(q_j)} \left(\prod_{i=1}^{s} \left(\frac{q_j}{p_i}\right)^{r_i}\right)^{v_j}\right) \\
&= \prod_{j=1}^{t} ((-1)^{\varepsilon(P)})^{v_j \varepsilon(q_j)} \left(\frac{q_j}{P}\right)^{v_j} \\
&= ((-1)^{\varepsilon(P)})^{\sum_{j=1}^{t} v_j \varepsilon(q_j)} \prod_{j=1}^{t} \left(\frac{q_j}{P}\right)^{v_j} \\
&= (-1)^{\varepsilon(P)\varepsilon(Q)} \left(\frac{Q}{P}\right),
\end{aligned}$$

aplicant el corol·lari 4.7.3 i de nou (4.3) i 4.6.1 2).
Anàlogament, b) es prova a partir de (4.3), 4.6.3, 4.6.4 i el corol·lari 4.7.3. □

Observacions.

1. Si P és un enter senar, a un enter qualsevol, no és cert en general que $\left(\frac{a}{P}\right)+1$ sigui el nombre de solucions de la congruència $x^2 \equiv a \pmod{P}$, com teníem pel símbol de Legendre. En efecte, tenim, per exemple $\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right)^2 = 1$ però $x^2 \equiv 2 \pmod{9}$ no té solucions ja que $x^2 \equiv 2 \pmod{3}$ no en té.

2. No és cert en general $\left(\frac{a}{P}\right) \equiv a^{(P-1)/2} \pmod{P}$. En efecte, tenim $\left(\frac{2}{9}\right) = 1$, $2^{(9-1)/2} = 2^4 = 16 \not\equiv 1 \pmod{9}$.

   Tampoc no és cert $\left(\frac{a}{P}\right) \equiv a^{\varphi(P)/2} \pmod{P}$. En el mateix exemple, tenim $\varphi(9) = 6, 2^{\varphi(9)/2} = 2^3 = 8 \not\equiv 1 \pmod{9}$.

Exercici. Sabent que 9907 és primer, calculeu $\left(\frac{1001}{9907}\right)$, primer usant el símbol de Legendre i després usant el símbol de Jacobi.

1) Amb el símbol de Legendre:

$$\left(\frac{1001}{9907}\right) = \left(\frac{7}{9907}\right)\left(\frac{11}{9907}\right)\left(\frac{13}{9907}\right),$$

pel punt 2. de 4.6.1.
Calculem cada un dels factors, aplicant 4.6.5.

$$\left(\frac{7}{9907}\right) = -\left(\frac{9907}{7}\right) = -\left(\frac{2}{7}\right) = -1$$

$$\left(\frac{11}{9907}\right) = -\left(\frac{9907}{11}\right) = -\left(\frac{7}{11}\right) = \left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = 1$$

$$\left(\frac{13}{9907}\right) = \left(\frac{9907}{13}\right) = \left(\frac{1}{13}\right) = 1$$

Obtenim

$$\left(\frac{1001}{9907}\right) = -1$$

2) Amb el símbol de Jacobi:

$$\begin{aligned}\left(\frac{1001}{9907}\right) &= \left(\frac{9907}{1001}\right) = \left(\frac{898}{1001}\right) = \left(\frac{2}{1001}\right)\left(\frac{449}{1001}\right) = \left(\frac{449}{1001}\right) = \left(\frac{1001}{449}\right) \\ &= \left(\frac{103}{449}\right) = \left(\frac{449}{103}\right) = \left(\frac{37}{103}\right) = \left(\frac{103}{37}\right) = \left(\frac{29}{37}\right) = \left(\frac{37}{29}\right) = \left(\frac{8}{29}\right) \\ &= \left(\frac{2}{29}\right) = -1,\end{aligned}$$

aplicant 4.7.4.
L'us del símbol de Jacobi evita haver de factoritzar abans d'aplicar la llei de reciprocitat quadràtica. Com no es coneix cap algoritme de factorització d'enters en temps polinomial, el càlcul amb el símbol de Jacobi és més ràpid.

Capítol 5

Aplicacions

5.1 Tests de primeritat

5.1.1 Test de Solovay-Strassen

Pel petit teorema de Fermat, tenim, per un enter n,

$$n \text{ primer} \quad \Rightarrow a^{n-1} \equiv 1 \pmod{n} \text{ per a tot enter } a \text{ primer amb } n. \tag{5.1}$$

Per tant, si, donat un enter n, trobem un enter a primer amb n tal que $a^{n-1} \not\equiv 1 \pmod{n}$, podem assegurar que n no és primer. En canvi, la implicació contrària de (5.1) no és certa. Un contraexemple és $n = 561$: tenim $561 = 3 \times 11 \times 17$, per tant 561 no és primer, i es compleix $a^{560} \equiv 1 \pmod{561}$ per a tot enter a primer amb 561. En efecte, aplicant el petit teorema de Fermat a $3, 11$ i 17, obtenim, per a tot enter a primer amb 561 (observem que si a primer amb 561, aleshores és primer amb $3, 11$ i 17),

$$\begin{aligned} a^2 &\equiv 1 \pmod{3} \Rightarrow a^{560} = (a^2)^{280} \equiv 1 \pmod{3}, \\ a^{10} &\equiv 1 \pmod{11} \Rightarrow a^{560} = (a^{10})^{56} \equiv 1 \pmod{11}, \\ a^{16} &\equiv 1 \pmod{17} \Rightarrow a^{560} = (a^{16})^{35} \equiv 1 \pmod{17}. \end{aligned}$$

Ara

$$\left.\begin{aligned} a^{560} &\equiv 1 \pmod{3} \\ a^{560} &\equiv 1 \pmod{11} \\ a^{560} &\equiv 1 \pmod{17} \end{aligned}\right\} \Rightarrow a^{560} \equiv 1 \pmod{3 \times 11 \times 17 = 561}.$$

La proposició següent dóna una condició necessària i suficient per a que un enter natural senar sigui primer.

Proposició 5.1.1. *Sigui $m > 1$ un nombre enter senar. L'enter m és primer si i només si es compleix*

$$b^{\frac{m-1}{2}} \cdot \left(\frac{b}{m}\right) \equiv 1 \pmod{m},$$

per a tot enter b primer amb m.

Demostració. Si m és primer, pel criteri d'Euler 4.6.2, la congruència és certa per a tot enter b primer amb m.
Veiem ara que, si m no és primer, podem trobar un enter b primer amb m pel qual no sigui certa. Distingim dos casos.

1. m és divisible pel quadrat d'un nombre primer senar p.

   Posem $m = p^v n$, amb $v \geq 2, p \nmid n$. Sigui g una arrel primitiva mòdul p^v. Pel teorema xinès dels residus, existeix un enter b tal que

   $$b \equiv g^{p^{v-2}(p-1)} \pmod{p^v} \text{ i } b \equiv 1 \pmod{n}.$$

   Com $p-1$ és parell, b és quadrat mòdul p^v i per tant mòdul p; tenim doncs $\left(\frac{b}{p}\right) = 1$. Com $b \equiv 1 \pmod{n}$, tenim $\left(\frac{b}{n}\right) = 1$. Obtenim doncs

   $$\left(\frac{b}{m}\right) = \left(\frac{b}{p}\right)^v \left(\frac{b}{n}\right) = 1.$$

   Ara $b \equiv 1 \pmod{n} \Rightarrow b^{(m-1)/2} \equiv 1 \pmod{n}$. Com g és arrel primitiva mòdul p^v, el seu ordre mòdul p^v és $\varphi(p^v) = p^{v-1}(p-1)$. Aplicant 4.5.10, obtenim que b té ordre p mòdul p^v. Per tant, $b^{(m-1)/2} \not\equiv 1 \pmod{p^v}$ ja que $p \nmid (m-1)/2$. Tenim doncs

   $$b^{(m-1)/2} \not\equiv 1 \pmod{m}$$

   i, per tant

   $$b^{(m-1)/2} \cdot \left(\frac{b}{m}\right) \not\equiv 1 \pmod{m}.$$

2. m és producte de 2 o més nombres primers senars diferents.

   Posem $m = pn$ amb $p \nmid n$. Com que el nombre d'elements de $(\mathbb{Z}/p)^*$ que són quadrats és $(p-1)/2$, podem escollir b no quadrat mòdul p. Pel teorema xinès dels residus, podem escollir b satisfent a més $b \equiv 1 \pmod{n}$. Tenim doncs

   $$\left(\frac{b}{p}\right) = -1, \left(\frac{b}{n}\right) = 1$$

   que implica

   $$\left(\frac{b}{m}\right) = \left(\frac{b}{p}\right) \cdot \left(\frac{b}{n}\right) = -1.$$

   D'altra banda, $b \equiv 1 \pmod{n} \Rightarrow b^{(m-1)/2} \equiv 1 \pmod{n}$. Tenim doncs $b^{(m-1)/2} \not\equiv \left(\frac{b}{m}\right) \pmod{n}$ i, per tant $b^{(m-1)/2} \not\equiv \left(\frac{b}{m}\right) \pmod{m}$. □

Volem usar la proposició 5.1.1 per obtenir un test de primeritat.

Observació. Si m és un enter senar compost i calculem

$$b^{\frac{m-1}{2}} \cdot \left(\frac{b}{m}\right) \pmod{m}$$

per a b primer amb m, el resultat és $\not\equiv 1$ per al menys la meitat dels valors de b mòdul m. En efecte, si m no és primer, existeix b primer amb m tal que

$$b^{\frac{m-1}{2}} \cdot \left(\frac{b}{m}\right) \not\equiv 1 \pmod{m}.$$

Ara, per a cada enter a, primer amb m, tal que

$$a^{\frac{m-1}{2}} \cdot \left(\frac{a}{m}\right) \equiv 1 \pmod{m},$$

tindrem

$$(ab)^{\frac{m-1}{2}} \cdot \left(\frac{ab}{m}\right) \not\equiv 1 \pmod{m}.$$

Com $ab \equiv a'b \pmod{m} \Rightarrow a \equiv a' \pmod{m}$, per a cada enter a, determinat mòdul m, pel qual la congruència és certa, en tenim un pel qual la congruència no és certa.
Obtenim doncs que, si m no és primer i triem a l'atzar un enter b primer amb m, la probabilitat que es compleixi la congruència

$$b^{(m-1)/2} \cdot \left(\frac{b}{m}\right) \equiv 1 \pmod{m} \tag{5.2}$$

és $< 1/2$. Per tant, si triem a l'atzar F enters b primers amb m, amb $1 < b < m-1$, la probabilitat que es compleixi la congruència (5.2) per a tots ells és $< 2^{-F}$. Observem que, per a $b = \pm 1$, es compleix la congruència.

Donem ara l'algoritme del test de Solovay-Strassen. Té com a input un enter senar $m \geq 9$, que es vol determinar si és primer, i un nombre positiu F, que és cota superior pel nombre d'enters b escollits a l'atzar pels quals es comprova si es compleix la congruència (5.2).

Test de Solovay-Strassen.

1. Llegir m i F
2. Si és $F = 0$, escriure "m és probablement primer" i acabar
3. Triar a l'atzar un enter b, amb $2 \leq b \leq m-2$
4. Calcular $x := b^{(m-1)/2} \pmod{m}$
5. Si $x \not\equiv \pm 1 \pmod{m}$, escriure "m és compost" i acabar
6. Calcular el símbol de Jacobi $y := \left(\frac{b}{m}\right)$
7. Si $x \not\equiv y \pmod{m}$, escriure "m és compost" i acabar
8. Fer $F = F - 1$ i tornar a 2).

Per a cada enter b, $2 \leq b \leq m-2$, triat a l'atzar l'algoritme calcula $b^{(m-1)/2} \pmod{m}$. Si el resultat no és ± 1, es pot concloure que m no és primer pel petit teorema de Fermat. En cas contrari, l'algoritme calcula el símbol de Jacobi $\left(\frac{b}{m}\right)$.

Si no es compleix la congruència (5.2), es pot concloure que m no és primer per la proposició 5.1.1. Si per F valors de b triats a l'atzar, es compleix la congruència (5.2), tenim una probabilitat alta que m sigui primer.

5.1.2 Certificats de primeritat

Veurem la caracterització dels nombres primers mitjançant l'existència d'arrels primitives. Necessitem el següent lema previ sobre la funció φ d'Euler.

Lema 5.1.2. *Sigui n un enter positiu. Aleshores n és primer si i només si $\varphi(n) = n - 1$.*

Demostració. Ja vam veure $\varphi(p) = p-1$, per a p primer positiu. Suposem ara que n no és primer. Aleshores o bé $n = 1$ o bé n és compost. Tenim $\varphi(1) = 1$. Ara, si n és compost, té un divisor d amb $1 < d < n$, per tant al menys un dels $n-1$ enters $1, 2, \ldots, n-1$ no és primer amb n i per tant $\varphi(n) \leq n - 2$. □

Teorema 5.1.3 (de Lucas)**.** *Si n és un enter positiu i existeix un enter a tal que*

$$a^{n-1} \equiv 1 \pmod{n} \ i \ a^{(n-1)/p} \not\equiv 1 \pmod{n}$$

per a tot primer p dividint $n-1$, aleshores n és primer.

Demostració. Com $a^{n-1} \equiv 1 \pmod{n}$, l'ordre $ord_n a$ de a a $(\mathbb{Z}/n)^*$ divideix $n-1$ per 4.5.9. Volem veure que és igual a $n-1$. Suposem $ord_n a \neq n-1$. Aleshores, existeix un enter $d > 1$ tal que $n - 1 = d \cdot ord_n a$. Sigui p un divisor primer de d. Tenim

$$a^{(n-1)/p} = a^{(d \cdot ord_n a/p} = (a^{ord_n a})^{d/p} \equiv 1 \pmod{n}$$

que contradiu la hipòtesi del teorema $a^{(n-1)/p} \not\equiv 1 \pmod{n}$ per a tot primer p dividint $n-1$. Tenim doncs $ord_n a = n-1$. Com $ord_n a$ divideix $\varphi(n)$, per 4.5.7, i $\varphi(n) \leq n-1$, obtenim $\varphi(n) = n-1$ i, pel lema, n és primer. □

Exemple. Sigui $n = 2029$. Els divisors primers de 2028 són $2, 3$ i 13. Tenim

$$2^{2028} \equiv 1 \pmod{2029}, 2^{1014} \equiv -1 \pmod{2029},$$
$$2^{676} \equiv 975 \pmod{2029}, 2^{156} \equiv 302 \pmod{2029}.$$

Aplicant el teorema obtenim que 2029 és primer.

Observació. Si n és primer, una arrel primitiva mòdul n satisfà les condicions de l'enter a del teorema de Lucas.

Corol·lari 5.1.4. *Si n és un enter positiu senar i a un enter positiu tal que*

$$a^{(n-1)/2} \equiv -1 \pmod{n} \ i \ a^{(n-1)/p} \not\equiv 1 \pmod{n}$$

per a tot divisor primer senar p de $n-1$, aleshores n és primer.

Demostració. Tenim $a^{(n-1)/2} \equiv -1 \pmod{n} \Rightarrow a^{n-1} \equiv 1 \pmod{n}$ per tant es compleixen les hipòtesis del teorema. □

Exemple Sigui $n = 3001$. Els divisors primers senars de 3000 són 3 i 5. Tenim

$$14^{1500} \equiv -1 \pmod{3001}, 14^{1000} \equiv 934 \pmod{3001}, 14^{600} \equiv 1998 \pmod{3001}.$$

Aplicant el corol·lari obtenim que 3001 és primer.

A partir del corol·lari 5.1.4, podem determinar si un enter n donat és primer, si coneixem els divisors primers de $n-1$, fent servir l'algoritme següent. Aquest algoritme intenta trobar un enter a complint les condicions del corol·lari fent tries aleatòries. Té com a dades un enter n senar més gran que 3, els divisors primers de $n-1$ i el nombre K, que és una cota del nombre de tries que es volen fer.

Algoritme.

1. Llegir n, K i els divisors primers p_i, $1 \leq i \leq r$, de $n-1$, amb $p_1 = 2$.
2. Si és $K < 1$, escriure que potser n és compost i acabar.
3. escollir a l'atzar un enter a tal que $2 \leq a \leq n-2$.
4. Calcular $x := a^{(n-1)/2} \pmod{n}$
5. Si $x \not\equiv -1 \pmod{n}$, fer $K = K - 1$ i tornar al pas 2.
6. Fer $i = 2$
7. Si és $i > r$, escriure que n és primer, escriure a i acabar.
8. Calcular $x := a^{(n-1)/p_i} \pmod{n}$

9. Si és $x \equiv 1 \pmod{n}$, fer $K = K - 1$ i tornar al pas 2.

10. Fer $i = i + 1$ i tornar al pas 7.

Observació. Si $n > 3$ és un nombre primer, el nombre d'arrels primitives mòdul n és $\varphi(n-1)$. Per tant la probabilitat que un enter a escollit a l'atzar en l'interval $2 \leq a \leq n-2$ sigui arrel primitiva mòdul n és

$$\frac{\varphi(n-1)}{n-3} > \frac{\varphi(n-1)}{n-1} = \prod_{p|n-1} \left(1 - \frac{1}{p}\right).$$

El test és doncs probabilístic ja que no podem assegurar que trobarem una arrel primitiva. D'altra banda, si $n-1$ és divisible per pocs primers o per primers grans, aquesta probabilitat no és gaire petita.

Observació. Si l'algoritme anterior ens retorna un enter a amb les condicions del corol·lari 5.1.4, podem certificar que n és primer donant els divisors primers $p_1, \ldots, p_r$ de $n-1$ i l'enter a. La persona a qui proporcionem aquestes dades pot comprovar que $p_1, \ldots, p_r$ són efectivament tots els divisors primers de $n-1$ fent divisions successives i que l'enter a compleix les condicions del corol·lari 5.1.4.

5.1.3 Nombres de Mersenne. Test de Lucas-Lehmer

Un *nombre de Mersenne* és un enter de la forma $2^p - 1$, amb p enter. Posem

$$M_p = 2^p - 1.$$

Un *primer de Mersenne* és un nombre de Mersenne primer.

Proposició 5.1.5. *Si M_p és primer, aleshores p és primer.*

Demostració. Suposem que p és compost. Si $p = mn$, amb $1 < m, n < p$, a partir de la identitat $X^n - 1 = (X-1)(X^{n-1} + X^{n-2} + \cdots + X + 1)$, tenim la igualtat $2^p - 1 = 2^{mn} - 1 = (2^m)^n - 1 = (2^m - 1)(2^{m(n-1)} + 2^{m(n-2)} + \cdots + 2^m + 1)$, que és una factorització no trivial de M_p, per tant M_p és compost.

Exemples. $M_2 = 2^2 - 1 = 3, M_3 = 2^3 - 1 = 7, M_5 = 2^5 - 1 = 31, M_7 = 2^7 - 1 = 127$ són primers; $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ no és primer.

Per saber si un nombre de Mersenne és primer, s'usa el test de Lucas-Lehmer.

Teorema 5.1.6 (Test de Lucas-Lehmer)**.** *Considerem la successió* $\{e_n\}_{n\geq 1}$ *definida per inducció per les fòrmules*

$$e_1 := 4,\ e_{n+1} := e_n^2 - 2.$$

Sigui $p > 2$ *un nombre primer. El nombre de Mersenne* M_p *és primer si i només si se satisfà la congruència*

$$e_{p-1} \equiv 0 \pmod{M_p}.$$

Demostració. Veure A. Travesa, "Aritmètica" VII.5.

Si p és gran, el test de Lucas-Lehmer determina si M_p és primer en un temps inferior al dels tests de primeritat aplicables a qualsevol tipus d'enters. Per aquesta raò, els primers més grans que es coneixen són primers de Mersenne. El primer de Mersenne més gran conegut actualment és $2^{42643801} - 1$ que té 12837064 xifres decimals (veure Great Internet Mersenne Prime Search, www.mersenne.org).

5.2 Algoritmes de factorització

5.2.1 Mètode de Fermat

El mètode de factorització de Fermat es basa en el resultat següent.

Proposició 5.2.1. *Sigui* $m > 1$ *un nombre enter senar. Considerem els conjunts*

$$A = \{(a,b) \in \mathbb{N}\times\mathbb{N} : m = ab \ i\ \ 1 \leq b \leq a\},$$
$$X = \{(x,y) \in \mathbb{N}\times\mathbb{N} : m = x^2 - y^2 \ i\ \ 0 \leq y < x\}.$$

Les assignacions

$$(a,b) \mapsto (\frac{a+b}{2}, \frac{a-b}{2}),\ (x,y) \mapsto (x+y, x-y)$$

defineixen aplicacions entre A *i* X*, bijectives i inverses una de l'altra.*

Demostració. Sigui $(a,b) \in A$. Com m és senar i $m = ab$, a i b són tots dos senars i per tant $x = (a+b)/2, y = (a-b)/2$ són enters. Com $1 \leq b \leq a$, tenim $0 \leq y < x$. A més $x^2 - y^2 = ((a+b)^2 - (a-b)^2)/4 = ab = m$. Per tant $(a,b) \mapsto ((a+b)/2, y = (a-b)/2)$ defineix una aplicació f de A en X.

Sigui ara $(x, y) \in X$. Com $0 \leq y < x$, tenim $1 \leq b = x - y \leq a = x + y$. Tenim $ab = (x + y)(x - y) = x^2 - y^2 = m$. Per tant $(x, y) \mapsto (x + y, x - y)$ defineix una aplicació g de X en A.
Veiem ara que les dues aplicacions són inverses una de l'altra. En efecte $g(f(a, b)) = g((a+b)/2, (a-b)/2) = ((a+b+a-b)/2, (a+b-a+b)/2) = (a, b)$ i $f(g(x, y)) = f(x + y, x - y) = ((x + y + x - y)/2, (x + y - x + y)/2) = (x, y)$. □

El mètode de factorització de Fermat busca solucions de l'equació $m = x^2 - y^2$, amb x, y enters. Posem $x = [\sqrt{n}] + 1$ ([ ] indica part entera), $y = 1$ i calculem

$$t := m - x^2 + y^2.$$

Si $t = 0$, tenim una factorització no trivial $m = (x+y)(x-y)$. Si $t > 0$, augmentem x en 1. Si $t < 0$, augmentem y en 1. Procedim d'aquesta manera fins a obtenir $t = 0$.

Exemple. Factoritzem 8439 amb el mètode de Fermat. Tenim $91 < \sqrt{8439} < 92$, per tant prenem $x = 92, y = 1$. Fem els càlculs

$$\begin{aligned}
8439 - 92^2 + 1^2 &= -24 < 0 \\
8439 - 92^2 + 2^2 &= -21 < 0 \\
8439 - 92^2 + 3^2 &= -16 < 0 \\
8439 - 92^2 + 4^2 &= -9 < 0 \\
8439 - 92^2 + 5^2 &= 0
\end{aligned}$$

Obtenim doncs $8439 = 92^2 - 5^2 = (92 + 5)(92 - 5) = 97 \cdot 87$.

Factoritzem ara 9379. Tenim $96 < \sqrt{9379} < 97$, per tant prenem $x = 97, y = 1$. Fem els càlculs

$$\begin{aligned}
9379 - 97^2 + 1^2 &= -29 < 0 \\
9379 - 97^2 + 2^2 &= -26 < 0 \\
9379 - 97^2 + 3^2 &= -21 < 0 \\
9379 - 97^2 + 4^2 &= -14 < 0 \\
9379 - 97^2 + 5^2 &= -5 < 0 \\
9379 - 97^2 + 6^2 &= 6 > 0 \\
9379 - 98^2 + 6^2 &= -189 < 0 \\
9379 - 98^2 + 7^2 &= -176 < 0 \\
9379 - 98^2 + 8^2 &= -161 < 0 \\
9379 - 98^2 + 9^2 &= -144 < 0
\end{aligned}$$

$$\begin{aligned} 9379 - 98^2 + 10^2 &= -125 < 0 \\ 9379 - 98^2 + 11^2 &= -104 < 0 \\ 9379 - 98^2 + 12^2 &= -81 < 0 \\ 9379 - 98^2 + 13^2 &= -56 < 0 \\ 9379 - 98^2 + 14^2 &= -29 < 0 \\ 9379 - 98^2 + 15^2 &= 0 \end{aligned}$$

Obtenim doncs $9379 = 98^2 - 15^2 = (98 + 15)(98 - 15) = 113 \cdot 83$.

El mètode de Fermat és efectiu només quan l'enter m és producte de dos factors propers.

5.2.2 Algoritme p-1 de Pollard

Proposició 5.2.2. *Sigui $m > 1$ un nombre enter compost, p un divisor primer de m, k un múltiple de $p - 1$, a un enter primer amb m. Aleshores*

$$\mathrm{mcd}(a^k - 1, m) > 1.$$

Demostració. Com $\mathrm{mcd}(a, m) = 1$, p no divideix a. Pel petit teorema de Fermat, tenim doncs $a^{p-1} \equiv 1 \pmod{p}$, que implica $a^k \equiv 1 \pmod{p}$, és a dir $p \mid a^k - 1$. Com per hipòtesi p divideix m, tenim $p \mid \mathrm{mcd}(a^k - 1, m)$ i per tant $\mathrm{mcd}(a^k - 1, m) > 1$. □

A partir d'aquest resultat, dissenyem l'algoritme següent per factoritzar l'enter m.

Algoritme p-1 de Pollard

1. Escollir un enter k que sigui múltiple de tots els enters més petits o iguals que una cota K. Per exemple $k = K!$ o $k = \mathrm{mcm}(\{n \in \mathbb{N} : n \leq K\})$.

2. Escollir un enter a entre 2 i $m - 2$. Per exemple $a = 2$ o bé a triat aleatòriament.

3. Calcular a^k mòdul m amb l'algoritme binari d'exponenciació.

4. Calcular $d = \mathrm{mcd}(a^k - 1, m)$ amb l'algoritme d'Euclides, amb el valor de a^k mòdul m calculat en el pas anterior.

5. Si $d = 1$ o bé $d = m$ escriure "no s'ha pogut factoritzar m" i acabar

6. Escriure "d".

Observacions. Si r és residu de la divisió entera de a^k entre m, $r \equiv a^k \pmod{m}$, per tant $r-1 \equiv a^k - 1 \pmod{m}$ i $\mathrm{mcd}(a^k-1, m) = \mathrm{mcd}(r-1, m)$.
Si m té algun divisor primer p tal que $p-1$ és divisible per factors primers petits, aquest algoritme factoritza l'enter m.

Exemple 1. Apliquem l'algoritme de Pollard a l'enter $m = 540143$. Prenem $K = 8, k = \mathrm{mcm}(1,2,3,4,5,6,7,8) = 840, a = 2$. Tenim

$$a^{840} \equiv 53047 \pmod{m},\ \mathrm{mcd}(m, 53046) = 421.$$

Obtenim doncs la factorització de m:

$$m = 421 \times 1283.$$

Observem que $420 = 2^2 \times 3 \times 5 \times 7$, és a dir té factors primers petits. L'enter k que hem escollit és un múltiple de 420 i per això hem pogut factoritzat m.

Exemple 2. Considerem l'enter $m = 491389$. Tenim $m = 383 \times 1283$, amb $382 = 2 \times 191, 1282 = 2 \times 641$, on $191, 641$ són primers. En aquest cas, l'enter m no té cap divisor primer p tal que $p-1$ tingui només factors primers petits. Considerant el divisor primer $p = 383$, per factoritzar m amb el mètode de Pollard, hauríem de prendre $K \geq 191$ per tal de tenim k múltiple de $p - 1 = 382$.

5.3 Criptosistemes de clau privada

5.3.1 Criptosistema de Cèsar

Considerem l'alfabet format per les 26 lletres de A a Z més l'espai en blanc. La xifra de Cèsar, que va ser usada per Juli Cèsar en les seves campanyes militars consisteix en fer còrrer les lletres un nombre determinat k de llocs. Si, per exemple, agafem $k = 5$, transformem cada lletra de l'alfabet en la que té a sota en la taula següent.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
F	G	H	I	J	K	L	M	N	O	P	Q	R	S

O	P	Q	R	S	T	U	V	W	X	Y	Z	
T	U	V	W	X	Y	Z		A	B	C	D	E

El text "JULI CESAR VA CONQUERIR TOTA LA GALIA" queda xifrat com "OZQNEHJXFWE FEHTSVZJWNWEYTYFEQFELFQNF".

Per explicar la xifra de Cèsar de forma rigorosa, assignem a cada lletra de l'alfabet un nombre enter comprès entre 0 i 26,

$$\begin{array}{rcl} A & \mapsto & 0 \\ B & \mapsto & 1 \\ & \dots & \\ Z & \mapsto & 25 \\ & \mapsto & 26 \end{array}$$

Els enters $0, 1, \dots, 26$ són un sistema complet de representants de $\mathbb{Z}/27$. Considerem l'aplicació

$$\begin{array}{rccc} f: & \mathbb{Z}/27 & \to & \mathbb{Z}/27 \\ & a & \mapsto & a+5 \end{array}$$

El xifratge consisteix doncs en assignar a cada lletra del text el seu equivalent numèric, aplicar a aquest l'aplicació f i assignar a cada enter obtingut la lletra de l'alfabet que li correspon. L'aplicació f es diu *transformació xifradora.*
Per desxifrar el missatge xifrat, apliquem la inversa de l'aplicació f

$$\begin{array}{rccc} f^{-1}: & \mathbb{Z}/27 & \to & \mathbb{Z}/27 \\ & a & \mapsto & a-5 \end{array}$$

L'aplicació f^{-1} es diu *transformació desxifradora.* L'enter 5 es diu *clau de xifratge.*
El text inicial (o text en clar) es transforma mitjançant la transformació xifradora en text xifrat, que és el que ens transmet. Per la xifra de Cèsar, si coneixem la clau de xifratge també podem desxifrar.
Si interceptem un text xifrat que sabem que s'ha xifrat amb la xifra de Cèsar, podem endevinar la clau a partir de la freqüència amb que apareix cada lletra. A cada llengua hi ha unes lletres que s'usen més que les altres. En català, les lletres més usades són la E i la A. L'espai en blanc apareix més freqüentment que qualsevol lletra. Si el text xifrat és suficientment llarg i comptem quantes vegades hi apareix cada lletra, podem pensar que la lletra que hi apareix més correspon a una lletra freqüent en l'idioma utilitzat i determinar la clau.

Exercici. Considerem el text xifrat següent
"TIHEQNZIHLMHKM-IZHKWV-Q-AMQEHMVHNMZHKWZZMZHTM-HTTM
AZM-HBVHVWUJZMHLMAMZUQVIAHLMHTTWK-"
on - indica l'espai en blanc. Comptem quantes vegades hi apareix cada lletra. Tenim

A	B	C	D	E	F	G	H	I	J	K	L	M	N
4	1	0	0	2	0	0	14	4	1	4	3	13	2

O	P	Q	R	S	T	U	V	W	X	Y	Z	-
0	0	4	0	O	6	2	5	4	0	0	9	6

Per tant la lletra més freqüent és la H. Podem pensar doncs que correspon a l'espai en blanc, és a dir que la clau de xifratge és 8. Aplicant la transformació desxifradora $a \mapsto a - 8$, obtenim el text en clar:
"LA XIFRA DE CESAR CONSISTEIX EN FER CORRER LES LLETRES UN NOMBRE DETERMINAT DE LLOCS"

En comptes d'assignar un valor numèric a cada lletra de l'alfabet, podem trencar el text en clar en blocs de k lletres i assignar un valor numèric a cada bloc. Aquests blocs es diuen *unitats de missatge*. Si tenim un alfabet de N lletres, a cada unitat de missatge $a_1 \dots a_k$ li fem correspondre $N^{k-1}a_1 + \dots Na_{k-1} + a_k$, es a dir l'enter que té $a_1 \dots a_k$ com a xifres en base N. És un enter comprès entre 0 i $N^k - 1$.

Exemple. Suposem que tenim l'alfabet format per 26 lletres (les 26 lletres A-Z) i considerem dígrafs, és a dir unitats de missatge de 2 lletres. Aleshores l'assignació de valors numèrics als dígrafs és

$$\begin{aligned}
\text{AA} &\mapsto (00)_{26} = 0 \\
\text{AB} &\mapsto (01)_{26} = 1 \\
&\vdots \\
\text{AZ} &\mapsto (0(25))_{26} = 25 \\
\text{BA} &\mapsto (10)_{26} = 26 \\
\text{BB} &\mapsto (11)_{26} = 27 \\
&\vdots \\
\text{BZ} &\mapsto (1(25))_{26} = 51 \\
&\vdots \\
\text{ZZ} &\mapsto ((25)(25))_{26} = 25 \times 26 + 25 = 675 = 26^2 - 1
\end{aligned}$$

5.3.2 Criptosistemes afins

Considerem dígrafs com a unitats de missatge. Si l'alfabet consta de N lletres, tenim N^2 dígrafs. Considerem la transformació xifradora

$$\begin{array}{rccl} f: & \mathbb{Z}/N^2 & \to & \mathbb{Z}/N^2 \\ & x & \mapsto & f(x) = ax + b \pmod{N^2} \end{array} \tag{5.3}$$

Per a que f sigui bijectiva, cal que a sigui invertible mòdul N^2, és a dir, $\mathrm{mcd}(a, N) = 1$. La clau del sistema és el parell $(a, b) \in (\mathbb{Z}/N^2)^* \times (\mathbb{Z}/N^2)$. La transformació desxifradora és

$$\begin{array}{rccl} f^{-1}: & \mathbb{Z}/N^2 & \to & \mathbb{Z}/N^2 \\ & y & \mapsto & a^{-1}y - a^{-1}b \pmod{N^2} \end{array}$$

Exemple. Agafem l'alfabet {A,...,Z}. Volem xifrar "ARITMETICA". Primer trenquem el text en dígrafs: AR IT ME TI CA. Les lletres del text tenen els següents valors numérics

$$\text{A} \mapsto 0,\ \text{C} \mapsto 2,\ \text{E} \mapsto 4,\ \text{I} \mapsto 8,\ \text{M} \mapsto 12,\ \text{R} \mapsto 17,\ \text{T} \mapsto 19$$

i, per tant, els dígrafs en tenen els següents

$$\begin{array}{lcl} \text{AR} & \mapsto & 17 \\ \text{IT} & \mapsto & 8 \times 26 + 19 = 227 \\ \text{ME} & \mapsto & 12 \times 26 + 4 = 316 \\ \text{TI} & \mapsto & 19 \times 26 + 8 = 502 \\ \text{CA} & \mapsto & 2 \times 26 + 0 = 52 \end{array}$$

Xifrem amb una transformació afí amb clau (a, b), on $a = 5, b = 2$. Obtenim

$$\begin{array}{lcllcl} f(17) & = & 5 \times 17 + 2 & \equiv 87 \pmod{26^2} & = & ((3)(9))_{26} \\ f(227) & = & 5 \times 227 + 2 & \equiv 461 \pmod{26^2} & = & ((17)(19))_{26} \\ f(316) & = & 5 \times 316 + 2 & \equiv 230 \pmod{26^2} & = & ((8)(22))_{26} \\ f(502) & = & 5 \times 502 + 2 & \equiv 484 \pmod{26^2} & = & ((18)(16))_{26} \\ f(52) & = & 5 \times 52 + 2 & \equiv 262 \pmod{26^2} & = & ((10)(2))_{26} \end{array}$$

Busquem ara els dígrafs corresponents:

$$\begin{array}{lcl} ((3)(9))_{26} & \mapsto & \text{DJ} \\ ((17)(19))_{26} & \mapsto & \text{RT} \\ ((8)(22))_{26} & \mapsto & \text{IW} \\ ((18)(16))_{26} & \mapsto & \text{SQ} \\ ((10)(2))_{26} & \mapsto & \text{KC} \end{array}$$

El missatge xifrat és doncs "DJRTIWSQKC".

Observació. Pot semblar que quan utilitzem un sistema de xifratge afí amb unitats de missatge de més d'una lletra, no es pot desxifrar fent anàlisi de freqüencies com per la xifra de Cèsar. Tantmateix no és així. Suposem que fem servir dígrafs i la transformació xifradora (5.3). Sigui x l'equivalent numèric d'un dígraf i $y = f(x)$. Escrivim x, y en base N, $x = x_1N + x_2, y = y_1N + y_2$. Igualment, per a a i b, posem $a = a_1N + a_2, b = b_1N + b_2$. Tenim

$$\begin{aligned} f(x) &= ax + b = (a_1N + a_2)(x_1N + x_2) + (b_1N + b_2) \\ &= (a_2x_1 + a_1x_2 + b_1)N + a_2x_2 + b_2 \pmod{N^2} \end{aligned}$$

i, per tant, y_2 és la resta de la divisió de $a_2x_2 + b_2$ entre N i depen només de x_2. Podem doncs fer anàlisi de freqüències amb les lletres situades en posició parella per determinar el valor de a_2 i b_2 i després amb les situades en posició senar per determinar a_1 i b_1.

5.3.3 Criptosistema de Vigenère

La xifra de Vigenère intenta evitar l'anàlisi de freqüències combinant xifres de Cèsar amb claus diferents. Suposem que volem xifrar el missatge
EL XIFRATGE VIGENERE COMBINA XIFRES DE CESAR AMB CLAUS DIFERENTS
Considerem l'alfabet {A,...,Z} de 26 lletres, és a dir no tenim en compte els espais en blanc. Dividim el text en blocs de 5 lletres:
ELXIF RATGE VIGEN ERECO MBINA XIFRE SDECE SARAM BCLAU SDIFE RENTS
Xifrem aplicant una xifra de Cèsar a cada lletra d'un bloc $x_0x_1x_2x_3x_4$ amb diferents claus. Fem

$$\begin{aligned} y_0 &= f_0(x_0) = x_0 + 3 \pmod{26} \\ y_1 &= f_1(x_1) = x_1 + 8 \pmod{26} \\ y_2 &= f_2(x_2) = x_2 + 6 \pmod{26} \\ y_3 &= f_3(x_3) = x_3 + 24 \pmod{26} \\ y_4 &= f_4(x_4) = x_4 + 11 \pmod{26} \end{aligned}$$

i prenem $y_0y_1y_2y_3y_4$ com a resultat del xifratge. El text inicial queda xifrat com

HTDGQUIZEPYQMCYHZKAZPJOLLAQLPPVLKAPVIXYXEKRYFVLODPUMTRD

La longitud dels blocs en que dividim el text es diu *periode*. En aquest exemple el periode és 5. Observem que la mateixa lletra es xifra de maneres diferents. Per exemple la primera "E" es xifra com "H" i la "E" de XIFRATGE es xifra com "P". També lletres diferents es poden xifrar amb la mateixa lletra. Per exemple la "N" i la "A" de COMBINA es xifren totes dues com "L".
Vigenère va introduir aquest xifratge l'any 1586. Fins al segle XIX es va considerar indesxifrable. De fet es pot deduïr el periode a partir de combinacions de lletres freqüents, com ara en català "en", "es", "els","que", "per", i després fer anàlisi de freqüències amb les lletres situades en el mateix lloc de cada bloc.

5.4 Criptosistemes de clau pública

En els criptosistemes que hem vist fins ara, si coneixem la clau de xifratge, també podem desxifrar. La seguretat del sistema es basa doncs en amagar la clau. Habitualment, quan s'usa un sistema d'aquest tipus, les claus es canvien amb freqüència.
El 1976, W. Diffie i M. Hellman van descobrir un tipus de criptosistema diferent, el *criptosistema de clau pública*. Un criptosistema de clau pública té la propietat que si algú coneix la clau xifradora no pot trobar la clau desxifradora sense una computació que demana un temps prohibitiu. És a dir la transformació xifradora f no és invertible en un temps de càlcul realístic sense tenir informació addicional. Això permet fer pública la clau xifradora. El criptosistema pot tenir diferents usuaris, cada un amb la seva clau, que es poden publicar, com si fos una guia telefònica. Si algú vol enviar un missatge a l'usuari A, el xifra amb la seva clau xifradora K_A.

5.4.1 Criptosistemes de tipus RSA

El criptosistema RSA, designat per les inicials dels seus creadors Rivest, Shamir i Adleman, és el més conegut dels criptosistemes de clau pública. Es basa en la dificultat computacional per factoritzar enters molt grans.
El funcionament del criptosistema RSA segueix el següent esquema.
Cada usuari escull dos nombres primers p, q molt grans (és a dir d'aproximadament 100 xifres decimals) i efectua $n = pq$. Coneixent la factorització de n, podem calcular la funció φ d'Euler de n

$$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - p - q + 1.$$

Després l'usuari escull un enter e entre 1 i $\varphi(n)$, primer amb $\varphi(n)$, de forma aleatòria. Finalment, calcula l'invers d de e mòdul $\varphi(n)$.
L'usuari fa pública la clau de xifratge $K_X = (n, e)$ i amaga la clau de desxifratge $K_D = d$. La transformació xifradora és

$$\begin{array}{rccc} f: & \mathbb{Z}/n & \to & \mathbb{Z}/n \\ & x & \mapsto & x^e \pmod n \end{array}$$

i la desxifradora

$$\begin{array}{rccc} f^{-1}: & \mathbb{Z}/n & \to & \mathbb{Z}/n \\ & y & \mapsto & y^d \pmod n \end{array}.$$

Les dues aplicacions són efectivament inverses una de l'altra ja que $ed \equiv 1 \pmod{\varphi(n)}$ implica $x^{ed} \equiv x \pmod n$ pel teorema d'Euler 4.5.5. Si p i q estan ben escollits, el càlcul de d no és possible sense conèixer la factorització de n i aquest no es pot realitzar en un temps realístic. En particular, p i q no han de ser propers, per evitar que n es pugui factoritzar amb el mètode de Fermat.

Observació. Definim f sobre $\mathbb{Z}/n$ però cada usuari té una clau amb un valor de n diferent. El procès és el següent. Si tenim un alfabet de N lletres, prenem dos enters positius k, l amb $k < l$ i fem unitats de missatge de k lletres en el text en clar i de l lletres en el text xifrat. Cada usuari escull els seus dos primers p, q de forma a tenir

$$N^k < n = pq < N^l.$$

Aleshores a cada unitat de missatge del text en clar li correspon un enter x amb $0 \leq x < N^k$. Tots aquests enters són diferents mòdul n. Fem $y = f(x)$, definit mòdul n. Com $n < N^l$, y dóna un enter ben determinat mòdul N^l.

Exemple. Agafem $N = 26, k = 3, l = 4$. Tenim $26^3 = 17576 < n < 26^4 = 456976$. Suposem que l'usuari A té la clau xifradora $(n_A, e_A) = (46927, 39423)$ i li volem enviar el missatge "YES". L'equivalent numèric és $24 \times 26^2 + 4 \times 26 + 18 = 16346$. Apliquem la transformació xifradora

$$16346^{39423} \pmod{46927} = 21166.$$

Escrivim l'enter obtingut en base 26

$$21166 = 1 \times 26^3 + 5 \times 26^2 + 8 \times 26 + 2.$$

Passant a lletres de l'alfabet, obtenim "BFIC" que és el missatge que enviem. El receptor A coneix la clau desxifradora $(n_A, d_A) = (46927, 26767)$ i, després d'obtenir l'equivalent numèric de "BFIC", calcula $21166^{26767} \pmod{46927} = 16346$ i obté "YES".

5.4.2 El problema del logaritme discret

Una altra operació aritmètica que té la propietat de no ser calculable en un temps de computació factible és el logaritme discret.

Definició 5.4.1. Siguin m un enter i b un element de $(\mathbb{Z}/m)^*$. El *logaritme discret* d'un element y de $(\mathbb{Z}/m)^*$ en base b és un enter x tal que $b^x = y$.

Exemple. Siguin $m = 19, b = 2$. Tenim que 2 és arrel primitiva mòdul 19, per tant tot element de $(\mathbb{Z}/19)^*$ té logaritme discret en base 2.
Si escrivim les potències de 2 a $(\mathbb{Z}/19)^*$, obtenim

$$2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 13, 2^6 = 7, 2^7 = 14, 2^8 = 9, 2^9 = 18, 2^{10} = 17,$$
$$2^{11} = 15, 2^{12} = 11, 2^{13} = 3, 2^{14} = 6, 2^{15} = 12, 2^{16} = 5, 2^{17} = 10, 2^{18} = 1.$$

Per exemple, $log_2 7 = 6$. El logaritme en base 2 a $(\mathbb{Z}/19)^*$ queda determinat mòdul $\varphi(19) = 18$.
Si prenem $b = 4$, les potències de 4 són

$$4, 4^2 = 16, 4^3 = 7, 4^4 = 9, 4^5 = 17, 4^6 = 11, 4^7 = 6, 4^8 = 5, 4^9 = 1.$$

Per tant $y = 8$ no té logaritme discret en base 4. Per a $y = 7$, tenim $4^3 = 4^{12} = 7$, per tant podem posar $log_4 7 = 3$ i també $log_4 7 = 12$. Per als elements y de $(\mathbb{Z}/19)^*$ que tenen logaritme discret en base 4, aquest està determinat mòdul l'ordre de 4 a $(\mathbb{Z}/19)^*$, que és igual a 9.

Si b és arrel primitiva mòdul m, tot element y de $(\mathbb{Z}/m)^*$ té logaritme discret en base b i, per un element y de $(\mathbb{Z}/m)^*$, $log_b y$ és únic mòdul $\varphi(m)$.

5.4.3 El criptosistema de ElGamal

Comencem fixant un enter m gran i un element b de $(\mathbb{Z}/m)^*$, preferentment que sigui un generador de $(\mathbb{Z}/m)^*$. Recordem que existeixen arrels primitives mòdul m si $m = 2, 4, p^r, 2p^r$ amb p primer senar.

Suposem que usem unitats de missatge en el text en clar amb equivalent numèric $x < m$. Cada usuari A tria a l'atzar un enter a, amb $0 < a < \varphi(m)$. Aquest enter a és la clau secreta de desxiframent. La clau pública de xifratge és l'element $b^a \in (\mathbb{Z}/m)^*$. Per enviar un missatge x a l'usuari A, escollim un enter k a l'atzar i enviem a A la parella d'elements de $\mathbb{Z}/m$

$$(b^k, xb^{ak})$$

Podem calcular b^{ak}, sense conèixer a, fent $(b^a)^k$. Quan rep el missatge, l'usuari A recupera el missatge x a partit de la seva clau secreta a fent

$$xb^{ak} \cdot (b^k)^{-a}$$

Una persona que intercepti el missatge no pot calcular $(b^k)^a$. Per fer-lo, necessitaria un mètode efectiu per calcular el logaritme discret.

5.4.4 Autentificació

En criptografia de clau pública hi ha una manera fàcil d'identificar-se. Suposem que A i B són usuaris del sistema. Siguin f_A, f_B les seves funcions xifradores. Sigui P_A la signatura de A, formada pel nom, cognom i eventualment altres dades personals, com el DNI. Com la clau xifradora de B és pública, una tercera persona podria enviar a B $f_B(P_A)$ i B no sabria que no és A qui li envia el missatge. Per a que B pugui tenir la certesa que el missatge ve de A, l'usuari A li envia $f_B(f_A^{-1}(P_A))$ al principi o al final del seu missatge. La resta del missatge la xifra simplement aplicant-li f_B. Quan B rep el missatge, el desxifra amb la seva funció desxifradora f_B^{-1}. Aleshores la signatura de A queda en la forma $f_A^{-1}(P_A)$, B li aplica la clau xifradora f_A per poder llegir-la i té la certesa que el missatge ve de A, ja que només A coneix f_A^{-1}.

5.4.5 Generació i intercanvi de claus

En general, en els sistemes de clau pública, el xifratge és més lent. Sovint es fa servir un sistema de clau privada per l'intercanvi habitual de correspondència i un sistema de clau pública per l'intercanvi de claus.
Suposem que el sistema de clau pública és un criptosistema afí

$$\begin{array}{ccc} \mathbb{Z}/N^2 & \to & \mathbb{Z}/N^2 \\ x & \mapsto & ax+b \pmod{N^2}. \end{array}$$

Generem aleatòriament un enter c, $0 \leq c < N^4$ i l'escrivim en base N, $c = c_3N^3 + c_2N^2 + c_1N + c_0$. Prenem $a = c_3N + c_2, b = c_1N + c_0$. Si a no és primer amb N, fem una altra tria.

Descrivim ara el sistema d'intercanvi de claus de Diffie-Hellman. Si dos usuaris A i B volen posar-se d'acord sobre la clau que faran servir per xifrar els missatges que intercanviaran, fixen un enter m i prenen un generador g de $(\mathbb{Z}/m)^*$. L'usuari A escull un enter aleatori a entre 1 i $\varphi(m)$, que guarda secret, i calcula $g^a \pmod m$ que fa públic. L'usuari B escull un enter aleatori b entre 1 i $\varphi(m)$, que guarda secret, i calcula $g^b \pmod m$ que fa públic. La clau secreta que comparteixen és g^{ab}. L'usuari A la calcula fent $(g^b)^a$ i l'usuari B fent $(g^a)^b$. Un tercer usuari coneix només g^a i g^b. La dificultat computacional de calcular g^{ab} a partir només de g^a i g^b és equivalent a la de calcular el logaritme discret i per tant no es pot portar a la pràctica.

Capítol 6

Apèndix

6.1 El conjunt $\mathbb{N}$ dels nombres enters.

El conjunt $\mathbb{N}$ dels nombres enters naturals satisfà les propietats següents.

1. $\mathbb{N}$ és un conjunt totalment ordenat;
2. $\mathbb{N}$ té un primer element, és a dir un mínim, i no té màxim;
3. tot element de $\mathbb{N}$ té un element següent i tot element de $\mathbb{N}$ diferent de 0 té un element anterior;
4. tot subconjunt no buit de $\mathbb{N}$ té un primer element i tot subconjunt acotat de $\mathbb{N}$ té màxim.

6.2 Operacions en un conjunt.

Si A és un conjunt no buit, una *operació interna* a A és una aplicació de $A \times A$ en A. Indiquem la imatge de (a, b) per aquesta operació per $a * b$, o bé $a + b$ o bé ab i diem que a A tenim definida l'operació $*$, una suma, un producte, respectivament.

Exemples. La suma de vectors de $\mathbb{R}^n$ és una operació interna . A $\mathbb{Z}$ tenim definides dues operacions internes, la suma i el producte.

Sigui $*$ una operació interna definida en el conjunt A.

1. Diem que $*$ és *associativa* si $(a * b)c = a * (b * c)$, per a a, b, c elements de A qualssevol.

2. Diem que $*$ és *commutativa* si $a*b = b*a$, per a a, b elements de A qualssevol.

3. Diem que $e \in A$ és *element neutre* per $*$ si $a * e = e * a = a$ per a qualsevol element a de A.

4. Si e és element neutre per $*$ i a és un element de A, diem que un element b de A és *simètric* de a per $*$ si $a * b = b * a = e$.

Si l'operació interna és suma, indiquem l'element neutre per 0 i diem oposat l'element simètric, escrivim $-a$ l'oposat de a; si l'operació interna és producte, indiquem l'element neutre per 1 i diem invers l'element simètric, escrivim a^{-1} l'invers de a.
Si A és un conjunt dotat de dues operacions internes: $+, \cdot$, diem que $\cdot$ és *distributiva* respecte de $+$ si $a \cdot (b + c) = a \cdot b + a \cdot c$, per a a, b, c elements de A qualssevol.

6.3 Definició de grup, anell, cos.

Un *grup* és un conjunt no buit dotat d'una operació interna associativa, amb element neutre i tal que tot element té simètric. Si a més l'operació és commutativa diem que el grup és commutatiu o abelià.

Exemples.

1. $\mathbb{R}^n$ amb la suma de vectors és un grup commutatiu.

2. $\mathbb{Z}$ amb la suma és un grup commutatiu.

3. $\mathbb{Q}$ amb la suma és un grup commutatiu.

4. $\mathbb{R}$ amb la suma és un grup commutatiu.

5. El conjunt de matrius $n \times n$ amb coeficients a $\mathbb{R}$, de determinant no nul, és un grup amb el producte de matrius. Si $n \geq 2$, és grup no commutatiu.

Un *anell* és un conjunt A no buit dotat de dues operacions internes: $+, \cdot$ tals que

1. $+$ és associativa, commutativa, amb 0 i tot element de A té oposat;

2. $\cdot$ és associativa i distributiva respecte de $+$.

Si a més, $\cdot$ és commutativa, diem que A és anell commutatiu. Si A té element neutre per $\cdot$, diem que és un anell amb unitat.
Un element a d'un anell commutatiu amb unitat A es diu *invertible* si té invers a A.

Exemples.

1. $\mathbb{Z}$ amb la suma i el producte és anell commutatiu amb unitat.
2. El conjunt de matrius $n \times n$ amb la suma i el producte de matrius és anell amb unitat.

A més, a $\mathbb{Z}$ es compleix,

$$a, b \in \mathbb{Z}, a \neq 0 \text{ i } \ b \neq 0 \Rightarrow ab \neq 0.$$

Com a conseqüència, tenim la llei de simplificació:

$$a, b, c \in \mathbb{Z}, a \neq 0 \text{ i } \ ab = ac \Rightarrow b = c.$$

Un *cos* és un anell commutatiu amb unitat tal que tot element no nul és invertible.

Exemples.

1. $\mathbb{Q}$ amb la suma i el producte és cos.
2. $\mathbb{R}$ amb la suma i el producte és cos.
3. $\mathbb{C}$ amb la suma i el producte és cos.