Universitat de Barcelona

Apunts

Segon Semestre

Aritmètica (ARI)

Autor:
Mario Vilar

Professor:
Dr. Luis Dieulefait

3 de juny de 2021

Universitat de Barcelona

Introducció

This silence for my sin you did impute,
Which shall be most of my glory, being dumb;
For I impair not beauty, being mute,
When other would give life and bring a tomb.

William Shakespeare

Abans de començar, una petita introducció a aquests apunts pels quals, a causa de la seva extensió, es pot veure fàcilment que he ampliat més que no pas reduït el temari...

Primer de tot, es trobarà que hi ha un índex, on hi distingim els diferents apartats ordenats d'una manera certament poc satisfactòria pel que fa a l'ordre cronològic del curs, sinó que he seguit més aviat el meu propi criteri. Hi ha capítols, seccions, subseccions (i fins i tot subsubseccions). Pel que fa al pes d'aquestes estructures en els encapçalaments:

1. el número de l'última secció/subsecció figurarà en cada cantonada superior de pàgina parella (per exemple, *1.2*);
2. el nom del capítol es trobarà a la part dreta de la capçalera de les pàgines parelles (per exemple, "Divisibilitat i nombres primers");
3. el nom de l'última secció/subsecció de la pàgina, a la cantonada dreta superior de les pàgines parelles (per exemple, "Polinomis: algorisme d'Euclides").

A més, hi ha una taula en què es veu fàcilment que s'ha seguit una mena de *sorting-by-color* per poder treballar de manera més eficient amb els diferents tipus d'enunciats matemàtics. En els encapçalaments, aleshores, tenim:

- el número de l'últim teorema, definició... de la pàgina en qüestió es trobarà a les pàgines senars, a la cantonada superior dreta (per exemple, **1.2.3**).

Teorema de prova. *Aquest és un teorema de prova. Els teoremes, les proposicions, els lemes, els corol·laris, les propietats, les conjectures i els processos tindran aquest format.*

Definició de prova. Aquesta és una definició de prova. Les definicions, els exemples i les notacions tindran aquest format.

Remarca de prova. Aquesta és una remarca de prova. Les remarques tindran aquest format.

Figura 1: Els diferents formats d'enunciats.

Índex

Taula

Capítol 1

Capítol 2

Capítol 3

Capítol 6

Capítol 7

Capítol 1

Enters i funcions aritmètiques

1.1

La divisió euclidiana

La divisió entera

Teorema 1.1.1 (La divisió entera)**.** *Siguin a i b nombres naturals, $b \neq 0$. Existeixen nombres naturals q, r tals que $a = bq + r$ i $0 \leq r < b$. Aquestes condicions determinen unívocament els nombres q, r.*

Hem de demostrar existència i unicitat.

Demostració de l'existència. Si $b > a$, podem assignar $q = 0$ i $r = a$. Aleshores, les dues propietats $a = bq + r$ i $0 \leq r < b$ són clares. Suposem, al contrari, $a \geq b$, i considerem el conjunt $A := \{n \in \mathbb{N} \mid a < b(n+1)\}$. Com que $b \geq 1$, se satisfan les desigualtats $a < a + 1 \leq b(a+1)$, de manera que $a \in A$ i podem afirmar que A és un subconjunt no buit de nombres naturals. Sigui q el primer element d'A i posem $r = a - bq$. Com que $q \in A$, se satisfà la propietat $a < b(q+1) = bq + b$, és a dir, $r = a - bq < b$. D'altra banda, si fos $q = 0$, seria $a < b$, la qual cosa contradiria la hipòtesi. Tenim, doncs, $q \geq 1$. Aleshores, $q - 1$ seria un nombre natural i no pertany a A perquè $q - 1 < q$ i q és el primer element d'A. En conseqüència, ha de ser $a \geq b(q - 1 + 1) = bq \implies r = a - bq \geq 0$. ■

Demostració de la unicitat. Suposem que q, q', r, r' són nombres naturals tals que $a = bq + r, a = bq' + r'$, i que $0 \leq r < b$ i $0 \leq r' < b$. Com que $r < b$ i $r' \geq 0$, és $r - r' < b$. Suposant $q \geq q'$ i a l'inrevés arribem a contradiccions. Aleshores, $q = q'$. Al seu torn, se satisfà que $r - r' = b(q' - q) = 0$, és a dir, $r = r'$. Per tant, la parella q, r és l'única que satisfà les dues propietats $a = bq + r$ i $0 \leq r < b$. ■

A continuació, haurem de provar la validesa d'aquest resultat per a tots els nombres enters $a, b \in \mathbb{Z}, b \neq 0$. Notem que el residu s'agafa sempre positiu.

Proposició 1.1.2 (Divisió euclidiana)**.** *Siguin a, b nombres enters, $b \neq 0$. Existeixen nombres enters q, r tals que $a = bq + r$ i $0 \leq r < |b|$. Aquestes condicions determinen unívocament els nombres q, r.*

Demostració. En el cas que $a \geq 0, b > 0$, ja hem provat l'existència, ja que $a, b \in \mathbb{N}$. Suposem encara que $b > 0$, però ara que $a < 0$. La divisió entera del nombre natural $-a$ entre el nombre natural b ens proporciona nombres enters q_1, r_1 tals que $-a = bq_1 + r_1, 0 \leq r_1 < b$. Si és $r_1 = 0$, prenem $q = -q_1$ i $r = 0$ i obtenim la igualtat $a = bq + r$, i les desigualtats $0 \leq r < b$ que volem. En canvi, si és $r_1 \neq 0$, podem definir $q = -q_1 - 1$ i $r = b - r_1$, de manera que la igualtat $a = b \cdot (-q_1) - r_1 = b \cdot (-q_1 - 1) + (b - r_1)$ ens proporciona les propietats $a = bq + r, 0 < r < b$ que volem demostrar.

Ara suposem $b < 0$. Llavors, se satisfà $-b > 0$ i, pel que ja hem demostrat, existeixen nombres enters q_1, r_1 tals que $-a = (-b)q_1 + r_1, 0 \leq r_1 < -b = |b|$. Canviant el signe de la igualtat, tenim que $a = bq_1 - r_1$. Si $r_1 = r = 0$, prenem $q = q_1$ i $r = r_1 = 0$ i ja hauríem acabat. Si $r_1 \neq 0$, prenem $q = q_1 + 1$ i $r = -b - r_1$; com que $r_1 < -b$, resulta que $r > 0$ i, com que $r_1 > 0$ és $r < -b = |b|$. Per tant, q i r satisfan, efectivament, les propietats que hem anunciat.

Ens queda veure, en últim lloc, la unicitat. Suposem que q, q', r, r' són nombres enters tals que $a = bq + r, a = bq' + r'$, i que $0 \leq r < |b|$ i $0 \leq r' < |b|$. Si suposem que $q' \neq q$, obtenim la desigualtat $|r - r'| = |b||q' - q| \geq |b|$, que contradiu el fet que $|r - r'| < |b|$, desigualtat que es dedueix de les dues $0 \leq r < |b|$ i $|b| > r \geq 0$. Per tant, ha de ser $q' = q$. Però, igual que més amunt, $r - r' = b(q - q') = 0$; és a dir, $r = r'$. Per tant, la parella q, r és l'única que satisfà alhora les dues propietats enunciades. ■

Bases de numeració

Proposició 1.1.3. *Sigui $b > 1$ un nombre natural qualsevol. Per a tot nombre natural $x > 0$, existeix $n \geq 0$ i existeixen nombres $x_0, x_1, \ldots, x_n \in \{0, 1, \ldots, b-1\}$ únics tals que $x_n \neq 0$ i $x = x_0 + x_1 b + x_2 b^2 + \ldots + x_n b^n$.*

Demostració. Cal demostrar existència i unicitat. Demostrarem l'existència per inducció sobre x. Si suposem que $0 < x < b$, podem posar $n = 0$, $x_0 = x$, és clar que aquesta assignació mostra l'existència dels nombres $x_0, \ldots, x_n$ per a x. Suposem, doncs $x \geq b$ i que per a tot nombre enter positiu $q < x$ la propietat d'existència és certa. Fem la divisió entera de x per b en la forma $x = bq + x_0$, amb $0 \leq x_0 < b$. Com que $x \geq b$, ha de ser $0 < q < x$: per hipòtesi d'inducció existeixen nombres $x_1, \ldots, x_n \in \{0, 1, 2, \ldots, b-1\}$ tals que $x_n \neq 0$ i $q = x_1 + x_2 b + \ldots + x_n b^{n-1}$. Per tant, existeixen nombres $x_0, x_1, \ldots, x_n \in \{0, 1, 2, \ldots, b-1\}$ tals que $x = x_0 + bq = x_0 + x_1 b + \ldots + x_n b^n$, tal i com volíem veure.

Ara hem de demostrar unicitat. Donada una expressió qualsevol de la forma $x = x_0 + x_1 b + \ldots + x_n b^n$, amb $n \geq 0$ i $x_0, x_1, \ldots, x_n \in \{0, 1, \ldots, b-1\}$, $x_n \neq 0$, els nombres naturals x_0 i $q = x_1 + x_2 b + \ldots + x_n b^{n-1}$, són, respectivament, el residu i quocient de la divisió entera de x per b; la unicitat de la divisió entera ens ensenya que x i b determinen unívocament x_0 i q, i això demostra la unicitat de x_0. Ara, per inducció, com q és unívocament determinat per x i b, i els nombres $x_1, \ldots, x_n$ són unívocament determinats per q i b, obtenim la unicitat desitjada. ■

Definició 1.1.4 (Expressió en base b del nombre x)**.** L'expressió $x = x_0 + x_1 b + \ldots + x_n b^n$, on $b > 1$, $x_0, x_1, \ldots, x_n \in \{0, 1, \ldots, b-1\}$, $x_n \neq 0$.

Proposició 1.1.5. *Les xifres de l'expressió en base b^k de qualsevol nombre són els nombres naturals les expressions dels quals en base b s'obtenen en agrupar de k en k les xifres de l'expressió de x en base b.*

Proposició 1.1.6. *Sigui $b > 1$ un nombre enter. Donat un nombre enter x, existeixen $\epsilon \in \{-1, 1\}$ i una successió de nombres enters $\{x_m\}_{m\geq 0}$ tals que:*

1. *Per a tot $m \geq 0$, $x_m \in \{0, 1, \ldots, b-1\}$,*
2. *Existeix $n \geq 0$ i per a tot $m \geq n$ és $x_m = 0$,*
3. *$x = \epsilon \sum_{m\geq 0} x_m b^m$.*

A més, la successió $\{x_m\}_{m\geq 0}$ i el valor de ϵ són únics per a cada nombre enter $x = 0$, la successió és única però ϵ no està determinat.

1.2

Equacions diofantines lineals

Definició 1.2.1 (Equació diofantina lineal)**.** Una equació diofantina lineal és una equació en diverses variables. $f(x_1, \ldots, x_n) = 0$, on f és un polinomi de coeficient enters i de la qual es busquen les solucions enteres.

Teorema 1.2.2. *L'equació $ax+by = n$ té solució en enters (x_0, y_0) si, i només si, $d = \text{mcd}(a, b)$ divideix a n. En el cas que existeixi una solució (x_0, y_0), hi ha infinites solucions (x, y) i aquestes s'expressen en funció de (x_0, y_0) i un paràmetre $t \in \mathbb{Z}$ mitjançant la fórmula:*

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t. \tag{1.2.1}$$

Demostració. Definim $B = \frac{b}{d}$ i $A = \frac{a}{d}$. Si existeix solució (x_0, y_0) en els enters es compleix que $ax_0 + by_0 = n$, d'on com $d \mid a$ i $d \mid b$ concloem que $d \mid n$. Recíprocament, si $d \mid n$, definim $N = \frac{n}{d}$. Sabem, per 3.2.4, que existeixen enters x', y' tals que $d = ax' + by'$. Si multipliquem per N a banda i banda de la igualtat, obtenim:

$$n = a(x'N) + b(y'N) \implies (x'N, y'N) \text{ solució de } ax + by = n. \tag{1.2.2}$$

Pel que fa a la segona part de la demostració, sigui (x_0, y_0) una solució de $ax + by = n$. Com $a = dA$ i $b = dB$, amb $d = \text{mcd}(a, b)$ es té que $\text{mcd}(A, B) = 1$. Suposem que es té una altra solució (x_1, y_1) de la mateixa equació. Tenim que

$$ax_0 + by_0 = n = ax_1 + by_1 \iff a(x_0 - x_1) = b(y_1 - y_0) \xrightarrow{/d} A(x_0 - x_1) = B(y_1 - y_0). \tag{1.2.3}$$

D'aquí extraiem, tenint en compte que $\text{mcd}(A, B) = 1$, que $B \mid (x_0 - x_1)$ i $A \mid (y_1 - y_0)$, de tal manera que $y_1 - y_0 = \omega A$ i $x_0 - x_1 = \rho B$, per a $\rho, \omega \in \mathbb{Z}$. Si substituïm, $A\rho B = b\omega A \implies \rho = \omega$. Per tant,

$$\begin{array}{l} x_1 = x_0 - \rho B, \\ y_1 = y_0 + \rho A. \end{array} \xrightarrow{t=-\rho} \begin{array}{l} x_1 = x_0 + t\frac{b}{d}, \\ y_1 = y_0 - t\frac{a}{d}. \end{array} \tag{1.2.4}$$

Ens falta veure que per a tot enter t els enters x_1, y_1 donats per les dues últimes expressions de (1.2.4) són sempre solucions de l'equació. ■

Proposició 1.2.3. *Siguin a, b, c nombres enters. L'equació diofantina $aX + bY = c$ té solució si, i només si,* $\text{mcd}(a, b)$ *és un divisor de c.*

Proposició 1.2.4. *Siguin (x_1, y_1), (x_2, y_2) solucions enteres a l'equació diofantina $ax+by = c$, és a dir, siguin $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ nombres enters tals que $ax_1 + by_1 = c$ i $ax_2 + by_2 = c$. Posem $d := \text{mcd}(a, b)$ i escrivim $a = da'$ i $b = db'$, amb $a', b' \in \mathbb{Z}$. Aleshores, existeix un nombre enter t tal que $x_2 = x_1 + tb'$, $y_2 = y_1 - ta'$, és a dir, podem escriure $(x_2, y_2) = (x_1, y_1) + t(b', -a)$.*

Proposició 1.2.5. *Siguin $a_1, \ldots, a_n, b \in \mathbb{Z}$. Condició necessària i suficient perquè l'equació diofantina $a_1X_1 + a_2X_2 + \ldots + a_nX_n = b$ tingui solució és que $\text{mcd}(a_1, \ldots, a_n)$ divideixi b.*

Demostració. Si d és un divisor qualsevol de tots els coeficients $a_1, \ldots, a_n$, aleshores d també divideix $a_1x_1 + \ldots + a_nx_n = b$. Recíprocament, si $d = \text{mcd}(a_1, \ldots, a_n)$ existeixen nombres enters $\lambda_1, \ldots, \lambda_n$ tals que

$$a_1\lambda_1 + \ldots + a_n\lambda_n = d. \tag{1.2.5}$$

Si escrivim $b = db'$, amb $b' \in \mathbb{Z}$ i posem $x_i = \lambda_i b'$, $1 \leq i \leq n$, aleshores $a_1x_1 + a_2x_2 + \ldots + a_nx_n = (a_1\lambda_1 + \ldots + a_n\lambda_n)b' = db' = b$, de manera que obtenim una solució de l'equació, com volíem. ■

Exemple 1.2.6. Calculeu les solucions enteres de l'equació

$$165x + 60y + 105z + 30t = 225$$

Demostració. Primer de tot cal calcular el $d = \text{mcd}(165, 60, 105, 30)$.

$$d = \text{mcd}(165, 60, 105, 30) = \text{mcd}(15, 105, 30) = \text{mcd}(15, 30) = 15$$

i com que $15|225$, l'equació té solucions.

- **Solucions de t.** Sigui $d_1 = \text{mcd}(165, 60, 105) = \text{mcd}(15, 105) = 15$. Volem trobar les solucions $t, \phi_1 \in \mathbb{Z}$ de l'equació $15\phi_1 + 30t = 225$. Aplicant 3.2.4 obtenim que

  $$15 \cdot 15 + 30 \cdot 0 = 225$$

  per tant,

  $$\begin{cases} \phi_1 = 15 + 2 \cdot k_1 \\ t = -k_1 \end{cases} \qquad k_1 \in \mathbb{Z} \tag{1.2.6}$$

- **Solucions de z**
  Sigui $d_2 = \text{mcd}(165, 60) = 15$. Volem trobar totes les solucions $z, \phi_2 \in \mathbb{Z}$ de l'equació $15\phi_2 + 105z = 15\phi_1$.
  Utilitzant l'Identitat de Bezóut tenim que

  $$15 \cdot 1 + 105 \cdot 0 = 15$$

  però com que volem $15\phi_1$ en comptes de 15. Hem de multiplicar cada terme per ϕ_1. D'aquesta manera obtenim

  $$15 \cdot \phi_1 + 105 \cdot 0 = 15 \cdot \phi_1$$

  aleshores,

  $$\begin{cases} \phi_2 = \phi_1 + 7 \cdot k_2 \\ z = -k_2 \end{cases} \qquad k_2 \in \mathbb{Z} \tag{1.2.7}$$

- **Solucions de** x, y Per últim, podem trobar les solucions de $x, y \in \mathbb{Z}$ utilitzant l'equació $165x + 60y = 15\phi_2$. Utilitzant l'Identitat de Bezóut obtenim

$$165 \cdot (-1) + 60 \cdot 3 = 15$$

però com que volem $15\phi_2$ en comptes de 15. Hem de multiplicar cada terme per ϕ_2. D'aquesta manera obtenim

$$165 \cdot (-\phi_2) + 60 \cdot (3 \cdot \phi_2) = 15\phi_2$$

aleshores,

$$\begin{cases} x = -\phi_2 + 4 \cdot k_3 \\ y = 3 \cdot \phi_2 - 11 \cdot k_3 \end{cases} \qquad k_3 \in \mathbb{Z} \tag{1.2.8}$$

Com que ens interessa tenir-ho tot en funció del paràmetres $k_1, k_2, k_3 \in \mathbb{Z}$, hem de treballar amb (1.2.6), (1.2.7), (1.2.8) per tal d'aïllar x, y, z, t.

$$\begin{cases} x = 4 \cdot k_3 - 7 \cdot k_2 - 2 \cdot k_1 - 15 \\ y = -11 \cdot k_3 + 21 \cdot k_2 + 6 \cdot k_1 + 45 \\ z = -k_2 \\ t = -k_1 \end{cases} \tag{1.2.9}$$

Per a demostrar que (1.2.9) és el conjunt de solucions de l'equació $165x+60y+105z+30t = 225$ val amb substituir en x, y, z, t l'expressió obtinguda en (1.2.9) i obtenir 225.

$$\begin{aligned} 225 &= 165x + 60y + 105z + 30t \\ &= 165(4k_3 - 7k_2 - 2k_1 - 15) + 60(-11k_3 + 21k_2 + 6k_1 + 45) + 105(-k_2) + 30(-k_1) \\ &= 660k_3 - 1155k_2 - 330k_1 - 2475 - 660k_3 + 1260k_2 + 360k_1 + 2700 - 105k_2 - 30k_1 \\ &= (660 - 660)k_3 + (-1155 + 1260 - 105)k_2 + (-330 + 360 - 30)k_1 + (-2475 + 2700) \\ &= 0k_3 + 0k_2 + 0k_1 + 225 \\ &= 225 \end{aligned}$$

■

Ternes pitagòriques

Compte! S'avancen conceptes de capítols posteriors. Es recomana saltar aquesta secció i després tornar a ella. Es posa aquí ja que no és sinó part d'equacions diofantines.

Definició 1.2.7 (Ternes pitagòriques)**.** Imaginem que volem trobar totes les solucions en enters positius de la següent equació:

$$x^2 + y^2 = z^2. \tag{1.2.10}$$

Aquestes solucions reben el nom de *ternes pitagòriques*. Això es desprèn del teorema de Pitàgores, ja que per ell sabem que donen lloc a un triangle rectangle de costats enters.

Exemple 1.2.8. $3^2 + 4^2 = 5^2 = 25$.

Per a començar, observarem que si $x, y, z \in \mathbb{Z}_{>0}$, solució de (1.2.10), i si $d = \text{mcd}(x, y, z)$, aleshores podem escriure $x = dX, y = dY, z = dZ$, amb $X, Y, Z \in \mathbb{Z}_{>0}, \text{mcd}(X, Y, Z) = 1$. Veiem, doncs, que

$$(dX)^2 + (dY)^2 = (dZ)^2 \implies X^2 + Y^2 = Z^2. \tag{1.2.11}$$

Per trobar totes les solucions de (1.2.10) és suficient amb trobar totes aquelles solucions X, Y, Z de $\text{mcd}(X, Y, Z) = 1$ i, a partir d'elles, amb multiplicar als tres enters per un $k \in \mathbb{Z}$ arbitrari, s'obtenen totes les solucions de l'equació.

Definició 1.2.9 (Solució primitiva)**.** És una solució (X, Y, Z) amb la propietat $\text{mcd}(X, Y, Z) = 1$.

Proposició 1.2.10. *En una solució primitiva, els elements són coprimers dos a dos.*

Demostració. Ara calcularem totes les solucions primitives de (1.2.10), així que donada una solució primitiva (X, Y, Z), veiem que s'ha de complir que $\text{mcd}(X, Y) = \text{mcd}(X, Z) = \text{mcd}(Y, Z) = 1$. Provem, solament, que $\text{mcd}(X, Y) = 1$. La resta es prova amb el mateix argument. Si anomenem $d = \text{mcd}(X, Y)$, aleshores de l'equació 1.2.10 obtenim que $0 \equiv X^2 + Y^2 \equiv Z^2 \pmod{d}$: d també compleix que $d \mid Z^2$. Si suposem que $d > 1$, aleshores hi ha, com a mínim, un primer p que divideix d: en particular, $p \mid X, Y, Z$. Això contradiu la hipòtesi que la terna X, Y, Z és primitiva. Amb la qual cosa, queda provat que $\text{mcd}(X, Y) = 1$. ■

Proposició 1.2.11. *X, Y tenen diferent paritat.*

Demostració. X, Y no poden ser tots dos parells ja que són coprimers. Si fossin ambdós senars, podríem reduir l'equació 1.2.10 mòdul 4 i obtindríem $2 \equiv X^2 + Y^2 \equiv Z^2 \pmod{4}$, la qual cosa és una contradicció, ja que un quadrat mòdul 4 solament pot caure en la classe del 0 o en la de l'1. ■

Ara que sabem que X, Y tenen diferent paritat podem suposar que X és parell i Y senar i, evidentment, Z ha de ser imparell. Com $Z - Y$ i $Z + Y$ són ambdós parells, podem introduir noves variables: $Z - Y = 2s, Z + Y = 2r; r, s \in \mathbb{Z}$. Desfent el canvi de variables, veiem fàcilment que ens queda:

$$Y = r - s, Z = r + s. \tag{1.2.12}$$

Veiem que aquestes noves variables r, s han de ser coprimeres i de diferent paritat: si hi hagués un divisor comú $d > 1$ entre r i s veiem de les dues fórmules de (1.2.12) que d divideix a Y i a Z, contradient el fet que els elements de la terna X, Y, Z són coprimers dos a dos. També es dedueix de (1.2.12) que com Y, Z són imparells i r, s tenen diferent paritat. Com X és parell, podem escriure $X = 2W, W \in \mathbb{Z}$. Substituint les variables X, Y, Z per les variables W, r, s a la fórmula de (1.2.10) obtenim

$$X^2 = Z^2 - Y^2 \implies 4W^2 = (Z - Y)(Z + Y) = 4rs,\ W^2 = rs. \tag{1.2.13}$$

Com sabem, a més, que r, s són coprimers, aleshores existeixen $u, v \in \mathbb{Z}$ tals que $r = u^2, s = v^2, W = uv$. Noti's que com r, s tenen diferent paritat, u, v també són de diferent paritat. Queda provat, doncs, que qualsevol hipotètica solució primitiva X, Y, Z de (1.2.10) serà de la forma

$$X = 2uv, Y = u^2 - v^2, Z = u^2 + v^2, \tag{1.2.14}$$

amb $u, v \in \mathbb{Z}_{>0}, \text{mcd}(u, v) = 1$ i de diferent paritat.

Proposició 1.2.12. *Qualsevol terna X, Y, Z obtinguda com en (1.2.14) d'$u, v \in \mathbb{Z}_{>0}, u > v, \mathrm{mcd}(u, v) = 1$ i de diferent paritat és una terna d'enters positius que és solució primitiva de (1.2.10).*

Demostració. Hi ha prou amb verificar la identitat: $(2uv)^2 + (u^2 - v^2)^2 = (u^2 + v * 2)^2$, que surt aplicant fàcilment la fórmula del quadrat d'un binomi. Falta amb verificar que és primitiva i, per a això, veurem que no hi ha cap factor primer p en comú entre X, Y, Z.

Suposem, raonant per l'absurd, que existeix un primer p tal que $p \mid X, Y, Z$. Com Y, Z són imparells, tenim que $p > 2$. Per tant, com $p \mid X$ i $X = 2uv$, tenim que $p \mid u$ o bé $p \mid v$ (Lema Fonamental de l'Aritmètica). Suposarem que $p \mid u$ (l'altre cas és totalment anàleg): com $p \mid u$ i $p \mid Z = u^2 + v^2$ tenim que $p \mid v^2 = Z - u^2$ i, per tant, que $p \mid v$. Però com que u, v són coprimers, no poden ser ambdós múltiples de p, així que $p = 1$, però p no és primer. Aquesta contradicció prova que cap primer pot dividir a X, Y, Z, amb la qual cosa la terna X, Y, Z, com en (1.2.14), és una solució primitiva de (1.2.10).

Finalment, recordem que per a obtenir la solució general d'(1.2.10) hi ha prou amb multiplicar per un enter $k > 0$ a les solucions primitives. Per tant, la solució general de (1.2.10) és

$$\begin{aligned} X &= 2kuv, \\ Y &= k(u^2 - v^2), \\ Z &= k(u^2 + v^2), \end{aligned} \tag{1.2.15}$$

amb $k > 0$ i $u, v \;\big|\; \mathrm{mcd}(u, v) = 1, u > v$ i de diferent paritat. ■

1.3

Funcions aritmètiques

Les funcions aritmètiques modelen els principals objectes en teoria de nombres [Mos04]. Aquelles que tenen una relació més directa són les següents:

$$\begin{aligned}
\pi(n) &= \sum_{p \le n} 1 && \text{el nombre de primers que no excedeixen } n, \\
\omega(n) &= \sum_{p \mid n} 1 && \text{el nombre de factors primers diferents d'} n, \\
\Omega(n) &= \sum_{p^i \mid n} 1 && \text{el nombre de potències primes factors d'} n, \\
\tau(n) &= \sum_{d \mid n} 1 && \text{el nombre de divisors d'} n, \\
\sigma(n) &= \sum_{d \mid n} d && \text{la suma dels divisors d'} n, \\
\sigma_k(n) &= \sum_{d \mid n} d^k && \text{la suma dels } k\text{-divisors d'} n, \\
\varphi(n) &= \sum_{\substack{\mathrm{mcd}(a,n)=1 \\ 1 \le a \le n}} d && \text{la funció phi d'Euler.}
\end{aligned}$$

Com ja veurem en capítols posteriors, la funció φ d'Euler compte el nombre de primers més petits que n que són coprimers amb n. Una generalització de $\tau(n)$ i $\sigma(n)$ és $\sigma_k(n)$, donat que $\sigma_0(n) = \tau(n)$ i $\sigma_1(n) = \sigma(n)$.

Capítol 2

Polinomis

2.1

Cos i anell

Introduirem aquest capítol amb la definició de cos. En polinomis acostumarem a treballar amb $\mathbb{K}[x]$, o sigui que serà força útil conèixer el concepte.

Definició 2.1.1 (Operació interna)**.** Si A és un conjunt no buit, una *operació interna* a A és una aplicació d'$A \times A$ en A. Indiquem la imatge d'(a, b) per aquesta aplicació per $a \circledcirc b$. Tenim:

$$\begin{array}{rccc} \circledcirc: & A \times A & \longrightarrow & A \\ & (a,b) & \longmapsto & f(a,b) = a \circledcirc b \end{array} \tag{2.1.1}$$

Sigui $\circledcirc$ una operació interna definida en el conjunt A:

1. Diem que $\circledcirc$ és **associativa** si $(a \circledcirc b) \circledcirc c = a \circledcirc (b \circledcirc c)$, per a a, b, c elements d'A, qualssevol.
2. Diem que $\circledcirc$ és **commutativa** si $a \circledcirc b = b \circledcirc a$, per a $a, b \in A$.
3. Diem que $e \in A$ és **element neutre** per $\circledcirc$ si $a \circledcirc e = e \circledcirc a = a$ per a qualsevol element $a \in A$.
4. Si e és element neutre per $\circledcirc$ i a és un element d'A, diem que un element b d'A és **simètric** d'a per $\circledcirc$ si $a \circledcirc b = b \circledcirc a = e$.

Definició 2.1.2 (Suma)**.** Sigui $a \in A$. Definim la suma com una operació interna amb element neutre 0, amb oposat l'element simètric $-a$.

Definició 2.1.3 (Producte)**.** Amb element neutre 1, i diem invers d'a l'element simètric a^{-1}.

Si A és un conjunt dotat d'una operació interna $\circledcirc$ i B és un subconjunt d'A, diem que B és estable per $\circledcirc$ si es compleix

$$a, b \in B \implies a \circledcirc b \in B. \tag{2.1.2}$$

Definició 2.1.4 (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 *abelià*.

Definició 2.1.5 (Anell)**.** És un conjunt A no buit dotat de dues operacions internes, la suma i el producte, tals que:

- la suma és associativa, commutativa, amb element neutre 0 i oposat,
- el producte és associatiu i distributiu respecte de la suma.

Si, a més, el producte és commutatiu, direm que A és **anell commutatiu**. Si A té element neutre pel producte, direm que és un **anell amb unitat**.

Definició 2.1.6 (Element invertible)**.** Un element d'a amb unitat A es diu invertible si té invers A. Si a és element invertible de l'anell A es compleix $ab = 0 \implies b = 0$, ja que $ab = 0 \implies a^{-1}(ab) = a^{-1} \cdot 0 = 0$, i d'altra banda, $a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$.

Definició 2.1.7 (Cos). Un cos és un anell commutatiu amb unitat en què tot element no nul és invertible.

Exemple 2.1.8. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, amb la suma i el producte usuals, són cossos.

2.2 Definició

Definició 2.2.1. Sigui K un cos. Recordem que això vol dir que en el conjunt K hi ha definides dues operacions, que normalment anomenarem suma i producte, amb unes certes propietats. Un polinomi $P(x)$ a coeficients en K és una expressió de la forma:

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \quad n \geq 0, a_0, \ldots, a_n \in \mathbb{K}. \tag{2.2.1}$$

Es diu que x és la variable i que a_i són els coeficients de $P(x)$.

Definició 2.2.2 (Polinomis constants)**.** Són aquells en què $n = 0$, és a dir, són de la forma $P(x) = a_0$, amb $a_0 \in \mathbb{K}$. Un cas particular n'és el polinomi nul $P(x) = 0$.

Propietat 2.2.3. *Tot polinomi no nul s'escriu de forma única tal que*

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \tag{2.2.2}$$

amb $a_n \neq 0, n \geq 0$. *n és el grau del polinomi i el denotem per* $\mathrm{gr}(P(x))$.

Suma i producte de polinomis

Per a sumar polinomis, se suma coeficient a coeficient (amb la suma de $\mathbb{K}$) i per a multiplicar-los, s'aplica la propietat distributiva: aplicant la regla $x^n x^m = x^{n+m}$, i agrupant després termes on la x tingui el mateix exponent. Així doncs, la suma és associativa i commutativa, amb element neutre i oposat. El producte és associatiu, commutatiu i distributiu respecte de la suma. Existeix element neutre pel producte.

Observació 2.2.4. Noti's que el polinomi constant 1 és el neutre del producte, i el polinomi nul 0 és el neutre de la suma, per la definció de cos, $\mathbb{K}$, que hem vist a la secció anterior.

Propietat 2.2.5. *Siguin $P(x), Q(x)$ polinomis en $K[x]$:*

1. $\mathrm{gr}(P(x) \pm Q(x)) \leq \max\{\mathrm{gr}(P(x)), \mathrm{gr}(Q(x))\}$,
2. $\mathrm{gr}(P(x \cdot Q(x)) = \mathrm{gr}(P(x)) + \mathrm{gr}(Q(x))$.

Corol·lari 2.2.6. *Els polinomis $P(x)$ que tenen inversa, és a dir, polinomis tals que existeix un polinomi $Q(x)$ amb $P(x)Q(x) = 1$ són els polinomis constants no nuls.*

Capítol 3

Divisibilitat i nombres primers

3.1

Propietats bàsiques de la divisibilitat

Proposició 3.1.1. *Si a i b són dos nombres diferents de 0, el seu producte ab és diferent de 0.*

Proposició 3.1.2 (Llei de simplificació)**.** *Siguin a, b, c nombres enters. Si $bc = ac$ i $c \neq 0$, llavors $b = a$.*

Definició 3.1.3. Siguin $a, b \in \mathbb{Z}$, qualssevol. Direm que a és un múltiple de b si existeix un nombre enter q tal que $a = bq$. Direm que b és un divisor d'a si existeix un nombre enter $q \neq 0$ tal que $a = bq$. Si a és múltiple de b, escriurem $b \mid a$; en cas contrari, $b \nmid a$.

Proposició 3.1.4. *Si $a, b \in \mathbb{Z}$, no tots nuls, i n un enter amb $n \mid a$, $n \mid b$, aleshores $n \mid d = \mathrm{mcd}(a, b)$. Es té, per tant, que el màxim comú divisor és el major dels divisors comuns i és múltiple de qualsevol divisor comú.*

Lema 3.1.5 (Lema fonamental de l'Aritmètica)**.** *Si p és primer i $a, b \in \mathbb{Z}$ tals que $p \mid ab$, aleshores $p \mid a$ o $p \mid b$.*

Demostració. Suposem que p no divideix b. Com p és primer, és evident que $\mathrm{mcd}(p, b) = 1$, ja que hem dit que p no divideix b i p no té altres divisors a part de l'1. Aplicant la identitat de Bézout, es dedueix l'existència d'enters x, y tals que

$$1 = bx + py. \tag{3.1.1}$$

Multiplicant a a ambdós bandes de la igualtat obtenim:

$$a = abx + apy. \tag{3.1.2}$$

Com, per hipòtesi, $p \mid ab$, es té, per la transitivitat de la divisibilitat que veurem més endavant en aquests apunts, que $p \mid apy$. Per (3.1.2) deduïm que $p \mid a$. ■

Lema 3.1.6 (Lema d'Euclides)**.** *Si $a, b, c \in \mathbb{Z}$ tals que $b \mid ac$ i $\mathrm{mcd}(a, b) = 1$, aleshores $b \mid c$.*

Demostració. Es prova d'una manera semblant a 3.1.5. Com $\mathrm{mcd}(a, b) = 1$, la identitat de Bézout ens diu que existeixen enters x, y tals que $1 = ax + by$. Multiplicant per c a banda i banda de la igualtat obtenim $c = cax + cby$ i com, per hipòtesi, es té que $b \mid ac$, també val $b \mid cax$, i com clarament $b \mid cby$, concluïm que $b \mid c$. ■

Corol·lari 3.1.7. *Si p és un nombre primer i $a_1, \ldots, a_r \in \mathbb{Z}$ tals que $p \mid a_1, \ldots, a_r$, aleshores $p \mid a_i$ per algun $i \in \{1, 2, \ldots, r\}$.*

Teorema 3.1.8 (Propietats de la divisibilitat**).** *Si a, b, i c, m, n són enters, aleshores:*

1. *$a \mid a$: reflexivitat.*
2. *Si $c \mid b$ i $b \mid a \implies c \mid a$: transitivitat.*
3. *Si $a \mid b$ i $b \mid a$, aleshores $b = a$ o $b = -a$.*
4. *Si $b \mid a$ i $b \mid c \implies b \mid am + cn$: linealitat.*
5. *$b \mid a$ i $b \mid c \implies cb \mid ca$: multiplicativitat.*
6. *Si $cb \mid ca$ i $c \neq 0$, aleshores $b \mid a$: llei de simplificació.*
7. *$1 \mid n$: 1 divideix tot.*
8. *$n \mid 1 \implies n = \pm 1$: 1 i -1 són els únics divisors d'1.*
9. *$d \mid 0$: qualsevol nombre divideix zero.*

Polinomis: propietats bàsiques de la divisibilitat

Definició 3.1.9. Si $a(x), b(x) \in \mathbb{K}[x]$, diem que $b(x)$ divideix a $a(x)$ si existeix $c(x) \in \mathbb{K}[x]$ amb

$$a(x) = b(x)c(x), \tag{3.1.3}$$

i ho denotem amb $b(x) \mid a(x)$. En aquest cas, diem que $b(x)$ és un divisor d'$a(x)$.

Lema 3.1.10. *Si $P(x) \in \mathbb{K}[x]$ és un polinomi no nul, els polinomis constants $c \in \mathbb{K}$ no nuls i els de la forma $c \cdot P(x)$ amb c constant no nula divideixen $P(x)$.*

Demostració. Simplement a partir de les igualtats trivials següents ho comprovem:

$$P(x) = c \cdot (c^{-1} \cdot P(x)) \text{ i } P(x) = c^{-1} \cdot (c \cdot P(x)). \tag{3.1.4}$$

■

Teorema 3.1.11. *Siguin $a(x), b(x), c(x), s(x), t(x) \in \mathbb{K}[x]$.*

1. *Si $a(x) \mid b(x)$ i $a(x) \mid c(x) \implies a(x) \mid s(x)b(x) + t(x)c(x)$,*
2. *si $a(x) \mid b(x)$ i $b(x) \mid c(x) \implies a(x) \mid c(x)$ i*
3. *si $a(x) \mid b(x) \implies a(x)s(x) \mid b(x)s(x)$. La recíproca és certa si $s(x) \neq 0$.*

Definició 3.1.12. Si $P(x) \in \mathbb{K}[x]$, els polinomis de la forma $c \cdot P(x)$ amb c constant no nul·la s'anomenen polinomis associats a $P(x)$. La relació entre el polinomi i els seus associats és una relació d'equivalència.

Proposició 3.1.13. *Si $a(x), b(x) \in \mathbb{K}[x]$, aleshores*

$$a(x) \text{ és associat a } b(x) \iff a(x) \mid b(x) \wedge b(x) \mid a(x), \tag{3.1.5}$$

és a dir, si es divideixen mútuament.

Demostració.
$\implies$ Suposant que són associats, $a(x) = c \cdot b(x)$. Per 3.1.10, $a(x) \mid b(x)$. $b(x) \mid a(x)$ és trivial.
$\impliedby$ Suposant $a(x) \mid b(x), b(x) \mid a(x)$. Tenim $b(x) = a(x)u(x)$ i $a(x) = b(x)v(x)$. Substituint, $b(x) = b(x)v(x)u(x)$. Suposant $a(x), b(x) \neq 0$ ens queda $u(x)v(x) = 1$, $u(x), v(x)$ tenen invers i $a(x), b(x)$ són associats. ■

Proposició 3.1.14. *Dos polinomis associats tenen el mateix conjunt de divisors.*

3.2

Algorisme d'Euclides

Definició 3.2.1 (Divisor comú)**.** Un divisor comú entre dos nombres enters a, b és un nombre enter d tal que $d \mid a$ i $d \mid b$.

Definició 3.2.2 (Màxim comú divisor, recordatori)**.** Donats nombres enters qualssevol a, b, d, direm que d és un màxim comú divisor d'a i b si a, b són múltiples de d i per a tot altre nombre enter δ tal que a, b siguin múltiples de δ, el nombre d també és un múltiple de δ.

Proposició 3.2.3. *Donats dos enters a i b no nuls, el següent algorisme és finit i dona com a resultat $d = \mathrm{mcd}(a, b)$:*

1. *Suposarem $a > b$. En particular, $a > b > 0$. Com $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, a) = \mathrm{mcd}(|a|, |b|)$, podem suposar $a \geq b > 0$ (el cas $b = 0$ és trivial, ja que $\mathrm{mcd}(a, 0) = |a|$.*
2. *Si $a = b$ el resultat és $\mathrm{mcd}(a, b) = a$. Per tant, suposem que $a > b > 0$.*
3. *Si $r_1 = 0$, tenim que $b|a$, així $\mathrm{mcd}(a, b) = b$.*
4. *Si $r_1 \neq 0$, cal calcular q_2, r_2 tals que $b = r_1 q_2 + r_2$, amb $0 \leq r_2 < r_1$. Si $r_2 = 0$, aleshores $\mathrm{mcd}(a, b) = r_1$.*
5. *En definitiva, donats r_{j-1} i r_{j-2}, amb $j > 2$, si ambdós són no nuls, calculem q_j i r_j tals que $r_{j-2} = r_{j-1} q_j + r_j$, amb $0 \leq r_j < r_{j-1}$.*
6. *Suposem ara i l'últim índex tal que la resta r_i és no nul·la. Per tant, es té que $r_i = 0$ i $r_{i+1} = 0$. Aleshores, existeix un q_{i+1} tal que $r_{i-1} = r_i q_{i+1} + 0$. Afirmem, doncs, que per a aquest índex i es té que $\mathrm{mcd}(a, b) = r_i$.*

Lema 3.2.4 (Identitat de Bézout)**.** *Siguin $a, b \in \mathbb{Z}$, no tots dos nuls i $d = \mathrm{mcd}(a, b)$. Aleshores, existeixen nombres enters x i y tals que*

$$d = ax + by. \tag{3.2.1}$$

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

$$\begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}. \tag{3.2.2}$$

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

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} b \\ r_1 \end{pmatrix} \tag{3.2.3}$$

i, per a cada i, $r_i = r_{i+1} q_{i+2} + r_{i+2} \implies r_{i+2} = r_i - r_{i+1} q_{i+2}$, que dona:

$$\begin{pmatrix} r_{i+1} \\ r_{i+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+2} \end{pmatrix} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}. \tag{3.2.4}$$

Si r_n és la primera resta nul·la, obtenim

$$\begin{pmatrix} r_{n-1} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \begin{pmatrix} r_{n-3} \\ r_{n-2} \end{pmatrix}$$
$$= \cdots = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} = \begin{pmatrix} s & t \\ * & * \end{pmatrix} \tag{3.2.5}$$

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

Observació 3.2.5. També podem calcular els coeficients de la identitat de Bézout aïllant successivament les restes de cada divisió començant per la última.

Proposició 3.2.6. *Siguin a, b, c nombres enters. Aleshores:*

1. $\mathrm{mcd}(a,b) = \mathrm{mcd}(b,a)$,
2. $\mathrm{mcd}(a, \mathrm{mcd}(b,c)) = \mathrm{mcd}(\mathrm{mcd}(a,b), c)$,
3. $\mathrm{mcd}(ca, cb) = c \cdot \mathrm{mcd}(a,b)$.

Demostració. Demostrem 3. Podem suposar que els nombres $a, b, c, \mathrm{mcd}(a,b), \mathrm{mcd}(ca,cb)$ són positius. Siguin $d := \mathrm{mcd}(a,b)$ i $e := \mathrm{mcd}(ca,cb)$: cal veure que $e = cd$. Com que ca i cb són múltiples comuns de cd, el nombre e és múltiple de cd. D'altra banda, podem escriure $d = am + bn$, per a certs enters m, n. Ara, com e és $\mathrm{mcd}(ca,cb)$, els nombres ca i cb són múltiples de e, de manera que $cam + cbn = cd$ és múltiple de e. Per tant, $e = cd$. ■

Lema 3.2.7. *$\forall a, b \in \mathbb{Z}$, tenim:*

$$\mathrm{mcd}(a,b) = \mathrm{mcd}(b,a) = \mathrm{mcd}(\pm a, \pm b) = \mathrm{mcd}(a, b-a) = \mathrm{mcd}(a, b+a) = \mathrm{mcd}(a, b-an). \quad (3.2.6)$$

Polinomis: algorisme d'Euclides

Teorema 3.2.8 (Divisió euclídea de polinomis). *Si $a(x), b(x) \in \mathbb{K}[x]$, amb $b(x) \neq 0$, existeixen polinomis únics $q(x), r(x)$, anomenats quocient i resta, respectivament, tals que*

$$a(x) = b(x)q(x) + r(x), \quad \mathrm{gr}(r(x)) < \mathrm{gr}(b(x)). \quad (3.2.7)$$

Definició 3.2.9 (MCD, polinomis). Si $a(x), b(x) \in \mathbb{K}[x]$, no ambdós nuls, un polinomi $d(x) \in \mathbb{K}[x]$ és un màxim comú divisor d'$a(x)$ i $b(x)$ si:

1. $d(x) \mid a(x)$ i $d(x) \mid b(x)$,
2. $\forall s(x) \in \mathbb{K}[x]$ tal que $s(x) \mid a(x)$ i $s(x) \mid b(x) \implies s(x) \mid d(x)$.

Proposició 3.2.10.

1. *Si $d(x)$ i $d'(x) \in \mathbb{K}[x]$ són ambdós màxim comú divisor d'$a(x), b(x) \in \mathbb{K}[x]$, aleshores $d(x)$ i $d'(x)$ són associats.*
2. *Si $d(x)$ és MCD d'$a(x)$ i $b(x)$, tot associat de $d(x)$ també ho és.*

Demostració.

1. Com $d(x)$ és $\mathrm{mcd}(a(x), d(x))$, i $d'(x)$ és un divisor comú, es té $d'(x) \mid d(x)$, i aplicant-ho a l'inrevés, tenim que $d(x) \mid d'(x)$. Per 3.1.13, $d(x), d'(x)$ són associats.
2. Sigui $d(x)$ un $\mathrm{mcd}(a(x), b(x))$ i sigui $c \in \mathbb{K}$ una constant no nul·la. Considerem $cd(x)$. Com $d(x) \mid a(x)$, veiem que $d(x) \mid c^{-1}a(x)$. D'aquí, $c \cdot d(x) \mid a(x)$. Anàlogament, com $d(x) \mid b(x)$, concluïm que $cd(x) \mid b(x)$. En altres paraules, $cd(x)$ és un divisor comú d'$a(x)$ i $b(x)$. Sigui ara $s(x)$ un divisor comú d'$a(x)$ i $b(x)$. En conseqüència, $s(x) \mid d(x)$, d'on traiem que $s(x) \mid cd(x)$.

■

Proposició 3.2.11. *Si $a(x), b(x), c(x) \in \mathbb{K}[x]$, no nuls, es té que:*

$$\operatorname{mcd}(a(x), b(x)) = \operatorname{mcd}(a(x) - c(x)b(x), b(x)). \tag{3.2.8}$$

Demostració. És fàcil veure que els divisors comuns d'ambdós costats són els mateixos, per les propietats de la divisibilitat: $d \mid a$ i $d \mid b \implies d \mid a - cb$. Recíprocament, si $d \mid a - cb$ i $d \mid b \implies d \mid a - cb$ i $d \mid cb \implies d \mid a$. ■

Proposició 3.2.12 (Algorisme d'Euclides amb polinomis**).** *Siguin $a(x), b(x) \in \mathbb{K}[x]$, no nuls, amb $\operatorname{gr}(a) \geq \operatorname{gr}(b)$.*

1. *Dividint, $a(x) = b(x)q(x) + r_0(x)$, amb $\operatorname{gr}(r_0(x)) < \operatorname{gr}(b(x))$. Per la proposició prèvia,*
2. $\operatorname{mcd}(a(x), b(x)) = \operatorname{mcd}(a(x) - b(x)q(x), b(x)) = \operatorname{mcd}(b(x), r_0(x))$.
3. *Si $r_0(x) = 0 \implies b(x) \mid a(x)$ i $\operatorname{mcd}(a(x), b(x)) = \operatorname{mcd}(b(x), 0) = b(x)$, i aquí acaba l'algorisme.*
4. *Si $r_0(x) \neq 0 \implies b(x) = q_1(x)r_0(x) + r_1(x)$, $\operatorname{gr}(r_1(x)) < \operatorname{gr}(r_0(x))$. Si $r_1(x) = 0$, deduïm que $\operatorname{mcd}(a(x), b(x)) = \operatorname{mcd}(b(x), r_0(x)) = \operatorname{mcd}(r_0(x), 0) = r_0(x)$.*
5. *Si $r_1(x) \neq 0$, procedim amb la divisió de $r_0(x)$ entre $r_1(x)$ i així successivament.*
6. *Suposem l'expressió general:*

$$r_i(x) = r_{i+1}(x)q_{i+2}(x) + r_{i+2}(x),\ 0 \leq i \leq n-1, r_i \neq 0 \tag{3.2.9}$$

   S'arribarà a un determinat n tal que a $r_{n+1}(x) = 0$, ja que el grau va decreixent en la successió dels $r_i(x)$. Així, s'arribarà al polinomi nul en un nombre finit de passos.
7. *D'aquí concloem que $\operatorname{mcd}(a(x), b(x)) = \operatorname{mcd}(b(x), r_0(x)) = \operatorname{mcd}(r_0(x), r_1(x)) = \ldots = \operatorname{mcd}(r_n(x), 0) = r_n(x)$, és a dir, l'*mcd *és l'últim residu no nul que apareix en l'algorisme d'Euclides.*

Exemple 3.2.13. Volem calcular el màxim comú divisor dels polinomis $A(X) = X^5 - X^3 - X^2 - 2X + 2, B(X) = X^4 + 3X^3 - X^2 - 6X - 2$. Fent la divisió d'$A(X)$ entre $B(X)$ obtenim el quocient $Q_1(X) = X - 3$ i resta $R_1(X) = 9X^3 + 2X^2 - 18X - 4$. Fent la divisió de B entre R_1 obtenim quocient $Q_2(X) = \frac{1}{9}X + \frac{25}{81}$ i resta $R_2(X) = \frac{31}{81}X^2 - \frac{62}{81} = \frac{31}{81}(X^2 - 2)$. Fent la divisió d'$R_1(X)$ entre $R_2(X)$ obtenim $Q_3(X) = \frac{81}{31}(9X + 2)$ i $R_3(X) = 0$. Per tant, tenim que $\operatorname{mcd}(A(X), B(X)) = X^2 - 2$.

Lema 3.2.14 (Identitat de Bézout amb polinomis**).** *Si $a(x), b(x) \in \mathbb{K}[x]$, no ambdós nuls, i $d(x)$ és el* mcd *d'$a(x)$ i $b(x)$, existeixen $s(x), t(x) \in \mathbb{K}[x]$ tals que $s(x)a(x) + t(x)b(x) = d(x)$.*

Demostració. Es podria raonar de manera anàloga a 3.2.4. La observació posterior a 3.2.4 també seria vàlida. ■

Definició 3.2.15 (Polinomi irreductible**).** Sigui $P(x) \in \mathbb{K}[x]$, $\operatorname{gr}(P(x)) > 0$, diem que $P(x)$ és irreductible si no pot descomposar-se com

$$P(x) = f(x)g(x),\ \operatorname{gr}(f(x)) < \operatorname{gr}(P(x)) \wedge \operatorname{gr}(g(x)) < \operatorname{gr}(P(x)). \tag{3.2.10}$$

Observem que un polinomi $P(x)$ de grau 1 sempre és irreductible, ja que $P(x) = f(x)g(x)$ necessita de $\operatorname{gr}(g(x)) = 1$ i $\operatorname{gr}(f(x)) = 0$.

Proposició 3.2.16. *Si $P(x) \in \mathbb{K}[x]$ és irreductible, els seus únics divisors són els polinomis constants c i els associats $cP(x)$, amb $c \in \mathbb{K}$ no nul.*

Proposició 3.2.17. *Si $P(x) \in \mathbb{K}[x]$, $c \in \mathbb{K}$ no nul, $P(x)$ irreductible $\iff$ $cP(x)$ irreductible.*

Demostració. Si $cP(x)$ és irreductible, és evident que $P(x)$ també ho és, ja que és una descomposició no trivial: $P(x) = f(x)g(x), \mathrm{gr}(f), \mathrm{gr}(g) < \mathrm{gr}(p)$, donaria lloc a una descomposició no trivial de $cP(x)$: $cP(x) = (cf(x))p(x)$. La recíproca es prova anàlogament. ■

Proposició 3.2.18. *Siguin $P(x)$ irreductibles en $\mathbb{K}[x]$. Sigui $a(x) \in \mathbb{K}[x]$. Aleshores, o $P(x) \mid a(x)$ o $\mathrm{mcd}(P(x), a(x)) = 1$.*

3.3

Nombres primers

Definició 3.3.1 (Nombre primer)**.** Un nombre enter n és un nombre primer si, i només si, $n \neq 0, 1, -1$ i els únics divisors de n són $1, -1, n, -n$. Els nombres enters no són ni el $0, 1, -1$, ni tampoc són primers, s'anomenen compostos.

Teorema 3.3.2 (Teorema d'Euclides)**.** *El conjunt dels nombres primers és infinit.*

Lema 3.3.3. *Per tot nombre primer P existeix un altre nombre primer P tal que $P < R$.*

Demostració del lema 3.3.3. Considerem un nombre primer P. Sigui $R = P! + 1$. Com $P \leq P!$, tenim que $P < R$. Demostrem per reducció a l'absurd que R és primer. *Suposem llavors que R és compost.* Sigui Q un factor primer de R. *Un factor primer és un nombre primer que apareix en la descomposició en factors primers de R.* Com Q és un factor primer de R, tenim que $Q \leq R$, però, com que Q és primer i R és compost, deduïm que $Q < R$. Per tant, $Q \leq P!$. Doncs, Q és un factor primer de $P!$.
Però com Q és un factor primer de R, tenim que Q és un divisor de $R = P! + 1$.
Així doncs, com Q és un divisor de $P!$ i és també un divisor de $P! + 1$, deduïm que Q és divisor de 1 i, per tant, que $Q = 1$, la qual cosa és impossible donat que Q és primer (i per tant, $Q \geq 2$). ■

Demostració del teorema d'Euclides. Demostrem el teorema d'Euclides per reducció a l'absurd. Suposem que el conjunt A dels nombres primers és finit. Sigui, doncs, P l'últim nombre primer, el qual existeix perquè estem suposant que A és finit. Aplicant llavors el lema 3.3.3, obtenim que existeix un nombre primer R tal que $P < R$. Però llavors, P no és l'últim nombre primer, amb la qual cosa arribem a una contradicció. ■

Lema 3.3.4 (Divisibilitat de nombres compostos)**.** *Si n és un enter que no és primer, és divisible per un primer p positiu tal que $p \leq \sqrt{n}$.*

Demostració. Com que n i $-n$ tenen els mateixos divisors, podem suposar $n > 0$. Per la definició de nombre primer, si n no ho és, tenim que $n = m_1 m_2, m_1, m_2 \in \mathbb{Z} \setminus \{1, n\}$. Podem suposar $m_1 \leq m_2$ i tenim que $m_1 \leq \sqrt{n}$. Si m_1 és primer, ja estem. Si no, podem escriure $m_1 = q_1 q_2$, amb $q_1, q_2 \in \mathbb{Z} \setminus \{1, m_1\}$. Si q_1 és primer, ja estem. Si no, reiterem el procés. Com que $m_1 > q_1 > \cdots$, en un nombre finit de passos trobem un divisor primer d'n més petit o igual que $\sqrt{|n|}$. ■

Distribució de primers

Lema 3.3.5. *Si $n \geq 1$ és un nombre natural no nul, cadascun dels nombres $(n+1)!+2, \ldots, (n+1)!+n+1$ és compost.*

Demostració. En efecte, $(n+1)!+m$ és estrictament més gran que m i és divisible per m, per a $2 \leq m \leq n+1$; per tant, $(n+1)!+m$ és compost. ■

Corol·lari 3.3.6. *Per a tot nombre enter $n \geq 1$, existeix un nombre natural primer p tal que $p+1, \ldots, p+n$ són nombres compostos.*

Definició 3.3.7. Per a tot nombre enter $r \geq 1$ escriurem p_r per a indicar l'r-èsim nombre natural primer que apareix en la successió dels nombres naturals.

Proposició 3.3.8. *Per a tot nombre enter $r > 2$ se satisfà la desigualtat*

$$p_r < \prod_{i=1}^{r-1} p_i. \tag{3.3.1}$$

Teorema 3.3.9 (Postulat de Bertrand)**.** *Sigui $n \geq 1$ un nombre natural no nul qualsevol. Existeix un nombre natural primer p tal que $n < p \leq 2n$.*

3.4 Teorema fonamental de l'Aritmètica (TFA)

Proposició 3.4.1. *Siguin a, b, c nombres enters. Suposem que $a \mid bc$ i que $\mathrm{mcd}(a,b) = 1$, és a dir, a i b són primers entre si. Llavors, $a \mid c$.*

Proposició 3.4.2. *Siguin a, b nombres enters i sigui p un nombre natural primer. Si p divideix el producte ab i p no divideix a, llavors, p divideix b.*

Demostració. Suposem que p és un nombre primer i que p divideix el producte ab i no divideix a. Com que p és primer, els únics divisors de p són $\pm 1, \pm p$; i, com que a no és divisible per p, és $\mathrm{mcd}(p,a) = 1$. En virtut de la proposició anterior, $p \mid b$. ■

Proposició 3.4.3. *Tot nombre natural és producte de primers.*

Teorema 3.4.4 (Teorema Fonamental de l'Aritmètica)**.** *Sigui $a \neq 0, \pm 1$ un nombre enter. Existeixen nombres naturals primers $p_1, \ldots, p_n$ i existeix $\epsilon \in \{-1, 1\}$ tals que $a = \epsilon p_1 p_2 \ldots p_n$. A més, llevat de l'ordre, ϵ i els nombres p_i són únics.*

Demostració. Si $a < 0$, prenem $\epsilon = -1$ i, si $a > 0$, prenem $\epsilon = 1$. D'aquesta manera, i com que el producte de nombres naturals és un nombre natural, és suficient demostrar que tot nombre natural $a > 1$ s'expressa de manera única, llevat de l'ordre, com a producte de nombres naturals primers.

Si a és primer, aleshores a és el producte de 1 per a, que és primer. Això demostra l'existència de descomposició en aquest cas. Ara podem procedir per inducció; si a no és primer, aleshores a és divisible per un nombre natural primer, posem p_1. Com que a no és primer, el nombre $b = \frac{a}{p_1} < a$ és un nombre natural menor estricte que a; per hipòtesi d'inducció, podem suposar

que b és producte de nombres primers, $b = p_2 \dots p_n$; aleshores, $a = p_1 p_2 \dots p_n$ també és producte de nombres primers.

Resta veure la unicitat de la descomposició. Per a això, suposem que $a = \epsilon p_1 p_2 \dots p_n = \epsilon' q_1 q_2 \dots q_m$, amb $\epsilon, \epsilon' \in \{-1, 1\}$ i $p_1, \dots, p_n, q_1, \dots, q_m$ nombres naturals primers. Com que els productes $p_1 p_2 \dots p_n$ i $q_1 q_2 \dots q_m$ són nombres naturals, els dos signes han de coincidir; això demostra la igualtat $\epsilon' = \epsilon$ i, en conseqüència, la igualtat $p_1 \dots p_n = q_1 \dots q_m$.

D'altra banda, com que el nombre p_1 és un divisor primer del producte $q_1 \dots q_m$, p_1 ha de dividir algun dels factors; reordenem, si convé, els nombres q_j, a fi de poder suposar que p_1 divideix q_1. Com que q_1 és primer, ha de ser $p_1 = q_1$. Si simplifiquem, obtenim la nova igualtat $p_2 \dots p_n = q_2 \dots q_m$. Repetim successivament aquest procés amb $p_2, \dots, p_n$: obtenim que ha de ser $m \geq n, p_i = q_i$, per a $1 \leq i \leq n$ i $1 = q_{n+1} \dots q_m$. Però 1 no és divisible per cap nombre primer, de manera que $n = m$ i ja hem acabat. ■

Observació 3.4.5. Podem agrupar els nombres primers que apareixen a la descomposició i escriure-la en la forma

$$a = \epsilon \prod_p p^{v_p(a)}, \tag{3.4.1}$$

amb $v_p \geq 0$ i el producte estès a tots els naturals primers diferents. Aquesta expressió té sentit, ja que $v_p = 0$ per a tots els nombres primers p llevat d'una quantitat finita i, per tant, el producte és finit.

Definició 3.4.6. Si $a = \epsilon \prod_p p^{v_p(a)}$ és la descomposició en factors primer d'un nombre enter $a \neq 0$, el nombre natural $v_p(a)$ s'anomena *valoració p-àdica* d'a. Per a completar la definició en $a = 0$, s'escriu $v_p(0) = \infty$.

Proposició 3.4.7. *Donat un nombre primer p, les valoracions p-àdiques de nombres enters $a, b, a + b, ab$ estan relacionades de la manera següent:*

1. $v_p(1) = 0$,
2. $v_p(ab) = v_p(a) + v_p(b)$,
3. $v_p(a + b) \geq \min(v_p(a), v_p(b))$.

Observació 3.4.8. D'aquí, és molt fàcil demostrar que $v_p(\mathrm{mcd}(a, b)) = \min(v_p(a), v_p(b))$

Teorema Fonamental de l'Aritmètica: polinomis

Lema 3.4.9 (Lema Fonamental de l'Aritmètica**).** *Sigui $P(x)$ irreductible en $\mathbb{K}[x]$. Si $P(x) \mid a(x)b(x) \implies P(x) \mid a(x) \vee P(x) \mid b(x)$.*

Demostració. Suposem que $P(x) \nmid a(x)$. Per 3.2.18, tenim que $\mathrm{mcd}(P(x), a(x)) = 1$. Aplicant la identitat de Bézout, existeixen $s(x), t(x)$ tals que $P(x)s(x) + a(x)t(x) = 1$. Multiplicant per $b(x)$, obtenim $P(x)s(x)b(x) + a(x)t(x)b(x) = b(x)$. Dividint a banda i banda per $P(x)$:

$$\frac{P(x)s(x)b(x)}{P(x)} + \frac{a(x)t(x)b(x)}{P(x)} = \frac{b(x)}{P(x)} \iff s(x)b(x) + t(x)q(x) = \frac{b(x)}{P(x)} \implies P(x) \mid b(x). \tag{3.4.2}$$

■

Aplicant inducció sobre el nombre de factors, es dedueix fàcilment el següent corol·lari:

Corol·lari 3.4.10. *Sigui $P(x) \in \mathbb{K}[x]$ irreductible. Si $P(x) \mid a_1(x) \cdots a_r(x)$, se segueix que per a algun $i \in \{1, 2, \ldots, r\}$, $P(x) \mid a_i(x)$.*

Teorema 3.4.11 (Teorema de Descomposició en Factors Irreductibles)**.** *Sigui $f(x) \in \mathbb{K}[x], \operatorname{gr}(f(x)) > 0$. Aleshores, $f(x)$ es descomposa com a producte de polinomis irreductibles,*

$$f(x) = P_1(x) \cdots P_r(x). \tag{3.4.3}$$

Així mateix, si es té una altra descomposició en producte d'irreductibles $f(x) = Q_1(x) \cdots Q_s(x)$, $r = s$. I, després de reordenar si cal, es té que $P_i(x)$ i $Q_i(x)$ són associats, per a tot $i \in \{1, 2, \ldots, r\}$.

Demostració. Hem de provar existència i unicitat. Provem primerament l'existència i després la unicitat.

1. Si $f(x)$ és irreductible el resultat és trivial. De fet, aquest cas particular prova allò que volem per tot polinomi de grau 1. Si no ho és, $f(x) = f_1(x)f_2(x)$, $\operatorname{gr}(f_1), \operatorname{gr}(f_2) < \operatorname{gr}(f)$. Per tant, podem aplicar la hipòtesi d'inducció per afirmar que tant $f_1(x)$ com $f_2(x)$ es poden descompondre com a producte d'irreductibles.
2. La unicitat es prova com en el cas del TFA aplicat als $\mathbb{Z}$. Partint de les dues expressions de $f(x) = P_1(x) \cdots P_r(x) = Q_1(x) \cdots Q_s(x)$: com $P_1(x)$ és irreductible i divideix a un producte, ha de dividir algun $Q_i(x)$. Reordenant, si cal, suposem $P_1(x) \mid Q_1(x)$. Com $Q_1(x)$ és irreductible, i $P_1(x)$ té grau positiu per definició d'irreductible, han de ser associats: $P_1(x) = c_1 Q_1(x)$. Per tant, cancel·lant P_1 i Q_1 a la igualtat anterior, posant c_1 a l'inici, ens queda: $c_1 P_2(x) P_3(x) \cdots P_r(x) = Q_2(x) Q_3(x) \cdots Q_S(x)$.
   Iterant el raonament, concloem que $P_2(x)$ és associat de $Q_2(x)$ i, així, successivament, que cada $P_i(x)$ és associat d'algun $Q_i(x)$. És fàcil veure que ha de ser $r = s$: si no fos així, s'arribaria a la igualtat entre una constant i un producte de polinomis de grau positiu ($\perp$).

■

Observació 3.4.12. Si treballem amb polinomis irreductibles mònics, aconseguim que els factors irreductibles quedin unívocament determinats. És a dir, vegem que si $f(x) \in \mathbb{K}[x], \operatorname{gr}(f) > 0$, i coeficient principal a_n, es té:

$$f(x) = a_n \cdot P_1(x) P_2(x) \cdots P_r(x), \tag{3.4.4}$$

on els P_i són mònics i irreductibles. Una tal descomposició en mònics i irreductibles és única excepte per l'ordre dels factors.

Arrels de polinomis (aplicades a la descomposició)

Podem veure un polinomi com una funció de $\mathbb{K}$ en $\mathbb{K}$, és a dir, substituint la x per un valor $k \in \mathbb{K}$ obtenim la seva imatge $P(k) \in \mathbb{K}$. Són particularment útils les arrels d'un polinomi, que són aquells valors $k \in \mathbb{K}$ tals que $P(k) = 0$, si és que existeixen.

Teorema 3.4.13. *Si $k \in \mathbb{K}$ i $P(x) \in \mathbb{K}[x]$, el valor $P(k)$ coincideix amb el residu de dividir $P(x)$ per $(x - k)$.*

Demostració. Com $x-k$ és de grau 1, és evident que el residu de dividir $P(x)$ entre $(x-k)$ serà un polinomi constant r. Es té que $P(x) = (x-k)Q(x)+r$. Substituint: $P(k) = 0 \cdot Q(x)+r = r$. ■

Corol·lari 3.4.14. *k és arrel de $P(x) \iff (x-k) \mid P(x)$.*

Demostració. A partir del teorema anterior, suposant $P(k) = 0$, és a dir, que k és arrel de $P(x)$, equival a dir que el residu de dividir $P(x)$ entre $(x-k)$ és igual a 0, és a dir, que $(x-k) \mid P(x)$. ■

Definició 3.4.15. Si $c \in \mathbb{K}$ és arrel de $P(x) \in \mathbb{K}[x]$, diem que té multiplicitat i si i és la major potència tal que $(x-c)^i \mid P(x)$. És evident que es té $i \geq 1$.

Teorema 3.4.16 (Goldbach)**.** *No existeix cap polinomi no constant $f(X) \in \mathbb{Z}[x]$ tal que $f(N)$ sigui primer per a tot nombre enter N.*

Capítol 4

Congruències lineals

4.1 Introducció

Recordem breument una sèrie de conceptes introductoris útils en aquest capítol.

Definició 4.1.1 (Relació de A en B)**.** Si A i B són dos conjunts, una relació de A en B és un subconjunt de $A \times B$.

Definició 4.1.2. Si $R \subseteq A \times B$ és una relació i $(a, b) \in R$, direm que *a està relacionat amb b per R*. En moltes ocasions escriurem aRb en lloc de $(a, b) \in \mathbb{R}$.

Sigui R una relació sobre un conjunt A:

Definició 4.1.3 (Relació reflexiva)**.** Diem que R és **reflexiva** si per a tot $a \in A$, aRa.

Definició 4.1.4 (Relació irreflexiva)**.** Diem que R és **irreflexiva** si per a tot $a \in A$, és fals que aRa.

Definició 4.1.5 (Relació simètrica)**.** Diem que R és **simètrica** si per a tot $a, b \in A$,

$$aRb \implies bRa. \tag{4.1.1}$$

Definició 4.1.6 (Relació antisimètrica)**.** Diem que R és **antisimètrica** si per a tot $a, b \in A$,

$$aRb \wedge bRa \implies a = b. \tag{4.1.2}$$

Definició 4.1.7 (Relació transitiva)**.** Diem que R és **transitiva** si per a tot $a, b, c \in A$,

$$aRb \wedge bRc \implies aRc. \tag{4.1.3}$$

Definició 4.1.8 (Relació d'ordre en A)**.** Diem que R és una **relació d'ordre en** A si R és reflexiva, antisimètrica i transitiva.

Definició 4.1.9. Diem que R és una **relació d'ordre total en** A si R és una relació d'ordre en A tal que per a tot $x, y \in A$ es té que xRy o yRx.

Definició 4.1.10 (Ideal)**.** Un ideal $\mathfrak{a}$ d'un anell A és un subconjunt no buit $\mathfrak{a} \subseteq A$ tal que si $a, b \in \mathfrak{a}$ i $\lambda \in A$, aleshores $a + b, \lambda a \in \mathfrak{a}$.

Proposició 4.1.11. *Sigui $\mathfrak{a} \subseteq \mathbb{Z}$ un ideal qualsevol. Existeix un enter a tal que $\mathfrak{a} = a\mathbb{Z}$.*

4.2 Definició i propietats bàsiques

Definició 4.2.1. Sigui $n \in \mathbb{Z} > 0$. Donats $a, b \in \mathbb{Z}$, direm que a és congruent amb b mòdul n, i escriurem $a \equiv b \pmod{n}$ si $n \mid a - b$.

En particular, si en la divisió entera entre a i n es té quocient q i residu r, $0 \leq r < n$, es compleix

$$a = nq + r \implies a - r = nq \implies n \mid a - r \implies \mathbf{a \equiv r} \pmod{\mathbf{n}}. \tag{4.2.1}$$

En altres paraules, tot enter a és congruent mòdul n amb un únic nombre $r \in \{0, 1, \ldots, n-1\}$, ja que si $a \equiv r \pmod{n}$ i $0 \leq r < n$, aleshores r ha de ser, necessàriament, el residu de la divisió d'a entre n.

Proposició 4.2.2. *Sigui $n \in \mathbb{Z}$. La relació de congruència mòdul n és una relació d'equivalència; és a dir, si a, b, c són nombres enters qualssevol, se satisfan les propietats següents:*

1. ***Reflexiva**: $a \equiv b \pmod{n}$;*
2. ***simètrica**: si $a \equiv b \pmod{n}$, aleshores $b \equiv a \pmod{n}$;*
3. ***transitiva**: si $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n}$, aleshores $a \equiv c \pmod{n}$.*

Demostració. No demostrarem les dues primeres propietats perquè són evidents. Pel que fa a la transitivitat, si $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n} \implies n \mid a-b$ i $n \mid b-c \implies n \mid (a-b)+(b-c) = a - c \implies a \equiv c \pmod{n}$. ∎

Definició 4.2.3 (Classes residuals). Els enters queden repartits en les n classes d'equivalència (són n perquè, recordem, cadascun té un representant $r \in \{0, 1, \ldots, n-1\}$, que és un conjunt de cardinal n): les classes residuals mòdul n. Sigui $u \in \mathbb{Z}$, denotarem per $\hat{u}$ la classe residual que conté a u. Al conjunt d'aquestes classes residuals el denotarem $\mathbb{Z}/n\mathbb{Z}$, és a dir,

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}. \tag{4.2.2}$$

Definició 4.2.4 (Classes residuals, alternativa). Sigui $n \geq 2, n \in \mathbb{Z}$. Per a tot $a \in \mathbb{Z}$, anomenarem classe residual d'a mòdul n el conjunt $\overline{a} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$. Cada element $b \in \overline{a}$ s'anomena un representant de la classe. Aleshores, clarament, $b \in \overline{a} \implies \overline{b} = \overline{a}$.

Proposició 4.2.5.

1. *Per a tot enter q, $\overline{a} = \overline{a + qn}$,*
2. *Hi ha exactament n classes residuals diferents $\overline{a}$ mòdul n: són els conjunts $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.*

Exemple 4.2.6. El conjunt $\mathbb{Z}/4$ de les classes residuals mòdul 4 consta de quatre elements o classes: $\mathbb{Z}/4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, que són:

1. Classe del 0: $\overline{0} = \{\ldots, -8, -4, 0, 4, 8, 12, \ldots\}$, en altres paraules, els múltiples del 4;
2. Classe de l'1: $\overline{1} = \{\ldots, -7, -3, 1, 5, 9, 13, \ldots\}$, en altres paraules, els múltiples del $4 + 1$;
3. Classe del 2: $\overline{2} = \{\ldots, -6, -2, 2, 6, 10, 14 \ldots\}$, en altres paraules, els múltiples del $4 + 2$;
4. Classe del 3: $\overline{3} = \{\ldots, -5, -1, 3, 7, 11, 15 \ldots\}$, en altres paraules, els múltiples del $4 + 3$.

Propietat 4.2.7. *La suma, resta i producte en $\mathbb{Z}$ indueixen operacions anàlogues (amb idèntiques propietats commutativa, associativa i distributiva) en aquestes classes residuals, doncs estan ben definides, és a dir, no depenen del representant escollit en la classe habitual:*

$$\begin{aligned} a \equiv a' \pmod{n},\ b \equiv b' \pmod{n} \\ \implies a + b \equiv a' + b' \pmod{n} \\ \implies a - b \equiv a' - b' \pmod{n} \\ \implies a \cdot b \equiv a' \cdot b' \pmod{n} \end{aligned} \tag{4.2.3}$$

Demostració. Les dues primeres es dedueixen fàcilment de $n \mid x, n \mid y \implies n \mid x \pm y$. Per al cas del producte, de la propietat $n \mid x \implies n \mid xz$, es dedueix que $a \equiv a' \pmod{n} \implies ab \equiv a'b \pmod{n}$. Per altra banda, com que $b \equiv b' \pmod{n} \implies a'b \equiv a'b' \pmod{n}$. Ajuntant les dues: $a \cdot b \equiv a' \cdot b' \pmod{n}$. ■

Observació 4.2.8. A partir de les propietats anteriors, se segueix que $\forall s \geq 0$, $a \equiv b \pmod{n} \implies a^s \equiv b^s \pmod{n}$. També, si $P(x)$ és un polinomi amb coeficients en $\mathbb{Z}$, es té $a \equiv b \pmod{n} \implies P(a) \equiv P(b) \pmod{n}$.

Proposició 4.2.9. *Sigui n un nombre enter. Les propietats següents són equivalents:*

1. *l'anell $\mathbb{Z}/n\mathbb{Z}$ és un cos,*
2. *el nombre n és equivalent.*

Observació 4.2.10. Recordem que un cos és un anell commutatiu tal que els elements neutres per a la suma i per a la multiplicació són diferents i tot element diferent del neutre per a la suma té un invers per a la multiplicació.

Proposició 4.2.11. *Si $n \geq 1$, i es té enters a, b, c amb $ac \equiv bc \pmod{n}$, amb $d = \mathrm{mcd}(c, n)$, es té $a \equiv b \pmod{\frac{n}{d}}$.*

Demostració. Com $d = \mathrm{mcd}(c, n)$, si anomenem $\frac{c}{d} = c'$ i $\frac{n}{d} = n'$, es té que $\mathrm{mcd}(c', n') = 1$. Substituint $c = dc'$ i $n = dn'$ i operant:

$$\begin{aligned} adc' \equiv bdc' \pmod{n} &\iff dn' \mid (dac' - dbc') = d(ac' - bc') \iff n' \mid (ac' - bc') \\ &\iff n' \mid c'(a - b) \xrightarrow{\mathrm{mcd}(c', n') = 1} n' \mid a - b \implies a \equiv b \pmod{n}. \end{aligned} \tag{4.2.4}$$

■

Corol·lari 4.2.12. *Si a, b, c, n, $\mathrm{mcd}(c, n) = 1$, aleshores $ac \equiv bc \pmod{n} \implies a \equiv b \pmod{n}$.*

Lema 4.2.13. *Sigui R un conjunt de n enters que representen a totes les classes residuals $\mathbb{Z}/n\mathbb{Z}$. Sigui a un enter tal que $\mathrm{mcd}(a, n) = 1$. Aleshores $aR = \{ax \mid x \in R\}$ també compleix que els seus elements representen totes les classes de $\mathbb{Z}/n\mathbb{Z}$.*

Demostració. Com R posseeix n elements, que sabem que recorren totes les classes residuals mòdul n, aR també posseeix n elements. Com hi ha n classes residuals mòdul n, provar que els elements d'aR representen a totes les classes residuals és equivalent a provar que cap parell d'ells representa a la mateixa classe residual. Suposem que es tenen $x, x' \in R$ tals que $ax \equiv ax' \pmod{n} \implies x = x'$. Per tant, diferents elements d'aR no cauen en la mateixa classe residual mòdul n. ■

Proposició 4.2.14. *Si $n > 1$ i $a, b \in \mathbb{Z}, \mathrm{mcd}(a, n) = 1 \implies ax \equiv b \pmod{n}$ té solució, i és única mòdul n.*

Demostració. Si agafem $R = \{0, 1, \ldots, n-1\}$ com $\mathrm{mcd}(a, n) = 1$ veiem que a i R compleixen les condicions del lema previ, així doncs sabem que $aR = \{0, 1, \ldots, n-1\}$ recorre totes les classes residuals. En particular, algun element cau en la classe de b, és a dir, existeix i tal que $ai \equiv b \pmod{n}$.

Per a veure la unicitat (com a classe mòdul n), suposem que tenim dos enters x, x' amb $ax \equiv b \equiv ax' \pmod{n}$. D'aquí, per 4.2.12 i $\mathrm{mcd}(a, n) = 1$, tenim que $x \equiv x' \pmod{n}$. ■

Definició 4.2.15 (Element invertible)**.** Són elements invertibles mòdul m aquells a tals que existeix una solució per a la congruència $ax \equiv 1 \pmod{m}$. En aquest cas, a un b tal que $ab \equiv 1 \pmod{m}$, l'anomenem *invers d'a mòdul m*.

Proposició 4.2.16. *Si $a, b \in \mathbb{Z}$, $n > 1$, es té que $ax \equiv b \pmod{n}$ té solució si, i només si, $\mathrm{mcd}(a, n) \mid b$. En particular, en el cas $b = 1$: a té invers mòdul $n \iff a$ coprimer amb n.*

Demostració. Sigui $g = \mathrm{mcd}(a, n)$. Suposem que existeix un $x \in \mathbb{Z}$, solució de la congruència $n \mid ax - b$. Ara, com $g \mid n \implies g \mid ax - b$. A més, com es té que $g \mid a$, $g \mid ax$. Per tant, $g \mid (ax - (ax - b)) = b$.

Recíprocament, suposem que $g \mid b$. Aleshores, com $g \mid a$, $g \mid n$ i $g \mid b$, es té l'equivalència

$$n \mid ax - b \iff \frac{n}{g} \mid \frac{a}{g}x - \frac{b}{g}. \tag{4.2.5}$$

Per tant, l'equació $ax \equiv b \pmod{n}$ té solució si, i només si, l'equació $\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{n}{g}}$ té solució. Com $\mathrm{mcd}(\frac{a}{g}, \frac{n}{g}) = 1$, sabem que per la proposició prèvia té solució. ■

Lema 4.2.17. *Siguin $a_1, \ldots, a_k$, n enters amb $a_i \mid n, i \in \{1, 2, \ldots, k\}$ tals que els a_i són coprimers dos a dos. Es té que $a_1 a_2 \cdots a_k \mid n$.*

Proposició 4.2.18. $\mathrm{mcd}(a, m) = 1 \iff a$ *és invertible mòdul* m.

Demostració.

$\implies$ Suposant $\mathrm{mcd}(a, m) = 1$, per la identitat de Bézout existeixen $s, t \in \mathbb{Z}$ tals que $sa + tm = 1$. D'aquí, veiem que $1 - sa = tm$, d'on $sa \equiv 1 \pmod{m}$. Concloem que existeix l'invers d'a mòdul m, el qual es pot calcular resolent una identitat de Bézout.

$\impliedby$ Suposant l'existència de l'invers d'a mòdul m, es dedueix que hi ha solució per a l'equació $sa - tm = 1$, d'on es dedueix que a és coprimer amb m.

■

Definició 4.2.19. Anomenarem les classes residuals mòdul m formades per elements que tenen invers mòdul m (compleixen que $\mathrm{mcd}(a, m) = 1$) *classes invertibles mòdul m*.

4.3

El teorema xinès del residu

Teorema 4.3.1 (Teorema Xinès del Residu (TXR)). *Donats $m_1, \ldots, m_k$ enters positius coprimers dos a dos, i enters $c_1, \ldots, c_k$, el sistema de congruències*

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \qquad \vdots \\ x \equiv c_k \pmod{m_k} \end{cases} \tag{4.3.1}$$

Té solució, i la solució és única mòdul $m = m_1 m_2 \cdots m_k$.

Demostració. Si definim $M_i = \frac{m}{m_i}$ per a $i = 1, 2, \ldots, k$ es té $m = m_i M_i$. Observi's que M_i és el producte de tots els m_i amb $i \neq j, j \in \{1, 2, \ldots, k\}$. És fàcil veure que $\mathrm{mcd}(a, b) = 1$ i $\mathrm{mcd}(a, c) = 1 \implies \mathrm{mcd}(a, bc) = 1$, i el mateix pel cas de més de dos factors, per la qual cosa, al ser els m_i coprimers dos a dors, veiem que $\mathrm{mcd}(m_i, M_i) = 1$. D'aquí, per 4.2.14 concloem que existeix n_i tal que $n_i M_i \equiv 1 \pmod{m_i}$ per a tot $i = 1, \ldots, k$. Considerem l'enter $x = \sum_{i=1}^{k} n_i M_i c_i$. Aleshores, es té $x \equiv n_i M_i c_i \equiv 1 \cdot c_i \pmod{m_i}$, resolent x el sistema.

Per a veure la unicitat mòdul m, siguin x, y solucions del sistema. Aleshores, $x \equiv c_i \equiv y \pmod{m_i}$ per a tot $i = 1, \ldots, r \implies m_i \mid x - y$, per a tot $i = 1, 2, \ldots, r$. Com els m_i són coprimers dos a dos, el lema previ implica que $m \mid x - y$, és a dir, $x \equiv y \pmod{m}$. ■

Observació 4.3.2. La demostració permet calcular, en qualsevol exemple donat, la solució del sistema. El pas més complex és el càlcul de inversos per a elements coprimers amb el mòdul, cosa que es redueix fàcilment a resoldre la identitat de Bézout, doncs $ax \equiv 1 \pmod{m} \iff ax - 1 = my$, per a algun enter y, $\iff ax - my = 1$, que és la identitat de Bézout per a a i $-m$, donat que $\mathrm{mcd}(a, -m) = \mathrm{mcd}(a, m) = 1$.

4.4

Petit teorema de Fermat

Teorema 4.4.1 (Petit teorema de Fermat). *Sigui p un nombre primer i a un enter no divisible per p. Es té:*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{4.4.1}$$

Demostració. Considerem $R = \{0, 1, \ldots, p-1\}$ que compleix que els p elements de R representen totes les classes residuals mòdul p. Com la condició "a no divisible per p"és equivalent a $\mathrm{mcd}(a, p) = 1$, doncs p és primer, aplicant el lema de la classe anterior veiem que els elements de $aR = \{0, a, \ldots, (p-1)a\}$ també representen a totes les classes residuals mòdul p. Considerem ara conjunts anàlegs, però amb el 0 exclòs: $R' = R \setminus \{0\}$ i $R'' = aR \setminus \{0\}$. Deduïm que tant els $p-1$ elements d'R' com els $p-1$ elements d'R'' recorren les $p-1$ classes residuals mòdul p diferents de les classes del 0. Per tant, si multipliquem tots els elements d'ambdós conjunts tenim la congruència:

$$1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv a \cdot (2a) \cdot \cdots \cdot (p-1)a \pmod{p} \implies (p-1)! \equiv a^{p-1} \cdot (p-1)! \pmod{p}. \tag{4.4.2}$$

Aplicant la cancel·lativa, ja que $(p-1)!$ és coprimer amb p i y, obtenim $1 \equiv a^{p-1} \pmod{p}$. ■

Demostració alternativa del petit teorema de Fermat. L'enunciat d'aquest teorema ens diu que per a p primer i a amb p no dividint a a es té que $a^{p-1} \equiv 1 \pmod{p}$. Hem de veure que això equival a dir $a^p \equiv a \pmod{p}$. De fet, per a passar de la primera a la segona congruència sol fa falta multiplicar per a ambdós membres, i per a passar de la segona a la primera cal cancel·lar a, cosa que es pot fer donat que $\mcd(a,p) = 1$. Per tant, el teorema equival a provar $a^p \equiv a \pmod{p}$.

Com és evident que $a = 0$ compleix la propietat i que si un enter la compleix el seu oposat també, podem reduir-ho al cas $a > 0$. Volem provar-ho per a tot a sense restriccions, així que procedim per inducció.

1. Cas inicial: $a = 1$, és evident.
2. Suposem un $a \geq 1$ que compleix la proposició (hipòtesi d'inducció) i vegem també que és certa per a $a+1$. Aplicant la fórmula del binomi de Newton:

$$(a+1)^p \equiv \sum_{j=0}^{p} a^j = \sum_{j=0}^{p} \frac{p!}{j!(p-j)!} a^j \equiv a^p + 0 + \cdots + 0 + 1 \pmod{p}. \tag{4.4.3}$$

   Aplicant la hipòtesi d'inducció $a^p \equiv a \pmod{p}$, concloem que: $(a+1)^p \equiv (a+1) \pmod{p}$. Això acaba la prova per inducció.

■

Teorema 4.4.2 (Teorema de Fermat-Wiles)**.** *Si $n > 2$, l'equació $X^n + Y^n = Z^n$ no té solucions enteres positives.*

4.5 Funció phi d'Euler

Definició 4.5.1. Designarem per $(\mathbb{Z}/n\mathbb{Z})^*$ el grup multiplicatiu format pels elements invertibles de l'anell $\mathbb{Z}/n\mathbb{Z}$. Així, $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{b} \in \mathbb{Z}/n\mathbb{Z} \mid b \in \mathbb{Z}, \mcd(b,n) = 1\}$.

Definició 4.5.2 (Funció φ d'Euler)**.** Donat $n > 1, n \in \mathbb{Z}$. Anomenem $\varphi(n)$ a la quantitat de classes residuals en $\mathbb{Z}/n\mathbb{Z}$ que són invertibles mòdul n (o, equivalentment, que són coprimers amb n).

Exemple 4.5.3. $\varphi(6) = 2$. De fet, solament enters 1 i 5 de l'interval $[1,6]$ són coprimers amb 6. Ara suposem un p primer, $\varphi(p) = p - 1$: això es dedueix a partir del fet que la única classe no invertible mòdul p és la d'enters divisibles per p, és a dir, la classe dels congruents amb 0 mòdul p.

Teorema 4.5.4 (Teorema d'Euler)**.** *Sigui $n > 1$ i $a \in \mathbb{Z}$ amb $\mcd(a,n) = 1$. Aleshores, es compleix que $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Demostració. Sigui $S = \{x_1, x_2, \ldots, x_r\}$, format per un representant de cada classe invertible mòdul n, amb $|S| = r = \varphi(n)$. Comencem provant un anàleg al lema de la classe anterior però ara per a aquestes classes invertibles.

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

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

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

$$x_1 \cdots x_r \equiv ax_1 \cdots ax_r \pmod{n}, \tag{4.5.1}$$

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

Propietats de la funció phi d'Euler

Definició 4.5.5. La funció φ que apareix en el teorema d'Euler té per valor $\varphi(n)$, amb $n > 0$, el cardinal del conjunt $(\mathbb{Z}/n\mathbb{Z})^*$, que és igual al cardinal de

$$U_n = \{a \mid 1 \leq a \leq n, \text{mcd}(a,n) = 1\}. \tag{4.5.2}$$

Definició 4.5.6. Una funció $f : \mathbb{N} \longrightarrow \mathbb{R}$ s'anomena multiplicativa si, $\forall a, b \in \mathbb{N}$ amb $\text{mcd}(a,b) = 1$ es té que $f(ab) = f(a)f(b)$.

Propietat 4.5.7.

1. *φ és multiplicativa,*
2. *si p és primer, $\varphi(p^r) = p^{r-1}(p-1)$.*

Demostració. Si $a, b \in \mathbb{N}$, $\text{mcd}(a,b) = 1$, volem veure que $\varphi(a,b) = \varphi(a) \cdot \varphi(b)$. Recordar que $\varphi(a)$ és el cardinal de $(\mathbb{Z}/a\mathbb{Z})^*$, o, el que és el mateix, U_a. I el mateix és vàlid per $\varphi(b)$ i per a $\varphi(ab)$. El que volem demostrar, doncs, és que

$$|(\mathbb{Z}/a\mathbb{Z})^*| \cdot |(\mathbb{Z}/b\mathbb{Z})^*| = |(\mathbb{Z}/ab\mathbb{Z})^*|, \tag{4.5.3}$$

on $|C|$ denota el cardinal d'un conjunt C. Per tal de provar-ho, construïm una funció tal que

$$f : (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^* \longrightarrow (\mathbb{Z}/ab\mathbb{Z})^*. \tag{4.5.4}$$

Sigui $\overline{C_1} \in (\mathbb{Z}/a\mathbb{Z})^*$ i $\overline{C_2} \in (\mathbb{Z}/b\mathbb{Z})^*$. Pel Teorema Xinès de la Resta, existeix $\overline{C} \in (\mathbb{Z}/ab\mathbb{Z})^*$ amb $C \equiv C_1 \pmod{a}$ i $C \equiv C_2 \pmod{b}$. La condició que $\overline{C} \in (\mathbb{Z}/ab\mathbb{Z})^*$, és a dir, que és invertible en $\mathbb{Z}/ab\mathbb{Z}$ es desprèn del fet que per ser C_1 coprimer amb a i C_2 coprimer amb b, al ser C solució del sistema C també és coprimer amb a i amb b, aleshores amb ab, amb la qual cosa $\text{mcd}(C, ab) = 1$. Definim aleshores $f(\overline{C_1}, \overline{C_2}) = \overline{C}$.

Vegem que f és injectiva: si $f(\overline{C_1}, \overline{C_2}) = \overline{C} = f(\overline{C_3}, \overline{C_4}) \implies C_1 \equiv C \equiv C_3 \pmod{a}$ i $C_2 \equiv C \equiv C_4 \pmod{b}$, d'on $\overline{C_1} = \overline{C_3} \in (\mathbb{Z}/a\mathbb{Z})^*$ i $\overline{C_2} = \overline{C_4} \in (\mathbb{Z}/b\mathbb{Z})^*$, és a dir, f és injectiva.

Vegem que f és exhaustiva: donat $\overline{C} \in (\mathbb{Z}/ab\mathbb{Z})^*$, considerem $\overline{C_1}$ la corresponent classe residual mòdul a i $\overline{C_2}$ la corresponent classe mòdul b. Així, es té que $C \equiv C_1 \pmod{a}$ i $C \equiv C_2 \pmod{b}$, aleshores, $\text{mcd}(C_1, a) = \text{mcd}(C_2, b) = 1$, és a dir, $\overline{C_1} \in (\mathbb{Z}/a\mathbb{Z})^*$ i $\overline{C_2} \in (\mathbb{Z}/b\mathbb{Z})^*$. Per tant, f és exhaustiva.

Com f és una funció bijectiva del producte $(\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$ en $(\mathbb{Z}/ab\mathbb{Z})^*$, concloem que (4.5.3) és certa, amb la qual cosa queda provat que $\varphi(ab) = \varphi(a) \cdot \varphi(b)$. Sabem que $\varphi(p^r)$ és el cardinal del conjunt $U_{p^r} = \{a \mid 1 \leq a \leq p^r, \mathrm{mcd}(a, p^r) = 1\}$. Com p és primer, la condició $\mathrm{mcd}(a, p^r) = 1$ equival a $\mathrm{mcd}(a, p) = 1$ que, al seu torn, equival que a no és múltiple de p. Com hi ha un múltiple de p cada p enters consecutius, la quantitat de múltiples de p en l'interval $[1, p^r]$ és $\frac{p^r}{p} = p^{r-1}$. Aleshores,

$$|U_{p^r}| = p^r - p^{r-1} = p^{r-1}(p-1). \tag{4.5.5}$$

Es pot consultar la demostració de [Gra98, pàg. 136 - 1.7], més breu. ■

Corol·lari 4.5.8. *Si $n \geq 1$, amb $n = \prod_{i=1}^{r} p_i^{s_i}$ es té que*

$$\varphi(n) = n \cdot \prod_{i=1}^{r} \frac{p_i - 1}{p_i}. \tag{4.5.6}$$

Corol·lari 4.5.9. *Per a tot nombre $n \in \mathbb{Z}, n \geq 3$, el nombre $\varphi(n)$ és parell.*

Proposició 4.5.10. *Sigui $N \geq 1, N \in \mathbb{Z}$. Se satisfà $\sum_{d|N} \varphi(d) = N$, on la suma s'estén a tots els divisors d d'N tals que $1 \leq d \leq N$.*

4.6 Teorema de Wilson

Teorema 4.6.1 (Teorema de Wilson). *Sigui p un nombre primer. Aleshores, es té*

$$(p-1)! \equiv -1 \pmod{p}. \tag{4.6.1}$$

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

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

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

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

4.7 Teorema de Lagrange

Teorema 4.7.1. *Sigui $F(x)$ polinomi a coeficients enters de grau $d > 0$. Sigui p un nombre primer. Suposem que no tots els coeficients de f són divisibles per p. El nombre de classes de congruència mòdul p que són solució de la congruència $F(x) \equiv 0 \pmod{p}$ és menor o igual a d.*

Demostració. Apliquem inducció en d. Si $d = 1$, ja hem vist que una congruència lineal $ax+b \equiv 0 \pmod{p}$ té com a màxim una solució mòdul p (de fet si a no és divisible per p, té una sola solució, i si a és divisible per p, la hipòtesi implica que b no ho és, i per tant la congruència no té solució).

Sigui F de grau $d > 1$ i considerem $F(x) \equiv 0 \pmod{p}$. Si no hi hagués cap solució el resultat quedaria provat. Suposem, per tant, que existeix x_0 tal que $F(x_0) \equiv 0 \pmod{p}$. Si fem la divisió de polinomis de $F(x)$ entre $(x - x_0)$ obtenim:

$$F(x) = G(x)(x - x_0) + r, \tag{4.7.1}$$

amb $\operatorname{gr}(G(x)) = d - 1$ i r constant. Avaluant en x_0 ambdós membres, obtenim $F(x_0) = r$, i com $F(x_0) \equiv 0 \pmod{p}$ concloem que $r \equiv 0 \pmod{p}$. Per tant, ens queda $F(x) \equiv G(x)(x - x_0) \pmod{p}$.

És evident que la hipòtesi que ni tots els coeficients de F són divisibles per p també l'ha de complir G. Per hipòtesi d'inducció, sabem que G posseeix, com a molt, $d - 1$ arrels mòdul p. Sigui y_0 una solució de $F(y_0) \equiv 0 \pmod{p}$. Com $F(x) \equiv G(x)(x - x_0) \pmod{p}$, avaluant en y_0 obtenim $F(y_0) \equiv G(y_0)(y_0 - x_0) \equiv 0 \pmod{p}$, la qual cosa equival a $p \mid G(y_0)(y_0 - x_0)$. Per LFA, deduïm que p ha de dividir algun dels dos factors:

$$p \mid G(y_0) \vee p \mid (y_0 - x_0) \iff G(y_0) \equiv 0 \pmod{p} \vee y_0 \equiv x_0 \pmod{p}. \tag{4.7.2}$$

Amb la qual cosa, la classe de congruència de y_0 ha de ser una de les $\leq d - 1$ classes que són arrels mòdul p de $G(x)$ o bé la classe de la solució inicial x_0. Per tant, concloem que hi ha com a màxim d classes de congruència que són arrels mòdul p de $F(x)$. ■

4.8 Apunts finals

Ordre

El teorema d'Euler té com a conseqüències immediates que per a tot nombre enter $N \geq 2$ i tot element $b \in (\mathbb{Z}/N\mathbb{Z})^*$ existeix un exponent $m \geq 1$ tal que $b^m = 1$, i que el menor exponent m per al qual se satisfà aquesta igualtat per a tots els elements $b \in (\mathbb{Z}/N\mathbb{Z})^*$ també satisfà la desigualtat $m \leq \varphi(N)$ [Gra98].

Definició 4.8.1 (Ordre)**.** Sigui $m \geq 1$ i a coprimer amb m. Anomenem *ordre d'a mòdul m* al menor enter positiu e tal que $a^e \equiv 1 \pmod{m}$.

Observació 4.8.2. L'ordre d'a mòdul m solament depèn de la classe de congruència d'a mòdul m, i solament es defineix per a les classes invertibles mòdul m.

Observació 4.8.3. Sabem pel teorema d'Euler que, com $\text{mcd}(a,m) = 1$, es té $a^{\varphi(m)} \equiv 1 \pmod{m}$. Per tant, l'ordre d'$a$ mòdul m existeix i es menor o igual que $\varphi(m)$.

Lema 4.8.4 ($e \mid \varphi(m)$). *Sigui a enter amb $\text{mcd}(a,m) = 1$ i sigui e l'ordre d'a mòdul m. Sigui k l'enter positiu tal que $a^k \equiv 1 \pmod{m}$. Aleshores, $e \mid k$. En particular, es té que $e \mid \varphi(m)$.*

Demostració. Es té $0 < e \leq k$. Si apliquem divisió entera, obtenim que $k = eq + r$, amb $q, r \in \mathbb{Z}$ i $0 \leq r < e$. Com $a^e \equiv 1 \pmod{m} \implies a^{eq} \equiv 1 \pmod{m}$. Aleshores $a^r \equiv a^r \cdot 1 \equiv a^r \cdot a^{eq} \equiv a^{r+eq} \equiv a^k \equiv 1 \pmod{m}$.

És a dir, $a^r \equiv 1 \pmod{m}$. D'aquí, per ser $0 \leq r < e$, de la minimalitat d'e es dedueix que $r = 0$. Amb la qual cosa, $e \mid k$. Com pel teorema d'Euclides sabem que $a^{\varphi(m)} \equiv 1 \pmod{m}$, concloem que $e \mid \varphi(m)$. ■

Corol·lari 4.8.5. *Si $\text{mcd}(a,m) = 1$ i e és l'ordre d'a mòdul m, i es té que $a^s \equiv a^t \pmod{m}$, aleshores $s \equiv t \pmod{e}$.*

Demostració. Per al cas $s > t$: com $\text{mcd}(a,m) = 1$, es dedueix que $\text{mcd}(a^t, m) = 1$, podem aplicar la cancel·lativa i obtenir $a^{s-t} \equiv 1 \pmod{m}$. El lema previ implica, per tant, que $e \mid s-t$, i tal cosa equival a $s \equiv t \pmod{e}$. ■

Proposició 4.8.6. *L'ordre de qualsevol element d'un grup finit divideix l'ordre del grup.*

Lema 4.8.7. *Siguin $N \geq 2, N \in \mathbb{Z}$ i $b \in (\mathbb{Z}/N\mathbb{Z})^*$ un element qualsevol i m l'ordre de b en $(\mathbb{Z}/N\mathbb{Z})^*$. Per a tot $k \in \mathbb{Z}_{>0}$, l'ordre de b^k és $\frac{m}{\text{mcd}(k,m)}$.*

Demostració. Siguin d l'ordre de b^k i $n := \frac{m}{\text{mcd}(k,m)}$; cal veure que $n = d$. Observem, en primer lloc, que $kn = \frac{k}{\text{mcd}(k,m)}m$; com que $\frac{k}{\text{mcd}(k,m)}$ és un nombre enter, el nombre kn és un múltiple de m i, en conseqüència, $(b^k)^n = b^{kn} = 1$. Per tant, l'ordre de b^k és un divisor de n. Recíprocament, com que $b^{dk} = 1$, obtenim que dk és múltiple d'm; en dividir per $\text{mcd}(k,m)$ obtenim que n divideix el producte $d\frac{k}{\text{mcd}(k,m)}$; i, com que $\text{mcd}\left(n, \frac{k}{\text{mcd}(k,m)}\right) = 1$, ha de ser $n \mid d$. Les dues relacions de divisibilitat $d \mid n$ i $n \mid d$ ens ensenyen que $n = d$, com volíem demostrar. ■

Observació 4.8.8. Aquest lema anterior se satisfà per a elements d'un grup finit qualsevol; és a dir, si $b \in G$ és un element d'ordre m d'un grup finit G, l'ordre de l'element b^k és $\frac{m}{\text{mcd}(k,m)}$, per a tot nombre enter k. La demostració és idèntica a la que hem fet per al cas $G = (\mathbb{Z}/N\mathbb{Z})^*$.

Algorisme binari d'exponenciació

Algorisme 4.8.9 (Algorisme binari d'exponenciació). *Donats enters $a, b, m \geq 2$, i $b = b_k 2^k + b_{k-1}2^{k-1} + \cdots + b_1 2 + b_0$ és l'expressió de b en base 2. Volem calcular $a^b \pmod{m}$. L'algorisme és el següent:*

1. *Posem $x = 1$.*
2. *Si és $b = 0$, escriure x i acabar.*
3. *Si b és senar, fer $x = xa \pmod{m}$.*
4. *Fer $b = \lceil \frac{b}{2} \rceil$ i assignar $a = a^2 \pmod{m}$. Tornar al segon pas.*

Capítol 5

Arrels primitives

5.1

Nombres complexos: Propietats bàsiques

Si $\mathbb{R}$ denota el cos dels nombres reals, sabem que per a tot $x \in \mathbb{R}$ es té que $x^2 \geq 0$. Així doncs, l'equació $x^2 + 1 = 0$ no té solucions en $\mathbb{R}$, és a dir, en $\mathbb{R}$ no existeix $\sqrt{-1}$. Creem el cos $\mathbb{C}$ dels nombres complexos, que contindrà el cos dels $\mathbb{R}$, en què existirà un nombre i tal que $i^2 = -1$.

Anomenarem $\mathbb{C}$ al conjunt de les expressions de la forma $a + bi, a, b \in \mathbb{R}$, on $a + bi = a' + b'i \iff a = a', b = b'$, dotada d'una extensió de les operacions usuals de $\mathbb{R}$: suma, producte, resta i divisió per un element no nul, sent els elements 0 i 1 els neutres per a la suma i el producte, respectivament.

Proposició 5.1.1. *Definim:*

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}, \tag{5.1.1}$$

amb la suma

$$(a, b) + (a', b') = (a + a', b + b') \tag{5.1.2}$$

i un producte per escalars

$$c(a, b) = (ca, cb), \tag{5.1.3}$$

on $c \in \mathbb{R}$ i $\mathbb{R}^2$ és espai vectorial amb aquestes operacions. Aleshores, la suma és associativa; commutativa; amb element neutre, el $(0, 0)$; amb element oposat, $(-a, -b)$.

Proposició 5.1.2. *També definim el producte com*

$$(a, b) \cdot (a', b') = (aa' - bb', ab' + ba'). \tag{5.1.4}$$

Aleshores el producte és associatiu; commutatiu; amb element neutre, el $(1, 0)$; la distributivitat respecte la suma; element invers: $(a + bi) \cdot \left(\dfrac{a}{a^2 - b^2} - \dfrac{b}{a^2 - b^2} i \right) = 1$.

Ara considerem $(a, b) = a + bi$. A partir d'aquí, tenim la redefinició de les operacions de suma i producte següent:

Propietat 5.1.3.

1. *Suma: $(a + bi) + (c + di) = (a + c) + (b + d)i$. La resta seria anàloga.*
2. *Multiplicació: $(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$.*

Observació 5.1.4. Aleshores, l'invers de la fracció d'inversos $\frac{a+bi}{c+di}$ és $\frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}$.

Definició 5.1.5. Per tot això, $\mathbb{C}$ dotat de totes les operacions anteriors és un cos tal que $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$: el **cos dels nombres complexos**.

Definició 5.1.6. A l'expressió $a+bi$ se l'anomena forma binòmica del nombre complex $z = a+bi$

Per tal de calcular l'invers, es calcula com a cas particular per a la divisió, en la qual es multiplica pel conjugat, de la següent manera:

$$z^{-1} = \frac{1}{z} = \frac{1}{z}\frac{\overline{z}}{\overline{z}} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i. \tag{5.1.5}$$

Mòdul i argument d'un nombre complex: forma polar

Com hem fet abans, en la forma polar cal utilitzar que $a + bi = (a, b) \in \mathbb{R}^2$: l'eix de les x correspon a la part real i el de les y, a la part imaginària. Per tant, hem passat de la recta real al pla complex.

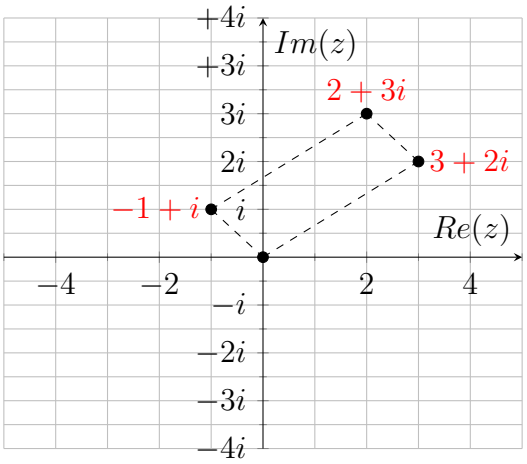

Figura 5.1: Representació de tres nombres complexos.

Definició 5.1.7 (Mòdul)**.** Si $P = (a, b) \in \mathbb{R}^2$ és el punt corresponent a $z = a + bi$, el mòdul de z, que anomenarem $|z|$ és la longitud del segment OP, on $O = (0, 0)$. Pel teorema de Pitàgores, tenim que

$$|z| = \sqrt{a^2 + b^2}. \tag{5.1.6}$$

Observació 5.1.8. Observem que $|z| \geq 0$ i que $|z| = 0 \iff z = 0$. També tenim la igualtat $z \cdot \overline{z} = (a + bi)(a - bi) = a^2 + b^2 = z^2$.

Definició 5.1.9 (Argument)**.** Si $P = (a, b)$ és el punt que representa a $z = a + b$ i l'argument de z és l'angle que formen el semieix positiu de les x amb el vector $\vec{OP}$. Està ben definit excepte per a $z = 0$. Si anomenem α a l'argument es té que $\tan\alpha = \frac{b}{a} \implies \alpha = \arctan\frac{b}{a}$. S

Definició 5.1.10 (Complex en forma binòmica)**.** Si $z = a + bi$ i $|z|$ és el mòdul de z i α el seu argument (suposem $z \neq 0$) diem que $|z|, \alpha$ són la forma polar del nombre complex z. És a dir, la forma polar de $z = a + bi$ ve donada per les coordenades pilars del punt $P = (a, b)$.

Notació 5.1.11. Denotem r_α el nombre complex de mòdul $r \geq 0$ i argument α. Noti's que sempre es pot reduir α tal que compleixi $0 \leq \alpha \leq 2\pi$.

Definició 5.1.12 (Forma polar i forma binòmica)**.** Si un complex z té forma polar r_α veiem que la seva forma binòmica és $a = r \cdot \cos\alpha$ i $b = r \cdot \sin\alpha$.

Operacions en forma polar

Siguin $z_1 = r_{1_{\alpha_1}}$ i $z_2 = r_{2_{\alpha_2}}$:

1. Producte: $z_1 \cdot z_2 = (r_1 \cdot r_2)_{\alpha_1+\alpha_2}$,
2. Quocient ($z_2 \neq 0$): $\frac{z_1}{z_2} = (\frac{r_1}{r_2})_{\alpha_1-\alpha_2}$.

D'aquí es dedueix la fórmula per a la potència d'un nombre complex en forma polar:

$$z = r_\alpha \implies z^n = r^n_{n\alpha}. \tag{5.1.7}$$

Fórmula d'Euler

Teorema 5.1.13 (Fórmula d'Euler). *Es compleix que*

$$e^{i\alpha} = \cos\alpha + i\sin\alpha. \tag{5.1.8}$$

Demostració. Considerem diverses sèries de Taylor

$$\begin{aligned} e^x &= \sum_{n=0}^{\infty} \frac{x^n}{n} \\ \sin x &= \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!} = x - \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots \\ \cos x &= \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!} = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots \end{aligned} \tag{5.1.9}$$

Operem les diferents sèries per veure que

$$\begin{aligned} e^{i\alpha} &= \sum_{n=0}^{\infty} \frac{(i\alpha)^n}{n!} = 1 + \frac{i\alpha}{1!} - \frac{\alpha^2}{2!} - \frac{i\alpha^3}{3!} + \frac{\alpha^4}{4!} + \cdots \\ &= 1 - \frac{\alpha^2}{2!} + \frac{\alpha^4}{4!} - \frac{\alpha^6}{6!} + \frac{\alpha^8}{8!} + \cdots + \frac{i\alpha}{1!} - \frac{i\alpha^3}{3!} + \frac{i\alpha^5}{5!} + \cdots = \\ &= \cos\alpha + i\left(\frac{\alpha}{1!} - \frac{\alpha^3}{3!} + \frac{\alpha^5}{5!} + \cdots\right) = \cos\alpha + i\sin\alpha. \end{aligned} \tag{5.1.10}$$

■

Teorema 5.1.14 (Identitat d'Euler). *Es compleix que*

$$e^{i\pi} + 1 = 0. \tag{5.1.11}$$

Demostració. És un cas particular per a $\alpha = \pi$. ■

5.2

Arrels de la unitat

A partir d'aquesta fórmula podem determinar les arrels n-èsimes de la unitat, és a dir, els $z \in \mathbb{C}$ tals que $z^n = 1$:

$$r^n_{n\alpha} = 1_0 \iff r = 1 \text{ i } n\alpha = 2k\pi, k \in \mathbb{Z} \iff r = 1 \text{ i } \alpha = \frac{2k\pi}{n}, k \in \{0, 1, \ldots, n-1\}. \tag{5.2.1}$$

Definició 5.2.1 (Arrels n-èsimes de la unitat)**.** Per tant, les arrels n-èsimes de la unitat són complexos $z_0, \ldots, z_{n-1}$ amb forma polar $z_k = 1_{2k\pi/n}, k \in \{0, 1, \ldots, n-1\}$. Per tant, expressades en forma binòmica són

$$z_k = \cos\left(\frac{2k\pi}{n}\right) + \sin\left(\frac{2k\pi}{n}\right) i \tag{5.2.2}$$

Vegem de quins polinomis a coeficients en $\mathbb{Z}$ són arrels n-èsimes de la unitat. Clarament, si ζ és arrel n-èsima de la unitat, és arrel de $x^n - 1 = 0$. Amb la qual cosa, si $n > 1$ també és arrel de $\frac{x^n-1}{x-1} = x^{n-1} + x^{n-2} + \cdots + x + 1$. En general aquest polinomi no és irreductible, però per al cas $n = p$, amb p primer, es pot comprovar que sí ho és.

Definició 5.2.2 (Arrel n-èsima primitiva ζ)**.** Així doncs, per a $n > 1$ diem que ζ és arrel n-èsima primitiva de la unitat si es compleix que $\zeta^n = 1$ i n és el mínim exponent positiu amb aquesta propietat.

Observació 5.2.3. Per al cas $n = p$, p primer, es pot veure que si es compleix $\zeta^p = 1$ i $\zeta \neq 1$, aleshores ζ és arrel p-èsima primitiva de la unitat. També, el conjunt de totes les arrels p-èsimes és $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ i totes elles són arrels del polinomi irreductible $x^{p-1}+x^{p-2}+\cdots+x+1$. Aquestes arrels primitives de la unitat són, en forma polar:

$$z_k = 1_{\frac{2\pi k}{p}}, k \in \{1, 2, \ldots, p-1\}. \tag{5.2.3}$$

En el cas d'un $n > 1$ arbitrari, pot veure's que hi ha exactament $\varphi(n)$ arrels n-èsimes primitives de la unitat, les quals són, en forma polar, $z_k = 1_{\frac{2\pi k}{n}}, k \in \{1, 2, \ldots, p-1\}, \text{mcd}(k, n) = 1$.

5.3

Arrel n-èsima d'un nombre complex

Donat qualsevol $z \in \mathbb{C}$ usant la fórmula per a les potències d'un complexe, podem calcular les arrels n-èsimes de z tal i com vam fer per la unitat, en l'apartat anterior.

w és l'arrel n-èsima de z, amb $w = r'_\alpha$ i $z = r_\alpha \implies w^n = (r'_{\alpha'})^n = r'^n_{n\alpha} = r_\alpha \implies r' = \sqrt[n]{r}$ i $\alpha' = \frac{\alpha+2k\pi}{n}, k \in \{0, \ldots, n-1\}$. La última igualtat prové d'identificar dos angles que difereixen en un múltiple de 2π, d'on α' ha de complir

$$n\alpha' = \alpha + 2k\pi. \tag{5.3.1}$$

Proposició 5.3.1 (Fórmula de De Moivre)**.** *Per a les arrels n-èsimes d'un nombre complex $z = r(\cos\alpha + i\sin\alpha)$:*

$$\sqrt[n]{z} = \sqrt[n]{r}(\cos\left(\frac{\alpha + 2k\pi}{n}\right) + i\sin\left(\frac{\alpha + 2k\pi}{n}\right)), \quad k \in \{0, 1, \ldots, n-1\}. \tag{5.3.2}$$

Corol·lari 5.3.2. *D'aquí es desprèn que per a tot $z \neq 0, z \in \mathbb{C}$, z posseeix exactament n arrels n-èsimes en $\mathbb{C}$. En particular, el polinomi $x^n - z = 0$ descomposa totalment (és a dir, en factors de grau 1) sobre $\mathbb{C}$.*

Teorema 5.3.3 (Teorema fonamental de l'Àlgebra)**.** *Si $P(x) \in \mathbb{C}[x]$ és un polinomi de grau $n > 0$, existeixen $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$ arrels de $P(x)$ amb multiplicitats $e_1, \ldots, e_r$ tals que $e_1 + \cdots e_r = n$, és a dir, que $P(x)$ es descomposa totalment en $\mathbb{C}$:*

$$P(x) = A(x - \alpha_1)^{e_1} \cdots (x - \alpha_r)^{e_r}. \tag{5.3.3}$$

Observació 5.3.4. L'enunciat anàleg és fals en $\mathbb{Q}[x]$ o en $\mathbb{R}[x]$, com es veu en l'exemple del polinomi $x^2 + 1$, que és irreductible en ambdós cossos.

Si el polinomi té coeficients enters, si tingués arrels racionals aquestes es podrien trobar examinant un conjunt finit de candidats.

Proposició 5.3.5 (Criteri de Gauss)**.** *Sigui $P(x)$ un polinomi amb coeficients en $\mathbb{Z}$*

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \operatorname{gr}(P(x)) > 0. \tag{5.3.4}$$

Si $\alpha \in \mathbb{Q}$ fos arrel de $P(x)$, escrita com a $\alpha = \frac{u}{v}$, amb $u, v \in \mathbb{Z}, \operatorname{mcd}(u, v) = 1$, aleshores $u \mid a_0 \wedge v \mid a_n$.

5.4 Arrels primitives: Propietats bàsiques

Definició 5.4.1. Si a és un enter amb $\operatorname{mcd}(a, m) = 1$ i l'ordre d'a mòdul m és igual a $\varphi(m)$ diem que a és *arrel primitiva mòdul m*.

Observació 5.4.2. No és cert que per a calcular qualsevol mòdul m existeixen arrels primitives. Per exemple, si $m = 8$ no hi ha arrels primitives: tota classe a invertible mòdul 8 compleix $a^2 \equiv 1 \pmod 8$ i per tant té ordre 1 o 2, amb la qual cosa no existeixen elements d'ordre $\varphi(8) = 4$.

Teorema 5.4.3. *Sigui m un mòdul i sigui a una arrel primitiva mòdul m. Aleshores els elements del conjunt $S = \{a, a^2, \ldots, a^{\varphi(m)}\}$ recorren les classes residuals invertibles mòdul m.*

Demostració. Com $\operatorname{mcd}(a, m) = 1$ també $\operatorname{mcd}(a^i, m) = 1$ per a tot $i = 1, 2, \ldots, \varphi(m)$, amb la qual cosa tots els elements d'$S = \{a, a^2, \ldots, a^{\varphi(m)}\}$ corresponen a classes invertibles mòdul m. Com la quantitat de classes invertibles mòdul m és $\varphi(m)$, és suficient amb provar que tots els elements cauen en classes residuals diferents.

Per hipòtesi, l'ordre d'a mòdul m és $\varphi(m)$, per la qual cosa si suposem que $a^i \equiv a^j \pmod m$ concloem que $i \equiv j \pmod{\varphi(m)}$, amb la qual cosa $i = j$, doncs ambdós valors estan en l'interval $[1, \varphi(m)]$. Això prova que els elements d'S cauen tots en classes residuals diferents i, en conseqüència, recorren totes les classes $\varphi(m)$ classes residuals invertibles mòdul m. ■

Provem ara l'afirmació recíproca:

Proposició 5.4.4. *Sigui m un mòdul i a coprimer amb m tal que els elements d'$S = \{a, a^2, \ldots, a^{\varphi(m)}\}$ recorren totes les classes residuals invertibles mòdul m. Aleshores, a és arrel primitiva mòdul m.*

Observació 5.4.5. La conclusió dels dos resultats previs és que l'existència d'una arrel primitiva mòdul m és equivalent a l'existència d'una classe invertible mòdul m les potències del qual generen tot $(\mathbb{Z}/m\mathbb{Z})^*$.

Provarem molts casos de la següent equivalència: *existeixen arrels primitives mòdul* $m \iff m = 1, 2, 4, p^r \ o \ 2p^r$, amb p primer imparell.

Lema 5.4.6. *Si* $n \geq 1$ *es té que*

$$n = \sum_{d|n} \varphi(d). \tag{5.4.1}$$

Demostració. Considerem $\mathbb{Z}/n\mathbb{Z}$ el conjunt de totes les classes residuals mòdul n, el qual té n elements. Partirem el conjunt d'acord al valor de $\mathrm{mcd}(x, n)$ per a x un representant de cada classe residual (ho podem fer perquè el mcd en la classe no depèn del representant clarament), el qual agafem en l'interval $1 \leq x \leq n$.

Tenim que $\mathrm{mcd}(x, n) \mid n$, ara si considerem per a cada element a que divideix a n el conjunt

$$R_a = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{mcd}(x, n) = a\}. \tag{5.4.2}$$

Es té que $\mathbb{Z}/n\mathbb{Z}$ queda partit en aquest conjunt R_a on a recorre els divisors d'n. Per tant es té que

$$\mathbb{Z}/n\mathbb{Z} = \coprod_{a|n} R_a, \tag{5.4.3}$$

on $\coprod$ denota unió disjunta de conjunts. Per tant, n (el cardinal de $\mathbb{Z}/n\mathbb{Z}$) és igual a la suma dels cardinals dels conjunts R_a quan a recorre als divisors d'n. Ens queda per determinar el cardinal d'aquests conjunts R_a.

Si $a \mid n$ i $x \in \{1, 2, \ldots, n\}$, x tal que compleix $x \in R_a \implies \mathrm{mcd}(x, n) = a$, amb la qual cosa podem escriure $x = ia, n = a'a$, amb $0 < i \leq a'$ (que equival a $0 < x \leq n$) i $\mathrm{mcd}(i, a') = 1$ (aquesta condició equival a $\mathrm{mcd}(x, n) = a$).

Per tant, hi ha tants elements en R_a com enters i tals que $0 < i \leq a', \mathrm{mcd}(i', a) = 1$. En conseqüència, hi ha $\varphi(a')$ elements en R_a on $a' = \frac{n}{a}$. Doncs,

$$n = |(\mathbb{Z}/n\mathbb{Z})| = \sum_{a|n} |R_a| = \sum_{a|n} \varphi\left(\frac{n}{a}\right). \tag{5.4.4}$$

Aquest sumatori és sobre tots els divisors a d'n. De fet, quan a recorre tots els divisors d'n, $\frac{n}{a}$ també recorre tots els divisors d'n, així que concloem

$$n = \sum_{d|n} \varphi(d). \tag{5.4.5}$$

■

Per a provar el següent lema, recordem el petit teorema de Fermat. En el fons, aquest teorema estableix que si p és primer la congruència de grau $p - 1$ $x^{p-1} \equiv 1 \pmod{p}$ posseeix $p - 1$ solucions (totes les classes mòdul p diferents de la del 0).

Recordem també que gràcies al teorema de Lagrange sabem que si $F(x)$ és un polinomi a coeficients enters de grau $k > 0$ (i tal que la seva reducció ens dona)

Lema 5.4.7. *Si* p *és primer i* $d > 0$ *és un divisor de* $p - 1$ *la congruència*

$$x^d \equiv 1 \pmod{p} \tag{5.4.6}$$

té exactament d *solucions.*

Demostració. Per a començar, sabem gràcies al teorema de Lagrange que no pot tenir més de d solucions. Com $p-1=kd$, es té la factorització

$$x^{p-1}-1=(x^d)^k-1=(x^d-1)\cdot Q(x), \tag{5.4.7}$$

on $Q(x)$ és un polinomi a coeficients enters, de grau $p-1-d$. Per tal de veure-ho més fàcil, podem pensar $\alpha=x^d$. De fet, fixem-nos que hem dividit el conjunt de solucions en dues "bosses", on a priori no sabem quantes hi ha en cada lloc.

Com ja hem esmentat anteriorment, sabem gràcies al teorema de Fermat que la congruència $x^{p-1}\equiv 0 \pmod p$ posseeix $p-1$ solucions. Per (5.4.7), si r és solució d'aquesta congruència, o bé r és solució de $x^d-1\equiv 0 \pmod p$, o bé ho és de $Q(x)\equiv 0 \pmod p$. Aquí hem usat LFA, ja que p és primer: si p divideix un producte, ha de dividir algun dels factors. Aleshores, si r és arrel mòdul p del polinomi producte, també ho serà d'algun dels polinomis que es multipliquen.

Per tant, de les $p-1$ solucions de $x^{p-1}\equiv 0 \pmod p$, totes les que no siguin solució de $x^d-1\equiv 0 \pmod p$ han de ser solució de la congruència de grau $p-1-d$: $Q(x)\equiv 0 \pmod p$, aleshores tenim per Lagrange que hi ha un màxim de $p-1-d$ d'elles.

Tenim, per tant, un conjunt de $p-1$ classes mòdul p de les quals un màxim de $p-1-d$ ***no*** resolen la congruència $x^d\equiv 0 \pmod p$ i, en conseqüència, hi haurà un mínim de d d'aquestes classes mòdul p que sí resolen aquesta congruència. ■

Teorema 5.4.8. *Si p és primer i $d>0$ és divisor de $p-1$, de les d classes mòdul p que són solució de*

$$x^d\equiv 1 \pmod p, \tag{5.4.8}$$

hi ha exactament $\varphi(d)$ d'elles que tenen ordre d mòdul p. En particular, hi ha $\varphi(p-1)$ classes invertibles mòdul p que tenen ordre $p-1$ mòdul p, és a dir, que són arrels primitives mòdul p.

Observació 5.4.9. El teorema implica, en particular, que existeixen arrels primitives mòdul p per a tot p primer.

Demostració. Sigui r un element d'una classe invertible mòdul p, d'ordre d'd. En particular, és solució de la congruència $x^d-1\equiv 0 \pmod p$. Així doncs, la quantitat de classes que són solució de $x^d-1\equiv 0 \pmod p$ i tenen ordre d és igual a la quantitat de classes invertibles mòdul p d'ordre d. Per a cada d divisor de $p-1$ anomenarem $\Psi(d)$ a aquesta quantitat.

Sabem que tot element en $\{1,2,\dots,p-1\}$ té per ordre mòdul p a un divisor de $p-1$, d'on

$$\sum_{d\mid p-1}\Psi(d)=p-1. \tag{5.4.9}$$

En altres paraules, la igualtat anterior surt de partir el conjunt de les classes invertibles mòdul p en subconjunts d'acord a l'ordre mòdul p dels seus elements.

Per altra banda, vam veure en 5.4.6 que es té $n=\sum_{d\mid n}\varphi(d)$. D'aquí, $p-1=\sum_{d\mid p-1}\varphi(d)$. Per tant, el nostre objectiu serà provar que per a tot $d\mid p-1$ es té que $\Psi(d)\leq\varphi(d)$, ja que aleshores $p-1=\sum_{d\mid n}\Psi(d)\leq\sum_{d\mid p-1}\varphi(d)=p-1$, d'on obtindríem

$$\Psi(d)=\varphi(d). \tag{5.4.10}$$

És a dir, la quantitat de solucions $x^d-1\equiv 0 \pmod p$ que tenen ordre d és $\varphi(d)$, tal i com volem provar. Sense més dilació, provem que $\Psi(d)\leq\varphi(d)$ per a tot $d\mid p-1$.

Sigui d un divisor de $p-1$ i sigui $f \in \{1,2,\ldots,p-1\}$ d'ordre d mòdul p. Si no existís un tal f, aleshores $\Psi(d) = 0 \leq \varphi(d)$ i ja hauríem acabat. Considerem d els nombres $f_h = f^h$, amb exponent $h \in \{0,1,\ldots,d-1\}$. Tenim $f^d \equiv 1 \pmod{p} \implies f^{hd} \equiv 1 \pmod{p} \implies$ els d nombres f_h, amb $h \in \{0,1,\ldots,d-1\}$ són tots solució de $x^d \equiv 1 \pmod{p}$. A més, són dos a dos no congruents mòdul p, ja que si $h \geq h'$ i $f_h \equiv f_{h'} \pmod{p} \implies f^h \equiv f^{h'} \pmod{p} \implies f^{h-h'} \equiv 1 \pmod{p}$ i com $0 \leq h-h' \leq d-1$ i f té ordre d concloem que $h = h'$. Després, com la congruència $x^d \equiv 1 \pmod{p}$ té d solucions mòdul p, vegem que els nombres f_h recorren, sense repetir, totes les classes mòdul p que són solució d'aquesta congruència.

En particular, tota la classe d'ordre d està representada per algun f_h. A més, és fàcil veure que si f té ordre d mòdul p, aleshores f_h té ordre menor o igual que $\frac{d}{\mathrm{mcd}(d,h)}$ mòdul p. D'aquí es dedueix que si f_h també té ordre d, aleshores $\mathrm{mcd}(d,h) = 1$. Servint-nos que tota la classe d'ordre d està representada per algun f_h, concloem que la quantitat de classes mòdul p d'ordre d és, com a molt, la quantitat de classes coprimeres amb d, és a dir,

$$\Psi(d) \leq \varphi(d), \tag{5.4.11}$$

per a tot $d \mid p-1$, tal i com necessitàvem demostrar. ■

Corol·lari 5.4.10. *Per a tot p primer existeixen arrels primitives mòdul p.*

Exemple 5.4.11.

1. Si $m = 4, \varphi(4) = 2$ i 3 té ordre 2 mòdul 4, tenim que 3 és arrel primitiva mòdul 4.
2. Si $m = 8, \varphi(8) = 4$, les 4 classes invertibles mòdul 8 tenen ordre 1 o 2, ja que:

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}, \tag{5.4.12}$$

aixó que no existeixen arrels primitives mòdul 8.

Si $r \geq 3$ vegem que no existeixen arrels primitives mòdul 2^r usant el següent lema:

Lema 5.4.12. *Si l'equació $x^2 \equiv 1 \pmod{m}$ posseeix més de dues solucions, aleshores no existeixen arrels primitives mòdul m.*

Demostració. Ho demostrarem pel contrarrecíproc. Suposem que existeixen arrels primitives mòdul m i sigui a una tal arrel. Això significa que l'ordre a mòdul m és $\varphi(m)$, i ja vam veure que en aquest cas es té que el conjunt $\{a, a^2, \ldots, a^{\varphi(m)}\}$ recorre les $\varphi(m)$, totes, classes invertibles mòdul m.

Donat $w \mid w^2 \equiv 1 \pmod{m}$, es té un $r \in \{1,2,\ldots,\varphi(m)\}$ tal que $w \equiv a^r \pmod{m}$. Elevant al quadrat, tenim que

$$a^{2r} \equiv 1 \pmod{m}, \tag{5.4.13}$$

i com a té ordre $\varphi(m) \implies \varphi(m) \mid 2r$. Tenint en compte que $r \in \{1,2,\ldots,\varphi(m)\}$, és evident que $r = \varphi(m)$ o bé, si $\varphi(m)$ és parell, també podem considerar $r = \varphi(m)/2$, que equival a $m > 2$.

Per tant, un w que és solució de $x^2 \equiv 1 \pmod{m}$ ha de complir $w \equiv a^r \pmod{m}$ per a $r = \varphi(m)$ o $r = \varphi(m)/2$, amb la qual cosa solament hi ha, com a màxim, dues solucions d'aquesta congruència quadràtica, contradient la hipòtesi del lema, tal i com volíem veure. ■

Corol·lari 5.4.13. *Si $r \geq 3$ i $m = 2^r$ no existeixen arrels primitives mòdul m.*

Demostració. Pel lema previ, tenim prou amb provar que hi ha més de dues solucions per a $x^2 \equiv 1 \pmod{2^r}$. D'una banda, tenim les solucions trivials $1, 2^r - 1$. Per una altra, com

$$x^2 - 1 \equiv 0 \pmod{2^r} \iff (x+1)(x-1) \equiv 0 \pmod{2^r}. \tag{5.4.14}$$

Per a qualsevol z senar que s'esculli, com $2 \mid z+1$, hi haurà prou amb què es tingui $2^{r+1} \mid z-1$ per tal que serveixi. Per tant, podem agafar, per exemple, $z = 2^{r-1} + 1$ com a solució de la congruència quadràtica. És fàcil veure que per a tot $r \geq 3$ aquest z compleix $1 < z < 2^r - 1$, així que podem concloure que hi ha tres solucions (com a mínim) per a la congruència $x^2 \equiv 1 \pmod{2^r}$. ■

Corol·lari 5.4.14. *Si p i q són dos primers imparells diferents i $m = pq$, no existeixen arrels primitives mòdul m.*

Demostració. Aplicant novament el lema 5.4.12, hi ha prou amb demostrar que hi ha més de dos solucions $x^2 \equiv 1 \pmod{m}$. Aquesta congruència equival a

$$(x+1)(x-1) \equiv 0 \pmod{pq} \iff \begin{matrix} (x+1)(x-1) \equiv 0 \pmod{p} \\ (x+1)(x-1) \equiv 0 \pmod{q} \end{matrix}, \tag{5.4.15}$$

que equival a

$$\begin{matrix} x \equiv \pm 1 \pmod{p} \\ x \equiv \pm 1 \pmod{q} \end{matrix}. \tag{5.4.16}$$

Agafant ambdós signes en cada congruència obtenim, en total, 4 sistemes de congruències lineals, on cadascun d'ells posseeix una solució única mòdul pq segons TXR. Per tant, hi ha almenys 4 solucions de $x^2 \equiv 1 \pmod{m}$, d'on per 5.4.12 deduïm que no existeixen arrels primitives mòdul m. ■

Proposició 5.4.15. *Si p és un primer imparell i $m = 2p$ existeixen arrels primitives mòdul p.*

Demostració. Comencem per calcular $\varphi(m) = \varphi(2p) = \varphi(2)\varphi(p) = p - 1$. Busquem, aleshores, un element d'ordre $p-1$ mòdul m.

Sigui a una arrel primitiva mòdul p. Com també $a + p$ és arrel primitiva mòdul p i algun d'aquests dos nombres és senar, deduïm que existeix un nombre b en l'interval $[1, 2p]$ que és imparell i és arrel primitiva mòdul p. Clarament, aquest b és coprimer amb $m = 2p$ i pel teorema d'Euler es compleix

$$b^{\varphi(2p)} \equiv b^{p-1} \equiv 1 \pmod{p}. \tag{5.4.17}$$

A més, com b és arrel primitiva mòdul p, té ordre $p-1$ mòdul p. Aleshores, si $1 \leq e < p-1$:

$$b^e \not\equiv 1 \pmod{p} \implies b^e \not\equiv 1 \pmod{2p}. \tag{5.4.18}$$

Per tant, l'ordre de b mòdul $m = 2p$ és $p - 1 = \varphi(m)$.

A més de tots els resultats anteriors, també es pot veure que si p és un primer imparell i $r > 0$ aleshores existeixen arrels primitives mòdul p^r, és a dir, classes invertibles mòdul p^r, l'ordre de les quals $\varphi(p^r) = (p-1)p^{r-1}$. Aquest resultat solament l'hem provat sol en el cas $r = 1$. Per a la resta de casos $1, 2, 4, p^r, 2 \cdot p^r$, la demostració queda fora de l'abast del nostre nivell. ■

Corol·lari 5.4.16 (Criteri, arrels primitives)**.** *Com a conseqüència de l'anterior demostració, obtenim el criteri següent: existeixen arrels primitives mòdul $m > 0$ si, i només si, m és igual a $1, 2, 4, p^r, 2 \cdot p^r$, on $r \geq 1$, on p és un primer imparell.*

5.5

Congruències quadràtiques

Introducció

Ja sabem que una congruència polinòmica de la forma $f(x) \equiv 0 \pmod{p}$, on p és un nombre primer i $f(X)$ és un polinomi de coeficients enters i grau d, no pot tenir més de d solucions. Considerem un polinomi $f(X) := aX^2 + bX + c; a, b, c \in \mathbb{Z}, a \neq 0$ i un nombre primer p. Si $p \mid a$, la congruència $f(x) \equiv 0 \pmod{p}$ no és res més que la congruència lineal $bx + c \pmod{p}$. Es tracta, doncs, de calcular les solucions $x \in \mathbb{Z}$ de les congruències de la forma $ax^2 + bx + c \equiv 0 \pmod{p}$, on $a, b, c \in \mathbb{Z}$, p primer i $p \nmid a$.

Proposició 5.5.1. *Siguin $a, b, c \in \mathbb{Z}$ i p un nombre primer senar que no divideix a. La congruència $ax^2 + bx + c \equiv 0 \pmod{p}$ té solucions si, i només si, en té la congruència $y^2 \equiv b^2 - 4ac \pmod{p}$. A més, les solucions de les dues estan relacionades per la congruència $y \equiv 2ax + b \pmod{p}$.*

Sigui p primer. Per a cada enter a no divisible per p plantegem la congruència quadràtica

$$x^2 \equiv a \pmod{p}. \tag{5.5.1}$$

Observació 5.5.2.

- En el cas que a és divisible per p, és a dir, $a \equiv 0 \pmod{p}$, aquesta congruència té la solució trivial $x \equiv 0 \pmod{p}$.
- El problema solament depèn de la classe de congruència d'a mòdul p.

Definició 5.5.3 (Residu quadràtic)**.** Si existeix solució de l'equació (5.5.1), diem que a és un *residu quadràtic* mòdul p. En cas contrari, diem que a és un *no-residu quadràtic* mòdul p.

Congruències polinòmiques

Proposició 5.5.4. *Sigui $f(X) := a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[x]$ un polinomi de coeficients enters $a_0, \ldots, a_n$. Siguin p un nombre natural primer i $v \geq 1$ un nombre enter. Suposem que $x \in \mathbb{Z}$ és un nombre enter tal que $f(x) \equiv 0 \pmod{p^v}$. Llavors, la quantitat de nombres enters y tals que $0 \leq y < p^{v+1}, y \leq x \pmod{p^v}$ i $f(y) \equiv 0 \pmod{p^{v+1}}$ és donat per:*

$$\begin{cases} 1, & \text{si } f'(x) \not\equiv 0 \pmod{p}; \\ 0, & \text{si } f'(x) \equiv 0 \pmod{p} \text{ i } f(x) \not\equiv 0 \pmod{p^{v+1}}; \text{i} \\ p, & \text{si } f'(x) \equiv 0 \pmod{p} \text{ i } f(x) \equiv 0 \pmod{p^{v+1}}, \end{cases} \tag{5.5.2}$$

on $f'(X)$ és el polinomi derivat del polinomi $f(X)$.

A més, les solucions $y \pmod{p^{v+1}}$ de la congruència $f(X) \equiv 0 \pmod{p^{v+1}}$ tals que $y \equiv x \pmod{p^v}$ es calculen de la manera següent:

1. *Si $f'(x) \not\equiv 0 \pmod{p}$ és $y := x + \lambda p^v$, on λ és l'única solució mòdul p de la congruència lineal, $\lambda f'(x) + \frac{f(x)}{p^v} \equiv 0 \pmod{p}$.*
2. *Si $f'(x) \equiv 0 \pmod{p}$, es mira si $f(x) \equiv 0 \pmod{p^{v+1}}$; si la congruència no se satisfà, no hi ha solucions y tals que $y \equiv x \pmod{p^v}$; i si se satisfà, les solucions y cercades són els p nombres $y := x + \lambda p^v$, per a $0 \leq \lambda \leq p - 1$.*

Euler

Proposició 5.5.5. *Sigui p un primer imparell. De les $p-1$ classes residuals mòdul p diferents de la del 0, $\frac{p-1}{2}$ són residus quadràtics. En particular, si α és una arrel primitiva mòdul p i, per tant, $\alpha, \ldots, \alpha^{p-1}$ recorren les $p-1$ classes invertibles mòdul p, es té que α^k és residu quadràtic mòdul p si, i només si, k és parell.*

Demostració. Si k és parell, és a dir, $k = 2w$, es té que $\alpha^k = (\alpha^w)^2$ és un quadrat, així que la congruència $\alpha^k \equiv x^2 \pmod{p}$ té la solució $x = \alpha^w$, és a dir, α^k és residu quadràtic mòdul p. De totes maneres, hem obtingut que $\frac{p-1}{2}$ classes residuals mòdul p que són residus quadràtics, doncs hi ha $\frac{p-1}{2}$ nombres parells en l'interval $[1, p-1]$.

Com ja tenim $\frac{p-1}{2}$ residus quadràtics, queda sol per veure que el nombre de classes invertibles corresponents a residus quadràtics és exactament $\frac{p-1}{2}$. Això provarà que, en particular, α^k és residu quadràtic solament quan k és parell.

Si β és solució de la congruència $y^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Pel teorema de Lagrange, aquesta congruència no pot tenir més de $\frac{p-1}{2}$ solucions, amb la qual concloem que no pot haver-hi més de $\frac{p-1}{2}$ residus quadràtics. ∎

Proposició 5.5.6 (Criteri d'Euler). *Sigui p un primer imparell i a un enter no divisible per p. Aleshores:*

$$a^{\frac{p-1}{2}} \begin{cases} 1 & \text{si } a \text{ és residu quadràtic mòdul } p, \\ -1 & \text{si } a \text{ és no-residu quadràtic mòdul } p. \end{cases} \tag{5.5.3}$$

Demostració. Sigui $b = a^{\frac{p-1}{2}} \implies b^2 \equiv a^{p-1} \equiv 1 \pmod{p}$. Aleshores, $b = a^{\frac{p-1}{2}}$ és solució de la congruència quadràtica $x^2 \equiv 1 \pmod{p}$. Sabem que aquesta congruència té solament dues solucions: $x \equiv 1 \pmod{p}$ i $x \equiv -1 \pmod{p}$. Per tant,

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}. \tag{5.5.4}$$

Si a és residu quadràtic mòdul p: $a \equiv u^2 \pmod{p}$ per a algun enter u, aleshores $a^{\frac{p-1}{2}} \equiv u^{p-1} \equiv 1 \pmod{p}$ gràcies a PTFermat. Tenim, per tant, $\frac{p-1}{2}$ classes residuals, aquelles corresponents a residus quadràtics, que resolen la congruència $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ i, com sabem pel teorema de Lagrange, aquesta congruència no pot tenir més de $\frac{p-1}{2}$ solucions. En paraules més mundanes podríem dir que "ja no caben més solucions"així que per la resta, és a dir, per a tot residu no-quadràtic β es té: $\beta^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. De (5.5.4) deduïm que per a un tal β necessàriament

$$\beta^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{5.5.5}$$

∎

Símbol de Legendre

Definició 5.5.7 (p-èsim símbol de Legendre d'a). Si p és primer i $a \in \mathbb{Z}$, definim el *Símbol de Legendre* com:

$$\left(\frac{a}{b}\right) = \begin{cases} 0 & \text{si } p \mid a, \\ 1 & \text{si } p \nmid a \text{ i } a \text{ és residu quadràtic mòdul } p, \\ -1 & \text{si } p \nmid a \text{ i } a \text{ és no-residu quadràtic mòdul } p. \end{cases} \tag{5.5.6}$$

Observació 5.5.8. Notem que per escriure'l es faria servir, normalment, una línia horitzontal entre a i p. Nosaltres, per no confondre'l, farem servir una discontínua.

Propietat 5.5.9 (Propietats del Símbol de Legendre).

1. $a \equiv b \pmod p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
2. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$, *si p és un primer imparell;*
3. *propietat multiplicativa,* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;
4. *si* $p \nmid c \implies \left(\frac{c^2 b}{p}\right) = \left(\frac{b}{p}\right)$.

Demostració.

1. És evident que el fet que la congruència $x^2 \equiv a \pmod p$ tingui solucions o no, només depèn de la classe residual d'a mòdul p, tal i com per a ser divisible per p; per tant, si $a \equiv b \pmod p$, llavors $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. Si a és divisible per p, $a^{\frac{p-1}{2}}$ també ho és i la congruència en aquest cas seria trivial: $0 \equiv 0 \pmod p$. Si $p \nmid a$, se segueix que demostrar 5.5.9.2 correspon amb el Criteri d'Euler fent ús del Símbol de Lagrange.
3. Es dedueix fàcilment del punt anterior:
$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p. \tag{5.5.7}$$
4. Se segueix del punt anterior, ja que
$$\left(\frac{c^2 b}{p}\right) = \left(\frac{c^2}{p}\right)\left(\frac{b}{p}\right) = 1 \cdot \left(\frac{b}{p}\right) = \left(\frac{b}{p}\right), \tag{5.5.8}$$
on hem utilitzat el fet que c^2, al ser un quadrat i no ser divisible per p, ha de ser residu quadràtic mòdul p. Recordem, de fet, que de la congruència $c^2 \equiv x^2 \equiv 0 \pmod p$ extraiem $x \equiv c \pmod p$.

■

Proposició 5.5.10. *Si p és un primer senar, es té*
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{5.5.9}$$

Demostració. Abans de demostrar-ho, vegem què ens intenta transmetre aquesta proposició. En essència, volem trobar aquells p per als quals el símbol de Legendre val 1. Per tant, serien aquells primers per als quals $(-1)^{\frac{p-1}{2}} = 1$. Fixem-nos que l'exponent ha de ser parell.

Usant 5.5.9.2 per al cas $a = -1$, ens queda que $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$. Com $p > 2$ i ambdós valors pertanyen a $a \in \{-1, 1\}$ de la congruència deduïm la igualtat $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

■

Corol·lari 5.5.11. *Sigui p un nombre primer senar. Aleshores,*
$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 4, \\ -1 & \text{si } p \equiv 3 \pmod 4. \end{cases} \tag{5.5.10}$$

Demostració. Només cal usar el criteri d'Euler; obtenim que $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$; però dos nombres que siguin ± 1 i que coincideixin mòdul p són iguals, ja que $p > 2$. Per tant, obtenim la primera igualtat. La segona és immediata, ja que $\frac{p-1}{2}$ és parell si $p \equiv 1 \pmod{4}$, la qual cosa equival a $\frac{p-1}{2} \equiv 0 \pmod{2} \iff p \equiv 1 \pmod{4}$, i senar si $p \equiv -1 \pmod{4}$. ■

Observació 5.5.12. Notem que aquest corol·lari és equivalent a dir que, aplicant el símbol de Legendre, -1 és residu quadràtic mòdul p, ja que el símbol de Legendre $\left(\frac{-1}{p}\right)$ és igual a 1.

Definició 5.5.13 (Funció sostre)**.** La funció sostre és una funció definida de la següent manera:

$$\begin{array}{rccl} \lceil\ \rceil: & \mathbb{R} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & \lceil x \rceil = \min\{k \in \mathbb{Z} \mid x \leq k\} \end{array} \tag{5.5.11}$$

Eisenstein

Lema 5.5.14 (Lema d'Eisenstein)**.** *Siguin p, q primers imparells diferents. Sigui $\lceil x \rceil$ la funció sostre. Es té*

$$\left(\frac{p}{1}\right) = (-1)^{\sum_u \lceil \frac{qu}{p} \rceil}, \tag{5.5.12}$$

on u recorre els nombres parells, amb $2 \leq u \leq p-1$.

Demostració. Per a u parell amb $2 \leq u \leq p-1$. Sigui $r(u)$ el residu de dividir qu per p, en altres paraules: $r(u) \equiv qu \pmod{p}$, amb $0 < r(u) < p$, doncs no pot donar 0 (cap dels dos nombres és múltiple de p).

Considerem ara els nombres $(-1)^{r(u)} r(u)$ i a cadascun d'ells li associem el representant de la seva classe residual mòdul p en l'interval $0 < x < p$:

$$(-1)^{r(u)} r(u) \equiv s(u) \pmod{p}, \tag{5.5.13}$$

amb $0 < s(u) < p$. Tots els $s(u)$ són parells, perquè si $r(u)$ és parell se segueix que $s(u) = r(u)$, però si $r(u)$ és imparell es té que $s(u) \equiv -r(u) \pmod{p} \implies s(u) = -r(u) + p$, que és parell.

A més, tots els $s(u)$ són diferents, ja que si tinguéssim $s(u) = s(t) \implies (-1)^{r(u)} r(u) \equiv (-1)^{r(t)} r(t) \pmod{p} \implies (-1)^{r(u)} qu \equiv (-1)^{r(t)} qt \pmod{p}$. Aplicant la propietat cancel·lativa a l'última expressió (l'apliquem perquè p és coprimer amb q) ens queda que $u \equiv \pm t \pmod{p}$.

Notem, però, que $u \equiv -t \pmod{p}$ no és possible, donat que, si no, seria $u = -t + p$ (hem usat el fet que u i t estan en l'interval $[1, p-1]$), contradient el fet que u, t són ambdós parells. Així doncs, tenim que $s(u) = s(t) \implies u \equiv t \pmod{p} \implies u = t$. En altres paraules, tots els $s(u)$ són diferents.

Per tant, tots els $s(u)$ són elements de l'interval $[1, p-1]$ i són tots parells i diferents entre ells, i hi ha $\frac{p-1}{2}$ d'ells (tants com u parells en aquest interval).

Concloem que els $s(u)$ són una permutació de $2, 4, \ldots, p-1$ (els u parells de l'interval $[1, p-1]$). Per tant, si considerem el producte de tots ells, ens queda:

$$\begin{aligned} s(2) \cdot s(4) \cdots s(p-1) = 2 \cdot 4 \cdots (p-1) &\implies (-1)^{r(2)} \cdot r(2) \cdot (-1)^{r(4)} \cdot r(4) \cdots (-1)^{r(p-1)} \cdot r(p-1) \\ &\equiv 2 \cdot 4 \cdots (p-1) \pmod{p} \\ \implies (-1)^{r(2)} \cdot 2 \cdot q \cdot (-1)^{r(4)} \cdot 4 \cdot q \cdots (-1)^{r(p-1)} \cdot (p-1) q &\equiv 2 \cdot 4 \cdot (p-1) \pmod{p}. \end{aligned} \tag{5.5.14}$$

Aplicant la propietat cancel·lativa,

$$(-1)^{r(2)+r(4)+\cdots+r(p-1)}q^{\frac{p-1}{2}} \equiv 1 \pmod{p} \implies (-1)^{r(2)+r(4)+\cdots+r(p-1)} \equiv q^{\frac{p-1}{2}} \pmod{p}. \tag{5.5.15}$$

D'altra banda, al dividir qu entre p, el quocient és $\lceil \frac{qu}{p} \rceil$ i el residu és $r(u)$, d'on $qu = p\lceil \frac{qu}{p} \rceil + r(u)$. Com qu és parell i p imparell, d'aquí veiem que $\lceil \frac{qu}{p} \rceil$ i $r(u)$ tenen la mateixa paritat. Per tant, la fórmula anterior equival a

$$q^{\frac{p-1}{2}} \equiv (-1)^{\sum_u \lceil \frac{qu}{p} \rceil} \pmod{p}, \tag{5.5.16}$$

amb u parell, $2 \leq u \leq p-1$. D'aquí, combinant amb el criteri d'Euler, tenim $\left(\frac{q}{p}\right) \equiv (-1)^{\sum_u \lceil \frac{qu}{p} \rceil} \pmod{p}$. Com ambdós membres valen 1 o -1, de la congruència mòdul p es dedueix la igualtat

$$\left(\frac{q}{p}\right) = (-1)^{\sum_u \lceil \frac{qu}{p} \rceil}. \tag{5.5.17}$$

■

Teorema 5.5.15 (Llei de la Reciprocitat Quadràtica)**.** *Siguin p, q primers imparells diferents. Es té:*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{5.5.18}$$

Demostració. Partim del lema d'Eisenstein $\left(\frac{q}{p}\right) = (-1)^{\sum_u \lceil \frac{qu}{p} \rceil}$, on u recorre els nombres parells de l'interval $[2, p-1]$. La suma en l'exponent compta la quantitat de punts de coordenades enteres tals que la seva coordenada x és parells i estan dins del triangle ABC en la figura 5.2. Com els catets d'ABC medeixen p i q, pel teorema de Tales per a tot $v \in [0, p]$ la vertical per v talla el segment AC en un punt amb coordenada $w = v \cdot \frac{q}{p}$.

Considerem, d'entre aquests punts, aquells que queden dins del trapezi $XYCB$, $X = \frac{p}{2}$. En altres paraules, aquells que tenen la coordenada x major que $\frac{p}{2}$. Com el total de punts amb coordenada x parell dins del rectangle $ZCBX$ és parell (ja que hi ha $q-1$ en cada columna):

$$\begin{aligned} &\implies \#\{\text{punts amb } x \text{ parell dins de } XYCB\} + \#\{\text{punts amb } x \text{ parell dins de } YZC\} = \\ &= \#\{\text{punts amb } x \text{ parell dins de } XYCB\} \equiv 0 \pmod{2} \\ &\implies \#\{\text{punts amb } x \text{ parell dins de } XYCB\} \equiv \#\{\text{punts amb } x \text{ parell dins de } YZC\} \pmod{2} \end{aligned} \tag{5.5.19}$$

D'altra banda, si considerem la quantitat de punts amb x parell dins de YZC, veiem per simetria respecte el punt Y que aquesta és igual a la quantitat de punts amb x imparell dins del triangle YZA.

Aplicant això que hem dit i (5.5.19), veiem que l'exponent de -1 en el lema d'Eisenstein és igual a

$$\begin{aligned} &\#\{\text{punts amb } x \text{ parell dins de } ABC\} = \#\{\text{punts amb } x \text{ parell dins de } AYX\} \\ &+ \#\{\text{punts amb } x \text{ parell dins de } XYCB\} \equiv \#\{\text{punts amb } x \text{ parell dins de } AYX\} \\ &+ \#\{\text{punts amb } x \text{ parell dins de } ZYC\} = \#\{\text{punts amb } x \text{ parell dins de } AYX\} \\ &+ \#\{\text{punts amb } x \text{ senar dins de } AYX\} = \#\{\text{punts } (x,y) \in \mathbb{Z}^2 \text{ dins de } AYX\} := \mu, \end{aligned} \tag{5.5.20}$$

on la congruència entre el segon i el tercer terme és mòdul 2. Així doncs, es té que $\left(\frac{q}{p}\right) = (-1)^{\mu}$. Un argument similar, però intercanviant els papers de p, q, permet provar que $\left(\frac{p}{q}\right) = (-1)^{\nu}$, on ν és la quantitat de punts de coordenades enteres dins del triangle WYA. Com no existeixen punts de coordenades enteres sobre el segment AY (pel teorema de Tales, com $\text{mcd}(p,q) = 1$ no pot donar-se que $\frac{y}{x} = \frac{q}{p}$, amb $x, y \in \mathbb{Z}$, $0 < x < p$) es té $\mu + \nu = \#\{\text{punts amb } x \text{ senar dins de } AXYW\} = \frac{p-1}{2}\frac{q-1}{2}$, amb la qual cosa $(-1)^{\mu+\nu} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Combinant amb les dues fórmules prèvies obtenim que $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\mu+\nu} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$). D'aquí:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{5.5.21}$$

■

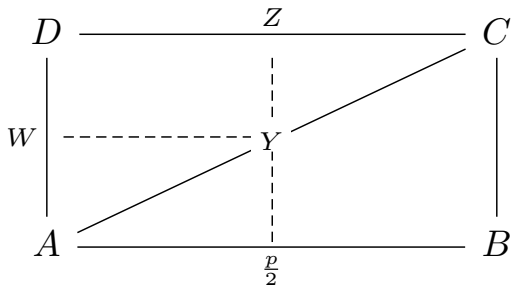

Figura 5.2: Figura esmentada representada gràficament. Notem que q correspon a la distància entre A i D i p a la de A i B, respectivament.

Proposició 5.5.16 (Nombre de solucions d'una equació congruencial)**.** *Si p és un nombre primer senar, el nombre de solucions de la congruència $x^2 \equiv a \pmod{p}$ és $1 + \left(\frac{a}{p}\right)$.*

Corol·lari 5.5.17. *Siguin p, q primers imparells diferents. Aleshores, es té:*

1. $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ *si almenys un d'aquests primers és congruent amb 1 mòdul 4, i*
2. $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$ *si tant p com q són congruents amb 3 mòdul 4.*

Demostració. És conseqüència directa de la llei de Reciprocitat Quadràtica. Per aquesta llei, vegem que $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ es compleix si, i només si, l'exponent de -1 en la fórmula, que és $\frac{p-1}{2}\frac{q-1}{2}$, és parell. Això, al seu torn, equival a dir que un dels dos factors ha de ser parell, així que s'ha de complir una de les següents opcions:

$$\begin{cases} p - 1 \equiv 0 \pmod 4 \iff p \equiv 1 \pmod 4 & \text{o bé} \\ q - 1 \equiv 0 \pmod 4 \iff q \equiv 1 \pmod 4 \end{cases} \tag{5.5.22}$$

■

Exemple 5.5.18. Gràcies a la llei de Reciprocitat Quadràtica, podem determinar si 3 és o no residu quadràtic mòdul p (recordar que la resposta a aquesta pregunta la dona el símbol de Legendre $\left(\frac{3}{p}\right)$) per a un primer p imparell donat $p \neq 3$. Aplicant el corol·lari anterior, dividim la prova en dos passos:

1. $p \equiv 1 \pmod 4$. En aquest cas tenim que

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 3 \\ -1 & \text{si } p \equiv 2 \pmod 3 \end{cases} \tag{5.5.23}$$

   És evident que 1 és residu quadràtic mòdul 3 i 2 no ho és.
2. En canvi, si $p \equiv 3 \pmod 4$, com 3 també és congruent amb 3 mòdul 4, el corol·lari diu que

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = \begin{cases} -1 & \text{si } p \equiv 1 \pmod 3 \\ 1 & \text{si } p \equiv 2 \pmod 3 \end{cases} \tag{5.5.24}$$

1 i 2 Ajuntant la informació dels dos casos, concloem que $\left(\frac{3}{p}\right) = 1$ si, i només si, està en els casos següents:

1. $p \equiv 1 \pmod 4$ i $p \equiv 1 \pmod 3$.
2. $p \equiv 3 \pmod 4$ i $p \equiv 2 \pmod 3$.

   Resolent aquests sistemes de dos congruències, ens queda que $p \equiv 1 \pmod{12}$ o bé $p \equiv 11 \equiv -1 \pmod{12}$. Per tant, el cas complementari és $\left(\frac{3}{p}\right) = -1 \iff p \equiv 5 \text{ o } 7 \pmod{12}$.

Per l'exemple, tenim, doncs, agafant alguns valors de prova, que $\left(\frac{3}{11}\right) = 1$ ja que $11 \equiv -1 \pmod{12}$, $\left(\frac{3}{17}\right) = -1$ ja que $17 \equiv 5 \pmod{12}$.

Gauss

Lema 5.5.19 (Lema de Gauss)**.** *Sigui p un primer imparell i a un enter no divisible per p. Sigui n la quantitat d'enters del conjunt $S = \{a, 2a, \left(\frac{p-1}{2}\right)a\}$ tals que al dividir-los per p s'obté una resta major que $\frac{p}{2}$. Aleshores, $\left(\frac{a}{p}\right) = (-1)^n$*

Demostració. Siguin $a_1, \ldots, a_n$ els elements de S tals que al dividir-los per p la resta és major que $\frac{p}{2}$. Siguin $b_1, \ldots, b_m$ els altres elements d'S, de manera que: $n + m = \frac{p-1}{2}$. Anomenarem a'_j, b'_j els elements corresponents a dividir els a_j i b_j per p. Es té, per tant, que

1. $\forall j \in \{1, 2, \ldots, n\}, a'_j \equiv a_j \pmod p$, amb $p - \frac{p-1}{2} = \frac{p+1}{2} \leq a'_j < p$,
2. $\forall j \in \{1, 2, \ldots, m\}, b'_j \equiv b_j \pmod p$, amb $0 \leq b'_j \leq \frac{p-1}{2}$.

Considerem ara un conjunt T tal que $T = \{p - a'_j \mid 1 \leq j \leq n\} \cup \{b'_j \mid 1 \leq j \leq m\}$. Provarem primer que $T = \{1, 2, \ldots, \frac{p-1}{2}\}$, provant en particular la inclusió cap a la dreta i que tots els elements de T són diferents.

$\subseteq$ $T \subseteq \{1, 2, \ldots, \frac{p-1}{2}\}$, això és trivial per als elements b'_j ja que cal element d'S és divisible per p (ja que són de la forma ak amb a no divisible per p i $0 < k \leq \frac{p-1}{2}$) i per tant cap residu pot ser zero. Per als elements de la forma $p - a'_j$ se segueix directament de $\frac{p+1}{2} \leq a'_j < p$.

$\neq$ Sabem que $n + m = \frac{p-1}{2}$, amb la qual cosa per a establir la igualtat entre conjunts ens és prou amb provar que els elements de la definició de T són diferents. Si $u, v \in \{1, 2, \ldots, \frac{p-1}{2}\}$ i $ua \equiv va \pmod p \implies u \equiv v \pmod p \implies u = v$, on hem usat que si dos elements són congrus mòdul p amb p primer i $u, v < p$ han de ser necessàriament iguals.
Aleshores, els n valors d'a'_j i, per tant, els n valors de $p - a'_j$ són tots diferents, així com els m valors de b'_j són tots diferents. Suposem ara, raonant per reducció a l'absurd, que existeix

$k \in [1,n]$ i $h \in [1,m]$ tals que $p - a'_k = b'_h$. Això implica que existeixen $u, v \in \{1, 2, \ldots, \frac{p-1}{2}\}$ tals que $p - ua \equiv va \pmod p$. D'aquí se segueix que

$$(u+v)a \equiv 0 \pmod p \tag{5.5.25}$$

i, per tant, com que $p \nmid a$, per LFA $p \mid (u+v)$. Com $2 \leq u+v \leq p-1$, la qual cosa és una contradicció. Així doncs, queda provat que els $n+m = \frac{p-1}{2}$ elements en la definició de T són tots diferents, d'on concloem que $T = \{1, 2, \ldots, \frac{p-1}{2}\}$.
A partir d'aquesta igualtat, multiplicant tots els elements d'aquest conjunt obtenim que

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv (p-a'_1)(p-a'_2)\cdots(p-a'_n)b'_1\cdots b'_m \equiv (-1)^n \cdot a'_1\cdots a'_n b'_1\cdots b'_m \\ &\equiv (-1)^n \cdot a_1\cdots a_n b_1\cdots b_m \equiv (-1)^n \cdot a(2a)\cdots\left(\frac{p-1}{2}a\right) \\ &\equiv (-1)^n \cdot a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \pmod p \xrightarrow{p\nmid\left(\frac{p-1}{2}\right)!} 1 \equiv (-1)^n \cdot a^{\frac{p-1}{2}} \pmod p \\ &\implies (-1)^n \equiv a^{\frac{p-1}{2}} \pmod p.\end{aligned} \tag{5.5.26}$$

Combinant amb el criteri d'Euler, ens queda que:

$$\left(\frac{a}{p}\right) \equiv (-1)^n \pmod p \implies \left(\frac{a}{p}\right) = (-1)^n. \tag{5.5.27}$$

■

Teorema 5.5.20. *Sigui p un primer imparell. Aleshores*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \text{ o } 7 \pmod 8 \\ -1 & \text{si } p \equiv 3 \text{ o } 5 \pmod 8 \end{cases} \tag{5.5.28}$$

Demostració. Considerem el conjunt S com en el lema de Gauss per al cas $a = 2$: $S = \{2, 4, \ldots, p-1\}$. Dividirem la prova en dos casos mòdul 4:

$p \equiv 1$ és fàcil determinar quins són els elements d'S tals que al dividir-los per p s'obté un residu major que $\frac{p}{2}$, doncs com ara els elements d'S són tots menors que p, ells mateixos són iguals als seus respectius residus mòdul p, per tant són: $\frac{p-1}{2}+2, \frac{p-1}{2}+4, \ldots, \frac{p-1}{2}+2\cdot\frac{p-1}{4} = p-1$, on hem usat la hipòtesi d'aquest primer cas, que $p \equiv 1 \pmod 4$, així que $\frac{p-1}{2}$ és parell i $\frac{p-1}{2}+2$ és el menor nombre par més gran que $\frac{p}{2}$.
Com el primer valor en aquesta llista és $\frac{p-1}{2}+2$ i l'últim és $\frac{p-1}{2}+2\frac{p-1}{4}$, on tots aquests nombres són parells, és clar que en total la quantitat d'elements d'S amb la propietat que al dividir-los per p s'obté un residu major que $\frac{p}{2}$ és $n = \frac{p-1}{4}$. Aplicant el lema de Gauss, concloem que si $p \equiv 1 \pmod 4 \implies \left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}$.
Ara bé, els primers $p \equiv 1 \pmod 4$ cauen en dues classes mòdul 8, poden complir $p \equiv 1 \pmod 8$ o $p \equiv 5 \pmod 8$. En el primer cas, $\frac{p-1}{4}$ és parell i en el segon, és senar. Per tant, concloem que

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 8 \\ -1 & \text{si } p \equiv 5 \pmod 8 \end{cases} \tag{5.5.29}$$

$p \equiv 3$ Ara, tots els elements de S tals que el residu de la divisió per p és major que $\frac{p}{2}$ són $\frac{p-1}{2}+1, \frac{p-1}{2}+3, \ldots, \frac{p-1}{2}+(2\frac{p+1}{4}-1) = p-1$. Aquí hem utilitzat que, en aquest cas, $\frac{p-1}{2}$ és imparell, així que el menor nombre parell major que $\frac{p}{2}$ és $\frac{p-1}{2}+1$. La quantitat d'elements d'aquest conjunt és, per tant, la quantitat de nombres senars en $\{1, 3, \ldots, 2\left(\frac{p+1}{4}\right)\}$, que és $\frac{p+1}{4}$.

Concloem que, en aquest cas, es té $n = \frac{p+1}{4}$ amb la qual cosa el Lema de Gauss ens dona que si $p \equiv 3 \pmod 4 \implies \left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}}$. Com en el cas anterior, separem en dos casos: $p \equiv 3 \pmod 8$ i $p \equiv 7 \pmod 8$. Concloem que:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 7 \pmod 8 \\ -1 & \text{si } p \equiv 3 \pmod 8 \end{cases} \tag{5.5.30}$$

Amb la qual cosa tenim l'expressió que desitjàvem al principi. ■

Proposició 5.5.21. *Siguin p, a, m com en el lema de Gauss. Aleshores,*

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} \lceil \frac{ka}{p} \rceil + (a-1)\frac{p^2-1}{8} \pmod 2. \tag{5.5.31}$$

En particular, si a és senar, ens queda

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} \lceil \frac{ka}{p} \rceil \pmod 2. \tag{5.5.32}$$

Demostració. La demostració és llarga i farragosa, a més que queda fora del nivell del curs. Es pot consultar a [Gra98, pàg. 186, 4.3] ■

Jacobi

Abans d'aplicar la llei de reciprocitat quadràtica, cal obtenir la descomposició en factors primers dels numeradors a dels símbols que apareixen en el càlcul, a fi d'assegurar que, després d'aplicar la llei de reciprocitat quadràtica, els denominadors siguin, efectivament, nombres primers senars. Per a resoldre aquest problema i evitar les descomposicions, s'introdueix el símbol de Jacobi.

Definició 5.5.22 (Símbol de Jacobi)**.** Siguin $n > 1$ un enter imparell i $a \in \mathbb{Z}$. Si $n = p_1^{e_1} \cdots p_r^{e_r}$ definim el *símbol de Jacobi* $\left(\frac{a}{n}\right)$ com

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1}\left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_r}\right)^{e_r}, \tag{5.5.33}$$

on en l'expressió anterior els factors de la dreta són símbols de Legendre. És evident, doncs, que el *símbol de Jacobi* generalitza al de Legendre.

Observació 5.5.23. Si n és compost i $\text{mcd}(a, n) = 1$, el valor del símbol de Jacobi $\left(\frac{a}{n}\right)$ *no determina de manera directa* si a és o no residu quadràtic mòdul n.

Exemple 5.5.24. Si $n = 15$ i $a = 2$ es té $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, però com no hi ha solució per a la congruència $x^2 \equiv 2 \pmod 3$ no pot haver-hi solució per a $x^2 \equiv 2 \pmod{15}$, així doncs 2 no és residu quadràtic mòdul 15.

Proposició 5.5.25. *Siguin P, P_1, P_2 nombres naturals senars i a, a_1, a_2 nombres enters qualsevol. Se satisfan les propietats següents:*

1. *si* $\mathrm{mcd}(a, P) > 1$, *aleshores* $\left(\frac{a}{P}\right) = 0$;
2. *si* $\mathrm{mcd}(a, P) = 1$, *aleshores* $\left(\frac{a}{P}\right) = \pm 1$ *i*
3. *si* $a \equiv a' \pmod{P}$, *aleshores* $\left(\frac{a}{P}\right) = \left(\frac{a'}{P}\right)$.

Propietat 5.5.26 (Propietats del símbol de Jacobi)**.** *Siguin $b, d \in \mathbb{Z}_{>1}$, imparells. Siguin també $a, c \in \mathbb{Z}$. Es té:*

1. *Si* $a \equiv c \pmod{b} \implies \left(\frac{a}{b}\right) = \left(\frac{c}{b}\right)$,
2. $\left(\frac{ac}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{c}{b}\right)$,
3. $\left(\frac{a}{bd}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{d}\right)$.

Demostració. 5.5.26.1 i 5.5.26.2 es dedueixen a partir que el símbol de Legendre té aquestes propietats. 5.5.26.3 surt directament de la definició del símbol de Jacobi. ■

Propietat 5.5.27 (Propietats de Reciprocitat de Jacobi)**.** *Siguin $a, b \in \mathbb{Z}_{>1}, \mathrm{mcd}(a, b) = 1$ i a, més, imparells.*

1. $\left(\dfrac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$,
2. $\left(\dfrac{2}{b}\right) = (-1)^{\frac{(b+1)(b-1)}{8}}$,
3. $\left(\dfrac{a}{b}\right) = \left(\dfrac{b}{a}\right)(-1)^{\frac{a-1}{2}\frac{b-1}{2}}$.

Observació 5.5.28. En el cas en què b sigui primer, la propietat b equival a la fórmula que ja vam provar per al símbol de Legendre $\left(\frac{2}{b}\right)$.

Lema 5.5.29. *Si a, b són enters imparells, aleshores* $\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b+1}{2} \pmod 2$.

Demostració. Com $a-1, b-1$ són ambdós parells, aleshores $(a-1)(b-1) \equiv 0 \pmod 4$. Això és fàcil de veure si considerem $a - 1 = 2\ell$ i $b - 1 = 2\gamma$, $\ell, \gamma \in \mathbb{Z}$ i $(a-1)(b-1) = 4\gamma\ell \pmod 4$. Així que $ab - a - b + 1 \equiv 0 \pmod 4 \implies ab + 1 \equiv a + b \pmod 4 \implies ab - 1 \equiv (a-1) + (b-1) \pmod 4$. I ens queda:

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b+1}{2} \pmod 2. \tag{5.5.34}$$

■

Lema 5.5.30. *Si $a, b \in \mathbb{Z}$, imparells:*

$$\frac{a^2b^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod 2. \tag{5.5.35}$$

Demostració. Com que $a \pm 1$ i $b \pm 1$ són parells, ens queda que $(a+1)(a-1)$ i $(b+1)(b-1)$ també ho seran, així que $a^2 - 1 \equiv 0 \pmod 4$ i $b^2 - 1 \equiv 0 \pmod 4$. D'això se segueix que $(a^2-1)(b^2-1) \equiv 0 \equiv a^2b^2 - a^2 - b^2 + 1 \pmod{16}$. Operant a ambdós membres de l'equivalència, ens queda $a^2b^2 - 1 \equiv a^2 + b^2 - 2 \equiv (a^2-1) + (b^2-1) \pmod{16}$. Podem dividir l'equació per una constant, en aquest cas 8, i ens queda la mateixa expressió que (5.5.35). ■

Lema 5.5.31. *Si $a, b, c \in \mathbb{Z}_{<1}$, imparells, suposant que $\left(\frac{a}{c}\right)\left(\frac{c}{a}\right) = (-1)^{\frac{a-1}{2}\frac{c-1}{2}}$ i que $\left(\frac{b}{c}\right)\left(\frac{c}{b}\right) = (-1)^{\frac{b-1}{2}\frac{c-1}{2}}$, aleshores,*

$$\left(\frac{ab}{c}\right)\left(\frac{c}{ab}\right) = (-1)^{\frac{ab-1}{2}\frac{c-1}{2}} \tag{5.5.36}$$

Demostració.

$$\left(\frac{ab}{c}\right)\left(\frac{c}{ab}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)\left(\frac{c}{a}\right)\left(\frac{c}{b}\right) = (-1)^{\frac{a-1}{2}\frac{c-1}{2}+\frac{b-1}{2}\frac{c-1}{2}} = (-1)^{\frac{c-1}{2}\left(\frac{a-1}{2}+\frac{b-1}{2}\right)} \xrightarrow{5.5.29} (-1)^{\frac{c-1}{2}\frac{ab-1}{2}}. \tag{5.5.37}$$

■

Després d'aquests lemes auxiliars, procedim a la demostració de la propietat 5.5.27.

Demostració de 5.5.27.

1. Provem 5.5.27.1 per inducció sobre el nombre de divisors primers de b. Sigui $b = p_1 p_2 \cdots p_r$, on els p_i són primers (no necessàriament tots primers) i $r \geq 1$. Si $r = 1$, b és primer i $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$ és una propietat ja demostrada del símbol de Legendre. Si $r > 1$, suposem que, per hipòtesi d'inducció, que la propietat és certa per al cas de $r-1$ divisors primers, per la qual cosa si $c = \frac{b}{p_r} \implies \left(\frac{-1}{c}\right) = (-1)^{\frac{c-1}{2}}$.
   Per altra banda, també es té (per ser p_r primer): $\left(\frac{-1}{p_r}\right) = (-1)^{\frac{p_r-1}{2}}$. On $\left(\frac{-1}{p_r}\right)$ correspon tant al símbol de Jacobi com al de Legendre, ja que el primer generalitza aquest últim. D'aquí, per 5.5.29, $\left(\frac{1}{b}\right) = \left(\frac{-1}{c}\right)\left(\frac{-1}{p_r}\right) = (-1)^{\frac{c-1}{2}}(-1)^{\frac{p_r-1}{2}} = (-1)^{\frac{c-1}{2}+\frac{p^r-1}{2}} = (-1)^{\frac{b-1}{2}}$. Això acaba la demostració per inducció sobre r.
2. Apliquem inducció sobre r, el nombre de divisors primers de b. Per a $r = 1$, és una propietat del símbol de Legendre equivalent a un resultat ja demostrat. Si $b = p_1 \cdots p_r$, amb $r > 1$, i sigui $c = \frac{b}{p_r}$. Per hipòtesi d'inducció, suposem que la propietat és certa per al cas de $r-1$ divisors, amb la qual cosa és certa per a c, és a dir: $\left(\frac{2}{c}\right) = (-1)^{\frac{c^2-1}{8}}$. També sabem (per ser p_r un nombre primer) que $\left(\frac{2}{p_r}\right) = (-1)^{\frac{p_r^2-1}{8}}$. D'aquí, per 5.5.30:

$$\left(\frac{2}{b}\right) = \left(\frac{2}{c}\right)\left(\frac{2}{p_r}\right) = (-1)^{\frac{c^2-1}{8}}(-1)^{\frac{p_r^2-1}{8}} = (-1)^{\frac{b^2-1}{8}}. \tag{5.5.38}$$

3. Apliquem inducció, però aquesta vegada sobre $n = r + s$, on r és el nombre de divisors primers de b i s el d'a, és a dir, $b = p_1 \cdots p_r$, $a = q_1 \cdots q_s$, amb tots els p_i i q_j primers. La base d'inducció és el cas $n = 2$, que equival a $r = s = 1$. En aquest cas, a i b són primers i el resultat ja va ser provat: és la llei de Reciprocitat Quadràtica.
   Si $n = r + s > 2$, suposem, sense pèrdua de generalitat que es té $r > 1$ (si no fos així, $s > 1$, que es tracta de manera anàloga). Sigui $c = \frac{b}{p_r}$. Suposem per hipòtesi d'inducció que la propietat és certa per a $n - 1 = r + s - 1$, és a dir, en el cas en què el total de divisors primers que posseeixen entre els dos nombres és $n - 1 = r + s - 1$. Com aquest és el cas per als nombres a, c tenim:

$$\left(\frac{a}{c}\right) = \left(\frac{c}{a}\right)(-1)^{\frac{a-1}{1}\frac{c-1}{2}} \iff \left(\frac{a}{c}\right)\left(\frac{c}{a}\right) = (-1)^{\frac{a-1}{2}\frac{c-1}{2}}. \tag{5.5.39}$$

   També podem aplicar la hipòtesi d'inducció al parell de nombres a, p_r, doncs en aquest cas el nombre total de divisors primers és $s + 1 \leq s + r - 1 = n - 1$. Per la qual cosa, es té

que $\left(\frac{a}{p_r}\right)\left(\frac{p_r}{a}\right) = (-1)^{\frac{a-1}{2}\frac{p_r-1}{2}}$. Aplicant 5.5.31 i obtenim

$$\left(\frac{a}{p_r c}\right)\left(\frac{p_r c}{a}\right) = (-1)^{\frac{a-1}{2}\frac{p_r c-1}{2}} \tag{5.5.40}$$

que, com $b = p_r c$, és el que volíem provar.

■

Conjectura 5.5.32 (Conjectura de Catalan)**.** *L'única solució en* $\mathbb{N}$ *de* $x^a - y^b = 1$ *per a* $a, b > 1$*,* $x, y > 0$ *és* $3^2 - 2^3$*.*

Capítol 6

Primeritat i factorització

6.1

Primeritat

Nombres pseudoprimers i de Carmichael

Recordem que 4.4.1 ens assegura que si n és un nombre natural primer i a un nombre enter tal que $\mcd(a,n)=1$, aleshores $a^{n-1}\equiv 1 \pmod{n}$. Però pot ser que n no sigui primer i que aquesta congruència també se satisfaci per a algun enter b tal que $\mcd(a,n)=1$.

Definició 6.1.1 (Nombre pseudoprimer)**.** Sigui $n>1$ un nombre enter, senar i compost i $a\in(\mathbb{Z}/n\mathbb{Z})^*, a\neq\pm 1$. Direm que n és pseudoprimer respecte de la base a si, i només si, $a^{n-1}\equiv 1 \pmod{n}$. Entendrem que si no s'especifica la base, s'està parlant d'$a=2$.

Observació 6.1.2. Si n és pseudoprimer en la base a, en particular a és coprimer amb n.

Definició 6.1.3 (Nombre de Carmichael)**.** Un nombre de Carmichael és un enter $n>1$ compost tal que és pseudoprimer en la base a per a tot $a \mid \mcd(a,n)=1$ (per a totes les bases coprimeres amb n). Equivalentment, podem definir-lo com aquell nombre senar i compost $n>1$ tal que per a tot nombre enter a que compleixi $\mcd(a,n)=1$ se satisfà la congruència $b^{N-1}\equiv 1 \pmod{N}$. El conjunt dels nombres de Carmichael és infinit.

Teorema 6.1.4 (Propietats de Carmichael)**.** *Els nombres de Carmichael compleixen les següents propietats:*

1. *Un nombre de Carmichael n és lliure de quadrats, és a dir, per a tot nombre primer p tal que $p \mid n$, aleshores $p^2 \nmid n$.*
2. *Sigui $n\in\mathbb{Z}_{>1}$, compost i lliure de quadrats. Aleshores,*

$$n \text{ és de Carmichael} \iff \forall p \mid (p \mid n) \wedge (p-1 \mid n-1). \tag{6.1.1}$$

3. *Un nombre de Carmichael té, com a mínim, tres divisors primers.*

Demostració. Demostrarem el primer apartat reduint a l'absurd. Suposem que es compleix $a^{n-1}\equiv 1 \pmod{n}$ per a tot a tal que $\mcd(a,n)=1$ i $p^2 \mid n$ per a algun primer p. Utilitzant la fórmula per a $\varphi(n)$ veiem que $p^2 \mid n \implies p \mid \varphi(n)$. Com $a^{n-1}\equiv 1 \pmod{n}$ i $p^2 \mid n \implies a^{n-1}\equiv 1 \pmod{p^2}$ per a tot a coprimer amb n. És fàcil veure que d'entre aquests a podem escollir un

valor a_0 que sigui arrel primitiva mòdul p^2: de fet, si posem $p = p_1, p_2, \ldots, p_r$ als factors primers d'n hi ha prou amb agafar a_0 solució del sistema:

$$\begin{cases} x \equiv \zeta \pmod{p^2}, \\ x \equiv 1 \pmod{p_2}, \\ \vdots \\ x \equiv 1 \pmod{p_r}. \end{cases} \tag{6.1.2}$$

On ζ és una arrel primitiva mòdul p^2 (per TXResidu, sabem que el sistema té solució). Com a_0 és arrel primitiva mòdul p^2 el seu ordre mòdul p^2 és $\varphi(p^2) = p(p-1)$. Com tenim que $a_0^{n-1} \equiv 1 \pmod{p^2} \implies p(p-1) \mid n-1$ i, en particular, veiem que $p \mid n-1$, la qual cosa és absurda ja que $p \mid n$. Aquesta contradicció prova que n és lliure de quadrats.

Pel que fa al segon apartat. Sigui n lliure de quadrats, és a dir, es té la descomposició en primers diferents $n = p_1 \cdots p_r$ tals que la seva valoració p-àdica és 1 per a tots els termes. Suposem que n és compost, és a dir, $r > 1$. Suposem que n és de Carmichael, és a dir, que $a^{n-1} \equiv 1 \pmod{n}$ per a tot $a \in (\mathbb{Z}/n\mathbb{Z})^*$. En particular, $a^{n-1} \equiv 1 \pmod{p_i}$. Amb el mateix argument que ja hem utilitzat en el primer apartat, veiem que d'entre tots els a coprimers amb n podem escollir una a tal que sigui arrel primitiva mòdul $p_i \implies \operatorname{ord}_{p_i}(a) = p_i - 1$. Ara, com que $a^{n-1} \equiv 1 \pmod{p_i}$ tenim que $p_i - 1 \mid n-1$. Recíprocament, suposem que per a tot p_i primer que divideix n es compleix $p_i - 1 \mid n-1$. Sigui a coprimer amb n (de tal manera que no és divisible per cap p_i). Per PTFermat, 4.4.1, $a^{p_i-1} \equiv 1 \pmod{p_i}$. D'aquí, com $n - 1 = k_i(p_i - 1)$ per a certs enters k_i, aleshores $a^{n-1} \equiv 1 \pmod{p_i}$ per a tot $i \in \{1, 2, \ldots, r\}$. Com $n = p_1 \cdots p_r$, aleshores, tal i com volíem:

$$a^{n-1} \equiv 1 \pmod{n}, \forall a \in (\mathbb{Z}/n\mathbb{Z})^*. \tag{6.1.3}$$

Ja per últim, sigui n un nombre de Carmichael. Podem suposar pel primer apartat que n és lliure de quadrats. Suposem que n posseeix solament dos divisors primers, és a dir, $n = pq$ amb p, q diferents. Sense pèrdua de generalitat, podem dir que $p < q$. Així doncs, pel segon apartat sabem que $q - 1 \mid p - 1$. D'altra banda,

$$n - 1 = pq - 1 = pq - p + p - 1 = p(q-1) + (p-1) \equiv p - 1 \pmod{q-1}. \tag{6.1.4}$$

D'aquí extraiem que $n - 1 \equiv 0 \pmod{q-1}$ i $n - 1 \equiv p - 1 \pmod{q-1}$ i $n - 1 \equiv p - 1 \pmod{q-1} \implies p - 1 \equiv 0 \pmod{q-1} \implies q - 1 \mid p - 1$. Però notem que tal resultat és absurd donat que $p - 1 < q - 1$. De tal manera, queda provat que tot nombre de Carmichael té com a mínim tres divisors primers. ■

Exemple 6.1.5 (Exemples de nombres de Carmichael)**.**

- $561 = 3 \cdot 11 \cdot 17$,
- $1105 = 5 \cdot 13 \cdot 17$,
- $41041 = 7 \cdot 11 \cdot 13 \cdot 41$.

Observació 6.1.6. Per a verificar que un enter compost és un nombre de Carmichael hi ha prou amb verificar que $a^{n-1} \equiv 1 \pmod{n}$ per a tot a coprimer amb n en l'interval $[2, n-1]$. Un enter que satisfaci totes aquestes congruències podrà ser o bé primer o bé un nombre de Carmichael.

Nombres fortament pseudoprimers

Definició 6.1.7 (Pseudoprimer d'Euler)**.** Sigui n un nombre compost i imparell. Sigui a coprimer amb n. Diem que n és pseudoprimer d'Euler respecte de la base a si $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$.

Observació 6.1.8. Tal i com vam veure durant la prova del test de Solovay-Strassen, si n és pseudoprimer d'Euler respecte d'a també és pseudoprimer respecte d'a i no existeixen nombres que siguin pseudoprimers d'Euler respecte tota base a coprimera amb n.

Definició 6.1.9 (Fortament pseudoprimer)**.** Sigui n un nombre imparell i compost, d'on $n-1 = 2^e t$ amb t imparell i $e > 0$. Sigui a coprimer amb n. Diem que n és fortament pseudoprimer d'a si es verifica que

$$a^t \equiv 1 \pmod{n} \text{ o bé } a^{2^i t} \equiv -1 \pmod{n},\ i \in \{0, 1, \ldots, e-1\}. \tag{6.1.5}$$

Proposició 6.1.10. *Si n és fortament pseudoprimer respecte d'una base a, aleshores és pseudoprimer d'Euler respecte d'a.*

Demostració. Dividim la prova en tres casos diferents:

1. Suposem que $a^t \equiv 1 \pmod{n} \implies a^{\frac{n-1}{2}} \equiv a^{2^{e-1}t} \equiv 1 \pmod{n}$. Calculem $\left(\frac{a}{n}\right)$. Sabem que $\left(\frac{a^t}{n}\right) = \left(\frac{1}{n}\right) = 1$ i també que $\left(\frac{a^t}{n}\right) = \left(\frac{a}{n}\right)^t$ i, per tant, $\left(\frac{a}{n}\right)^t = 1$ i com t és senar, aleshores $\left(\frac{a}{n}\right) = 1$. Doncs, tenim que $a^{\frac{n-1}{2}} \equiv 1 \equiv \left(\frac{a}{n}\right) \pmod{n}$.
2. Suposem que $a^{2^{e-1}t} \equiv -1 \pmod{n}$. Aleshores, $a^{\frac{n-1}{2}} \equiv a^{2^{e-1}t} \equiv -1 \pmod{n}$. Vegem que $\left(\frac{a}{n}\right) = -1$. Abans, però, una petita guia del que volem demostrar.

   Sigui p primer tal que $p \mid n$ (per la qual cosa, p imparell) i escrivim $p - 1 \equiv 2^{e'} s$ amb s imparell i $e' > 0$. Volem veure que (1) $e' \geq e$,

   $$(2)\ \left(\frac{a}{p}\right) = \begin{cases} -1, & \text{si } e' = e, \\ 1, & \text{si } e' > e. \end{cases} \tag{6.1.6}$$

   (1) $a^{2^{e-1}t} \equiv -1 \pmod{n} \implies a^{2^{e-1}ts} \equiv -1 \pmod{n} \implies a^{2^{e-1}t} \equiv -1 \pmod{p}$. Suposem que $e' < e \implies e' \leq e-1 \implies a^{2^{e'}ts} \not\equiv 1 \pmod{p} \implies a^{p-1} \equiv a^{2^{e'}s} \not\equiv 1 \pmod{p}$. Notem que usem que com que $2e'ts$ no és congruent amb 1, $2e't$ tampoc ho serà donat que un és múltiple de l'altre. Però ens queda $a^{p-1} \not\equiv 1 \pmod{p}$, contradient PTFermat.

   (2) Si $e = e'$: $\left(\frac{a}{p}\right) \equiv a^{2^{e-1}s} \pmod{p}$. Com aquest símbol de Legendre (essent a coprimer amb p) val ± 1, el seu valor no canvia si l'elevem a t (ja que t és imparell), així: $\left(\frac{a}{p}\right) \equiv a^{2^{e-1}s} \equiv a^{2^{e-1}st} \equiv -1 \pmod{p}$. Això queda provat ja que aquesta congruència l'hem provat a (1).

   Ara, si $e' > e$: com $a^{2^{e-1}t} \equiv -1 \pmod{n}$ elevem s (i canviem el mòdul n per mòdul p): $a^{2^{e-1}st} \equiv -1 \pmod{n} \implies a^{2^{e'-1}st} \equiv 1 \pmod{n}$, ja que $e' > e$. Pel criteri d'Euler, tenim que $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv a^{2^{e'-1}s} \pmod{n}$. Com $\left(\frac{a}{p}\right) = \pm 1$, ja que $\text{mcd}(a, p) = 1$, el seu valor no canviar a l'elevar-lo a t, aleshores $\left(\frac{a}{p}\right) \equiv a^{2^{e'-1}s} \equiv a^{2^{e'-1}st} \equiv 1 \pmod{n}$.

   Tornant al càlcul d'$\left(\frac{a}{n}\right)$. Escrivim: $n = \prod_{p|n} p$ (primers no necessàriament diferents). Aleshores, $\left(\frac{a}{n}\right) = \prod_{p|n} \left(\frac{a}{p}\right) = (-1)^k$, on k és el nombre de factors primers d'n tals que

$\left(\frac{a}{p}\right) = -1$, que pels resultats preliminars (1) i (2) sabem que k és igual a la quantitat de factors primers d'n amb $e' = e$ (sempre comptant multiplicitats). Volem provar que k és imparell i, així, $\left(\frac{a}{n}\right) = (-1)^k = -1 \equiv a^{\frac{n-1}{2}} \pmod{n}$.
Observem que $e' > e \implies p \equiv 1 \pmod{2^{e+1}}$ i $e' = e \implies p \equiv 1 + 2^e \pmod{2^{e+1}}$. Utilitzant això, ens queda:

$$\begin{aligned} &1 + 2^e \equiv 1 + 2^e t \equiv n \equiv \textstyle\prod_{p|n} p \equiv (1 + 2^e)^k \equiv 1 + k2^e \pmod{2^{e+1}} \\ &\implies 2^e(k-1) \equiv 0 \pmod{2^{e+1}} \implies k+1 \text{ parell} \implies k \text{ imparell.} \end{aligned} \tag{6.1.7}$$

3. Suposem que $a^{2^i t} \equiv -1 \pmod{n}$ amb $i \in \{0, 1 \ldots, e-2\}$. Com $i \leq e-2 < e-1$, tenim que: $a^{\frac{n-1}{2}} \equiv a^{2^{e-1}t} \equiv 1 \pmod{n}$. Per a calcular $\left(\frac{a}{n}\right)$, com en el segon cas, són necessaris resultats preliminars. Si p és primer imparell que divideix p i $p - 1 = 2^{e'}s$, s imparell i $e' > 0$, es pot veure que es compleixen que (c) $e' \geq i + 1$ i

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & \text{si } e' = i+1, \\ 1, & \text{si } e' > i+1. \end{cases} \tag{6.1.8}$$

La demostració d'aquestes dues propietats utilitza arguments similars als que ja hem vist en el segon cas, vegem-ho. Escrivim $n = \prod_{p|n} p$, primers p no necessàriament diferents. Aleshores, $\left(\frac{a}{n}\right) = \prod_{p|n}\left(\frac{a}{p}\right) = (-1)^k$, on k és el nombre de factors primers d'n tals que $\left(\frac{a}{p}\right) = -1$. Pels resultats preliminars (1) i (2) de l'anterior apartat, sabem que k és igual a la quantitat de factors primers d'n amb $e' = i + 1$.
Volem provar que k és parell, així que $\left(\frac{a}{n}\right) = (-1)^k = 1 \equiv a^{\frac{n-1}{2}} \pmod{n}$. Observem que $e' > i+1 \implies p \equiv 1 \pmod{2^{i+2}}$ i $e' = i+1 \implies p \equiv 1+2^{i+1} \pmod{2^{i+2}}$. Com $n = 1+2^e t$ i $i + 2 \leq e \implies n \equiv 1 \pmod{2^{i+2}}$. Aleshores, $1 \equiv n \equiv \prod_{p|n} p \equiv (1 + 2^{i+1})^k \equiv 1 + k2^{i+1} \pmod{2^{i+2}} \implies 2^{i+1}l \equiv 0 \pmod{2^{i+2}} \implies k$ parell. Per tant, k parell i $\left(\frac{a}{n}\right) = 1$, tal i com volíem veure.

■

6.2 Factorització

Mètode de Factorització de Fermat

Siguin $n = pq$, p i q primers (de l'ordre d'una potència de $\log n$ es té una manera eficient de factoritzar n.

Definició 6.2.1. Proposem un canvi de variables que permet escriure la factorització de n com una diferència de quadrats, és a dir, en lloc de trobar directament p, q proposem trobar abans a, b tals que

$$\begin{cases} p = a + b, \\ q = a - b. \end{cases} \tag{6.2.1}$$

D'on la igualtat $n = pq$ es transforma en $n = (a+b)(a-b) = a^2 - b^2$.

D'aquí se segueix que factoritzar n és equivalent a escriure-la com a diferència de quadrats les bases a i b de la qual no són consecutives, de manera que $a-b \neq 1$ i obtenim la factorització no trivial $n=(a+b)(a-b)$.

Observació 6.2.2. Les incògnites a, b són enteres, com es veu de resoldre el sistema de dues equacions. S'obté:

$$\begin{cases} a = \frac{p+q}{2}, b = \frac{p-q}{2}, \end{cases} \tag{6.2.2}$$

ja que p, q són imparells.

Proposició 6.2.3. *Si suposem que $p-q$ té un resultat petit, podem trobar a i b en una petita quantitat de casos.*

Exemple 6.2.4. Per exemple, si $a-b<\log n$, en efecte $b=\frac{p-q}{2}<\frac{\log n}{2}$ i $a=\frac{p+q}{2}$ compleix que

$$a^2-n=b^2<\left(\frac{\log n}{2}\right)^2 \implies a^2<n+\left(\frac{\log n}{2}\right)^2. \tag{6.2.3}$$

A més, $a^2-n=b^2>0 \implies a^2>n \implies a>\sqrt{n}$. Per tant,

$$\sqrt{n}<a<\sqrt{n+\left(\frac{\log n}{2}\right)^2}. \tag{6.2.4}$$

Per a trobar a es troba un per un els enters d'aquest interval. Vegem que la quantitat d'enters en aquest interval és, com a molt, $\frac{\log n}{2}$. Si anomenem U a aquesta quantitat tenim que $U<\sqrt{n+\left(\frac{\log n}{2}\right)^2}-\sqrt{n}$.

Ara sigui $V=\sqrt{n+\left(\frac{\log n}{2}\right)^2}+\sqrt{n}$. Veiem que $U<V$ i també que $UV=n+\left(\frac{\log n}{2}\right)^2-n=\left(\frac{\log n}{2}\right)^2$. Per tant, $U<\frac{\log n}{2}$.

Per tant, provem amb els enters d'aquest interval fins a trobar un a tal que $a^2-n=x$ sigui un quadrat perfecte. Calculem, partint d'una aproximació a $\sqrt{n}$, l'enter $\lceil\sqrt{n}\rceil$ (recordar 5.5.13) i, a partir d'aquest valor, trobar els valors d'a.

$$\begin{aligned} a &= \lceil\sqrt{n}\rceil+1, \text{ calcular } a^2-n=x \\ &= \lceil\sqrt{n}\rceil+2, \text{ calcular } a^2-n=x \\ &\vdots \end{aligned} \tag{6.2.5}$$

Quan calculem $a^2-n=x$, comprovem si el valor obtingut és un quadrat perfecte- Una manera fàcil de comprovar això últim és calcular, aproximadament, $\sqrt{n}$, agafar el valor $b\in\mathbb{Z}$ més proper a aquest valor i verificar si s'acompleix o no $b^2=x$. Una vegada trobat l'a tal que $a^2-n=x=b^2$, per $b\in\mathbb{Z}$, tenim que

$$n=a^2-b^2=(a+b)(a-b)=pq, \tag{6.2.6}$$

és a dir, tenim la factorització de n.

Observació 6.2.5 (Què passaria si aquesta factorització fos trivial?). Posem el cas de 6.2.4. Si fos el cas de $a-b=1$ tindríem que $a=b+1 \implies n=a+b=2b+1 \implies b=\frac{n-1}{2}$ i $a=\frac{n+1}{2}$, però com aquest valor d'a no pertany a l'interval

$$\left[\sqrt{n}, \sqrt{n+\left(\frac{\log n}{2}\right)^2}\right] \tag{6.2.7}$$

mai ens trobaríem en aquest cas. Tal fet té sentit perquè per a aquesta factorització trivial els dos factors són 1 i n, ja que no estan a prop l'un de l'altre.

El mètode que hem vist és ràpid sempre que $p - q$ sigui petit. En aquest cas, l'interval en què hem de buscar a té una longitud petita. Si es parteix de suposar que $p - q < W(\log n)^c$ per a $W, c \in \mathbb{Z}_{>0}$ també es dedueix que l'algorisme acabarà en ordre de temps polinomial en $\log n$.

Mètode de factorització de Pollard

El següent mètode permet donar una factorització eficient d'un enter $n = pq$ on p, q són primers grans, suposant que el primer p (o q, o el dos) és tal que $p-1$ (o $q-1$ o els dos) té la particularitat que és *B-smooth* en potències.

Definició 6.2.6 (*B-smooth*)**.** Donada una cota $B > 0$, diem que un enter és *B-smooth* si tots els factors primers d'x són menors que B.

Què fa dels *B-smooth* uns nombres tan útils? Per a un nombre molt gran, tenen una estructura multiplicativa força simple, tot i que tenen moltes xifres.

Definició 6.2.7 (*B-smooth* en potències)**.** Diem que un enter x és *B-smooth* en potències si al descomposar x en producte de primers:

$$x = p_1^{v_1(x)} p_2^{v_2(x)} \cdots p_n^{v_n(x)},\ p_i^{v_i(x)} \leq B,\ \forall i \tag{6.2.8}$$

En l'aplicació a la factorització d'un enter n, fixarem una cota B petita, de l'ordre de $\log n$ i per a aquest valor de B ens interessarà que cert valor sigui *B-smooth* en potències.

Donada una cota B comencem per precalcular el mínim comú múltiple de tots els enters menors o iguals a B:

1. Calcular el conjunt P de tots els primers $p \leq B$.
2. Calcular el producte $m = \prod_{p \in P} p^{\log_p B}$.

D'aquesta manera, hem format m amb tots els primers fins a B, cadascun dels quals amb el major exponent w tal que $p^w \leq B$, donat que $p^{\log_p B} = B$. Això prova que m és el mínim comú múltiple buscat.

Aquest valor el calculem per a una cota B de l'ordre de $\log n$ (la idea és agafar un B el més gran possible, sempre que el càlcul previ es pugui fer en un temps raonable). Una vegada calculat aquest valor, el mètode de Pollard intenta factoritzar $n = pq$ i funciona sota la condició que almenys un dels dos factors primers de n té la propietat que és *B-smooth* en potències.

El mètode de Pollard

Proposició 6.2.8 (Mètode de Pollard)**.** *Després de fixar la cota B, suposem que $n = pq$, amb p, q nombres primers i tals que $p - 1$ és B-smooth en potències. L'objectiu és trobar p i així factoritzar n calculant $q = \frac{n}{p}$. Triem un enter a tal que $1 < a < n$ a l'atzar. Suposarem que $p \nmid a$: això ocorre amb una probabilitat molt alta i, a més, si $p \mid a$ tindríem prou amb calcular* $\mathrm{mcd}(a, n)$ *amb l'algorisme d'Euclides per a trobar p.*

Per PTFermat, sabem que $a^{p-1} \equiv 1 \pmod{p}$. *Calculem* $m = \operatorname{mcm}(2, 3, \ldots, B)$. *Com* $p-1$ *és* B*-smooth en potències, si*

$$p-1 = p_1^{v_1(p)} p_2^{v_2(p)} \cdots p_r^{v_r(p)} \implies p_i^{v_i(p)} \leq B,\ \forall i \in \{1,2,\ldots,r\} \implies p_i^{v_i(p)} \mid m,\ \forall i \in \{1,2,\ldots,r\} \implies p-1 \mid m. \tag{6.2.9}$$

Adonem-nos que tenim un enter m *múltiple de* $p-1$ *(*$m = (p-1)k$*) sense conèixer-ne el seu valor ni el de* p. *Per tant, com* $a^{p-1} \equiv 1 \pmod{p} \implies a^m \equiv (a^{p-1})^k \equiv 1 \pmod{p} \implies p \mid a^m - 1$. *Per altra banda, com* $p \mid pq = n$, *podem calcular* $\operatorname{mcd}(a^m - 1, n)$ *amb l'algorisme d'Euclides i veure que solament tenim dues possibilitats:*

$$d = \begin{cases} p, \\ pq. \end{cases} \tag{6.2.10}$$

En el primer cas, $d = p$ *i, per tant, ja hem trobat el factor* p, *primer, de* n, *amb la qual cosa calculant* $q = \frac{n}{p}$ *tenim la factorització de* n. *En el segon cas, com* $d = n = pq$, *no ens dona la factorització de* n. *Aleshores,* $a^m - 1$ *també és divisible per* q *i, variant el valor de la base* a *i repetint l'algorisme per a diverses bases, això deixarà de succeir, excepte si l'exponent és també múltiple de* $q-1$, *cosa que solament pot ocórrer si* $q-1$ *és* B*-smooth en potències.*

És a dir, suposant que $p-1$ *és* B*-smooth en potències i se'ns dona el segon cas* $d = pq$, *en el qual no podem factoritzar* n, *com a causa directa ve que* $q-1$ *és també* B*-smooth en potències. Quan això passa, hem de modificar l'algorisme: canviarem la cota* B *per cotes menors fins a arribar a una cota* B' *tal que solament un dels factors primers d'*n, *posem* p, *tingui* $p-1$ *tal que sigui* B'*-smooth en potències i l'altre no ho sigui. Calculant, doncs, l'*m *i utilitzant-lo amb aquesta cota* B' *l'algorisme funcionarà, mitjançant el mètode dicotòmic.*

Proposició 6.2.9 (Mètode dicotòmic per a Pollard**).** *A partir del* B *inicial i suposant que aquest* B *no serveix per a factoritzar* n, *perquè cau en el cas* $d = \operatorname{mcd}(a^m - 1, n) = n$. *Els següents valors de la cota es calculen segons el mètode dicotòmic:*

Provem amb $\frac{B}{2}$. *Si per a aquesta cota tenim que* $\operatorname{mcd}(a^m - 1, n)$ *és igual a un factor primer de* n, *l'algorisme s'acaba. Si* $\operatorname{mcd}(a^m - 1, n)$ *és igual a 1, significa que la cota és molt petita i hem de provar un valor més gran. Si, en canvi,* $\operatorname{mcd}(a^m - 1, n) = n$ *és perquè aquesta nova cota segueix sent molt alta i, com a següent valor, escollim un més baix. Iterant aquest procés arribarem al valor* $B' < B$ *que permet factoritzar* n.

Observació 6.2.10.

1. El mètode dicotòmic garanteix que provarem, com a màxim, $\log_2 B$ valors per a la cota.
2. Per tant, l'algorisme acaba funcionant de manera eficient sempre que es compleixi la hipòtesi inicial: ha d'existir un valor de la cota B que no sigui massa gran i, per tant, que permeti calcular l'm tal i com s'indica, tal que per a com a mínim un dels factors primers d'n es compleixi que és B*-smooth* en potències.
3. Respecte el càlcul de $d = \operatorname{mcd}(a^m - 1, n)$, tot i que s'ha de fer amb l'algorisme d'Euclides per a un $a^m - 1$ massa gran tal càlcul esdevé impossible computacionalment. Per a resoldre aquest problema, hem de fer ús del següent resultat elemental:

$$x \equiv y \pmod{n} \implies \operatorname{mcd}(x, n) = \operatorname{mcd}(y, n). \tag{6.2.11}$$

Per tant, per a calcular d no fa falta conèixer el valor d'$a^m - 1$: solament necessitem el seu residu mòdul n. Per a trobar-lo, calculem la potència $a^m \pmod n$ usant l'exponenciació modular binària (és a dir, que utilitza la descomposició de m en base 2) i així calcularem de manera eficient la classe mòdul n d'a^m i de $a^m - 1$, sense haver de fer cap càlcul que involucri a nombres més grans que n^2.

6.3 Certificats de primeritat

Definició 6.3.1 (Test de primeritat)**.** Un test de primeritat és un algorisme determinístic per a determinar si un nombre és primer. Un test probabilísitic de primeritat és una prova o un conjunt de proves que es poden fer a un nombre enter N i que permeten determinar, amb una certa probabilitat d'error, que N és primer.

El mètode més evident per a determinar si un nombre enter donat $N > 1$ és primer o no consisteix a intentar dividir-lo successivament per tots els enters M tals que $1 < M < N$ [Gra98]. Si alguna divisió fos possible, aleshores N no seria primer. Aquest procediment ens comportaria fer N divisions, així que no és efectiu.

Tampoc és efectiu usar el teorema de Wilson, 4.6.1, ja que ens implicaria haver de calcular $(n-1)!$, per la qual cosa hauríem de fer $n-2$ multiplicacions (que, tot i que puguem reduir mòdul n, segueixen sent massa operacions).

De la mateixa manera ens passaria si intentéssim usar el Petit Teorema de Fermat, 4.4.1, com a criteri de primeritat: hauríem de verificar que $\forall a \in [2, n-1]$ coprimer amb n es té que $a^{n-1} \equiv 1 \pmod n$, amb la qual cosa n pot ser o bé primer o bé un nombre de Carmichael. Cal afegir que els nombres de Carmichael són terriblement inusuals, així que probablement estiguem en el cas que n sigui primer. Així doncs, hauríem de calcular $\varphi(n)$ exponenciacions mòdul n (i això, un altre cop, és un nombre massa gran). Una opció força vàlida seria comprovar la congruència $a^{n-1} \equiv 1 \pmod n$ per a uns pocs valors d'a, per exemple $a \leq \log n$. D'aquesta forma, si n compleix les congruències podrà ser o bé un pseudoprimer en base a per a tot $a \leq \log n$ o bé, molt probablement, un nombre primer.

Test de Solovay-Strassen

Proposició 6.3.2 (Test de Solovay-Strassen)**.** *Sigui $n > 1$, imparell. Són equivalents:*

1. *n és primer,*
2. *$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n$ per a tot $a \in (\mathbb{Z}/n\mathbb{Z})^*$.*

Demostració.

$1 \Rightarrow 2$ És directament el criteri d'Euler.

$2 \Rightarrow 1$ Suposem, raonant per reducció a l'absurd, que n és compost. Si a és coprimer amb n, tenim que $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n$ d'on, elevant al quadrat veiem que $a^{n-1} \equiv 1 \pmod n$, aleshores, n és un nombre de Carmichael. Per les propietats ja vistes per a aquests nombres, sabem que $n = p_1 \cdots p_r$ amb els p_i primers senars i diferents, i $r \geq 3$. Sigui a un enter coprimer

amb p_1 tal que $\left(\frac{a}{p_1}\right) = -1$. Si plantegem el sistema de congruències

$$\begin{aligned} x &\equiv a \pmod{p_1} \\ x &\equiv 1 \pmod{p_2} \\ &\vdots \\ x &\equiv 1 \pmod{p_r} \end{aligned} \tag{6.3.1}$$

sabem per TXResidu que existeix una solució x_0 amb $1 \leq x_0 \leq n$. A més, com a és coprimer amb p_1 veiem que x_0 és coprimer amb tots els p_i (doncs tots els residus del sistema són coprimers amb els corresponents mòduls): per tant, $\text{mcd}(x_0, n) = 1$. Per tant, podem calcular el símbol de Jacobi:

$$\left(\frac{x_0}{n}\right) = \left(\frac{x_0}{p_1}\right)\left(\frac{x_0}{p_2}\right)\cdots\left(\frac{x_0}{p_r}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{1}{p_r}\right) = (-1)(1)\cdots(1) = -1. \tag{6.3.2}$$

Per hipòtesi, $x_0^{\frac{n-1}{2}} \equiv \left(\frac{x_0}{n}\right) \equiv -1 \pmod{n} \implies x_0^{\frac{n-1}{2}} \equiv -1 \pmod{p_2}$, però, per altra banda, $x_0 \equiv 1 \pmod{2}$ per ser solució del sistema de congruències i tal cosa implica que $x_0^{\frac{n-1}{2}} \equiv 1 \pmod{p_2}$. D'aquesta contradicció deduïm que si n compleix 6.3.2.2, aleshores n és necessàriament primer.

■

A partir d'aquest criteri podem assegurar que un nombre senar major que 1 que compleix 6.3.2.2 és primer. El problema que ens trobem, però, és que verificar 6.3.2.2 requereix massa càlculs, ja que caldria verificar-ho per a tots els valors d'a en l'interval $[1, n]$ de coprimers amb n. De totes maneres, el fet de tenir un criteri de primeritat permet extreure un test eficient probabilístic que permet afirmar, amb una alta probabilitat, que un nombre és primer.

Proposició 6.3.3 (Test probabilístic de Solovay-Strassen)**.** *Sigui $n > 1, n \in \mathbb{Z}$ imparell. Siguin $a_1, \ldots, a_k$ nombres diferents coprimers amb n en l'interval $[1, n]$. Aleshores, si es té que $a_i^{\frac{n-1}{2}} \equiv \left(\frac{a_i}{n}\right) \pmod{n}$, per a tot $i = 1, 2, \ldots, k$ la probabilitat amb què n és primer és major o igual a $1 - \frac{1}{2^k}$.*

Demostració. Tal demostració no es troba dins del nivell d'aquest curs, però es pot consultar a [Gra98, pàg. 217], on es fa ús de morfismes de grups. ■

Test de Miller-Rabin

Si $n > 1$ i imparell que satisfà la propietat en la definició de fortament pseudoprimer per a tota base a coprimera amb n (excepte per la condició de ser compost). Aleshores, n és primer. El recíproc és cert.

Demostració. Per la proposició 6.1.10, n compleix $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$ per a tot a coprimer amb n. Pel test de Solovay-Strassen, n és primer. El fet que el recíproc és cert es desprèn de 4.4.1 (Fermat) i que la congruència $x^2 \equiv 1 \pmod{p}$ solament posseeix solucions 1 i -1. ■

Observació 6.3.4 (Test de primalitat AKS)**.** Es coneix un algorisme determinístic i polinomial (en $\log n$) per a determinar si un enter n és primer o no: el test de primalitat AKS.

Capítol 7

Criptografia

7.1

Criptografia de clau secreta

Cèsar

Definició 7.1.1 (Cifratge de Cèsar). En aquest criptosistema, el primer que s'ha de fer és codificar el missatge X donat, que suposarem que conté solament caràcters de l'alfabet (excloent els espais i la lletra ñ). Associarem a les 26 lletres de l'alfabet els nombres del 0 al 25 en l'ordre usual. La clau K es fixa com un enter en l'interval del 0 al 25.

Per a encriptar, donat un missatge X (que suposarem ja codificat, amb la qual cosa està format per enters del 0 al 25). A cadascun dels nombres que el formen li sumem K i reduïm el resultat mòdul 26 per a tornar a obtenir un altre cop obtenir enters en $[0, 25]$.

Si descodifiquem el missatge obtingut, és a dir, substituïm per les corresponents lletres de l'alfabet, obtenim el missatge Y que s'envia: el *missatge encriptat*. En essència, estem movent les lletres del missatge K posicions cap a la dreta.

Per a desencriptar el missatge Y rebut, el receptor ha de desfer el procés usant la clau secreta K: primer transforma les lletres de Y en nombres de l'interval $[0, 25]$ (codifica), després es resta K a cadascun dels nombres obtinguts i redueix el resultat mòdul 26 (agafa el representant $[0, 25]$ de cada resultat), i finalment transforma els nombres obtinguts en les corresponents lletres de l'alfabet.

Notació 7.1.2. Identifiquem un missatge de text amb el corresponent missatge codificat (és a dir, suposem que els missatges són cadenes d'enters en l'interval $[0, 25]$), els processos d'encriptatge i desencriptatge venen, per tant, donats per una funció i la seva inversa, ambdues a valors en $\mathbb{Z}/26\mathbb{Z}$, i aquesta funció és simplement sumar la component K en cada component, amb la suma en $\mathbb{Z}/26\mathbb{Z}$:

- $X = (x_1, \ldots, x_n) \in (\mathbb{Z}/26\mathbb{Z})^n \implies X + \vec{K} = (x_1 + K, x_2 + K, \ldots, x_n + K) \in (\mathbb{Z}/26\mathbb{Z})^n$.
- Si $X + \vec{K} := Y = (y_1, \ldots, y_n) \implies Y - \vec{K} = (y_1 - K, y_2 - K, \ldots, y_n - K) = X \in (\mathbb{Z}/26\mathbb{Z})^n$.

On X és el missatge a enviar i Y el missatge encriptat que s'envia. Després de desencriptar Y s'obté $Y - \vec{K}$, el qual correspon clarament al missatge original X, donat que s'han aplicat en les components les funcions inverses $F(x) = x + K, F^{-1}(y) = y - K$, ambdues definides en $\mathbb{Z}/26\mathbb{Z}$.

Exemple 7.1.3. Si dues persones A i B han acordat usar la clau $K = 10$ esbrina el missatge que ha enviat A si B rep $Y =$ WKVNSDYFSBEC.

Resolució. Codificant Y, obtenim que $C(Y) = \{22, 10, 21, 13, 18, 3, 24, 5, 18, 1, 4, 2\}$. Desencriptem restant $K = 10$ a cada component i reduint mòdul 26: $C(Y) - K = \{12, 0, 11, 3, 8, 19, 14, 21, 8, 17, 20, 18\}$. Les lletres corresponents a aquest missatge formen el missatge MALDITOVIRUS. ■

Definició 7.1.4 (Criptosistema)**.** Un *criptosistema* és una quíntupla (T, C, K, E, D) tal que

- T és el conjunt finit de textos possibles,
- C és el conjunt finit de textos encriptats possibles,
- K és el conjunt finit de claus possibles,
- per a cada $k \in K$, hi ha una funció d'encriptatge $e_k \in E$ i una funció de desencriptatge $d_k \in D$ tal que $d_k(e_k(x)) = x$, per a tot text $x \in T$.

Propietat 7.1.5 (Propietats d'un bon criptosistema)**.**

1. *Per a tot $k \in K$, les funcions d'encriptatge i desencriptatge e_k i d_k es poden calcular efectivament en un temps polinomial.*
2. *Donat un text encriptat, ha de ser difícil per un intrús sense la clau $k \in K$ poder-la trobar i el text original. En altres paraules, qualsevol atac que intenti sigui un algorisme no polinomial.*
3. *Aquesta dificultat ha de ser constant, tot i que l'enemic conegui com funciona el criptosistema: la seguretat es basa en mantenir secreta la clau K (principi de Kerchhoffs).*

El cifratge de Cèsar, descrit sota aquest esquema (assumint que el missatge ja s'ha codificat) té els següents elements:

1. $(T = \mathbb{Z}/26\mathbb{Z})^m$,
2. $C = (\mathbb{Z}/26\mathbb{Z})^m$, per a un m apropiat, $K = \mathbb{Z}/26\mathbb{Z}$,
3. Donat $k \in K$, la funció e_k, de T en C, és la funció que en cada component ve donada per $e_k(x) = x + k$. Per últim, la funció d_k de C en T és la que en cada component té la llei $d_k(y) = y - k$.

Observació 7.1.6. Recordar que com aquestes funcions estan definides en les classes residuals que formen $\mathbb{Z}/26\mathbb{Z}$ (on per a cada classe agafem sempre el representant de l'interval $[0, 25]$), les fórmules anteriors, per exemple $e_k(x) = x + k$. Cal interpretar-les com congruències mòdul 26.

Definició 7.1.7 (Transformacions afins)**.** Transformacions més generals són les transformacions afins:

$$f_{(a,b)} = E_{(a,b)}(m) \equiv am + b \pmod{26}, \tag{7.1.1}$$

amb $a, b \in \mathbb{Z}$ la clau $0 \leq a, b, m \leq 26$, i $\text{mcd}(a, 26) = 1$. Podríem definir la seva inversa, doncs, com

$$f^{-1}_{(a,b)} = D_{(a,b)}(c) \equiv a^{-1}(c - b) \pmod{26}, \tag{7.1.2}$$

on a^{-1} és la inversa multiplicativa d'a mòdul 26.

7.2

Criptografia de clau pública

RSA

Generalitats

La criptografia de clau pública radica en la idea d'una funció bijectiva f tal que donada f és impossible calcular pràcticament la seva inversa.

Si $S = \mathbb{Z}/n\mathbb{Z}$ per a $n = pq$, amb p i q primers grans, volem veure que existeixen funcions $f : S \longrightarrow S$ bijectives que, tot i que es conegui la seva expressió i el valor de n, no es coneixen algorismes que permetin calcular en temps quadràtic la seva inversa.

En particular, no es pot determinar la inversa de f excepte si es factoritza n, la qual cosa fa que el sistema sigui segur, ja que per a p i q suficientment grans no existeixen algorismes quadràtics per a factoritzar $n = pq$.

Exemple 7.2.1 (Funcionament d'un criptosistema de clau privada**).** Bob té una clau pública que, com bé indica el nom, és de domini públic. Identifiquem aquesta clau pública amb una funció f amb les propietats ja especificades. Quan Alice vol enviar un missatge $M \in S$ a Bob, l'encripta usant la clau pública $f : S \longrightarrow S$ obtenint $f(M) = X \in S$, el missatge encriptat. Serà únicament el Bob qui pugui desencriptar tal missatge, ja que comptarà amb informació secreta que li permetrà *precalcular* la funció inversa de f, f^{-1}. Aquesta informació privada és el que anomenem la seva *clau privada*: ara, Bob podrà desencriptar el missatge X obtenint $f^{-1}(X) = M$.

Vegem que, en cap cas, els dos han compartit informació secreta. De fet, no ha sigut (ni és) necessari que Alice conegui la clau privada: ella solament necessita la clau pública amb què encriptar el missatge.

En el sistema concret que veurem és $S = \mathbb{Z}/n\mathbb{Z}$ on el valor de n i de la funció f són públics, on $n = pq$ amb p i q primers grans i secrets. Veurem que la única manera que es coneix de determinar la inversa de f és coneixent els divisors primers p i q de n de manera que la seguretat del criptosistema es basa en què no existeixen algorismes eficients per a factoritzar tals n i trobar p, q.

Atacant RSA

Suposem que la clau pública de la Berta és (n, e) i la seva clau de desencriptatge és d tal que $ed \equiv 1 \pmod{\varphi(n)}$. Si fóssim capaços de factoritzar $n = pq$, aleshores podríem computar $\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1$. D'aquesta manera, podríem computar d i, com hem vist, sabríem factoritzar n. En altres paraules, podríem trencar el criptosistema RSA.

$\varphi(n)$

Suposem $n = pq$. Donat $\varphi(n)$, és molt fàcil computar p i q. Tenim que

$$\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1; \tag{7.2.1}$$

hem descobert tant $pq = n$ com $p + q = n + 1 - \varphi(n)$. Així doncs, coneixem el polinomi

$$x^2 - (p+q)x + pq = (x-p)(x-q), \tag{7.2.2}$$

les arrels del qual són p i q. Aquestes arrels es poden trobar fent ús de la fórmula quadràtica.

p,q Suposant que p i q són relativament propers, és fàcil factoritzar n usant el mètode de factorització de Fermat. Suposem $n = pq$ amb $p > q$. Aleshores,

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2. \tag{7.2.3}$$

Com que p i q estan relativament a prop,

$$s = \frac{p-q}{2} \tag{7.2.4}$$

és petit i

$$t = \frac{p+q}{2} \tag{7.2.5}$$

és lleugerament més gran que $\sqrt{n}$ i $t^2 - n = s^2$ és un quadrat perfecte. Aleshores, ens destinem a provar, tal i com hem proposat en 6.2.4,

$$\begin{aligned} t &= \lceil\sqrt{n}\rceil + 1, \text{ calcular } t^2 - n = s^2 \\ &= \lceil\sqrt{n}\rceil + 2, \text{ calcular } a^2 - n = s^2 \\ &\vdots \end{aligned} \tag{7.2.6}$$

Anem provant valors fins que $t^2 - n$ sigui un quadrat perfecte s^2. Aleshores, ens quedaria $p = t + s$ i $q = t - s$.

Bibliografia

[Ros84] H Rosen Kenneth. *Elementary number theory and its applications*. 1984.

[Que85] Michel Queysanne. *Algebra básica*. Vicens-Vives, 1985.

[Hal95] Paul R Halmos. *Linear algebra problem book*. Vol. 16. American Mathematical Soc., 1995.

[Gra98] Artur Travesa i Grau. *Aritmètica*. Vol. 25. Edicions Universitat Barcelona, 1998.

[Mos04] Leo Moser. *An introduction to the theory of numbers*. The Trillia Group, 2004.

[Ste08] William Stein. *Elementary number theory: primes, congruences, and secrets: a computational approach*. Springer Science & Business Media, 2008.

[CL09] Manuel Castellet i Irene Llerena. *Àlgebra lineal i geometria*. Vol. 1. Univ. Autònoma de Barcelona, 2009.

[Ma15] Dan Ma. *Solving Quadratic Congruences*. Utilitzat per a alguna consulta puntual. Des. de 2015. URL: `https://exploringnumbertheory.wordpress.com/2013/10/15/solving-quadratic-congruences/`.

[Cre] Teresa Crespo. *Aritmètica. Curs 2013-2014*.

Índex terminològic