APUNTS D'ARITMÈTICA

XEVI GUITART

Resum. Apunts de l'assignatura Artimètica de la Universitat de Barcelona, curs 2018–2019. Per a realitzar aquestes notes he consultat diverses fonts, principalment [NZM91], [Ste09] i [GH04]

Índex

Departament de Matemàtiques i Informàtica, Universitat de Barcelona, Catalunya
E-mail address: xevi.guitart@gmail.com.

1. Tema 1: Divisibilitat

L'aritmètica és l'estudi dels nombres enters:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Començarem aquest estudi parlant de la noció de divisibilitat.

1.1. Definicions i primeres propietats.

Definició 1.1. Donats a i b dos nombres enters, amb $a \neq 0$, diem que a divideix b si existeix $c \in \mathbb{Z}$ tal que $b = ac$. Ho escrivim $a \mid b$. També diem que a és un divisor de b i que b és un múltiple de a.

Exemple 1.2. $3 \mid 15$ i $4 \nmid 21$ (4 no divideix 21). També, $-7 \mid 35$ i $-7 \mid -35$.

Proposició 1.3 (Propietats de la divisibilitat)**.** *Si a, b, i c són nombres enters, aleshores:*

a) Si $a \mid b$ aleshores $a \mid bc$.
b) Si $a \mid b$ i $b \mid c$ aleshores $a \mid c$.
c) Si $a \mid b$ i $a \mid c$ aleshores $a \mid (b + c)$. Més en general, $a \mid (xb + yc)$ per a tot $x, y \in \mathbb{Z}$.
d) Si $a \mid b$ i $b \mid a$ aleshores $a = \pm b$.
e) Si a i b són positius, i $a \mid b$ aleshores $a \leq b$.

Demostració. Demostrem només la c) i deixem la resta com a exercici. Si $a \mid b$ i $a \mid c$ aleshores $b = ab'$ i $c = ac'$ per a certs $b', c' \in \mathbb{Z}$. Aleshores $xb + yc = xab' + yac' = a(xb' + yc')$, amb la qual cosa veiem que $a \mid (xb + yc)$. □

Definició 1.4. Un enter $n > 1$ diem que és primer si els seus únics divisors positius són 1 i n.

Exemple 1.5. La llista de nombres primers comença per $2, 3, 5, 7, 11, 13, 17, 19, \dots$

El conjunt dels nombres primers és un dels objectes més fascinants i més estudiat de les matemàtiques. Es poden plantejar moltes qüestions al voltant dels nombres primers, per exemple:

- Quants primers hi ha?
- Com podem trobar nombres primers? Hi ha alguna fórmula que els doni tots?
- Si ens donen un nombre enter, hi ha algun mètode "ràpid" per a determinar si és primer?
- Com estan distribuïts els nombres primers dins del conjunt de nombres naturals? Quina "proporció" de nombres naturals són primers?
- ....

Al llarg del curs veurem la resposta a alguna d'aquestes preguntes. La primera, per exemple, ja era coneguda per Euclides.

Teorema 1.6 (Euclides, $\sim$ 300 a.C.)**.** *Hi ha infinits nombres primers.*

Demostració. Siguin $p_1, p_2, \dots, p_n$ nombres primers. Veurem que existeix un primer no contingut en el conjunt $\{p_1, p_2, \dots, p_n\}$. Per a això, definim

$$N = p_1 p_2 \dots p_n + 1.$$

Si N és primer, aleshores $N > p_i$ per a tot i i per tant $N \neq p_i$ per a tot i. Si N no és primer, aleshores ha de ser divisible per algun primer q. Però necessàriament $q \neq p_i$ per a tot i, ja que si $q = p_i$ per a algun i, aleshores tindríem que $q \mid N$ i $q \mid N - 1$; però per la propietat c) de la Proposició 1.3 també $q \mid N - (N - 1)$, és a dir $q \mid 1$ que no pot ser. □

L'estudi dels nombres primers ve de lluny doncs, i segueix essent una de les àrees de recerca més actives en matemàtiques avui en dia. El seu comportament ha fascinat matemàtics de totes les èpoques. Una cita famosa que explica una mica el perquè és de Don Zagier, que en una conferència de 1975 digué:

"There are two facts about the distribution of prime numbers of which I hope to convince you so overwhelmingly that they will be permanently engraved in your hearts. The first is that, despite their simple definition and role as the building blocks of the natural numbers, the prime numbers grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behavior, and that they obey these laws with almost military precision" [1]

A part del seu atractiu matemàtic, els nombres primers tenen una gran importància pràctica. Això també ho anirem veient al llarg del curs. D'entrada, dins de l'aritmètica, són importants per què en un cert sentit són les peces fonamentals en què es descomponen els nombres enters.

Teorema 1.7 (Teorema Fonamental de l'Aritmètica)**.** *Tot nombre enter positiu es pot escriure com a producte de primers. Aquesta expressió és única, llevat de l'ordre en què escrivim els primers.*

Exemple 1.8. $50 = 2 \cdot 5 \cdot 5$, $130 = 2 \cdot 5 \cdot 13$, $17 = 17$, $60 = 2^3 \cdot 3 \cdot 5$

Observació 1.9. Aquest teorema és més subtil del que ens pot semblar a primera vista (és un resultat que hem après a l'escola i l'hem utilitzat sense problema des de llavors, amb la qual cosa potser el tenim tan interioritzat que ens sembla evident, però no ho és i cal demostrar-lo).

De moment, només demostrarem el fet que tot enter positiu es pot escriure com a producte de primers. Això sí que és senzill. Sigui $n > 1$ un enter. Si n no és divisible per cap nombre més gran que 1 i més petit que n, aleshores n és primer i ja hem acabat. Altrament, $n = n_1 \cdot n_2$ per a certs n_1 i n_2 amb $1 < n_i < n$. Aleshores podem repetir l'argument amb n_1 i n_2: o bé són primers o bé són producte de nombres més petits. I així successivament. Clarament el procés acaba i expressa n com a producte de primers.

El que és menys directe de demostrar és la unicitat; veurem la prova més endavant. Per a demostrar-la, introduirem alguns conceptes molt rellevants (divisió entera, màxim comú divisor, l'algoritme d'Euclides,...).

Observació 1.10. El teorema fonamental de l'aritmètica ens dóna un criteri per a decidir sobre la divisibilitat. Si $a, b \in \mathbb{Z}_{>0}$, els podem escriure com

$$\begin{aligned} a =& p_1^{r_1} p_2^{r_2} \dots p_n^{r_n}, \\ b =& p_1^{s_1} p_2^{s_2} \dots p_n^{s_n}, \end{aligned}$$

amb els p_i primers i $r_i, s_i \in \mathbb{Z}_{\geq 0}$ (és a dir, si un dels primers no apareix en una descomposició, el posem amb exponent 0). Aleshores a divideix b si i només si $r_i \leq s_i$ per a tot i.

1.2. **Divisió entera.**

Teorema 1.11 (Divisió entera)**.** *Siguin $a, b \in \mathbb{Z}$ amb $b \neq 0$. Existeixen uns únics enters q i r amb*

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

[1] Don Zagier, *The first* 50 *million prime numbers*, https://people.mpim-bonn.mpg.de/zagier/files/doi/10.1007/BF03039306/fulltext.pdf

Demostració. Farem només el cas $b > 0$, i deixem el cas $b < 0$ com a exercici. Considerem la successió

$$\ldots, a-2b, a-b, a, a+b, a+2b, \ldots \tag{1.1}$$

i denotem per r l'enter no negatiu més petit d'aquesta successió. Per construcció $r = a - qb + r$ per a algun enter q, i clarment $r < b$ (ja que altrament $0 \leq a + (q-1)b < r$ i hauríem trobat un element no negatiu de la successió estrictament menor que r). Això prova l'existència de q i r satisfent (1.1).

Veiem la unicitat. Si

$$a = bq' + r \quad \text{amb} \quad 0 \leq r' < b \tag{1.2}$$

aleshores restant (1.1) i (1.2) veiem que

$$r - r' = b(q - q').$$

Ara $0 \leq r, r' < b$ implica que $|r - r'| < b$. Però si $q \neq q'$ aleshores $b|q - q'| \geq b$ i per tant ha de ser $q = q'$, i també doncs $r = r'$. □

Exemple 1.12. Si dividim 7 per 3 tenim que $7 = 3 \cdot 2 + 1$. També podem dividir -7 per 3 i això és $-7 = 3(-3) + 2$. Fixem-nos que el residu sempre és un nombre entre 0 i $b - 1$.

Observació 1.13. Podem fer la divisió entera amb l'ajuda d'una calculadora: per a dividir 738 entre 151 calculem

$$\frac{738}{151} = 4.887\ldots$$

i el quocient és la part entera d'aquest nombre, és a dir 4; el residu es calcula aleshores com $738 - 4 \cdot 151 = 134$, amb la qual cosa veiem que $738 = 4 \cdot 151 + 134$.

Observació 1.14. Cal remarcar que hi ha un algoritme eficient per a calcular la divisió entera, és essencialment el mètode de divisió llarga que aprenem (o apreníem) a l'escola. Aquest algoritme (o variants) implementat en un software matemàtic fa possible dividir ràpidament nombres molt grans (de milers de xifres).

1.3. **Màxim comú divisor.**

Definició 1.15. El màxim comú divisor de dos nombres enters a i b és el nombre enter més gran que divideix a i b a la vegada. La notació que s'utilitza és $\mathrm{mcd}(a, b)$ o, quan no hi hagi perill de confusió, simplement (a, b).

Exemple 1.16. $\mathrm{mcd}(6, 9) = 3$; en efecte, els divisors positius de 6 són $1, 2, 3, 6$ i els divisors positius de 9 són $1, 3, 9$. De divisors comuns només hi ha 1 i 3, així que el més gran és 3.

Definició 1.17. Diem que a i b són coprimers, o relativament primers, si $\mathrm{mcd}(a, b) = 1$.

En aquest apartat veurem com podem calcular el màxim comú divisor de dos nombres. Una primera resposta és el mètode que aprenem a l'escola: si factoritzem a i b com

$$\begin{aligned} a &= p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}, \\ b &= p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}, \end{aligned}$$

amb els p_i primers i $r_i, s_i \in \mathbb{Z}_{\geq 0}$ aleshores

$$\mathrm{mcd}(a, b) = p_1^{\min(a,b)} \cdot p_2^{\min(a,b)} \ldots p_n^{\min(a,b)}.$$

Per exemple:

$$168 = 2^3 \cdot 3 \cdot 7$$
$$140 = 2^2 \cdot 5 \cdot 7$$

i per tant $\mathrm{mcd}(186, 140) = 2^2 \cdot 7 = 28$. Aquest mètode però no és del tot satisfactori per dos motius: el primer és que encara no hem demostrat el teorema fonamental de l'aritmètica (però això ho acabarem fent o sigui que aquest problema desapareixerà); el segon és que el mètode només és practicable si els enters són petits. En efecte, per a aplicar aquesta fórmula ens cal conèixer la factorització de a i b, i aquesta és una tasca complicada per a enters grans. No es coneixen avui en dia algoritmes eficients per a factoritzar, de manera que fins i tot amb la potència de càlcul dels ordinadors actuals no és possible factoritzar nombres enters d'uns quants centenars de xifres[2].

Tot seguit veurem un mètode molt més eficient per a calcular el màxim comú divisor: l'algoritme d'Euclides. Com el seu nom indica, aquest mètode ja era conegut per Euclides i de fet és un dels resultats més meravellosos de les matemàtiques. Amb aquest mètode, i amb l'ajuda d'un ordinador, podem calcular ràpidament el màxim comú divisor de nombres que tinguin milers de xifres[3].

Per començar, explicarem l'algoritme d'Euclides amb un exemple. Suposem que volem calcular $\mathrm{mcd}(168, 140)$. Dividim 168 per 140:

$$168 = 1 \cdot 140 + 28$$

El punt clau és el següent: si d és un enter tal que $d \mid 168$ i $d \mid 140$ aleshores $d \mid 28$ per l'apartat c) de la Proposició 1.3. D'altra banda, també veiem que si $d \mid 140$ i $d \mid 28$ aleshores $d \mid 168$. Així doncs, el conjunt de divisors comuns de 168 i 140 coincideix amb el conjunt de divisors comuns de 140 i 28, amb la qual cosa $\mathrm{mcd}(168, 140) = \mathrm{mcd}(140, 28)$. Hem reduït doncs el problema a calcular el màxim comú divisor d'una parella de nombres més petits. I ara podem repetir el procés, dividim 140 per 28 i en aquest cas veiem que

$$140 = 5 \cdot 28 + 0$$

i per tant $\mathrm{mcd}(140, 28) = 28$ i ja hem acabat. Doncs això és l'algoritme d'Euclides. Està basat en la proposició següent, la demostració de la qual deixem com a exercici (però el raonament és idèntic al que hem fet per 168 i 140):

Proposició 1.18. $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, a - qb)$ *per a tot* $q \in \mathbb{Z}$.

Així doncs, l'algoritme[4] d'Euclides és el següent: suposem que volem calcular $\mathrm{mcd}(a, b)$ amb $a > 0$ i $b \geq 0$.

(1) Fer la divisió entera $a = bq + r$;
(2) Si $r = 0$ aleshores $\mathrm{mcd}(a, b) = b$;
(3) Si $r \neq 0$, aleshores substituir (a, b) per (b, r) i tornar al punt (1).

[2] en aquest fet es basen molts dels mètodes criptogràfics que s'utilitzen actualment, això ho veurem més endavant

[3] de fet, cada cop que fem una compra per internet segurament un dels passos que fa el navegador és calcular algun màxim comú divisor amb l'algoritme d'Euclides

[4] no entrarem a donar una definició precisa del que és un algoritme, per a nosaltres serà suficient pensar en un algoritme com a mètode o procediment que es pot fer servir per a calcular una certa quantitat, que està garantit que finalitza i que retorna el resultat correcte.

Exemple 1.19. Calculem el màxim comú divisor de 532 i 123 fent les divisions successives:

$$\begin{aligned} 532 &= 4 \cdot 123 + 40 \Rightarrow (532, 123) = (123, 40) \\ 123 &= 3 \cdot 40 + 3 \Rightarrow (123, 40) = (40, 3) \\ 40 &= 13 \cdot 3 + 1 \Rightarrow (40, 3) = (3, 1) \\ 3 &= 3 \cdot 1 + 0 \Rightarrow (3, 1) = 1 \end{aligned}$$

amb la qual cosa $(532, 123) = 1$. Aquest procediment és fàcil de mecanitzar i de programar: comencem escrivint els dos nombres i anem omplint la seqüència de residus, on a cada pas calculem el residu resultat de dividir el nombre que està dues files més amunt pel de la fila immediatament superior:

$$\begin{aligned} &532 \\ &123 \\ 40 &= 532 - 4 \cdot 123 \\ 3 &= 123 - 3 \cdot 40 \\ 1 &= 40 - 13 \cdot 3 \end{aligned}$$

Observació 1.20. No farem una anàlisi detallada del nombre de passos amb què acaba aquest mètode en funció de la mida de a i b. Tot el que farem serà una observació de caire heurístic (i potser no gaire rigorosa), però que en certa manera ja ens dona una idea de per on van els trets. Cada cop que dividim a per b obtenim un residu r que està entre 0 i $b-1$. No sabem ben bé quin serà el residu però podem esperar que en mitjana (aquí pensem que repetim molts cops el pas de la divisió) estigui al voltant de $b/2$. Això suggereix que en cada pas la mida dels nombres involucrats es divideix per 2. Per exemple, esperem que per a calcular el màxim comú divisor de nombres de mida al voltant de $1.000.000 \simeq 2^{20}$ faran falta uns 20 passos.

1.4. **El mínim comú múltiple.**

Definició 1.21. El mínim comú múltiple de a i b és el més petit dels nombres enters positius que són múltiples de a i b a la vegada. Es denota per $\mathrm{mcm}(a, b)$ o per $[a, b]$.

Observació 1.22. Sempre existeixen múltiples comuns de a i b, per exemple ab.

La proposició següent ens diu com calcular el mínim comú múltiple a partir del màxim comú divisor.

Proposició 1.23. *Si $a > 0$ i $b > 0$ aleshores $[a, b](a, b) = ab$.*

Aquesta propietat serà conseqüència del lema següent:

Lema 1.24. *Si $a \mid m$ i $b \mid m$ aleshores $\frac{ab}{(a,b)} \mid m$.*

Demostració del lema. Posem $m = aa'$ amb $a' \in \mathbb{Z}$. Multiplicant per b tenim que $mb = aba'$, i dividint per (a, b):

$$\frac{mb}{(a,b)} = \frac{ab}{(a,b)} a'$$

d'on veiem que

$$\frac{ab}{(a,b)} \mid \frac{mb}{(a,b)}. \tag{1.3}$$

Canviant el paper de a i b en el raonament anterior, arribem a què

$$\frac{ab}{(a,b)} \mid \frac{ma}{(a,b)}. \tag{1.4}$$

Com que $\frac{a}{(a,b)}$ i $\frac{b}{(a,b)}$ són coprimers, per Bézout existeixen $x, y \in \mathbb{Z}$ tals que

$$\frac{ax}{(a,b)} + \frac{by}{(a,b)} = 1,$$

que podem multiplicar per m i obtenir que

$$\frac{max}{(a,b)} + \frac{mby}{(a,b)} = m. \tag{1.5}$$

De (1.3) i (1.4) veiem que

$$\frac{ab}{(a,b)} \mid x\frac{ma}{(a,b)} + y\frac{mb}{(a,b)} = m.$$

□

Demostració de la Proposició 1.23. El lema ens diu que si $m > 0$ és un múltiple comú de a i b aleshores $\frac{ab}{(a,b)} \mid m$ i per tant $\frac{ab}{(a,b)} \leq m$. Com que $\frac{ab}{(a,b)}$ és un múltiple comú de a i b, veiem que és el més petit de tots.

□

1.5. **Combinacions i identitat de Bézout.**

Definició 1.25. Donats $a, b \in \mathbb{Z}$ diem que la suma d'un múltiple de a i un múltiple de b és una combinació de a i b. Dit d'una altra manera, una combinació de a i b és un nombre de la forma

$$ax + by \text{ amb } x, y \in \mathbb{Z}.$$

L'objectiu d'aquest apartat és caracteritzar el conjunt de les combinacions de dos nombres a i b. Posem $d = \text{mcd}(a, b)$. Aleshores, si n és una combinació de a i b clarament $d \mid n$ (novament, per l'apartat c) de la Proposició 1.3). És a dir, tota combinació és múltiple de d. Resulta que el recíproc també és cert: tot múltiple de d és combinació de a i b. Això prové del resultat següent.

Proposició 1.26. *Si $d = (a, b)$ aleshores existeixen $x_0, y_0 \in \mathbb{Z}$ tals que*

$$d = x_0 a + y_0 b.$$

Demostració. Considerem el conjunt

$$A = \{ax + by | x, y \in \mathbb{Z}\},$$

i sigui $\ell = x_0 a + y_0 b$ l'enter positiu més petit que pertany a A. Veurem que $\ell = d$, i això finalitzarà la prova. Ho veurem en dos passos:

- Primer pas: $\ell \mid a$ i $\ell \mid b$. Per a provar-ho, suposem en primer lloc que $\ell \nmid a$. Aleshores dividint a per ℓ el residu serà diferent de 0 i tenim que

  $$a = \ell q + r \text{ amb } 0 < r < \ell.$$

  Però fixem-nos que

  $$r = a - \ell q = a - (x_0 a + y_0 b)q = (1 - q x_0)a + (-q y_0)b,$$

  és a dir que $r \in A$; el fet que $0 < r < \ell$ és doncs una contradicció amb el fet que ℓ és l'enter positiu més petit que pertany a A. Així doncs, veiem que $\ell \mid a$. Que $\ell \mid b$ es veu igual.

- Segon pas: $\ell \geq d$. En efecte, com que $d \mid a$ i $d \mid b$ podem posar $a = da'$ i $b = db'$ per a certs $a', b' \in \mathbb{Z}$. Per tant

$$\ell = x_0 a + y_0 b = d(x_0 a' + y_0 b')$$

  i per tant $d \mid \ell$. Com que d i ℓ són positius, això implica que $\ell \geq d$.

En resum: ℓ és un divisor comú de a i b que és més gran o igual que el màxim comú divisor de a i b. Necessàriament $\ell = d$. □

Corol·lari 1.27. *Si $m \mid a$ i $m \mid b$ aleshores $m \mid (a, b)$.*

Demostració. Acabem de veure que existeixen enters x, y tals que

$$(a, b) = xa + yb,$$

d'on és evident que $m \mid (a, b)$. □

També és important destacar la propietat següent, que de fet hem vist a la demostració de la proposició anterior.

Proposició 1.28. *Podem caracteritzar el màxim comú divisor de a i b com l'enter positiu més petit que es pot escriure de la forma $ax + by$ amb $x, y \in \mathbb{Z}$.*

Això ens permet demostrar fàcilment algunes propietats del màxim comú divisor.

Proposició 1.29. *a) Si $m \in \mathbb{Z}_{>0}$ aleshores $(ma, mb) = m(a, b)$;*
b) Si $m \mid a$ i $m \mid b$ amb $m > 0$, aleshores

$$(\frac{a}{m}, \frac{b}{m}) = \frac{1}{m}(a, b).$$

c) Si $d = (a, b)$ aleshores $(\frac{a}{d}, \frac{b}{d}) = 1$.

Demostració. a)

$$\begin{aligned}(ma, mb) &= \text{valor positiu més petit del conjunt } \{xma + ymb \mid x, y \in \mathbb{Z}\} = \\ &= m \cdot \text{valor positiu més petit del conjunt } \{xa + yb \mid x, y \in \mathbb{Z}\} = m(a, b).\end{aligned}$$

b) És un cas particular de a).
c) Cas particular de b).

□

Donats $a, b \in \mathbb{Z}$ sabem que existeixen $x, y \in \mathbb{Z}$ tals que

$$(a, b) = xa + yb. \tag{1.6}$$

De la identitat (1.6) se'n diu la identitat de Bézout, o de fet potser millor dir-ne una identitat de Bézout, ja que els enters x, y que satisfan aquesta identitat no són en absolut únics. Podem calcular de manera eficient una identitat de Bézout per a a, b utilitzant el que s'anomena l'algoritme d'Euclides estès. Per exemple, per a calcular una identitat de Bézout per a 532 i 123. Comencem escrivint cadascun d'aquests nombres com a combinació trivial d'ells:

$$\begin{aligned}532 &= 1 \cdot 532 + 0 \cdot 123 \\ 123 &= 0 \cdot 532 + 1 \cdot 123.\end{aligned}$$

Ara es tracta de repetir les operacions que hem fet a l'Exemple 1.19 per a calcular la seqüència dels residus a banda i banda de les igualtats anteriors, de manera que en cada pas anem obtenint una expressió del residu en aquell pas com a combinació de 532 i 123:

$$\begin{aligned} 532 &= 1 \cdot 532 + 0 \cdot 123 \\ 123 &= 0 \cdot 532 + 1 \cdot 123 \\ 40 &= 1 \cdot 532 - 4 \cdot 123 \\ 3 &= -3 \cdot 532 + 13 \cdot 123 \\ 1 &= 40 \cdot 532 - 173 \cdot 123. \end{aligned}$$

Com a conclusió de tota aquesta discussió sobre les combinacions és que les combinacions de a i b són exactament els múltiples de (a, b). La propietat important és que (a, b) es pot escriure com a combinació de a i b. Això ens permet demostrar la següent propietat fonamental[5] dels nombres primers.

Proposició 1.30 (Lema d'Euclides)**.** *Sigui p un nombre primer i siguin a i b nombres enters. Si $p \mid ab$ aleshores $p \mid a$ o $p \mid b$.*

Demostració. Suposem que $p \nmid a$. Aleshores com que p és primer necessàriament $(a, p) = 1$. Per tant, existeixen $x, y \in \mathbb{Z}$ tals que

$$1 = xa + yp.$$

Multiplicant aquesta identitat per b tenim que

$$b = xab + ybp.$$

Clarament $p \mid ybp$, mentre que $p \mid xab$ ja que $p \mid ab$ per hipòtesi. Així doncs p divideix la suma $xab + ybp = b$. □

Exercici 1.31. Proveu que, més en general, si $(a, b) = 1$ i $a \mid bc$ aleshores $a \mid c$.

Això ens permet demostrar, per fi, el teorema fonamental de l'aritmètica.

Teorema 1.32 (Teorema Fonamental de l'Aritmètica)**.** *Tot nombre enter positiu es pot escriure com a producte de primers. Aquesta expressió és única, llevat de l'ordre en què escrivim els primers.*

Demostració. Ja hem demostrar l'existència de la factorització en producte de primers, però fem-ho aquest cop de manera una mica més formal per inducció. El cas base de la inducció és $n = 1$ que és el producte buit de primers (o, si un no està còmode amb aquest cas una mica degenerat, podem prendre com a cas base $n = 2$ que és primer i per tant és evident que s'escriu com a producte de primers). Ara suposem que tot enter positiu m amb $m < n$ s'escriu com a producte de primers, i veiem que també és cert per a n. Si n és primer ja hem acabat, mentre que si n no és primer aleshores es pot escriure com $n = n_1 \cdot n_2$ per a certs enters $n_1 < n$ i $n_2 < n$. Per hipòtesi d'inducció cadascun d'ells s'escriu com a producte de primers, i per tant n també.

Veiem ara la unicitat. Suposem que tenim dues descomposicions

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s \tag{1.7}$$

on els p_i i els q_j són primers. D'aquesta expressió veiem que $p_1 \mid q_1 q_2 \dots q_s$ i com que p_1 és primer, pel Lema d'Euclides necessàriament divideix algun dels factors. Podem suposar (reordenant els q_j

[5]de fet aquesta propietat és tan important, que en certs contextos més generals es pren com a definició de primer; això es veurà en cursos posteriors d'àlgebra com ara a Estructures Algebraiques

si cal) que $p_1 \mid q_1$. Com que q_1 és primer això implica que $p_1 = q_1$. És a dir que a (1.7) podem cancel·lar p_1 i q_1 per a obtenir

$$p_2 \dots p_r = q_1 q_2 \dots q_s.$$

Repetint l'argument ara amb p_2 veiem que també podem cancel·lar p_2 i q_2, i així successivament. La conclusió és que necessàriament $r = s$ i que (reetiquetant potser els primers) $p_i = q_i$ per a tot i. □

1.6. **Equacions diofantines lineals amb dues incògnites.** Una equació diofantina (o diofàntica) és una equació polinòmica en la qual estem interessats només en les solucions enteres. Per exemple, cercar totes les parelles de nombres $(x, y) \in \mathbb{Z}^2$ tals que

$$12x + 14y = 6$$

és un exemple d'equació diofantina. A les equacions de la forma

$$ax + by = c$$

on els coeficients a, b, c són enters se les anomena equacions diofantines lineals amb dues incògnites. En general és difícil resoldre equacions diofantines, però les lineals es poden resoldre explícitament. De fet, ja tenim quasi tota la feina feta en el cas de dues variables, ja que és essencialment una reformulació de l'estudi que hem fet de les combinacions de a i b.

Proposició 1.33. *Siguin $a, b, c \in \mathbb{Z}$ i $d = (a, b)$. L'equació*

$$ax + by = c$$

té solucions enteres si i només si $d \mid c$. En cas que tingui solució, podem trobar una solució particular x_0, y_0 amb l'algoritme d'Euclides estès, i aleshores totes les solucions són de la forma

$$\begin{aligned} x &= x_0 + k\frac{b}{d} \\ y &= y_0 - k\frac{a}{d} \end{aligned}$$

amb $k \in \mathbb{Z}$ arbitrari.

Demostració. Per a la primera afirmació, una implicació és clara: si $ax + by = c$ per a alguns $x, y \in \mathbb{Z}$ aleshores clarament $d \mid c$. Veiem l'altra implicació: si $d \mid c$ posem $c = dc'$ amb $c' \in \mathbb{Z}$. Aleshores per Bézout existeixen enters x_0', y_0' tals que

$$ax_0' + by_0' = d.$$

Multiplicant tota la identitat per c' veiem que

$$ax_0'c' + by_0'c' = dc' = c$$

amb la qual cosa si posem $x_0 = x_0'c'$ i $y_0 = y_0'c'$ veiem que

$$ax_0 + by_0 = c \tag{1.8}$$

i per tant x_0, y_0 és una solució. També hem vist de passada com calcular-la: com que prové d'una identitat de Bézout podem fer-ho amb l'algoritme d'Euclides estès.

Falta provar la darrera afirmació. Sigui x, y una altra solució; és a dir, suposem que x, y són nombres enters tals que

$$ax + by = c. \tag{1.9}$$

Restant (1.8) de (1.9) veiem que

$$a(x - x_0) = b(y_0 - y). \tag{1.10}$$

Dividint per d a banda i banda

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y). \tag{1.11}$$

Aquí observem que encara que estiguin escrits en forma de fracció, a/d i b/d són nombres enters ja que $d \mid a$ i $d \mid b$. De (1.11) en veiem que $\frac{a}{d} \mid \frac{b}{d}(y_0 - y)$ i com que $(\frac{a}{d}, \frac{b}{d}) = 1$ necessàriament $\frac{a}{d} \mid (y_0 - y)$. Així doncs

$$y = y_0 - k\frac{a}{d}. \tag{1.12}$$

Substituïnt (1.12) a (1.10) n'obtenim que

$$x = x_0 + k\frac{b}{d}.$$

Finalment, només ens falta provar que si x_0, y_0 és una solució aleshores $x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d}$ també és solució per a tot valor de k. Això és una simple comprovació:

$$a(x_0 + k\frac{b}{d}) + b(y_0 - k\frac{a}{d}) = ax_0 + ak\frac{b}{d} + by_0 - bk\frac{a}{d} = c.$$

□

1.7. **Divisió entera de polinomis.** Moltes de les propietats que hem deduït per als enters a partir del teorema de la divisió entera tenen anàlegs per a polinomis amb coeficients en un cos, gràcies a l'existència també de divisió entera.

Sigui K un cos, i denotem per $K[x]$ el conjunt de polinomis amb coeficients a K,

$$K[x] = \{a_n x^n + a_{n-1}x^{n-1} + \dots a_1 x + a_0 \mid a_i \in K\},$$

amb la suma i producte de polinomis definits de la manera habitual.

Exemple 1.34. Un exemple de cos és el dels nombres racionals. De fet, si el lector no se sent còmode treballant amb aquest grau de generalitat en què K denota un cos qualsevol, per a fixar idees pot pensar en els polinomis a coeficients racionals $\mathbb{Q}[x]$. Altres exemples de cossos són $K = \mathbb{R}$ el cos dels nombres reals o $K = \mathbb{C}$ el cos dels nombres complexos. Més endavant en aquestes notes veurem uns altres exemples de cossos, que tenen la particularitat que tenen un nombre finit d'elements.

Teorema 1.35 (de la divisió entera de polinomis)**.** *Siguin $f(x), g(x) \in K[x]$ dos polinomis amb $g(x) \neq 0$. Existeixen uns únics $q(x), r(x) \in K[x]$ tals que*

$$f(x) = g(x)q(x) + r(x) \quad on \quad r(x) = 0 \text{ o bé } \operatorname{grau}(r(x)) < \operatorname{grau}(g(x)). \tag{1.13}$$

Demostració. L'existència de $q(x)$ i $r(x)$ satisfent les propietats de l'enunciat prové de l'algoritme de divisió de polinomis, anàleg a la divisió llarga de nombres enters.

Per a veure la unicitat, suposem que $q_1(x)$ i $r_1(x)$ són polinomis tals que

$$f(x) = g(x)q_1(x) + r_1(x) \quad \text{on} \quad r_1(x) = 0 \text{ o bé } \operatorname{grau}(r_1(x)) < \operatorname{grau}(g(x)) \tag{1.14}$$

i veiem que necessàriament $r_1(x) = r(x)$ i $q_1(x) = q(x)$. Restant (1.13) de (1.14) tenim que

$$g(x)\,(q(x) - q_1(x)) = r_1(x) - r(x). \tag{1.15}$$

Si $r_1(x) - r(x) = 0$, com que $g(x) \neq 0$ necessàriament ha de ser $q(x) = q_1(x)$ i ja hem acabat. Si $r_1(x) - r(x) \neq 0$, aleshores $q(x) - q_1(x) \neq 0$ i per tant

$$\text{grau}(r_1(x) - r(x)) < \text{grau}(g(x)) \leq \text{grau}(g(x)(q(x) - q_1(x)))$$

cosa que és una contradicció amb la igualtat (1.15) i per tant ha de ser $r_1(x) - r(x) = 0$. □

Exemple 1.36. Si $f(x) = x^3 + x + 1$ i $g(x) = 2x^2 + 4x + 6$ aplicant l'algoritme de divisió trobem que el quocient de dividir $f(x)$ per $g(x)$ és $q(x) = \frac{1}{2}x - \frac{1}{2}$ i el residu és $r(x) = -x + 4$. Fixem-nos que malgrat que $f(x)$ i $g(x)$ tenen coeficients enters, $q(x)$ ja no té coeficients enters sinó racionals. És per això que és important en el teorema de la divisió entera que els polinomis tinguin coeficients en un cos.

Definició 1.37. Siguin $f(x), g(x) \in K[x]$. Diem que $g(x)$ divideix $f(x)$ si existeix $h(x) \in K[x]$ tal que $f(x) = g(x)h(x)$. Utilitzem la notació $g(x) \mid f(x)$.

Tot seguit definim els polinomis irreductibles, que juguen un paper anàleg a $K[x]$ al dels nombres primers a $\mathbb{Z}$.

Definició 1.38. Diem que un polinomi $f(x) \in K[x]$, $f(x) \neq 0$, és irreductible si no existeix cap factorització de la forma $f(x) = g(x)h(h)$ amb $g(x)$ i $h(x)$ polinomis no constants (és a dir, de grau ≥ 1).

Teorema 1.39. *Siguin $f(x), g(x) \in K[x]$. Existeix un polinomi $h(x) \in K[x]$ tal que $h(x) \mid f(x)$, $h(x) \mid g(x)$, i tal que és combinació de $f(x)$ i $g(x)$; és a dir, és tal que*

$$h(x) = f(x)F(x) + g(x)G(x) \quad \textit{per a certs} \quad F(x), G(x) \in K[x].$$

Demostració. Considerem el conjunt de tots els polinomis que són combinació de $f(x)$ i $g(x)$:

$$A = \{f(x)F_0(x) + g(x)G_0(x) \mid F_0(x), G_0(x) \in K[x]\}.$$

Sigui $h(x)$ un polinomi de A de grau mínim d'entre els polinomis que són diferents de 0. Per construcció $h(x) = f(x)F(x) + g(x)G(x)$ per a certs polinomis $F(x), G(x)$, així que només cal veure que divideix $f(x)$ i $g(x)$. Veiem que divideix $f(x)$, i el raonament per a $g(x)$ és totalment anàleg. Raonem per contradicció, i suposem que $h(x) \nmid f(x)$. Aleshores quan fem la divisió entera

$$f(x) = g(x)q(x) + r(x)$$

obtenim un residu $r(x) \neq 0$ i tal que $\text{grau}(r(x)) < \text{grau}(g(x))$. Però com que

$$\begin{aligned} r(x) =& f(x) - g(x)q(x) = f(x) - (f(x)F(x) + g(x)G(x))\, q(x) \\ =& f(x)\,(1 - F(x)q(x)) + g(x)\,(-G(x)q(x)) \end{aligned}$$

veiem que $r(x)$ pertany a A i té grau menor que $h(x)$; això és una contradicció amb l'elecció de $h(x)$ com un element de grau mínim de A. □

Teorema 1.40. *Siguin $f(x), g(x) \in K[x]$ dos polinomis diferents de 0. Existeix un únic polinomi $d(x) \in K[x]$ satisfent les propietats següents:*

(1) $d(x)$ és mònic (i.e., el seu coeficient de grau màxim és 1);
(2) $d(x) \mid f(x)$ i $d(x) \mid g(x)$;
(3) $d(x) = f(x)F(x) + g(x)G(x)$ per a certs $F(x), G(x) \in K[x]$;
(4) qualsevol polinomi $m(x)$ tal que $m(x) \mid f(x)$ i $m(x) \mid g(x)$ compleix que $m(x) \mid d(x)$.

Demostració. Considerem un polinomi $h(x) = h_n x^n + h_{n-1}x^{n-1} + \dots h_1 x + h_0$ proporcionat pel Teorema 1.39 i definim $d(x) = \frac{1}{h_0}h(x)$. Per construcció és mònic, i de les propietats de $h(x)$ se'n dedueix que compleix les propietats (2) i (3). La propietat (4) es dedueix immediatament de (3).

Només ens resta veure la unicitat de $d(x)$. Suposem que $e(x)$ és un altre polinomi satisfent les quatre propietats de l'enunciat. Que $e(x)$ satisfaci la propietat (3) vol dir que $e(x) \mid f(x)$ i $e(x) \mid g(x)$; per la propietat (4) satisfeta per $d(x)$ veiem que $d(x) \mid e(x)$. Intercanviant els papers de $e(x)$ i $d(x)$ en l'argument anterior, veiem que també $e(x) \mid d(x)$. Per tant

$$e(x) = q_1(x)d(x) = q_1(x)q_2(x)e(x)$$

amb la qual cosa $q_1(x)q_2(x) = 1$ i per tant $q_1(x)$ i $q_2(x)$ són polinomis de grau 0, és a dir, elements de K. De la igualtat $e(x) = q_1(x)d(x)$ i del fet que $e(x)$ i $d(x)$ són mònics en deduïm que $q_1(x) = 1$ i per tant $e(x) = d(x)$. □

Definició 1.41. Del polinomi $d(x)$ del Teorema 1.40 se'n diu el màxim comú divisor de $f(x)$ i $g(x)$. Utilitzem també la notació $\mathrm{mcd}(f(x), g(x))$ o simplement $(f(x), g(x))$ si no hi ha perill de confusió.

El resultat següent és un anàleg del Lema d'Euclides.

Proposició 1.42. *Sigui $p(x) \in K[x]$ un polinomi irreductible. Si $p(x)$ divideix un producte de polinomis $f(x)g(x)$, aleshores $p(x) \mid f(x)$ o bé $p(x) \mid g(x)$.*

Demostració. Si $p(x) \nmid f(x)$ aleshores $\mathrm{mcd}(f(x), p(x)) = 1$, pel fet de ser $p(x)$ irreductible. Per tant, existeixen polinomis $P(x)$ i $F(x)$ tals que

$$1 = p(x)P(x) + f(x)F(x).$$

Multiplicant aquesta igualtat per $g(x)$ veiem que

$$g(x) = p(x)g(x)P(x) + f(x)g(x)F(x).$$

Com que $p(x)$ divideix els dos sumands de la part de la dreta de la igualtat, també divideix $g(x)$. □

Teorema 1.43. *Sigui $f(x) \in K[x]$ un polinomi de grau ≥ 1. Aleshores $f(x)$ es pot factoritzar com*

$$f(x) = cp_1(x)p_2(x)\dots p_k(x), \tag{1.16}$$

on $c \in K$ i els polinomis p_i són mònics i irreductibles. A més, aquesta factorització és única llevat de l'ordre dels factors.

Demostració. La demostració és anàloga a la demostració del Teorema Fonamental de l'Aritmètica. En primer lloc, l'existència de la factorització és senzilla: si $f(x)$ és irreductible ja hem acabat; si no ho és, es pot factoritzar com $f(x) = f_1(x)f_2(x)$ on $f_1(x)$ i $f_2(x)$ tenen grau més petit que $f(x)$; repetim el raonament per a cada factor $f_i(x)$: si $f_i(x)$ és irreductible ja estem, i si no ho és el factoritzem com a producte de factors de grau més petit. Aquest procés clarament acaba perquè en cada pas el grau dels factors disminueix, i el grau no pot ser negatiu. Això proporciona una descomposició de $f(x)$ en producte d'irreductibles, i ajustant la constant c podem fer-los mònics.

Per a veure la unicitat, suposem que tenim dues factoritzacions de f de forma que

$$cp_1(x)p_2(x)\dots p_k(x) = dq_1(x)q_2(x)\dots q_s(x) \tag{1.17}$$

on $d \in K$ i els $q_i(x)$ són mònics i irreductibles. D'aquesta igualtat veiem que $p_1(x) \mid q_1(x)q_2(x)\dots q_s(x)$ i per la proposició 1.42 veiem que divideix un dels factors que podem suposar (reordenant-los si cal) que és $q_1(x)$. Com que $q_1(x)$ és irreductible i mònic, això implica que $p_1(x) = q_1(x)$ i per tant els podem cancel·lar $p_1(x)$ i $q_1(x)$ a (1.17). Repetint l'argument arribem a què necessàriament $k = s$, $p_i = q_i$ per a tot $i = 1, \dots, k$, i finalment $c = d$. □

1.8. **Arrels de polinomis amb coeficients en un cos.** Sigui K un cos i $f(x)$ un polinomi amb coeficients a K

Definició 1.44. Diem que $\alpha \in K$ és una arrel de f si $f(\alpha) = 0$.

Exemple 1.45. Sigui $g(x) = x^2 + x + 1 \in \mathbb{Q}[x]$; aleshores $g(-1) = 0$ i per tant -1 és arrel de $g(x)$.

Proposició 1.46. *El residu de la divisió entera entre $f(x)$ i $x - \alpha$ és $f(\alpha)$.*

Demostració. Si dividim $f(x)$ pel polinomi $x - \alpha$, que és de grau 1, obtenim:

$$f(x) = q(x)(x - \alpha) + r(x)$$

on $r(x) = 0$ o bé $r(x)$ té grau 0. En qualsevol cas, $r(x)$ és un element de K. Podem denotar-lo simplement com r, de manera que

$$f(x) = q(x)(x - \alpha) + r$$

amb $r \in K$. Avaluant en $x = \alpha$ veiem que

$$f(\alpha) = q(\alpha)(\alpha - \alpha) + r$$

d'on $r = f(\alpha)$ com volíem veure. □

Corol·lari 1.47. *α és arrel de $f(x)$ si i només si $x - \alpha$ divideix $f(x)$.*

Demostració. Immediata. □

Definició 1.48. Si α és arrel de $f(x)$, la multiplicitat de α és la màxima potència de $x - \alpha$ que divideix $f(x)$.

Exemple 1.49. Sigui $g(x) = x^2 + 2x + 1$. Clarament $g(-1) = 0$ i per tant -1 és arrel de $g(x)$. En particular, $(x + 1) \mid g(x)$. Com que $(x + 1)^2 \mid g(x)$ però $(x + 1)^3 \nmid g(x)$, veiem que -1 és una arrel de $g(x)$ de multiplicitat 2.

Proposició 1.50. *Si $f(x) \in K[x]$ té grau $n \geq 1$ aleshores $f(x)$ té com a molt n arrels (comptades amb multiplicitat).*

Demostració. Farem inducció en el grau n. El cas $n = 1$ és evident; suposem doncs cert l'enunciat cert per a polinomis de grau $n - 1 \geq 1$ i veiem que també és cert per a polinomis de grau n.

Sigui α una arrel de $f(x)$. Aleshores podem escriure $f(x) = (x-\alpha)g(x)$ per a cert polinomi $g(x)$ de grau $n - 1$. Sigui β una arrel de $f(x)$. Aleshores

$$0 = f(\beta) = (\beta - \alpha)g(\beta).$$

En un cos, si el producte de dos elements és igual a 0 aleshores almenys un dels dos és 0; per tant, $\beta = \alpha$ o β és una arrel de $g(x)$. És a dir, hem vist que

$$\{\text{arrels de } f(x)\} = \{\beta\} \cup \{\text{arrels de } g(x)\}.$$

Com que $g(x)$ té grau $n-1$, sabem per hipòtesi d'inducció que té com a molt $n-1$ arrels comptades amb multiplicitat, d'on veiem que $f(x)$ té com a molt n arrels comptades amb multiplicitat. □

Observació 1.51. Aquest resultat no és cert si K no és un domini d'integritat[6].

[6]Per exemple, a $\mathbb{Z}/4\mathbb{Z}$ el polinomi $f(x) = 2x^2 + 2x$ té quatre arrels

2. Congruències

Suposem que volem trobar les solucions enteres de l'equació

$$x^2 + x = 2y^2 + 1.$$

Resulta que no en té cap: no existeixen enters x, y satisfent aquesta relació. En efecte, tant si x és parell com si és senar, tenim que $x^2 + x$ serà parell, mentre que $2y^2 + 1$ sempre és senar.

Aquest exemple senzill il·lustra que és útil classificar els nombres enters en parells i senars. Però això té les seves limitacions, per exemple el mateix raonament no funciona per a l'equació

$$3x^3 = y^2 + 1.$$

En aquest capítol veurem una generalització dels conceptes parell i senar. Una manera de pensar en aquestes nocions és que els nombres parells són els múltiples de 2, mentre que els senars són els nombres que no són múltiples de 2. Però ho podem pensar també de manera equivalent de la manera següent: els nombres parells són aquells que quan els dividim per 2 deixen residu 0, i els senars són els que deixen residu 1. És a dir, classifiquem els enters segons el residu que deixen quan els dividim per 2. La idea que hi ha darrera el concepte de congruència és generalitzar aquest fet i classificar els enters segons el residu que deixen quan els dividim per un nombre $n \geq 2$.

2.1. Definició i primeres propietats.

Definició 2.1. Sigui n un enter positiu. Donats $a, b \in \mathbb{Z}$ diem que a és congruent amb b mòdul n si $n \mid a - b$. També es diu que a i b són congruents mòdul n o que a és un residu de b mòdul n. La notació és $a \equiv b \pmod{n}$.

Exemple 2.2. $4 \equiv 6 \pmod{2}$, $7 \equiv 13 \pmod{}$, $17 \equiv 5 \pmod{6}$, $-11 \equiv 1 \pmod{4}$.

Exemple 2.3. $-11 \not\equiv 2 \pmod{7}$ (aquesta és la notació per a indicar que -11 i 2 no són congruents mòdul 7).

La proposició següent, la demostració de la qual és immediata a partir de les definicions, ens diu que ser congruent mòdul n és una relació d'equivalència.

Proposició 2.4. *Si $a, b, c, d \in \mathbb{Z}$ i $n \in \mathbb{Z}_{>0}$ aleshores:*

(1) $a \equiv b \pmod{n}$ si i només si $b \equiv a \pmod{n}$;
(2) $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n}$ implica $a \equiv c \pmod{n}$;
(3) $a \equiv a \pmod{n}$.

Proposició 2.5. *Si $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$ aleshores:*

(1) Si $a + c \equiv b + d \pmod{n}$ i $a - c \equiv b - d \pmod{n}$;
(2) $ac \equiv bd \pmod{n}$.

Demostració. (1) Com que $n \mid a-b$ i $n \mid c-d$, clarament $n \mid a-b+c-d$; és a dir, $n \mid a+c-(b+d)$ que és el mateix que dir que $a + c \equiv b + d \pmod{n}$. L'argument per a la resta és anàleg.

(2) Clarament $n \mid a - b$ implica que $n \mid ac - bc$; de la mateixa manera, $n \mid c - d$ implica que $n \mid bc - bd$. Per tant, $n \mid ac - bc + bc - bd$ d'on veiem que $n \mid ac - bd$.

□

Proposició 2.6. *(1) $ax \equiv ay \pmod{n} \iff x \equiv y \pmod{\frac{n}{(a,n)}}$.*
(2) $ax \equiv ay \pmod{n}$ i $(a, n) = 1 \implies x \equiv y \pmod{n}$.
(3) $x \equiv y \pmod{n}$ i $x \equiv y \pmod{n} \iff x \equiv y \pmod{[m, n]}$.

Demostració. (1) [$\Longrightarrow$] Com que $n \mid a(x-y)$ tenim que $a(x-y) = nm$ per a algun $m \in \mathbb{Z}$; dividint per (a,n) veiem que

$$\frac{a}{(a,n)}(x-y) = \frac{n}{(a,n)}m.$$

Observem que les dues fraccions són nombres enters, ja que el denominador divideix el numerador. Aquesta identitat doncs ens diu que $\frac{n}{(a,n)} \mid (x-y)$ i per tant $x \equiv y \pmod{\frac{n}{(a,n)}}$.
[$\Longleftarrow$] $\frac{n}{(a,n)} \mid (x-y) \Longrightarrow \frac{an}{(a,n)} \mid a(x-y) \Longrightarrow \frac{n}{(a,n)} \mid (ax-ay)$.

(2) És un cas particular de (1).

(3) Surt de les propietats del mínim comú múltiple.

□

2.2. **Classes de residus mòdul n.** Al conjunt dels nombres enters hi podem posar la relació d'equivalència "ser congruent mòdul n". Podem considerar doncs el conjunt de les classes d'equivalència per aquesta relació, que s'anomena el conjunt de classes de congruència mòdul n (o també el conjunt de classes de residus mòdul n).

La notació que utilitzarem serà la següent: si a és un enter, denotarem per $a \pmod n$ la classe d'equivalència de a mòdul n. Així doncs, $a \pmod n \in \mathbb{Z}/n\mathbb{Z}$. Quan el mòdul n amb el que treballem estigui clar també utilitzarem la notació $\overline{a}$ per a denotar la classe de a mòdul n.

Observació 2.7. Tot enter a és congruent mòdul n a un (i només un) dels nombres $0, 1, 2, \ldots, n-1$. Per a trobar quin, cal dividir a per n:

$$a = qn + r \text{ amb } 0 \leq r \leq n-1.$$

Aleshores $a \equiv r \pmod n$.

Exemple 2.8. Tot nombre és congruen mòdul 3 a $0, 1$ o 2. Hi ha doncs, tres classes de congruència mòdul 3:

$$\begin{aligned}\bar{0} &= \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}\\ \bar{1} &= \{\ldots, -5, -2, 1, 4, 7, \ldots\}\\ \bar{2} &= \{\cdots -4, -1, 2, 5, 8, 11, \ldots\}.\end{aligned}$$

En general, hi ha n classes d'equivalència mòdul n. Denotem per[7] $\mathbb{Z}/n\mathbb{Z}$ el conjunt de classes de congruència mòdul n:

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots \overline{n-1}\}.$$

Definició 2.9. Diem que $x_1, x_2, \ldots, x_n$ és un sistema complet de residus mòdul n si per a tot enter y existeix un i només un x_j tal que $y \equiv x_j \pmod n$.

Exemple 2.10. $0, 1, 2, \ldots, n-1$ és un sistema complet de residus mòdul n. Però n'hi ha d'altres, només cal escollir un representant de cada classe.

Exemple 2.11. Fixem-nos que $0 \equiv 10 \pmod 5$, $1 \equiv 6 \pmod 5$, $2 \equiv -3 \pmod 5$, $3 \equiv 13 \pmod 5$ i $4 \equiv -6 \pmod 5$. Per tant, $10, 6, -3, 13, -6$ és un sistema complet de residus mòdul 5, de manera que podem escriure

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{10}, \overline{6}, \overline{-3}, \overline{13}, \overline{-6}\}.$$

[7] aquest conjunt es llegeix "$\mathbb{Z}$ mòdul $n\mathbb{Z}$"; en assignatures posteriors d'àlgebra es veurà el perquè d'aquesta notació que ara pot resultar una mica extranya

A $\mathbb{Z}/n\mathbb{Z}$ hi podem definir dues operacions (suma i producte):

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Com és habitual, a vegades no posarem el punt del producte. Aquestes operacions estan ben definides. És a dir, no depenen del representant de la classe que escollim. Això és el que hem demostrat a la Proposició 2.5. A més, és immediat comprovar que se satisfan les propietats següents:

(1) $\overline{0} + \overline{a} = \overline{a}$ per a tot $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$;
(2) $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$ per a tot $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$;
(3) $\overline{a} + \overline{-a} = \overline{0}$ per a tot $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$;
(4) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ per a tot $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$;
(5) $(\overline{a}\overline{b})\overline{c} = \overline{a}(\overline{b}\overline{c})$ per a tot $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$;
(6) $\overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b} + \overline{a}\overline{c}$ per a tot $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$;
(7) $\overline{a}\overline{b} = \overline{b}\overline{a}$ per a tot $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$
(8) $\overline{1}\overline{a} = \overline{a}$ per a tot $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$.

Dit d'una altra manera, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ és un anell commutatiu.

2.3. **Classes d'invertibles.**

Definició 2.12. Diem que a és invertible mòdul n si existeix $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{n}$. Aleshores diem que b és l'invers de a mòdul n, i el denotem per $a^{-1} \pmod{n}$.

Observació 2.13. Equivalentment, $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ és invertible si existeix $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$. D'ara en endavant farem servir indistintament la notació amb congruències (que denota que estem fent operacions amb representants) i la notació amb classes mòdul n, que denota que fem operacions a $\mathbb{Z}/n\mathbb{Z}$.

Exemple 2.14. $2 \cdot 3 \equiv 1 \pmod{5}$ i per tant 3 és l'invers de 2 mòdul 5.

Observació 2.15. No sempre existeixen inversos mòdul n. Per exemple, 3 no és invertible mòdul 6. En efecte, si existís a tal que $3a \equiv 1 \pmod{6}$ aleshores multiplicant per 2 als dos costats $2 \cdot 3 \cdot a \equiv 2 \pmod{6}$; però això ens diria que $0 \equiv 2 \pmod{6}$ cosa que no és certa.

Definició 2.16. Diem que $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{a} \neq \overline{0}$, és un divisor de zero si existeix $\overline{b} \neq \overline{0}$ tal que $\overline{a} \cdot \overline{b} = \overline{0}$.

Proposició 2.17. *(1) $a \in \mathbb{Z}$ és invertible mòdul n si i només si $(a, n) = 1$.*
(2) $\overline{a}$ és un divisor de zero a $\mathbb{Z}/n\mathbb{Z}$ si i només si $(a, n) > 1$.

Demostració. (1) [$\Longrightarrow$] Si $ab - 1 = kn$ per a algun $k \in \mathbb{Z}$ aleshores $ab - kn = 1$ i clarament $(a, n) = 1$.
[$\Longleftarrow$] Si $(a, n) = 1$ per Bézout existeixen $x, y \in \mathbb{Z}$ tals que $ax + ny = 1$. Aleshores, reduïnt mòdul n veiem que $ax \equiv 1 \pmod{n}$ i per tant $a^{-1} \equiv x \pmod{n}$.
(2) [$\Longrightarrow$] Si $ab = kn$ per a certs $b, k \in \mathbb{Z}$ amb $n \nmid b$, aleshores $(a, n) > 1$.
[$\Longleftarrow$] Sigui $d = (a, n)$ amb $d > 1$. Aleshores $a\frac{n}{d} \equiv 0 \pmod{n}$ i $\frac{n}{d} \not\equiv 0 \pmod{n}$.

□

Observació 2.18. De la demostració de la proposició anterior veiem que podem inversos mòdul n amb l'algoritme d'Euclides estès. Si $(a, n) = 1$ aleshores amb aquest algoritme podem trobar

$x, y \in \mathbb{Z}$ tals que

$$ax + ny = 1,$$

de manera que $a^{-1} \equiv x \pmod{n}$.

2.4. **El teorema xinès del residu.**

Teorema 2.19. *Siguin $n_1, n_2, \ldots, n_r$ enters positius relativament primers dos a dos (i.e., $\mathrm{mcd}(n_i, n_j) = 1$ per $i \neq j$). Siguin també $a_1, a_2, \ldots, a_r$ nombres enters. Aleshores les congruències*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

tenen solucions comunes. Si x_0 és una solució, aleshores totes les solucions són de la forma

$$x = x_0 + kn_1n_2 \ldots n_r$$

amb $k \in \mathbb{Z}$ qualsevol. En particular, la solució és única mòdul $n = n_1n_2 \ldots n_r$.

Demostració. Per a cada $i \in 1, 2, \ldots, r$ tenim que $\frac{n}{n_i}$ és enter; a més, com que els mòduls són primers dos a dos tenim que $(\frac{n}{n_i}, n_i) = 1$. Sigui b_i l'invers de $\frac{n}{n_i}$ mòdul n_i. Per definició d'invers, tenim que $\frac{n}{n_i}b_i \equiv 1 \pmod{n_i}$, mentre que clarament $\frac{n}{n_i}b_i \equiv 0 \pmod{n_j}$ per a tot $j \neq i$. Així doncs, l'enter

$$x_0 = \sum_{k=0}^{r} \frac{n}{n_k} b_k a_k$$

satisfà que $x_0 \equiv a_i \pmod{n_i}$ per a tot i i és una solució del sistema. Qualsevol nombre de la forma $x_0 + kn$ amb $k \in \mathbb{Z}$ també és solució. Finalment, si x es una altra solució del sistema, tenim que $x \equiv x_0 \pmod{n_i}$ per a tot i; és a dir, tenim que $n_i \mid x - x_0$ per a tot i amb la qual cosa $\mathrm{mcm}(n_1, n_2, \ldots, n_r) \mid x - x_0$. Com que els n_i són coprimers dos a dos tenim que $\mathrm{mcm}(n_1, n_2, \ldots, n_r) = n$ i $x = x_0 + kn$ per algun $k \in \mathbb{Z}$. □

Exemple 2.20. El sistema

$$\begin{aligned} x &\equiv 3 \pmod{5} \\ x &\equiv 4 \pmod{11} \\ x &\equiv 7 \pmod{8} \end{aligned}$$

té solució ja que els mòduls son primers dos a dos. Aplicant el mètode descrit a la demostració podem trobar una solució:

$$\begin{aligned} b_1 &\equiv (11 \cdot 8)^{-1} \equiv 2 \pmod{5} \\ b_2 &\equiv (5 \cdot 8)^{-1} \equiv 8 \pmod{11} \\ b_3 &\equiv (5 \cdot 11)^{-1} \equiv 7 \pmod{8} \end{aligned}$$

i per tant $x_0 = 11 \cdot 8 \cdot 2 \cdot 3 + 5 \cdot 8 \cdot 8 \cdot 4 + 5 \cdot 11 \cdot 7 \cdot 7 = 4503$. Com que $4503 \equiv 103 \pmod{440}$ podem escriure la solució general com

$$x = 103 + 440k \text{ amb } k \in \mathbb{Z},$$

o també $x \equiv 103 \pmod{440}$.

Observació 2.21. Si els mòduls no són coprimers el sistema pot no tenir solució. Per exemple el sistema

$$\begin{aligned} x &\equiv 3 \pmod 6 \\ x &\equiv 2 \pmod 4 \end{aligned}$$

no té solució. La primera equació implica que $x \equiv 1 \pmod 2$, i la segona implica que $x \equiv 0 \pmod 2$ amb la qual cosa no pot haver-hi cap x satisfent les dues alhora.

Observació 2.22. Si els mòduls no són coprimers, el sistema pot tenir solució. Per exemple considerem el sistema:

$$\begin{aligned} x &\equiv 3 \pmod{10} \\ x &\equiv 8 \pmod{15}. \end{aligned}$$

La primera equació és equivalent a les dues equacions següents:

$$x \equiv 3 \pmod 2 \tag{2.1}$$

$$x \equiv 3 \pmod 5, \tag{2.2}$$

mentre que la segona equació és equivalent a:

$$x \equiv 8 \pmod 3 \tag{2.3}$$

$$x \equiv 8 \pmod 5. \tag{2.4}$$

Fixem-nos que (2.2) i (2.4) en realitat són la mateixa equació. Així doncs, el sistema original és equivalent al sistema:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 3, \end{aligned}$$

que té solució perquè els mòduls són primers dos a dos.

2.5. **El grup dels invertibles mòdul n.** Recordem que als enters hi hem definit la relació d'equivalènica $a \equiv b \pmod n$, i que denotem per $\mathbb{Z}/n\mathbb{Z}$ el conjunt de les classes d'equivalència:

$$\mathbb{Z}/n\mathbb{Z} = \{\text{classes d'equivalència} \pmod n\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Hi hem definit dues operacions, suma i producte:

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

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

i hem vist que estan ben definides (no depenen dels representants escollits) i que amb aquestes operacions $\mathbb{Z}/n\mathbb{Z}$ té estructura d'anell. També hem vist que un element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ és invertible pel producte si i només si $\mathrm{mcd}(a, n) = 1$. Recordem la definició d'invertible pel producte:

- $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ és invertible pel producte si existeix $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$
- equivalentment, $a \in \mathbb{Z}$ és invertible mòdul n si existeix $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{n}$.

Definició 2.23. Denotem per $(\mathbb{Z}/n\mathbb{Z})^*$ el conjunt de les classes invertibles mòdul n. És a dir:

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \colon \overline{a} \text{ és invertible}\} = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \colon \operatorname{mcd}(a,n) = 1\}.$$

Proposició 2.24. *$(\mathbb{Z}/n\mathbb{Z})^*$ és un grup amb el producte. S'anomena el grup dels invertibles mòdul n.*

Demostració. L'existència d'element neutre i de l'associativitat del producte ja l'havíem vista. Tot element té invers pel producte per definició de $\mathbb{Z}/n\mathbb{Z}$. □

Exemple 2.25. $(\mathbb{Z}/5\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, $(\mathbb{Z}/6\mathbb{Z})^* = \{\overline{1}, \overline{5}\}$, $(\mathbb{Z}/8\mathbb{Z})^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

Tot seguit definim l'anomenada funció fi d'Euler. És una funció $\phi \colon \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$.

Definició 2.26. Donat $n \in \mathbb{Z}_{>0}$ denotem per $\phi(n)$ el nombre d'enters k amb $0 \leq k \leq n-1$ tals que $\operatorname{mcd}(k,n) = 1$.

Exemple 2.27. $\phi(1) = 1$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(8) = 4$.

Observació 2.28. Sovint també s'utilitza la grafia alternativa de la lletra fi per a denotar aquesta funció: $\varphi(n)$. Les dues notacions es troben indistintament a la literatura.

Observació 2.29. Fixem-nos que per a $n > 1$ tenim que $\phi(n) = \#\,(\mathbb{Z}/n\mathbb{Z})^*$.

L'objectiu d'aquesta secció és trobar una fórmula per a $\phi(n)$. El primer pas és establir la fórmula en el cas que n sigui primer.

Lema 2.30. *Si p és primer aleshores $\phi(p) = p - 1$.*

Demostració. En efecte, dels p enters $0, 1, 2, \ldots, p-1$ només el 0 satisfà que el seu màxim comú divisor amb p és > 1. □

En particular, la proposició anterior ens diu que tot element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ diferent de 0 és invertible. Un anell on tot element $\neq 0$ és invertible pel producte s'anomena cos. Anotem aquest fet en forma de proposició, ja que ens serà útil més endavant.

Proposició 2.31. *Si p és primer $\mathbb{Z}/p\mathbb{Z}$ és un cos.*

Observació 2.32. Fixem-nos que $\mathbb{Z}/p\mathbb{Z}$ és un cos amb p elements; és doncs un cos finit, en contraposició amb els altre cossos $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ que tenen infinits elements. No ho veurem aquí, però es pot demostrar que per a tot primer p i per a tot $r \geq 1$ hi ha cossos finits de cardinal p^r, i recíprocament que tot cos finit té cardinal potència de primer.

Observació 2.33. Si n no és primer aleshores $\mathbb{Z}/n\mathbb{Z}$ no és un cos.

Lema 2.34. *Si p és primer i $r \geq 1$ aleshores $\phi(p^r) = p^{r-1}(p-1)$.*

Demostració. Fixem-nos que $(a, p^r) > 1$ si i només si $p \mid a$. Per tant, dels p^r enters entre 0 i $p^r - 1$ els que no tindran màxim comú divisor amb p^r igual a 1 seran els múltiples de p entre 0 i p^r, que són:

$$0, p, 2p, 3p, 4p, \ldots, (p^{r-1} - 1)p;$$

veiem que n'hi ha p^{r-1} de manera que $\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$. □

Proposició 2.35. *La funció ϕ d'Euler és multiplicativa. És a dir, si $(m,n)=1$ aleshores $\phi(mn)=\phi(m)\phi(n)$.*

Demostració. Definim l'aplicació

$$\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ a \pmod{mn} & \longmapsto & a \pmod{m} \end{array}$$

que envia la classe d'un enter a mòdul mn a la classe de a mòdul m. Fixem-nos que està ben definida ja que si $a\equiv b \pmod{mn}$ aleshores $a\equiv b \pmod{m}$. Fixem-nos també que si $(a,mn)=1$ aleshores $(a,m)=1$. Per tant, podem l'aplicació anterior restringeix a una aplicació en les classes d'invertibles:

$$\begin{array}{ccc} (\mathbb{Z}/mn\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^* \\ a \pmod{mn} & \longmapsto & a \pmod{m}. \end{array}$$

De la mateixa manera, també podem definir una aplicació

$$\begin{array}{ccc} (\mathbb{Z}/mn\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^* \\ a \pmod{mn} & \longmapsto & a \pmod{n}. \end{array}$$

De fet, podem ajuntar les dues aplicacions en una de sola, que anomenarem α:

$$\begin{array}{rccc} \alpha\colon & (\mathbb{Z}/mn\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^*\times(\mathbb{Z}/n\mathbb{Z})^* \\ & a \pmod{mn} & \longmapsto & (a \pmod{m}, a \pmod{n}). \end{array}$$

Si veiem que α és bijectiva ja haurem acabat, perquè aleshores comparant cardinials del conjunt d'arribada i de sortida tindrem que

$$\phi(mn)=\#\left(\mathbb{Z}/mn\mathbb{Z}\right)^*=\left(\#\left(\mathbb{Z}/m\mathbb{Z}\right)^*\right)\cdot\left(\#\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right)=\phi(m)\phi(n).$$

Veiem doncs que α és bijectiva:

- α és injectiva: Si $\alpha(a \pmod{mn})=\alpha(b \pmod{mn})$ aleshores $a\equiv b \pmod{m}$ i $a\equiv b \pmod{n}$. Per tant, $a\equiv b \pmod{[m,n]}$. Com que $(m,n)=1$, $[m,n]=mn$ i veiem que $a\equiv b \pmod{mn}$.
- α és exhaustiva: donats $c,d\in\mathbb{Z}$ tals que $(c,m)=1$ i $(d,n)=1$ pel teorema xinès del residu existeix $a\in\mathbb{Z}$ tal que

  $$\begin{aligned} a &\equiv c \pmod{m} \\ a &\equiv d \pmod{n}. \end{aligned}$$

  Observem que $(a,mn)=1$ ja que $(a,m)=(c,m)=1$ i $(a,n)=(d,n)=1$. Així doncs, a és invertible mòdul mn i $\alpha(a \pmod{mn})=(c \pmod{m}, d \pmod{n})$.

□

Observació 2.36. De fet, l'aplicació α de la demostració és el que s'anomena un homomorfisme de grups, però això no ho utilitzarem.

Proposició 2.37. *Si $n=p_1^{r_1}p_2^{r_2}\dots p_s^{r_s}$ amb els p_i primers diferents i els exponents $r_i\geq 1$, aleshores*

$$\phi(n)=(p_1-1)p_1^{r_1-1}(p_2-1)p_2^{r_2-1}\dots(p_s-1)p_s^{r_s-1}.$$

Demostració.

$$\begin{aligned} \phi(n) =& \phi(p_1^{r_1}p_2^{r_2}\dots p_s^{r_s}) \overset{\text{Lema 2.34}}{=} \phi(p_1^{r_1})\cdot\phi(p_2^{r_2})\dots\phi(p_s^{r_s}) \overset{\text{Prop 2.35}}{=} \\ =& (p_1-1)p_1^{r_1-1}(p_2-1)p_2^{r_2-1}\dots(p_s-1)p_s^{r_s-1}. \end{aligned}$$

□

Observació 2.38. La proposició anterior ens dóna la fórmula que buscàvem per a calcular $\phi(n)$. Aquesta fórmula és molt útil en molts aspectes, però remarquem que si n és un enter gran (per exemple un enter d'uns quants centenars de xifres) serà en general difícil calcular $\phi(n)$ amb aquesta fórmula, ja que per a aplicar-la cal conèixer una factorització de n i ja hem comentat que els nombres grans són computacionalment molt difícils de factoritzar. La dificultat de calcular $\phi(n)$ si no es coneix una factorització de n és la base del criptosistema RSA que veurem més endavant.

2.6. **Teorema d'Euler i Teorema Petit de Fermat.**

Teorema 2.39 (Euler)**.** *Si* $(a,n)=1$ *aleshores* $a^{\phi(n)} \equiv 1 \pmod{n}$.

Demostració. Siguin $r_1, r_2, \ldots, r_{\phi(n)} \in \mathbb{Z}$ representants de les classes invertibles mòdul n; és a dir, tals que

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{r}_1, \overline{r}_2, \ldots, \overline{r}_{\phi(n)}\}.$$

Considerem ara les classes $\overline{a}\cdot\overline{r}_1, \overline{a}\cdot\overline{r}_2, \ldots, \overline{a}\cdot\overline{r}_{\phi(n)}$. Fixem-nos que:

- Són totes diferents: si $\overline{a}\cdot\overline{r}_i = \overline{a}\cdot\overline{r}_j$, com que $\overline{a}$ és invertible podem cancel·lar-lo multiplicant per $\overline{a}^{-1}$ a cada costat de la igualtat i obtenim que $r_i = r_j$.
- Són totes inveribles, ja que el producte de dues classes invertibles és també invertible (per què?).

En resum, les classes $\overline{a}\cdot\overline{r}_1, \overline{a}\cdot\overline{r}_2, \ldots, \overline{a}\cdot\overline{r}_{\phi(n)}$ són $\phi(n)$ elements diferents de $(\mathbb{Z}/n\mathbb{Z})^*$; com que aquest conjunt té $\phi(n)$ elements, ha de ser

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a}\cdot\overline{r}_1, \overline{a}\cdot\overline{r}_2, \ldots, \overline{a}\cdot\overline{r}_{\phi(n)}\}.$$

Per tant

$$\prod_{i=1}^{\phi(n)} \overline{r_i} = \prod_{i=1}^{\phi(n)} \overline{a}\cdot\overline{r_i} = \overline{a}^{\phi(n)} \prod_{i=1}^{\phi(n)} \overline{r_i}.$$

Com que $\prod_{i=1}^{\phi(n)} \overline{r_i}$ és invertible (novament utilitzem que el producte d'invertibles és invertible) podem cancel·lar aquest terme i veiem que

$$\overline{a}^{\phi(n)} = \overline{1}.$$

Aquesta darrera igualtat és equivalent a què $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Un cas particular d'aquest resultat és el que es coneix amb el nom de Teorema Petit de Fermat.

Teorema 2.40 (Teorema Petit de Fermat)**.** *Si* p *és primer i* $p \nmid a$ *aleshores* $a^{p-1} \equiv 1 \pmod{p}$.

Observació 2.41. A vegades també es té en compte en el Teorema Petit de Fermat el cas en què $p \mid a$. L'enunciat general que inclou els dos casos és que per a tot a enter es té que $a^p \equiv a \pmod{p}$. Aquesta congruència és trivial quan $p \mid a$, mentre que quan $p \nmid a$ és equivalent al Teorema 2.40 ja que llavors a és invertible mòdul p.

Aquests resultats són útils, entre moltes altres coses, per a calcular potències de la forma $a^m \pmod{n}$ per a exponents m grans. En efecte, podem dividir m per $\phi(n)$:

$$m = q\phi(n) + r$$

i aleshores

$$a^m \equiv a^{q\phi(n)+r} \equiv \left(a^{\phi(n)}\right)^q \cdot a^r \equiv a^r \pmod{n}.$$

Exemple 2.42. Si volem calcular $3^{2415} \pmod 5$. Com que $\phi(5) = 4$ calculem que $2415 \equiv 3 \pmod 4$ i per tant

$$3^{2415} \equiv 3^3 \equiv 2 \pmod 5.$$

2.7. **Ordre i arrels primitives.**

Definició 2.43. Sigui a un enter amb $(a, n) = 1$. L'ordre de a mòdul n és l'enter positiu h més petit tal que $a^h \equiv 1 \pmod n$. Equivalentment, l'ordre de a mòdul n és h si

$$\overline{a}^h = \overline{1} \text{ a } \mathbb{Z}/n\mathbb{Z} \text{ i } \overline{a}^h \neq \overline{1} \text{ per a tot } h' \text{ amb } 0 < h' < h.$$

Observació 2.44. Pel Teorema d'Euler $a^{\phi(n)} \equiv 1 \pmod n$, o sigui que l'ordre de a mòdul n sempre és $\leq \phi(n)$.

Exemple 2.45.
- 5 té ordre 2 mòdul 8. En efecte, $5^1 \not\equiv 1 \pmod 8$, $5^2 \equiv 1 \pmod 8$.
- 3 té ordre 6 mòdul 7, ja que $3^1 \equiv 3 \pmod 7$, $3^2 \equiv 2 \pmod 7$, $3^3 \equiv 6 \pmod 7$, $3^4 \equiv 4 \pmod 7$, $3^5 \equiv 5 \pmod 7$, $3^6 \equiv 1 \pmod 7$.

Proposició 2.46. *L'ordre de a mòdul n divideix $\phi(n)$.*

Demostració. Denotem per h l'ordre de a mòdul n. Suposem que $h \nmid \phi(n)$ i veiem que arribem a una contradicció. Dividim $\phi(n)$ per h:

$$\phi(n) = qh + r \text{ amb } 0 < r < h \text{ (ja que } h \nmid \phi(n)).$$

Aleshores sabem que $a^h \equiv 1 \pmod n$ i que $a^{\phi(n)} \equiv 1 \pmod n$. Per tant:

$$1 \equiv a^{\phi(n)} \equiv a^{hq+r} \equiv \left(a^h\right)^q \cdot a^r \equiv a^r \pmod n.$$

Però per definició de ordre no pot existir cap $0 < r < h$ tal que $a^r \equiv 1 \pmod n$, i això és una contradicció. □

De fet, exactament la mateixa demostració dóna el resultat següent.

Proposició 2.47. *Si $a \in (\mathbb{Z}/n\mathbb{Z})^*$ és tal que $a^r = 1$ aleshores l'ordre de a divideix r.*

Definició 2.48. Diem que $a \in \mathbb{Z}$ amb $(a, n) = 1$ és una arrel primitiva mòdul n si el seu ordre mòdul n és $\phi(n)$.

Fixem-nos que si a és una arrel primitiva mòdul n aleshores

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a^0, a, a^2, \ldots, a^{\phi(n)-1}\}.$$

En efecte, només cal veure que els elements del conjunt de la dreta són tots diferents. Això és perquè si $a^x = a^y$ amb $0 \leq x, y \leq \phi(n) - 1$ aleshores (suposant que $x \geq y$) tenim que $a^{x-y} = 1$ amb $0 \leq x - y \leq \phi(n) - 1$ i com que l'ordre de a és $\phi(n)$ necessàriament ha de ser $x - y = 0$.

Exemple 2.49.
- Com que 3 és una arrel primitiva mòdul 5, tenim que $(\mathbb{Z}/5\mathbb{Z})^* = \{\overline{1}, \overline{3}, \overline{3}^2, \overline{3}^3\}$.
- Tot element a $(\mathbb{Z}/8\mathbb{Z})^*$ té ordre 1 o 2, i $\phi(8) = 4$. Així doncs no hi ha arrels primitives mòdul 8.

Fixem-nos doncs que no és cert que per a tot n existeixin arrels primitives mòdul n. El resultat següent ens diu que això és cert si el mòdul és primer.

Proposició 2.50. *Si p és primer aleshores hi ha arrels primitives mòdul p.*

Per a demostrar aquest resultat necessitarem un parell de lemes.

Lema 2.51. *Sigui p un primer i d un divisor de $p-1$. Aleshores el polinomi $x^d-1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ té d arrels a $\mathbb{Z}/p\mathbb{Z}$.*

Demostració. Posem $p-1 = d\cdot e$. Tenim la factorització

$$x^{p-1}-1 = (x^d-1)((x^d)^{e-1}+(x^d)^{e-2}+\cdots+x^d+1) = (x^d-1)g(x).$$

El teorema petit de Fermat ens diu que tot $b \in (\mathbb{Z}/p\mathbb{Z})^*$ satisfà que $b^{p-1}=1$. És a dir, el polimomi $x^{p-1}-1$ té $p-1$ arrels a $\mathbb{Z}/p\mathbb{Z}$. Ara bé, tota arrel de $x^{p-1}-1$ és arrel de x^d-1 o de $g(x)$, ja que $\mathbb{Z}/p\mathbb{Z}$ és un cos. Com que $g(x)$ té com a màxim $d(e-1) = p-1-d$ arrels, necessàriament x^d-1 té d arrels. □

Lema 2.52. *Si $a,b \in (\mathbb{Z}/p\mathbb{Z})^*$ tenen ordres r i s respectivament i $(r,s)=1$, aleshores ab té ordre rs.*

Demostració. Observem en primer lloc que

$$(ab)^{rs} = (a^r)^s\cdot(b^s)^r = 1;$$

per tant, l'ordre de ab divideix rs. Anomenem h l'ordre de ab, que podem escriure com $h=r_1s_1$ amb $r_1 \mid r$ i $s_1 \mid s$. Per definició d'ordre sabem que

$$a^{r_1s_1}b^{r_1s_1} = 1. \tag{2.5}$$

Elevant aquesta igualtat a $\frac{r}{r_1}$ tenim que

$$a^{rs_1}b^{rs_1} = b^{rs_1} = 1$$

d'on veiem que $s \mid rs_1$. Com que $(r,s)=1$ necessàriament ha de ser $s \mid s_1$ i per tant $s=s_1$. Elevant (2.5) a $\frac{s}{s_1}$ i repetint l'argument arribem a què $r=r_1$ amb la qual cosa $h=rs$. □

Demostració de la Proposició 2.50. El resultat és clarament cert si $p=2$, o sigui que podem suposar $p>2$. Factoritzem $p-1$ com

$$p-1 = q_1^{n_1}q_2^{n_2}\dots q_r^{n_r}$$

amb els q_i primers diferents i els $n_i>0$. Pel Lemma 2.51 sabem que

$$x^{q_i^{n_i}}-1 \text{ té } q_i^{n_i} \text{ arrels a } \mathbb{Z}/p\mathbb{Z};$$
$$x^{q_i^{n_i-1}}-1 \text{ té } q_i^{n_i-1} \text{ arrels a } \mathbb{Z}/p\mathbb{Z}.$$

Per tant, hi ha $q_i^{n_i}-q_i^{n_i-1}$ elements de $(\mathbb{Z}/p\mathbb{Z})^*$ tals que $b^{q_i^{n_i}}=1$ però $b_1^{q_i^{n_i-1}} \neq 1$. Aquests elements tenen ordre $q_i^{n_i}$.

Per a cada $i=1,\dots,r$ escollim $a_i \in \mathbb{Z}/p\mathbb{Z}$ un element d'ordre $q_i^{n_i}$, i posem

$$a = a_1\cdot a_2\dots a_r.$$

Pel Lemma 2.52 veiem que a té ordre $q_1^{n_1}\dots q_r^{n_r} = p-1$ i per tant és una arrel primitiva mòdul p. □

Hi ha un resultat de Gauss que dóna una caracterització completa de per a quins mòduls existeix alguna arrel primitiva.

Teorema 2.53 (Gauss)**.** *Existeix alguna arrel primitiva mòdul n si i només si $n = 1,2,4,p^\alpha$ o $2p^\alpha$ amb p un primer senar i $\alpha \geq 1$.*

Demostració. No la farem. □

Proposició 2.54. *Si existeix alguna arrel primitiva mòdul n aleshores hi ha $\phi(\phi(n))$ arrels primitives mòdul n.*

Demostració. Si hi ha alguna arrel primitiva, diguem-li a, aleshores tenim que

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a^0, a, a^2, \ldots, a^{\phi(n)-1}\}.$$

Tot seguit veurem que l'ordre de a^k és $\frac{\phi(n)}{(k,\phi(n))}$. En efecte, clarament

$$(a^k)^{\frac{\phi(n)}{(k,\phi(n))}} = (a^{\phi(n)})^{\frac{k}{(k,\phi(n))}} = 1$$

i per tant l'ordre de a^k divideix $\frac{\phi(n)}{(k,\phi(n))}$. Diguem-li h a l'ordre de a^k. Aleshores tenim que

$$(a^k)^h = 1$$

i per tant $\phi(n) \mid kh$ (ja que a té ordre $\phi(n)$). Per tant $\frac{\phi(n)}{(k,\phi(n))} \mid kh$ i d'aquí veiem que $\frac{\phi(n)}{(k,\phi(n))} \mid h$ que és el que ens faltava veure.

Així doncs, el nombre d'arrels primitives mòdul n és

$$\#\{a^k \colon 0 \leq k \leq \phi(n) - 1 \text{ i } \operatorname{ord}(a^k) = \phi(n)\} = \#\{a^k \colon 0 \leq k \leq \phi(n) - 1 \text{ i } (k, \phi(n)) = 1\} = \phi(n).$$

□

Conjectura 2.55 (Conjectura d'Artin)**.** *Sigui $a \in \mathbb{Z}$ tal que $a \neq -1$ i a no és un quadrat. Aleshores a és arrel primitiva mòdul p per a infinits primers p.*

Observació 2.56. El que afirma la conjectura no s'ha pogut demostrar fins ara ni tan sols per a un valor de a.

3. Nombres complexos

En aquesta secció introduirem el conjunt dels nombres complexos $\mathbb{C}$, que com veurem contenen de manera natural els nombres reals.

3.1. **Definicions bàsiques.** Per a justificar una mica la definició, comencem recordant els diferents tipus de nombres que coneixem fins ara, i que satisfan les inclusions

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Una manera com podem entendre el pas dels naturals als enters és per la necessitat de resoldre certes equacions. És a dir, hi ha equacions amb coeficients naturals com per exemple

$$x + 7 = 3$$

que no tenen cap solució natural. L'equació anterior és equivalent a $x + 4 = 0$ i per tant sí que té solució a $\mathbb{Z}$, $x = -4$. Ja estem molt familiaritzats amb el concepte de nombre enter negatiu i no ens presenta ja cap problema "conceptual". Però fixem-nos que -4, de fet, el podem pensar com un "símbol" que podem operar amb nombres naturals i que està caracteritzat per la propietat que $-4 + 4 = 0$. És a dir, tot el que necessitem saber de $x = -4$ és que és una solució de $x + 4 = 0$.

També, l'equació

$$3x - 5 = 0$$

té coeficients enters, però no té solució a $\mathbb{Z}$. Els racionals podem pensar que són el resultat d'afegir a $\mathbb{Z}$ totes les solucions d'equacions d'aquest estil. El nombre racional $5/3$ podem pensar-lo com un símbol que podem operar amb els enters, i l'únic que necessitem saber d'aquest símbol és que quan el multipliquem per 5 dóna 3 (és a dir, que és una solució de l'equació $3x - 5 = 0$).

Una construcció semblant ens porta a la definició dels nombres complexos a partir dels nombres reals. És a dir, els nombres complexos els obtindrem a partir dels reals afegint-hi la solució d'una equació que no té solucions a $\mathbb{R}$. Aquesta equació és

$$x^2 = -1.$$

Fixem-nos que no hi ha cap $x \in \mathbb{R}$ tal que $x^2 = -1$, ja que si $x \in \mathbb{R} \setminus \{0\}$ aleshores $x^2 > 0$. La solució és afegir als nombres reals un "símbol" que sigui solució d'aquesta equació. En matemàtiques[8] aquest símbol es denota habitualment amb la lletra i. Igual que en els casos anteriors, voldrem poder operar aquest símbol amb els nombres reals i voldrem considerar doncs expressions de la forma $a + bi$ amb a i b nombres reals.

Definició 3.1. Un nombre complex és un nombre de la forma $a + bi$ amb $a, b \in \mathbb{R}$, on $i^2 = -1$. Denotem per $\mathbb{C}$ el conjunt de nombres complexos.

Exemple 3.2. Exemples de nombres complexos són $1 + 3i$, $2.51 - 4.67544i$, $\pi + \frac{e}{2}i$, etc.

Observació 3.3. El nombre $a + 0i$ l'escrivim com a; fixem-nos que el podem identificar de manera natural amb el nombre real a, i això ens dóna la inclusió $\mathbb{R} \subset \mathbb{C}$. De manera semblant, el nombre $0 + bi$ normalment s'escriu com bi.

Definició 3.4. Si $z = a + bi \in \mathbb{C}$ aleshores

- a s'anomena la part real de z; farem servir la notació $\mathrm{Re}(z) = a$;
- b s'anomena la part imaginària de z; farem servir la notació $\mathrm{Im}(z) = b$;

[8]En contextos d'enginyeria elèctrica sovint s'utilitza la lletra j, ja que la i es reserva per a la intensitat

- el nombre complex $\bar{z} = a - bi$ s'anomena el complex conjugat (o simplement el conjugat) de z.

Observació 3.5. Fixem-nos que un nombre complex z és real si i només si $\mathrm{Im}(z) = 0$. També, z és real si i només si $z = \bar{z}$.

Podem sumar, restar i multiplicar nombres complexos fent servir les mateixes propietats que per als reals (associativa, commutativa, distributiva, etc.) i utilitzant que $i^2 = -1$. Per exemple

$$(2+3i) + (4+7i) = 2 + 4 + 3i + 7i = 2 + 4 + (3+7) = 6 + 10i;$$
$$(2+3i) \cdot (4+7i) = 3 \cdot 2 + 3 \cdot 4 + 2i + 4i^2 = 6 - 4 + 14i = 2 + 14i.$$

És a dir, si $z_1 = a_1 + b_1 i$ i $z_2 = a_2 + b_2 i$ aleshores definim

$$z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)i,$$
$$z_1 \cdot z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b1)i.$$

Fixem-nos que si $z = a + bi$ aleshores

$$z \cdot \bar{z} = a^2 + b^2.$$

En particular, si $z \neq 0$ aleshores $z \cdot \bar{z}$ pertany a $\mathbb{R}_{>0}$.

Definició 3.6. El mòdul de z és $|z| = \sqrt{z \cdot \bar{z}}$.

Podem dividir fàcilment un nombre complex per un nombre real: si $z_1 = a_1 + b_1 i$ i $c \in \mathbb{R}$ aleshores definim

$$\frac{z_1}{c} = \frac{a_1}{c} + \frac{a_2}{c} i.$$

Si volem dividir per un nombre complex diferent de 0 qualsevol, també ho podem fer multiplicant i dividint pel conjugat del denominador:

$$\frac{z_1}{z_2} = \frac{z_1 \cdot \bar{z}_2}{z_2 \cdot \bar{z}_2},$$

ja que aleshores ens reduïm al cas en què el denominador és un nombre real perquè ja hem vist que $z_2 \cdot \bar{z}_2 \in \mathbb{R}_{>0}$.

Exemple 3.7. $\frac{2+3i}{3+4i} = \frac{(2+3i)(3-4i)}{(3+4i)(3-4i)} = \frac{18+i}{3^2+4^2} = \frac{18}{25} + \frac{1}{25} i$.

Proposició 3.8. *Amb les definicions de suma, resta, producte i divisió que hem donat, els nombres complexos són un cos que conté els nombres reals.*

Demostració. Exercici. □

Proposició 3.9. *Si $z_1, z_2 \in \mathbb{C}$ aleshores:*

1. $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$.
2. $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$.
3. $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$.

Demostració. Exercici. □

3.2. **Representació gràfica i forma polar.** El nombre complex $z = a + bi$ el podem representar gràficament com el punt del pla $\mathbb{R}^2$ amb coordenades (a, b). Per exemple, el nombre i s'identifica amb el punt $(0, 1)$.

D'aquesta manera, podem identificar tot nombre complex amb un punt del pla i al revés, tot punt del pla dóna lloc a un nombre complex. Sovint es parla del "pla complex" per a referir-nos al fet que identifiquem els nombres complexos amb punts del pla. Amb aquesta identificació, els punts reals es corresponent amb els punts de la recta $y = 0$, que s'anomena la recta real.

Això dóna lloc a una representació alternativa dels nombres complexos, ja que un punt del pla també el podem especificar mitjançant les seves coordenades polars. Si $z = a + bi \in \mathbb{C}$ i anomenem r la distància entre z i $(0, 0)$, i θ l'angle que forma la semirecta que uneix $(0, 0)$ amb z amb la semirecta de l'eix positiu de les x aleshores s'utilitza la notació

$$z = r_\theta$$

per a denotar el nombre z en polars. De l'expressió $z = a+bi$ se li diu expressió cartesiana. Aplicant trigonometria bàsica trobem les fórmules per a passar de l'expressió cartesiana a l'expressió polar:

$$r = |z| = \sqrt{a^2 + b^2},$$
$$\theta = \begin{cases} \arctan(\frac{b}{a}) \text{ si } a > 0 \\ \arctan(\frac{b}{a}) + \pi \text{ si } a < 0. \end{cases}$$

També per a passar de l'expressió polar a la cartesiana:

$$z = r\cos\theta + ir\sin\theta.$$

Proposició 3.10. *Si $z_1 = r_{1\theta_1}$ i $z_2 = r_{2\theta_2}$ aleshores*

1. $z_1 \cdot z_2 = (r_1 r_2)_{\theta_1+\theta_2}$;
2. $\frac{z_1}{z_2} = (\frac{r_1}{r_2})_{\theta_1-\theta_2}$ *si* $z_2 \neq 0$.

Demostració. La fórmula per al producte és un càlcul, utilitzant que $z_j = r_j(\cos\theta_j + i\sin\theta_j)$:

$$\begin{aligned} z_1 \cdot z_2 &= r_1(\cos\theta_1 + i\sin\theta_1)r_2(\cos\theta_2 + i\sin\theta_2) \\ &= r_1 r_2\left((\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\sin\theta_1\cos\theta_2 + \sin\theta_2\cos\theta_1)\right) \\ &= r1r2\left(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)\right) = (r_1r_2)_{\theta_1+\theta_2}. \end{aligned}$$

La fórmula per al quocient és una conseqüència directa de la fórmula per al producte. □

Corol·lari 3.11. *Si $r = r_\theta$ i $n \in \mathbb{Z}_{\geq 0}$ aleshores $z^n = r^n_{n\theta}$. És a dir, z^n té mòdul r^n i argument $n\theta$.*

3.3. **Exponencial complexa.** Recordem que si $x \in \mathbb{R}$ aleshores definim e^x com

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \dots$$

És a dir, la sèrie anterior és convergent, i el límit és, per definició e^x. De manera anàloga, si prenem $z \in \mathbb{C}$ resulta que la sèrie

$$1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!} + \dots$$

també convergeix[9] a un nombre complex. Això ens permet definir e^z com

$$1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!} + \dots$$

Per tant, hem donat significat a què vol dir la funció exponencial avaluada en un argument complex (i això és una extensió natural de l'exponencial d'un nombre real). Fixem-nos que si l'avaluem en un nombre imaginari pur de la forma $i\theta$ amb $\theta \in \mathbb{R}$ tenim que

$$\begin{aligned} e^{i\theta} &= 1 + i\theta - \frac{\theta^2}{2!} - \frac{i\theta}{3!} + \frac{\theta^4}{4!} + + \frac{i\theta^5}{5!} - + \frac{\theta^6}{6!} + \dots \\ &= \left(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} + \dots\right) + i\left(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} + \dots\right) = \cos\theta + i\sin\theta, \end{aligned}$$

on hem identificat les sèries de Taylor del sinus i el cosinus en la darrera igualtat. Així doncs, hem obtingut:

Teorema 3.12 (Fórmula d'Euler)**.** *Si $\theta \in \mathbb{R}$ aleshores $e^{i\theta} = \cos\theta + i\sin\theta$.*

Observació 3.13. Si particularitzem la fórmula a $\theta = \pi$ obtenim que $e^{i\pi} + 1 = 0$.

Observació 3.14. Fixem-nos que $e^{i\theta}$ té mòdul 1 i argument θ. Així doncs, la fórmula d'Euler també es pot enunciar com $e^{i\theta} = 1_\theta$. En conseqüència, és molt habitual denotar el nombre r_θ com $re^{i\theta}$; aquesta forma de notació polar és molt freqüent.

3.4. **Arrels de polinomis.** Fixem-nos que, per construcció, $\mathbb{C}$ conté les arrels del polinomi $x^2 + 1$ (que són $\pm i$). De fet, $\mathbb{C}$ conté les arrels d'altres polinomis de $\mathbb{R}[x]$ que no tenen arrels a $\mathbb{R}$. Per exemple, tots els polinomis de grau 2 a coeficients reals tenen dues arrels (comptades amb multiplicitat) a $\mathbb{C}$; per exemple, el polinomi $x^2 + x + 1$ no té arrels reals perquè el discriminant és negatiu, però aplicant la fórmula per a les equacions de segon grau veiem que té les arrels complexes

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

Un altre exemple són els polinomis de la forma $x^n - 1$ amb $n \in \mathbb{Z}_{>0}$. Les arrels d'aquest polinomi s'anomenen arrels n-èssimes de la unitat (i és que tota arrel z satisfà que $z^n = 1$). Les arrels reals de $x^n - 1$ són $z = 1$ si n és senar i $z = \pm 1$ si n és parell. En canvi, el polinomi $x^n - 1$ té n arrels a $\mathbb{C}$; és a dir, hi ha n arrels de la unitat. Aquestes són els nombres

$$z_0 = 1, z_1 = 1_{\frac{2\pi}{n}}, z_2 = 1_{2.\frac{2\pi}{n}}, z_3 = 1_{3.\frac{2\pi}{n}}, \dots, z_{n-1} = 1_{(n-1).\frac{2\pi}{n}}.$$

Equivalentment, les arrels n-èssimes de la unitat són els nombres

$$z_k = e^{k\frac{2\pi i}{n}}, \ k = 0, 1, \dots, k-1.$$

És fàcil comprovar que tots aquests nombres són diferents i que satisfan $z_k^n = 1$ (utilitzant el Corol·lari 3.11, per exemple). Com que un polinomi amb coeficients en un cos té com a màxim tantes arrels com el grau, veiem que aquestes són totes les arrels de $x^n - 1$.

De fet, encara més és cert. Resulta que els complexos conten les arrels de qualsevol polinomi a coeficients reals, i fins i tot a coeficients complexos.

[9]En aquesta secció no serem gaire rigorosos amb els conceptes de convergència; en particular, no definirem què vol dir que una sèrie de nombres complexos convergeixi i farem manipulacions de sèries que no justificarem del tot. En cursos posteriors d'anàlisi tot això es veurà amb el rigor necessari, en aquesta secció en tindrem prou amb fer raonaments formals i intuïtius.

Teorema 3.15 (Teorema Fonamental de l'Àlgebra)**.** *Tot polinomi no constant de* $\mathbb{C}[x]$ *té alguna arrel a* $\mathbb{C}$*.*

Observació 3.16. Hi ha moltes demostracions d'aquest resultat, però malauradament totes elles utilitzen eines de les què no disposem, i ens allunyaria massa de l'objectiu del curs introduir-les.

Corol·lari 3.17. *Tot polinomi de grau* $n \geq 1$ *amb coeficients complexos té* n *arrels complexes, comptades amb multiplicitat.*

Demostració. Per inducció sobre n. El cas $n = 1$ és evident. Si $f(x) \in \mathbb{C}[x]$ té grau $n \geq 2$, pel Teorema Fonamental de l'Àlgebra sabem que té alguna arrel $\alpha \in \mathbb{C}$. Aleshores

$$f(x) = (x - \alpha)g(x)$$

amb $g(x)$ de grau $n - 1$. Per hipòtesi d'inducció $g(x)$ té $n - 1$ arrels comptades amb multiplicitat, i veiem que tota arrel de f és igual a α o a una arrel de $g(x)$; per tant, $f(x)$ té n arrels comptades amb multiplicitat. □

4. Residus quadràtics

En tot aquest capítol p denotarà un primer senar.

Definició 4.1. Un enter a no divisible per p es diu que és un residu quadràtic mòdul p si la congruència $x^2 \equiv a \pmod{p}$ té solució. Altrament es diu que a és un no residu quadràtic mòdul p.

Exemple 4.2.
- 2 és un residu quadràtic mòdul 7, ja que la congruència $x^2 \equiv 2 \pmod{7}$ té solució (les solucións són $x \equiv 3 \pmod{7}$ i $x \equiv 4 \pmod{7}$).
- 3 és un no residu quadràtic mòdul 7. En efecte, cap de les classes de congruència mòdul 7 elevada al quadrat dóna la classe del 3.

Observació 4.3. Que a sigui residu quadràtic mòdul p només depèn de la classe de congruència de a mòdul p. Per tant, podem parlar de si un element de $(\mathbb{Z}/p\mathbb{Z})^*$ és un residu quadràtic o no.

Exemple 4.4. Els residus quadràtics de $(\mathbb{Z}/7\mathbb{Z})^*$ són $1, 2$ i 4.

Proposició 4.5. *A $(\mathbb{Z}/p\mathbb{Z})^*$ hi ha $\frac{p-1}{2}$ residus quadràtics (i per tant $\frac{p-1}{2}$ no residus quadràtics).*

Demostració. És un exercici de la llista de problemes. □

4.1. Símbol de Legendre i criteri d'Euler.

Definició 4.6. (Símbol de Legendre): Si $a \in \mathbb{Z}$ i p és un primer senar definim

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

Exemple 4.7. $\left(\frac{2}{7}\right) = 1$ i $\left(\frac{3}{7}\right) = -1$.

Novament, $\left(\frac{a}{p}\right)$ només depèn de la classe de a mòdul p i per tant si $x \in \mathbb{Z}/p\mathbb{Z}$ té sentit parlar de $\left(\frac{x}{p}\right)$.

Proposició 4.8. *Tot residu quadràtic té exactament dues arrels quadrades diferents mòdul p.*

Demostració. Sigui a un residu quadràtic mòdul p. Això vol dir que $p \nmid a$ i que existeix $\alpha \in \mathbb{Z}$ tal que $\alpha^2 \equiv a \pmod{p}$. Aleshores $(-\alpha)^2 \equiv a \pmod{p}$ i veiem que $-\alpha$ també és arrel quadrada de a mòdul p. D'altra banda, α i $-\alpha$ són diferents mòdul p, ja que si $\alpha \equiv -\alpha \pmod{p}$ aleshores $p \mid 2\alpha$; però $p \nmid \alpha$ (perquè $p \nmid a$) i $p \nmid 2$, per tant $p \nmid 2\alpha$.

Suposem ara que β és una arrel quadrada de a mòdul p; és a dir, que $\beta^2 \equiv a \pmod{p}$. Aleshores $\alpha^2 \equiv \beta^2 \pmod{p}$ i per tant $p \mid \alpha^2 - \beta^2 = (\alpha + \beta)(\alpha - \beta)$. Com que p és primer, necessàriament $p \mid \alpha - \beta$ (i per tant $\beta \equiv \alpha \pmod{p}$) o $p \mid \alpha + \beta$ (i per tant $\alpha \equiv -\beta \pmod{p}$). □

Lema 4.9. *Si $a \in (\mathbb{Z}/p\mathbb{Z})^*$ és residu quadràtic aleshores a^k també ho és per a tot $k \in \mathbb{Z}$.*

Demostració. Si $\alpha^2 = a$ aleshores $(\alpha^k)^2 = a^k$ per a tot k. □

Proposició 4.10. *El símbol de Legendre és multiplicatiu. És a dir*

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

Demostració. Si $p \mid ab$ aleshores és immediat (la igualtat és $0 = 0$). Suposem doncs que $a, b \in (\mathbb{Z}/p\mathbb{Z})^*$. Farem la demostració per casos:

(1) Si $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$: aleshores existeix $\alpha, \beta \in (\mathbb{Z}/p\mathbb{Z})^*$ tals que $\alpha^2 = a$ i $\beta^2 = b$; per tant $(\alpha\beta)^2 = ab$ i veiem que $\left(\frac{ab}{p}\right) = 1$.

(2) Si $\left(\frac{a}{p}\right) = 1$ i $\left(\frac{b}{p}\right) = -1$: ens cal veure que $\left(\frac{ab}{p}\right) = -1$. En efecte, com que a^{-1} és residu quadràtic (pel lema anterior), si ab fos residu quadràtic tindríem que $a^{-1}ab$ també seria residu quadràtic (pel cas anterior on hem vist que el producte de residus és residu), la qual cosa contradiu la hipòtesi que $\left(\frac{b}{p}\right) = -1$.

(3) Si $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$: ens cal veure que $\left(\frac{ab}{p}\right) = 1$. Raonem per contradicció, suposant que ab és no residu quadràtic. Aleshores, si $r \in (\mathbb{Z}/p\mathbb{Z})^*$ és un residu quadràtic, pel cas anterior tenim que abr és un no residu. Per tant, el conjunt

$$\{abr \mid r \in (\mathbb{Z}/p\mathbb{Z})^* \text{ és residu quadràtic}\}$$

té cardinal $\frac{p-1}{2}$ (ja que hi ha $\frac{p-1}{2}$ residus quadràtics) i està format per elements que són tots ells no residus quadràtics. Per tant, és el conjunt de tots els no residus quadràtics de $(\mathbb{Z}/p\mathbb{Z})^*$. En particular, com que a és no residu tenim que $abr = a$ per a algun residu quadràtic r. Però d'aquí es dedueix que $b = r^{-1}$ i això és una contradicció, perquè b és no residu quadràtic i en canvi r^{-1} és residu quadràtic.

□

Teorema 4.11 (Criteri d'Euler)**.** *Tenim que* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Demostració. Si $p \mid a$ és evident. Suposem doncs que $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Sigui g una arrel primitiva mòdul p, de manera que

$$(\mathbb{Z}/p\mathbb{Z})^* = \{g^0, g^1, g^2, \ldots, g^{p-2}\}.$$

Fixem-nos que necessàriament $\left(\frac{g}{p}\right) = -1$, ja que altrament tot element de $(\mathbb{Z}/p\mathbb{Z})^*$ seria residu quadràtic.

D'altra banda, afirmem que $g^{\frac{p-1}{2}} = -1$. Veiem-ho: pel Teorema Petit de Fermat és clar que $g^{\frac{p-1}{2}}$ és arrel del polinomi $x^2 - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$. Ara bé, aquest és un polinomi amb coeficients en un cos, i per tant no pot tenir més arrels que el seu grau, en aquest cas 2. I sabem que ± 1 són dues arrels d'aquest polinomi o sigui que són totes les arrels. Per tant, o bé $g^{\frac{p-1}{2}} = -1$ o bé $g^{\frac{p-1}{2}} = 1$; la darrera opció no és possible perquè g és arrel primitiva i per tant té ordre $p - 1$, o sigui que ha de ser $g^{\frac{p-1}{2}} = -1$.

Per acabar, escrivim a com $a = g^k$ per a cert $k \in \{0, \ldots, p-2\}$. Aleshores

$$\left(\frac{a}{p}\right) = \left(\frac{g^k}{p}\right) = \left(\frac{g}{p}\right)^k = (-1)^k = \left(g^{\frac{p-1}{2}}\right)^k = \left(g^k\right)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}.$$

□

4.2. **Llei de reciprocitat quadràtica.** Si treballem amb un mòdul fixat és relativament senzill saber si una congruència quadràtica té solució o no (mitjançant el criteri d'Euler, per exemple). Però també podem pensar en variar el mòdul, i això dóna lloc a una qüestió més profunda. Per exemple, imaginem que volem saber per a quins primers senars p el 5 és residu quadràtic mòdul p. És a dir, es preguntem per a quins primers q la congruència

$$x^2 \equiv 5 \pmod{p}$$

té solució. Per a fer-nos una idea de per on pot anar la resposta, podem fer una taula per p petit:

q	3	7	11	13	17	19	23	29	31	37	41
RQ?	no	no	sí	no	sí	sí	no	no	sí	no	sí

En aquests casos, fixem-nos que els primers p per als quals 5 és un residu quadràtic mòdul p són aquells en què $p \equiv 1, 4 \pmod 5$. És això cert en general? Fixem-nos que també que 1 i 4 són justament els residus quadràtics mòdul 5. És a dir, que per a aquests primers valors de p sembla que 5 és un residu quadràtic mòdul p si i només si p és un residu quadràtic mòdul 5. El fet que aquesta relació és certa és un cas particular de l'anomenada Llei de Reciprocitat Quadràtica, que és un resultat que fou conjecturat per Euler i Legendre i finalment provat per Gauss al seu llibre Disquisitiones Aritmeticae (Gauss finalment va donar 8 demostracions diferents de la LRQ; avui en dia se'n coneixen més de 200 d'essencialment diferents).

Teorema 4.12 (Llei de Reciprocitat Quadràtica)**.** *Siguin p i q nombres senars diferents. Aleshores:*

(1) $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ *(Primera llei suplementària).*

(2) $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ *(Segona llei suplementària).*

(3) $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ *(Llei de reciprocitat quadràtica).*

La primer llei suplementària se segueix del Criteri d'Euler. Tot seguit veurem la cinquena demostració de Gauss de la LRQ (i de la segona llei suplementària). El primer resultat auxiliar que necessitem és l'anomenat Lemma de Gauss.

Teorema 4.13 (Lema de Gauss)**.** *Sigui p u primer senar i $(a,p) = 1$. Considerem els enters $a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)$ i els residus d'aquests nombres en fer la divisió entera per p; anomenem $r_1, r_2, \ldots, r_n$ els residus que siguin $> p/2$ i $s_1, s_2, \ldots, s_k$ els residus que siguin $< p/2$ (en particular $n + k = \frac{p-1}{2}$). Aleshores*

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Demostració. Comencem amb un parell d'observacions:

- per a tot i tenim que $0 < p - r_i < p/2$ i, a més, tots els nombres $p - r_i$ són diferents;
- $p - r_i \neq s_j$ per a tot i, j; en efecte, si $p - r_i = s_j$ aleshores

$$r_i \equiv \alpha a \pmod{p} \text{ per a cert } 1 \leq \alpha \leq \frac{p-1}{2},$$

$$s_j \equiv \beta a \pmod{p} \text{ per a cert } 1 \leq \beta \leq \frac{p-1}{2}.$$

Això implicaria que $p = r_i + s_j \equiv a(\alpha + \beta) \pmod{p}$ i per tant que $p \mid a(\alpha + \beta)$. Com que $p \nmid a$ hauria de ser $p \mid (\alpha + \beta)$, cosa que evidentment no pot ser.

D'aquestes dues observacions en deduïm que

$$\{p-r_1, p-r_2, \dots, p-r_n, s_1, s_2, \dots, s_k\} = \{1, 2, \dots, \frac{p-1}{2}\}. \tag{4.1}$$

i per tant que

$$(p-r_1)(p-r_2)\dots(p-r_n)s_1s_2\dots s_k\} = 1\cdot 2\dots\left(\frac{p-1}{2}\right).$$

Per tant, prenent classes mòdul p:

$$(-1)^n r_1\dots r_n s_1\dots s_k \equiv 1\cdot 2\dots\left(\frac{p-1}{2}\right) \pmod p.$$

Recordant la definició dels r_i i s_j veiem que

$$(-1)^n a\cdot 2a\cdot 3a\cdot\left(\frac{p-1}{2}\right)a \equiv 1\cdot 2\dots\left(\frac{p-1}{2}\right) \pmod p$$

i per tant

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

Invocant el Criteri d'Euler (Teorema 4.11) obtenim el resultat. □

Teorema 4.14. *Seguint amb les notacions del teorema anterior tenim que si a és senar aleshores*

$$n \equiv \sum_{j=1}^{n}\left\lfloor\frac{ja}{p}\right\rfloor \pmod 2,$$

on $\lfloor\cdot\rfloor$ denota la part entera. Si $a=2$, aleshores $n \equiv \frac{p^2-1}{8} \pmod 2$.

Remarca 4.15. Ajuntant aquest resultat amb el Lemma de Gauss veiem que si a és senar aleshores

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{n}\left\lfloor\frac{ja}{p}\right\rfloor} \tag{4.2}$$

i que per $a=2$ obtenim la segona llei suplementària:

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

Demostració. Fixem-nos que si $m\in\mathbb{Z}_{>0}$ i fem la divisió entera de m per p el quocient és justament $\left\lfloor\frac{m}{p}\right\rfloor$; és a dir, que si anomenem el residu de dividir m per p podem escriure:

$$m = p\cdot\left\lfloor\frac{m}{p}\right\rfloor + \mathrm{r}.$$

Aplicant aquesta igualtat per a $m=ja$ amb $j=1,\dots,\frac{p-1}{2}$ i recordant que $r_1,\dots,r_n,s_1,\dots,s_k$ són els residus de dividir els ja podem escriure:

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\cdot\left\lfloor\frac{ja}{p}\right\rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j.$$

Per (4.1) tenim que

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{n}(p - r_j) + \sum_{j=1}^{k} s_j = np - \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j.$$

Restant les dues darreres igualtats:

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\left(\sum_{j=1}^{\frac{p-1}{2}} \cdot \left\lfloor \frac{ja}{p} \right\rfloor - n\right) + 2\sum_{j=1}^{n} r_j.$$

Sumant la progressió aritmètica de la part esquerra i prenent classes mòdul 2 obtenim que

$$(a-1)\left(\frac{p^2-1}{8}\right) \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - n \pmod 2.$$

Si a és senar $a-1 \equiv 0 \pmod 2$ i això dóna directament la igualtat de l'enunciat. Si $a = 2$ aleshores $\left\lfloor \frac{2j}{p} \right\rfloor = 0$ per $1 \leq j \leq \frac{p-1}{2}$ d'on obtenim que $n \equiv \frac{p^2-1}{8} \pmod 2$. □

Demostració de la Llei de Reciprocitat Quadràtica. Definim el conjunt

$$S = \{(x,y) \in \mathbb{Z}^2 \colon 1 \leq x \leq \frac{p-1}{2},\ 1 \leq y \leq \frac{q-1}{2}\},$$

que té cardinal $\#S = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$. Definim ara els dos subconjunts de S següents:

$$S_1 = \{(x,y) \in S \colon qx > py\};$$
$$S_2 = \{(x,y) \in S \colon qx < py\}.$$

Fixem-nos que no pot ser que $qx = py$ amb $(x,y) \in S$ (ja que això implicaria que $p \mid x$, per exemple) i per tant tenim que

$$S = S_1 \sqcup S_2 \text{ (unió disjunta).}$$

Podem reescriure aquests conjunts com

$$S_1 = \{(x,y) \in S \colon 1 \leq x \leq \frac{p-1}{2}, 1 \leq y < \frac{qx}{p}\};$$
$$S_2 = \{(x,y) \in S \colon 1 \leq y \leq \frac{q-1}{2}, 1 \leq x < \frac{px}{q}\}.$$

Així doncs

$$\#S_1 = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor$$
$$\#S_2 = \sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{px}{q} \right\rfloor$$

i com que $\#S = \#S_1 + \#S_2$ veiem que

$$\sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{px}{q} \right\rfloor = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right).$$

Per tant

$$(-1)^{\sum_{x=1}^{\frac{p-1}{2}} \lfloor \frac{qx}{p} \rfloor} (-1)^{\sum_{y=1}^{\frac{q-1}{2}} \lfloor \frac{px}{q} \rfloor} = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$$

i per (4.2) tenim que

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

□

Exemple 4.16. La Llei de Reciprocitat Quadràtica és útil a l'hora de calcular símbols de Legendre, fent servir la propietat que $\left(\frac{q}{p}\right)$ depèn de com sigui q mòdul p. Per exemple:

$$\left(\frac{5}{103}\right) = \left(\frac{103}{5}\right)(-1)^{2\cdot 51} = \left(\frac{3}{5}\right) = -1.$$

$$\left(\frac{-42}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right) = (-1)^{30}(-1)^{\frac{61^2-1}{8}}\left(\frac{61}{3}\right)\left(\frac{61}{7}\right) = 1.$$

Exemple 4.17. També podem respondre a preguntes com: per a quins primers p el 5 és residu quadràtic mòdul p? Per la LRQ tenim que

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

Per tant, 5 és residu quadràtic mòdul p si i només si p és residu quadràtic mòdul 5, és a dir, si i només si $p \equiv 1, 4 \pmod 5$.

Exemple 4.18. Veiem ara per a quins p es té que 7 és residu quadràtic mòdul p. Per la LRQ:

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

Aquest producte val 1 si i només si els dos factors valen 1 o els dos valen -1. És a dir $\left(\frac{7}{p}\right) = 1$ si i només si

- $p \equiv 1, 2, 4 \pmod 7$ i $p \equiv 1 \pmod 4$, o bé
- $p \equiv 3, 5, 6 \pmod 7$ i $p \equiv 3 \pmod 4$.

Fent servir el teorema xinès del residu podem escriure aquestes condicions com a congruències mòdul 28:

$$\left(\frac{7}{p}\right) = 1 \iff \begin{cases} p \equiv 1, 25, 9 \pmod{28}, \text{ o bé} \\ p \equiv 3, 19, 27 \pmod{28}. \end{cases}$$

4.2.1. *Càlcul d'arrels quadrades.* Donat p senar i a amb $p \nmid a$ podem calcular ràpidament si $x^2 \equiv a \pmod{p}$ té solucions amb el criteri d'Euler (això és computacionalment eficient gràcies a l'algoritme d'exponenciació binària, veieu §5.2.1 més avall). Una pregunta natural és: en el cas en què tingui solució, com en calculem una? Dit d'una altra manera, si $\left(\frac{a}{p}\right) = 1$, com calculem una arrel quadrada de $a \pmod{p}$?

- Si $p \equiv 3 \pmod{4}$ aleshores $b = a^{\frac{p+1}{4}}$ n'és una. En efecte:
$$b^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} a \equiv \left(\frac{a}{p}\right) a \equiv a \pmod{p}.$$
- Si $p \equiv 1 \pmod{4}$ no es coneix cap algoritme determinístic que calculi una arrel quadrada de $a \pmod{p}$ en temps polinòmic (s'entén en temps polinòmic en $\log p$). Sí que hi ha algoritmes probabilístics polinòmics (però no els veurem aquí).

4.2.2. *Càlcul d'arrels k-èssimes.* Suposem que $(k, p-1) = 1$; aleshores tot $a \pmod{p}$ té arrels k-èssimes, i es poden calcular de manera fàcil. Suposem que $p \nmid a$ (el cas $p \mid a$ és trivial); per Bezout sabem que existeixen $m, n \in \mathbb{Z}$ tals que
$$mk + n(p-1) = 1.$$
En altres paraules, m és l'invers de k mòdul $p-1$. Aleshores a^m és una arrel k-èssima de a. En efecte:
$$(a^m)^k \equiv a^{1-n(p-1)} \equiv a \cdot (a^{p-1})^{-n} \equiv a \pmod{p},$$
on hem utilitzat el teorema petit de Fermat en el darrer pas. Veiem doncs que quan $(k, p-1) = 1$ podem calcular arrels k-èssimes prenent potències. Una generalització d'aquesta propietat és la base del mètode RSA que veurem al tema següent.

4.3. **Residus quadràtics mòdul n.** Sigui $n \in \mathbb{Z}_{>0}$ i $a \in \mathbb{Z}$ amb $(a, n) = 1$.

Definició 4.19. Diem que a és residu quadràtic mòdul n si la congruència
$$x^2 \equiv a \pmod{n}$$
té solució.

Observació 4.20. Com de costum, podem expressar (i ho farem sense més comentaris) aquesta noció en termes de classes mòdul n. Un element $a \in (\mathbb{Z}/n\mathbb{Z})^*$ és residu quadràtic si és un quadrat; és a dir, si existeix $b \in (\mathbb{Z}/n\mathbb{Z})^*$ tal que $b^2 = a$.

Començarem estudiant el cas en què n és la potència d'un primer senar.

Proposició 4.21. *Sigui p un primer senar amb $p \nmid a$ i sigui $r \in \mathbb{Z}_{>0}$. Aleshores a és residu quadràtic mòdul p^r si i només si ho és mòdul p, i en aquest cas té 2 arrels quadrades mòdul p^r.*

Demostració. Una direcció és molt fàcil, si existeix $\alpha \in \mathbb{Z}$ amb $\alpha^2 \equiv a \pmod{p^r}$ també es té que $\alpha^2 \equiv a \pmod{p}$.

Veiem l'altra implicació per inducció sobre r: Suposem que a és residu quadràtic mòdul p^r i veiem que aleshores també ho és mòdul p^{r+1}. Sigui α tal que $\alpha^2 \equiv a \pmod{p^r}$. Trobarem una solució de la congruència $x^2 \equiv a \pmod{p^{r+1}}$; veurem que l'equació
$$(\alpha + p^r x)^2 \equiv a \pmod{p^{r+1}}$$

té solució. En efecte, desenvolupant el quadrat

$$\alpha^2 + p^{2r}x^2 + 2p^r\alpha x \equiv a \pmod{p^{r+1}}$$

i com que $p^{2r} \equiv 0 \pmod{p^{r+1}}$ és equivalent a

$$\alpha^2 - a + 2p^r\alpha x \equiv 0 \pmod{p^{r+1}}.$$

Volem trobar doncs $x \in \mathbb{Z}$ tal que $p^{r+1} \mid \alpha^2 - a + 2p^r\alpha x$. Sabem que $\alpha^2 - a = bp^r$ per a cert $b \in \mathbb{Z}$. Aleshores

$$\alpha^2 - a + 2p^r\alpha x = p^r b + 2p^r\alpha x$$

i veiem que $p^{r+1} \mid \alpha^2 - a + 2p^r\alpha x$ si i només si $p \mid b + 2\alpha x$. És a dir, ens cal trobar $x \in \mathbb{Z}$ tal que $b + 2\alpha x \equiv 0 \pmod{p}$. Com que $p \nmid 2\alpha$ tenim que 2α és invertible mòdul p i podem prendre $x \equiv (-b)(2\alpha)^{-1} \pmod{p}$.

Veiem ara que si a és residu quadràtic mòdul p^r aleshores té dues arrels quadrades. En primer lloc, si $\alpha^2 \equiv a \pmod{p^r}$ aleshores $-\alpha$ és una altra arrel quadrada i $\alpha \not\equiv \alpha \pmod{p^r}$. Veiem que no n'hi ha més. Si β és una arrel quadrada aleshores $\beta^2 \equiv \alpha^2 \pmod{p^r}$. Això implica que $p^r \mid \alpha^2 - \beta^2 = (\alpha - \beta)(\alpha + \beta)$. Ara bé, p no pot dividir a la vegada $\alpha + \beta$ i $\alpha - \beta$, ja que si ho fes també dividiria la suma 2α. Per tant, o bé $p^r \mid \alpha - \beta$ o bé $p^r \mid \alpha + \beta$. □

Estudiem ara el cas en què el mòdul és una potència de 2.

Proposició 4.22. *Sigui a un enter senar. Aleshores:*

a) a és residu quadràtic mòdul 2 i té una arrel quadrada mòdul 2;
b) a és residu quadràtic mòdul 4 si i només si $a \equiv 1 \pmod 4$, i en aquest cas té dues arrels quadrades mòdul 4;
c) a és residu quadràtic mòdul 2^r per a $r \geq 3$ si i només si $a \equiv 1 \pmod 8$, i en aquest cas té 4 arrels quadrades mòdul 2^r.

Demostració. Els apartats *a*) i *b*) són obvis, veiem només el *c*). Es comprova fàcilment que l'únic residu quadràtic mòdul 8 és 1, i té quatre arrels quadrades. Ara fem inducció sobre r. Suposem que $\alpha^2 \equiv a \pmod{2^r}$, i busquem una arrel quadrada de a mòdul p^{r+1} de la forma $\alpha + 2^{r-1}x$:

$$(\alpha + 2^{r-1}x)^2 \equiv \alpha^2 + 2^{2r-2}x^2 + 2^r\alpha x \equiv a \pmod{2^{r+1}}.$$

Si $r \geq 2$ tenim que $2r - 2 \geq r + 1$, i escrivint $\alpha^2 - a = 2^r b$ veiem que l'equació és equivalent a

$$2^r b + 2^r\alpha x \equiv 0 \pmod{2^{r+1}}$$

que a la vegada és equivalent a $b + \alpha x \equiv 0 \pmod 2$ que té solució ja que α és senar.

Veiem l'afirmació sobre el nombre d'arrels. En primer lloc, si $\alpha^2 \equiv a \pmod{2^r}$ tenim que $-\alpha$ i $\pm\alpha + 2^{r-1}$ també són arrels. En efecte:

$$(\pm\alpha + 2^{r-1})^2 \equiv \alpha^2 + 2^{2r-2} \pm 2^r\alpha \equiv \alpha^2 \equiv a \pmod{2^r}.$$

Ara, si $\beta^2 \equiv a \pmod{2^r}$ aleshores $2^r \mid (\alpha + \beta)(\alpha - \beta)$. Però no pot ser que $4 \mid \alpha + \beta$ i $4 \mid \alpha - \beta$ ja que aleshores $4 \mid 2\alpha$ i sabem que α és senar. Per tant, o bé $2^{r-1} \mid \alpha - \beta$ o bé $2^{r-1} \mid \alpha + \beta$.

Suposem que $2^{r-1} \mid \alpha - \beta$. Si $2^r \mid \alpha - \beta$ aleshores $\alpha \equiv \beta \pmod{2^r}$. Si $2^r \nmid \alpha - \beta$ aleshores $\beta - \alpha = c \cdot 2^{r-1}$ amb c senar; posem $c = 2e + 1$ i veiem que $\beta - \alpha = 2^{r-1} + 2^r \cdot 2$. És a dir, $\beta \equiv \alpha + 2^{r-1}$.

De manera semblant, si $2^{r-1} \mid \alpha + \beta$ trobarem que o bé $\beta \equiv -\alpha \pmod{\beta}$ o bé $\beta \equiv -\alpha + 2^{r-1}$. □

Proposició 4.23. *Sigui $n = 2^r \prod_{i=1}^k p_i^{r_i}$ amb els p_i primers senars diferents i $r_i \geq 1$. Un enter a amb $(a,n) = 1$ és residu quadràtic mòdul n si i només si ho és mòdul 2^r i mòdul p_i per a tot i. Si és residu quadràtic, el nombre d'arrels quadrades mòdul n és*

$$\begin{cases} 2^k \text{ si } r = 0, 1 \\ 2^{k+1} \text{ si } r = 2 \\ r^{k+2} \text{ si } r \geq 3. \end{cases}$$

Demostració. És una consequència directa de les proposicions 4.21 i 4.22 i del Teorema Xinès del Residu. □

4.4. **El símbol de Jacobi.**

Definició 4.24. Sigui Q un enter senar positiu. Escrivim $Q = q_1 q_2 \dots q_s$ amb els q_i primers (no necessàriament diferents). Per a $P \in \mathbb{Z}$ definim el símbol de Jacobi

$$\left(\frac{P}{Q}\right) = \prod_{i=1}^{s} \left(\frac{P}{q_i}\right),$$

on $\left(\frac{P}{q_i}\right)$ denota el símbol de Lengedre.

Observació 4.25. Si Q és primer el símbol de Jacobi i el de Legendre coincideixen. D'aquesta manera, el símbol de Jacobi es pot entendre com una generalització del símbol de Jacobi i queda justificat l'ús de la mateixa notació.

Observació 4.26. Si P és residu quadràtic mòdul Q aleshores és residu quadràtic mòdul q_i per a tot i i per tant $\left(\frac{P}{Q}\right) = 1$. Fixem-nos però que el recíproc no és cert: si $\leq PQ = 1$ aleshores pot succeir que P sigui no residu quadràtic mòdul Q. Per exemple

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{5}{3}\right) = (-1)(-1) = 1$$

i en canvi 2 és no residu quadràtic mòdul 15.

Proposició 4.27. *El símbol de Jacobi té les propietats següents:*

(1) $\left(\frac{P}{Q}\right)\left(\frac{R}{Q}\right) = \left(\frac{PR}{R}\right)$;

(2) $\left(\frac{P}{Q}\right)\left(\frac{P}{R}\right) = \left(\frac{P}{QR}\right)$;

(3) Si $(P,Q) = 1$ aleshores $\left(\frac{P^2}{Q}\right) = \left(\frac{P}{Q^2}\right) = 1$;

(4) Si $P \equiv R \pmod{Q}$ aleshores $\left(\frac{P}{Q}\right) = \left(\frac{R}{Q}\right)$.

Demostració. Són totes elles immediates a partir de la definició i les propietats que ja coneixem del símbol de Legendre. □

Per a n un enter senar definim

$$\varepsilon(n) = \frac{p-1}{2} \pmod 2 \quad \text{i} \quad \omega(n) = \frac{n^2-1}{2} \pmod 2.$$

Lema 4.28. *(1) $\varepsilon(n)$ només depèn de la classe de n mòdul 4;*
(2) $\omega(n)$ només depèn de la classe de n mòdul 8.

Demostració. Si n és senar i $n' = n + 4\ell$ aleshores

$$\varepsilon(n) - \varepsilon(n') = \frac{n-1}{2} - \frac{n+4\ell-1}{2} = 2\ell \equiv 0 \pmod 2.$$

Això demostra la primera afirmació; la segona es fa de manera semblant. □

Gràcies a aquest lema, podem pensar ε i ω com aplicacions

$$\varepsilon\colon (\mathbb{Z}/4\mathbb{Z})^\times \longrightarrow \mathbb{Z}/2\mathbb{Z} \quad \text{i} \quad \omega\colon (\mathbb{Z}/8\mathbb{Z})^\times \longrightarrow \mathbb{Z}/2\mathbb{Z}.$$

És a dir, donada $\bar a \in (\mathbb{Z}/4\mathbb{Z})^\times$ definim $\varepsilon(\bar a) = \varepsilon(a)$, on a és un representant qualsevol de $\bar a$. De manera semblant, si $\bar a \in (\mathbb{Z}/8\mathbb{Z})^\times$ definim $\omega(\bar a) = \omega(a)$.

Lema 4.29. *Es satisfà que $\varepsilon(\bar a\bar b) = \varepsilon(\bar a) + \varepsilon(\bar b)$ i que $\omega(\bar a\bar b) = \omega(\bar a) + \omega(\bar b)$.*

Demostració. Demostrem només l'afirmació referent a ω, l'altra és similar. Calculem

$$\omega(\bar a\bar b) - \omega(\bar a) - \omega(\bar b) = \frac{(ab)^2-1}{8} - \frac{a^2-1}{8} - \frac{b^2-1}{8} = \frac{(a^2-1)(b^2-1)}{8} \equiv 0 \pmod 2.$$

□

Teorema 4.30 (Llei de Reciprocitat pel Símbol de Jacobi)**.** *Si P i Q són enters positius senars amb $(P,Q) = 1$ aleshores*

(1) $\left(\dfrac{-1}{Q}\right) = (-1)^{\varepsilon(Q)}$;

(2) $\left(\dfrac{2}{Q}\right) = (-1)^{\omega(Q)}$;

(3) $\left(\dfrac{P}{Q}\right)\left(\dfrac{Q}{P}\right) = (-1)^{\varepsilon(P)\varepsilon(Q)}$.

Remarca 4.31. Quan P i Q són primers això és la Llei de Reciprocitat Quadràtica pel símbol de Jacobi.

Demostració. Posem $P = \prod_{i=1}^r p_i$ i $Q = \prod_{j=1}^s q_j$ amb els p_i i q_j primers. Aleshores

$$\left(\frac{-1}{Q}\right) = \prod_{j=1}^s \left(\frac{-1}{q_j}\right) = \prod_{j=1}^s (-1)^{\varepsilon(q_j)} = (-1)^{\sum \varepsilon(q_j)} = (-1)^{\varepsilon(Q)}.$$

$$\left(\frac{2}{Q}\right) = \prod_{j=1}^s \left(\frac{2}{q_j}\right) = \prod_{j=1}^s (-1)^{\omega(q_j)} = (-1)^{\sum \omega(q_j)} = (-1)^{\omega(Q)}.$$

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

□

5. Aplicacions

5.1. **Introducció a la criptografia: nocions bàsiques de criptografia de clau privada.** La criptografia tracta sobre la transmissió confidencial d'informació en presència d'adversaris. És a dir, proporciona mecanismes per a intercanviar informació sense que una tercera persona que intercepti el missatge sigui capaç de saber-ne el significat. Fins a segle XX, les aplicacions eren bàsicament militars; per exemple, els oficials volien transmetre missatges a les tropes sense que l'enemic pogués entendre el missatge en cas que l'interceptés. A partir de la segona meitat del segle XX amb l'aparició i auge de les comunicacions digitals la criptografia ha esdevingut una eina d'ús diari en la nostra vida quotidiana. Per exemple, cada cop que comprem online o que introduïm la contrasenya del correu electrònic el navegador encripta el número de la carta de crèdit o la contrasenya abans d'enviar-los a través de la xarxa.

El problema és doncs el següent: l'Alice vol enviar certa informació a en Bob a través d'un canal de comunicació i sabem que una tercera persona, l'Eve, està escoltant i té accés a tot el que l'Alice li envia a en Bob. L'objectiu és xifrar el missatge abans de transmetre'l pel canal de manera que sigui comprensible només per a en Bob i, i que sigui del tot incomprensible per a l'Alice.

El mètode tradicional consisteix en resoldre el problema utilitzant *criptografia de clau pública*. L'exemple més fàcil és canviar cada lletra de l'alfabet un cert nombre de posicions. Per exemple, podem fer la substitució següent: $a \to d$; $b \to e$; $c \to f$; etcètera. És a dir, desplacem cada lletra 3 posicions cap a la dreta.

Exemple 5.1. El missatge xifrat per "ATACAR" seria "DWDFDU".

Una altra manera de pensar-ho és la següent: l'alfabet català té 26 lletres; fem correspondre a cada lletra un nombre mòdul 26 ($a \to 0$; $b \to 1$, etc.); per a xifrar un missatge, transformem les lletres en els nombres corresponents i sumem una quantitat d (mod 26) a cada nombre. Per a desxifrar un missatge, hem de fer l'operació inversa, en aquest cas restar d. Aquest mètode es coneix amb el nom de xifrat del Cèsar. Té dos inconvenients:

(1) Es pot trencar fàcilment, ja sigui per força bruta o fent anàlisi de freqüència (no totes les lletres són igual de freqüents; per exemple, en un text en català la lletra que apareix més sovint és molt probable que sigui la E i això dóna informació per a trobar la clau).
(2) L'Alice i en Bob han d'acordar una clau secreta. Fixem-nos que tothom que conegui la clau d pot desxifrar el missatge. Per tant, la clau només la poden conèixer l'Alice i en Bob (per això es diuen mètodes de clau privada).

El primer inconvenient es pot superar (fins a cert punt) amb una generalització del mètode que acabem de veure que s'anomena xifrat de Vigenere. També és un mètode de substitució, però la mateixa lletra es substitueix per lletres diferents segons la posició que ocupin al missatge. Ho veurem amb un exemple.

Exemple 5.2. Suposem que volem transmetre el missatge ATAQUEU A LES DOTZE. La clau ja no serà un únic nombre $d \in \mathbb{Z}/26\mathbb{Z}$, sinó uns quants nombres. Com que identifiquem $\mathbb{Z}/26\mathbb{Z}$ amb l'alfabet, podem pensar també que escollim una paraula clau. En el nostre cas, escollim com a paraula clau "COSA" (2 14 18 0). Ara xifrem sumant cada lletra del missatge amb la lletra de la clau (i repetim la clau tantes vegades com faci falta):

text clar	0	19	0	16	20	4	20	0	11	4	18	4	14	19	25	4
clau repetida	2	14	18	0	2	14	18	0	2	14	18	0	2	14	18	0
text xifrat	2	7	18	16	22	18	12	0	13	18	10	4	16	7	17	4

i això dóna el missatge xifrat CHSQWSMANSKDQHRE. Observem que això dificulta l'anàlisi de freqüència perquè, per exemple, la primera A es xifra com a J mentre que la segona A es xifra com a Z. També es dificulta l'atac per força bruta: si la clau té longitud n hi ha 26^n possibles claus. Això exemplifica un fenomen general: com més llarga és la clau més segur és el xifrat.

5.2. **Criptografia de clau pública: RSA.** La noció de criptografia de clau pública va ser introduïda per Diffie i Hellman l'any 1976. En un esquema de clau pública cada usuari té dues claus: una clau privada i una clau pública. Els missatges es xifren amb la clau pública i es desxifren amb la clau privada. El primer criptosistema de clau pública va ser publicat el 1978 per Rivest, Shamir i Adleman i es coneix amb el nom de RSA. Funciona de la manera següent.

Suposem que l'Alice vol enviar un missatge a en Bob. En Bob fa el següent:

(1) Escull p i q primers molt grans (de l'ordre de centenars de xifres).
(2) Calcula $n = p \cdot q$ i $\phi(n) = (p-1)\cdot(q-1)$.
(3) Escull un enter aleatori e tal que $(e, \phi(n)) = 1$.
(4) Calcula $d \equiv e^{-1} \pmod{\phi(n)}$; és a dir, d és l'invers de e mòdul $\phi(n)$.
(5) Fa públics els nombres n i e; aquesta és la clau pública d'en Bob, i tothom la coneix.
(6) Es guarda en secret els nombres p, q i d. Aquesta és la clau privada d'en Bob.
(7) Amb aquestes eleccions, els missatges que se li poden enviar a en Bob són elements de $(\mathbb{Z}/n\mathbb{Z})^*$.

Recordem que l'Alice vol enviar un missatge a en Bob, així que el primer que fa és consultar la clau pública (n, e) d'en Bob. Diguem-li $m \in (\mathbb{Z}/n\mathbb{Z})^*$ al missatge que l'Alice li vol enviar. El missatge xifrat (criptograma) el calcula com

$$c = m^e \pmod{n}$$

i és aquest c el que li envia a través del canal de comunicació.

Quan en Bob rep el criptograma c, el que ha de fer per a desxifrar-lo és calcular

$$c^d \pmod{n}.$$

En efecte, comprovem que això recupera el missatge m original. Com que $d \equiv e^{-1} \pmod{\phi(n)}$, això vol dir que existeix $k \in \mathbb{Z}$ tal que $ed = 1 + k\phi(n)$ i per tant

$$c^d \equiv m^{ed} \equiv m^{1+k\phi(n)} \equiv m \cdot \left(m^{\phi(n)}\right)^k \equiv m \pmod{n},$$

on hem utilitzat el Teorema d'Euler en la darrera igualtat.

La seguretat d'aquest mètode es basa en què no es coneixen mètodes eficients per a factoritzar enters. En efecte, tot el que ha de fer l'Eve per a descobrir el missatge és calcular també $c^d \pmod{n}$. El problema és que l'Eve només coneix el criptograma c, però no coneix d (és la clau privada d'en Bob, i no l'ha dit a ningú). El que sí coneix l'Eve és e, ja que això forma part de la clau pública d'en Bob. Aleshores la pregunta és: es pot calcular d a partir de e? Bé, d és l'invers de e mòdul $\phi(n)$ o sigui que semblaria que sí. Però l'Eve no sap $\phi(n)$ ja que això no forma part de la clau pública. L'únic que sap l'Eve és n. Aleshores la pregunta és: pot l'Eve calcular $\phi(n)$ a partir de n? Des d'un punt de vista teòric la resposta és que sí: com que $n = p \cdot q$, sabem que $\phi(n) = (p-1)(q-1)$. Ara bé, l'Eve només sap n i no sap ni p ni q. El que li cal és doncs[10] factorizar n. Però resulta que no hi ha mètodes eficients per a factoritzar, de manera que si n és un producte de primers grans el

[10]per a ser rigurosos l'argument que fem diu que si sap factoritzar n també sabrà calcular $\phi(n)$; deixem com a exercici comprovar que de fet el recíproc també és cert: si pot calcular $\phi(n)$ també podrà factoritzar n

temps que es necessita per a factoritzar n (fins i tot amb un ordinador dels més potents d'avui en dia) és de milers d'anys, així que a la pràctica no es pot fer.

Observació 5.3. És important remarcar que totes les operacions que cal fer per a calcular les claus públiques i privades i per a xifrar i desxifrar els missatges sí que es poden fer ràpidament. Per exemple, d es calcula fent un invers modular; això es pot fer eficientment amb l'algoritme d'Euclides. També les potències $m^e \pmod n$ i $c^d \pmod n$ es poden fer ràpidament utilitzant l'algoritme d'exponenciació binària, que expliquem tot seguit.

5.2.1. *Exponenciació binària.* Per a calcular

$$m^e \pmod n$$

podem fer-ho de manera naïf, però això comporta fer $e-1$ multiplicacions. Quan e és un nombre molt gran (de centenars de xifres) això és del tot impracticable fins i tot amb un ordinador[11].

Hi ha una manera millor de fer-ho. Comencem explicant-ho amb un exemple. Suposem que volem calcular

$$3^{16} \pmod{23}.$$

La manera naïf seria fer $3\cdots 3$ 16 vegades. Això és, 15 multiplicacions. Alternativament, podem començar calculant $3^2 \equiv 9 \pmod{23}$; aleshores ho elevem al quadrat: $3^4 \equiv 9^2 \equiv 12 \pmod{23}$; fem el quadrat una altra vegada: $3^8 \equiv 12^2 \equiv 6 \pmod{23}$; finalment, fem el quadrat una altra vegada: $3^{16} \equiv 6^2 \equiv 13 \pmod{23}$. Això han estat 4 multiplicacions enlloc de 16.

Ara, què té d'especial l'exponent 16? Doncs que $16 = 2^4$. Què passaria si volguéssim elevar a, diguem, 19? Podem utilitzar que $19 = 2^4 + 2 + 1$ i procedir així:

(1) Calculem 3^2 (1 multiplicació)
(2) Calculem $3^{2^2} = 3^2 \cdot 3^2$ (1 multiplicació)
(3) Calculem $3^{2^3} = 3^{2^2} \cdot 3^{2^2}$ (1 multiplicació)
(4) Calculem $3^{2^4} = 3^{2^3} \cdot 3^{2^3}$ (1 multiplicació)
(5) Finalment, calculem $3^{19} = 3^{2^4+2+1} = 3^{2^4} \cdot 3^2 \cdot 3$ (2 multiplicacions)

El que hem fet per a l'exponent 19, ho podem fer per a qualsevol exponent n, considerant la seva expressió binària:

$$n = n_r \cdot 2^r + n_{r-1} \cdot 2^{r-1} + \cdots n_2 \cdot 2^2 + n_1 \cdot 2 + n_0.$$

El nombre de multiplicacions serà doncs com a màxim $2\log_2 n$. Per exemple, si n té de l'ordre de 100 xifres decimals, és a dir, si $n \simeq 10^{100}$ podem calcular 10^n fent menys de $2\log_2(10^{100}) \simeq 665$ operacions.

Observació 5.4. Una observació senzilla, però molt important, és que quan fem els productes per a calcular $m^e \pmod n$, cal reduir el resultat $\bmod n$ després de cada producte. D'aquesta manera, tots els productes seran de nombres enters menors o iguals que n. Si intentem calcular m^e com a nombre enter i reduir mòdul n al final, això no cabrà a memòria.

[11]Suposem que tenim un processador a 3GHz, i suposem que pot fer una multiplicació per a cada tic de rellotge (això en realitat és molt optimista); el que trigaria a fer 10^{100} multiplicacions seria $10^{100}/(3\times 10^9) \simeq 3.33\times 10^{90}$ segons; això és aproximadament 7.65×10^{72} vegades l'edat de l'univers

Exemple 5.5. Suposem que en Bob escull $p = 5$ i $q = 11$, de manera que $n = 55$ i $\phi(n) = 40$. També escull $e = 3$ i calcula $d \equiv e^{-1} \pmod{40} \equiv 27 \pmod{40}$. Si l'Alice vol enviar el missatge $m = 32 \in (\mathbb{Z}/55\mathbb{Z})^*$ aleshores calcula

$$c = 32^3 \equiv 43 \pmod{55}.$$

En Bob rep $c = 43$ i per a recuperar el missatge calcula

$$43^{27} \equiv 32 \pmod{55}.$$

Observació 5.6.
- A la pràctica p i q són primers de 1024 bits (unes 300 xifres decimals).
- L'any 2009 es va factoritzar un enter n de 768 bits (232 dígits decimals); es van trigar 2 anys fent servir computació paral·lela (s'hauria trigat 2000 anys en un single core a 2.2GHz).
- A la pràctica RSA s'utilitza per a intercanviar claus de manera segura i aleshores s'utilitza un criptosistema de clau privada (són més ràpids).

Una prestació dels criptosistemes de clau pública, i de RSA en particular, és que permeten fer signatura digital. Això és, permeten afegir una signatura al missatge per a garantir la identitat de l'emissor.

Signatura digital RSA. Suposem que en Bob vol enviar un missatge m a l'Alice (aquí m pot estar xifrat o no), i afegir una signatura al missatge perquè l'Alice estigui segura que és en Bob qui envia el missatge. Aleshores en Bob calcula la signatura com

$$s = m^d \pmod{n},$$

on recordem que d és la clau privada d'en Bob. En Bob envia doncs (m, s) a l'Alice. L'Alice rep m i s, i per a comprovar que en efecte ha estat en Bob qui ha firmat el missatge calcula

$$s^e \pmod{n}.$$

Fixem-nos que si $s = m^d \pmod{n}$ aleshores

$$s^e \equiv m^{ed} \equiv m \pmod{n}.$$

Per tant, si $s^e \equiv m \pmod{n}$ podem estar convençuts que s s'ha calculat com $s = m^d \pmod{n}$ i per tant que ho ha calculat algú que coneixia la clau secreta d'en Bob. Podem estar convençuts que ho ha firmat en Bob doncs.

Observació 5.7. En tot això, estem assumint que l'Alice coneix l'autèntica clau pública d'en Bob (és a dir, que no hi ha algú fent-se passar per en Bob). Això es pot fer recuperant la clau pública d'en Bob d'una entitat certificadora en qui confiem o mitjançant un sistema de certificats digitals. Un certificat digital és un parell format per la clau pública d'en Bob i la clau pública d'en Bob signada digitalment per una entitat certificadora en qui confiem.

Una qüestió que no hem adreçat és: com es troben els primers p i q de 300 xifres?

5.3. **Com trobar primers grans.** Tal com hem vist a la secció anterior per a RSA necessitem trobar primers grans, de centenars de xifres. Certament existeixen primers arbitràriament grans, però com podem trobar-los? A la pràctica s'utilitzen els anomenats testos de primeritat. Un test de primeritat és un algoritme que, donat un enter n, ens diu si n és primer o si és compost[12]. El procediment emprat és doncs el següent:

(1) Es pren un enter n a l'atzar de la mida que volem (per a fixar idees, diguem de 200 xifres);

[12]Però en cas que sigui compost no ens retorna la seva factorització; en aquest sentit, un test de primeritat no és un algoritme de factorització

(2) Apliquem a n un test de primeritat;
(3) Si el resultat és que n és primer ja hem acabat, altrament tornem al primer pas.

Aquest mètode té una component aleatòria, ja que seleccionem enters a l'atzar. Si els primers de 200 xifres fossin molt escassos, potser no seria gaire bon mètode perquè costaria molt que un enter seleccionat a l'atzar fos primer. Però el mètode funciona molt bé a la pràctica perquè en realitat una proporció alta de nombres enters són primers. Per a quantificar aquesta afirmació, definim la funció $\pi(x)$ que per a un nombre real x compta el nombre de primers $\leq x$:

$$\pi(x) = \#\{n \leq x \text{ tals que } n \text{ és primer}\}.$$

En particular $\pi(x)/x$ és la fracció de nombres $\leq x$ que són primers. El teorema següent és el resultat clau.

Teorema 5.8 (Teorema del nombre primer)**.**

$$\lim_{x\to\infty} \frac{\pi(x)/x}{1/\log x} = 1$$

Aquest teorema no el demostrarem. Pertany al que s'anomena teoria analítica de nombres, i és que la manera natural de demostrar-lo és utilitzar eines analítiques que ens allunyarien del contingut del curs.

Fixem-nos que una conseqüència del teorema del nombre primer és que si x és un nombre molt gran aleshores

$$\frac{\pi(x)}{x} \simeq \frac{1}{\log x}.$$

Per exemple, per $x = 10^{200}$ tenim que $\pi(x)/x \simeq 0.0021 \simeq 1/460$. És a dir, aproximadament 1 de cada 460 nombres de menys de 200 xifres és primer. Això justifica que no haurem de fer gaires tries d'enters a l'atzar abans de trobar un primer.

5.4. **Testos de primeritat.** Començarem veient un test senzill que no s'utilitza a la pràctica, però una modificació seva sí que és eficient.

5.4.1. *Test de Fermat.* Es basa en el Teorema Petit de Fermat: si n és primer aleshores $a^{n-1} \equiv 1 \pmod{n}$ per a tot $1 < a < n$. Per tant, si $a^{n-1} \not\equiv 1 \pmod{n}$ per a algun $1 < a < n$ aleshores n és compost. En aquest cas diem que a és un testimoni en el test de Fermat per a n.

Exemple 5.9. 21 no és primer, ja que $2^{20} \equiv 4 \pmod{20}$.

Observació 5.10. Veiem que amb aquest test podem concloure que n és compost, però no obtenim cap factorització de n.

També veiem una característica important dels testos que veurem (i que són els que s'utilitzen a la pràctica): el test pot demostrar que un nombre és compost. Ara bé, si un nombre passa el test, no necessàriament és cert que sigui primer tal com veurem a continuació.

Definició 5.11. Si n és compost i a és un enter amb $1 < a < n$ tal que $a^{n-1} \equiv 1 \pmod{n}$ diem que n és pseudoprimer en base a.

Exemple 5.12. 341 és pseudoprimer en base 2, ja que $2^{340} \equiv 1 \pmod{341}$, i en canvi $341 = 11 \cdot 31$. Així doncs, 341 passaria el test de Fermat en base 2 tot i no ser primer.

Ens podríem preguntar si potser hi ha un nombre finit de casos com aquest. La resposta és que no.

Proposició 5.13. *Si n és pseudoprimer en base 2 aleshores $N = 2^n - 1$ també ho és.*

Demostració. Recordem que si $a \mid b$ aleshores $2^a - 1 \mid 2^b - 1$. En el nostre cas, $N - 1 = 2^n - 2 = 2(2^{n-1} - 1)$ i el segon factor és divisible per n (ja que n és pseudoprimer en base 2). Per tant $2^n - 1 \mid 2^{N-1} - 1$. Això ens diu que $2^{N-1} \equiv 1 \pmod{2^n - 1}$, és a dir, $2^{N-1} \equiv 1 \pmod{N}$. □

Corol·lari 5.14. *Hi ha infinits pseudoprimers en base 2.*

El problema s'agreuja perquè de fet hi ha enters que són compostos però són pseudoprimers per a totes les bases possibles. S'anomenen nombres de Carmichael.

Definició 5.15. Direm que n és un nombre de Carmichael si és compost i $a^{n-1} \equiv 1 \pmod{n}$ per a tot a amb $(a, n) = 1$.

Suposem que n satisfà que

- $n = p_1 p_2 \dots p_r$ és producte de primers diferents;
- per a cada i es té que $p_i - 1 \mid n - 1$.

Aleshores n és de Carmichael. En efecte, si $n - 1 = m_i(p_i - 1)$ tenim que $a^{p_i - 1} \equiv 1 \pmod{p_i}$ i per tant $a^{m_i(p_i-1)} \equiv 1 \pmod{p_i}$. És a dir, $p_i \mid a^{n-1} - 1$ per a tot i amb la qual cosa $n \mid a^{n-1} - 1$.

Exemple 5.16. $n = 561$ és nombre de Carmichael. La factorització és $561 = 2^4 \cdot 5 \cdot 7$.

La conclusió és que hi ha nombres que enganyen el test de Fermat. Tot seguit en veurem una modificació que sí que et pot emprar com a test de primeritat.

5.4.2. *Test de Miller–Rabin.* Sigui n un enter senar i suposem que té k factors primers. Recordem que si a té arrel quadrada mòdul n, aleshores té exactament 2^k arrels quadrades. Per tant, si un nombre té més de dues arrels quadrades mòdul n, aleshores n no pot ser primer. Aquesta és la base del test de Miller–Rabin.

L'explicarem primer amb un exemple: veiem que 561 no és primer. En primer lloc factoritzem $560 = 2^4 \cdot 35$. Escollim una base, per exemple $a = 7$. Ja hem vist que 561 és de Carmichael i per tant $7^{560} \equiv 1 \pmod{561}$, però fixem-nos que:

$$\begin{aligned} 7^{35} &\equiv 241 \pmod{561} \\ 7^{2\cdot} \equiv 241^2 &\equiv 298 \pmod{561} \\ 7^{2^2 \cdot 35} \equiv 298^2 &\equiv 166 \pmod{561} \\ 7^{2^3 \cdot 35} \equiv 166^2 &\equiv 67 \pmod{561} \\ 7^{2^4 \cdot 35} \equiv 67^2 &\equiv 1 \pmod{561}. \end{aligned}$$

Fixem-nos en la darrera congruència: ens diu que 67 és una arrel quadrada de 1 mòdul 561. Si 561 fos primer aleshores 1 només tindria dues arrels quadrades: 1 i -1. El fet que $67 \not\equiv \pm 1 \pmod{567}$ ens diu que 561 no és primer.

Ja veiem doncs el funcionament del test de Miller–Rabin per a un enter n senar qualsevol:

(1) Escrivim $n - 1 = 2^k m$ amb m senar;

(2) Escollim una base a amb $1 < a < n$ i calculem:

$$\begin{aligned} a^m &\pmod n \\ a^{2m} &\equiv (a^m)^2 \pmod n \\ a^{2^2m} &\equiv (a^{2m})^2 \pmod n \\ &\vdots \\ a^{2^{k-1}m} &\equiv (a^{2^{k-2}m})^2 \pmod n \\ a^{n-1} &\equiv a^{2^km} \equiv (a^{2^{k-1}m})^2 \pmod n. \end{aligned}$$

(3) Examinem els nombres $a^m, a^{2m}, a^{2^2m}, a^{2^{k-1}m}, a^{n-1}$. Si el darrer és diferent de 1 (mod n) aleshores n no és primer.

(4) Si $a^{n-1} \equiv 1 \pmod n$, ens fixem en el darrer nombre de la llista tal que $a^{2^im} \not\equiv 1 \pmod n$. Aquest nombre és una arrel quadrada de 1 (mod n), i per tant si $a^{2^im} \not\equiv -1 \pmod n$ aleshores n no és primer. Si $a^{2^im} \equiv -1 \pmod n$, aleshores escollim una altra base a i repetim el procés tornant al punt (2).

Si en alguna iteració trobem que per alguna base a el test detecta que n és compost, aleshores podem estar segurs que n és compost. Si, en canvi, repetim el test per a unes quantes bases diferents (diguem M bases) i en cap d'elles el test conclou que n sigui compost, aleshores podem inferir que n és bastant probable que sigui primer. Aleshores la pregunta és: com de probable? Bé, doncs es pot demostrar que si n és compost com a mínim $3/4$ parts de les bases són testimonis[13] per a la no primeritat de n. És a dir, que si n és compost la probabilitat de què passi el test amb una base a aleatòria és $< 1/4$. Per tant, si és compost passa el test per a M bases aleatòries amb probabilitat $< (1/4)^M$. És a dir, la probabilitat de què passi el test per a M bases però sigui compost és $< (1/4)^M$.

5.4.3. *Test de Solovay–Strassen.* Recordem el Criteri d'Euler: si n és primer i $(a, n) = 1$ aleshores

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

Per tant, si n és un enter amb $(a, n) = 1$ i

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

aleshores n és compost. Aquesta és la base del test.

La proposició següent ens diu que per a tot n compost sempre hi ha almenys una base que és testimoni.

Proposició 5.17. *Si n és un enter senar compost existeix a amb $(a, n) = 1$ tal que*

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}}.$$

[13] no demostrarem aquest resultat, però hi ha un raonament heurístic que ens pot convèncer de què la probabilitat que n passi el test tot i ser compost és $\leq 1/3$: si n és compost hi ha almenys 3 arrels quadrades diferents de 1 (mod n); així doncs, la probabilitat d'haver observat l'arrel -1 és $\leq 1/3$.

Demostració. Fem primer en cas en què n sigui lliure de quadrats, posem, $n = p_1 p_2 \dots p_r$ amb els p_i primers senars diferents. Sigui g un no residu quadràtic mòdul p_1. Pel Teorema Xinès del Residu existeix $a \in \mathbb{Z}$ tal que

$$\begin{aligned} a &\equiv g \pmod{p_1} \\ a &\equiv 1 \pmod{p_i} \text{ per a tot } i \geq 2. \end{aligned}$$

Aleshores

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_n}\right) = \left(\frac{g}{p_1}\right)\left(\frac{1}{p_2}\right)\dots\left(\frac{1}{p_r}\right) = -1.$$

D'altra banda $a^{\frac{n-1}{2}} \equiv 1 \pmod{p_2}$ (ja que $a \equiv 1 \pmod{p_2}$) i per tant $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{p_2}$ la qual cosa implica que $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$.

Suposem ara que n és de la forma $n = p_1^2 p_2 \dots p_r$. Prenem g una arrel primitiva mòdul p^2. Pel Teorema Xinès existeix a tal que

$$\begin{aligned} a &\equiv g \pmod{p_1^2} \\ a &\equiv 1 \pmod{p_i} \text{ per a } i > 1. \end{aligned}$$

Si fos $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}$ aleshores $a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$ i per tant $a^{\frac{n-1}{2}} \equiv 1 \pmod{p_1^2}$; és a dir

$$g^{\frac{n-1}{2}} \equiv 1 \pmod{p_1^2}.$$

Però això no és possible, perquè g té ordre $\phi(p_1^2) = p_1(p_1 - 1)$, i voldria dir que $p_1(p_1 - 1) \mid n - 1$ i per tant que $p_1 \mid n - 1$ que clarament no pot ser.

□

Proposició 5.18. *Si n és senar i compost almenys la meitat dels enters a tals que $0 < a < n$ i $(a, n) = 1$ satisfan que*

$$a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$$

Demostració. Definim el conjunt següent:

$$B = \{b\colon 0 < b < n \text{ i } \left(\frac{b}{n}\right) \equiv b^{\frac{n-1}{2}} \pmod{n}\} \subset (\mathbb{Z}/n\mathbb{Z})^\times.$$

N'hi ha prou amb veure que $\#B \leq \phi(n)/2$. Per la proposició anterior sabem que existeix $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ tal que $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$. Aleshores, per a tot $b \in B$ tenim que

$$\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \not\equiv a^{\frac{n-1}{2}} b^{\frac{n-1}{2}} \pmod{n}$$

i per la multiplicativitat del símbol de Jacobi

$$\left(\frac{ab}{n}\right) \not\equiv (ab)^{\frac{n-1}{2}} \pmod{n}.$$

És a dir, que la igualtat no se satisfà pels element de aB. Com que $\#B = \#aB$ i

$$B \cup aB \subset (\mathbb{Z}/n\mathbb{Z})^\times$$

tenim que $\#B \leq \phi(n)/2$.

□

Per tant, el test de Solovay–Strassen per a n senar consisteix en:

(1) Escollir $t \geq 1$ el nombre de rondes.
(2) Escollir un enter aleatori a amb $0 < a < n$.
(3) Si $(a, n) \neq 1$ o $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$ retorna (correctament) que n és compost.
(4) Altrament, és a dir si n passa el test amb base a, torna al punt (2).

Si n passa el test t vegades aleshores n és primer amb probabilitat $\geq 1 - (\frac{1}{2})^n$.

Observació 5.19. El símbol de Jacobi es pot calcular eficientment fent servir la Llei de Reciprocitat Quadràtica repetidament. Per exemple

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

En cada pas podem reduir el numerador mòdul el denominador, amb la qual cosa el nombre d'operacions que cal fer és semblant al de l'algoritme d'Euclides.

Referències

[GH04] B.H. Gross and J. Harris. *The Magic of Numbers*. Pearson Education, 2004.

[NZM91] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[Ste09] William Stein. *Elementary number theory: primes, congruences, and secrets*. Undergraduate Texts in Mathematics. Springer, New York, 2009. A computational approach.