Apunts d'Aritmètica

Marc Masdeu, UAB

Cursos 2018-19, 2019-20, 2020-21 i 2021-22

Índex

1. Primers i congruències

1.1 Divisibilitat

Teorema 1.1.1 — Divisió entera. Donats enters a i b amb $b > 1$, existeixen enters únics q i r tals que

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

L'enter q s'anomena el quocient d'a entre b, i r s'anomena el residu.

En general, diem que a divideix b si existeix un enter q tal que $aq = b$. Escriurem $a \mid b$.

Una primera aplicació és el fet que qualsevol enter admet representacions en qualsevol base:

Teorema 1.1.2 — representació m-àdica o en base m. Sigui $m \geq 2$. Aleshores tot enter positiu n es pot escriure de manera única com

$$n = a_0 + a_1 m + a_2 m^2 + \cdots + a_k m^k, \quad 0 \leq a_i \leq m-1, \quad a_k \neq 0.$$

on k és l'únic enter que satisfà

$$m^k \leq n < m^{k+1}.$$

Passem ara a parlar del màxim comú divisor (que escriurem gcd, de l'anglès *greatest common divisor*). El màxim comú divisor dels nombres a i b es defineix com

$$\gcd(a,b) = \max\{d \,:\, d \mid a \text{ i } d \mid b\}.$$

També definim $\gcd(0,0) = 0$.

Lema 1.1.3 Es té:

$$\gcd(a,b) = \gcd(b,a) = \gcd(\pm a, \pm b) = \gcd(a, b-a) = \gcd(a, b+a).$$

Demostració. Directament de la definició i el fet que si $d \mid a$ i $d \mid b$ aleshores $d \mid a \pm b$. ■

Observem que, com a conseqüència, també obtenim:

Corol·lari 1.1.4 Per a tot a, b i $t \in \mathbb{Z}$ es té

$$\gcd(a, b+at) = \gcd(a,b).$$

Aquest últim resultat ens permet calcular el màxim comú divisor entre dos nombres de manera ràpida. Comencem amb un exemple:

■ **Exemple 1.1.5** Calculem $\gcd(986, 289)$. Fent la divisió entera, obtenim

$$986 = 3 \cdot 289 + 119,$$

i per tant

$$\gcd(986, 289) = \gcd(3 \cdot 289 + 119, 289) = \gcd(119, 289).$$

Seguim ara amb una nova divisió:

$$289 = 2 \cdot 119 + 51,$$

que ens dona

$$\gcd(119, 289) = \gcd(119, 2 \cdot 119 + 51) = \gcd(119, 51).$$

Seguim amb

$$119 = 2 \cdot 51 + 17,$$

i per tant

$$\gcd(119, 51) = \gcd(2 \cdot 51 + 17, 51) = \gcd(17, 51).$$

Finalment, com que $51 = 17 \cdot 3$, obtenim $\gcd(17, 51) = 17$. ■

Aquest procediment es pot escriure en forma d'algoritme:

Algoritme 1.1.1 Calcula el màxim comú divisor de dos enters a i b.

```
def gcd(a,b):
    while b:
        a, b = b, a % b
    return a.abs()
```

També és fàcil de veure que

Lema 1.1.6 Per a tot $a, b, n \in \mathbb{Z}$ es té:

$$\gcd(an, bn) = |n| \gcd(a,b).$$

Demostració. Podem assumir (canviant signes i reordenant, si cal) que $a \geq b \geq 1$ i $n > 0$. Farem la demostració per inducció sobre $a + b \geq 2$. El cas base és $a = b = 1$ i és obvi. Per fer el cas general, escrivim

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

i aleshores

$$an = bnq + rn,$$

per tant:

$$\gcd(an,bn) = \gcd(bnq+rn,bn) = \gcd(rn,bn) = |n|\gcd(r,b) = |n|\gcd(a,b),$$

on a la tercera igualtat hem aplicat la hipòtesi d'inducció (com que $r < b \leq a$, tenim $r+b < a+b$). ■

Finalment, també és important veure que el gcd satisfà una maximalitat més forta que la que diu explícitament la seva definició:

Lema 1.1.7 Siguin $a,b,n \in \mathbb{Z}$ i suposem que $n \mid a$ i $n \mid b$. Aleshores $n \mid \gcd(a,b)$.

Demostració. Escrivim $a = na'$ i $b = nb'$. Per tant,

$$\gcd(a,b) = \gcd(na',nb') = n\gcd(a',b')$$

i veiem que n divideix $\gcd(a,b)$. ■

1.2 Factorització d'enters

Recordem que un primer és un nombre positiu p que té exactament dos divisors positius (1 i p). L'objectiu d'aquesta subsecció és demostrar el següent resultat, que ens diu que els nombres primers són els "blocs" amb els quals es construeixen tots els nombres naturals.

Teorema 1.2.1 — Teorema fonamental de l'aritmètica. Tot enter positiu n es pot escriure com a producte de primers:

$$n = p_1 p_2 \cdots p_r.$$

A més, aquesta descomposició és única, llevat de la possible reordenació dels factors.

Remarca 1.2.2 Fixem-nos que això no passa en altres anells commutatius. Per exemple, a $R = \mathbb{Z}[\sqrt{-5}]$ l'element $6 \in R$ es pot escriure com $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, i cadascun dels quatre elements 2, 3, $1+\sqrt{-5}$ i $1-\sqrt{-5}$ té exactament dos divisors llevat de les unitats ± 1 (serien "primers" amb la definició que hem donat, però s'anomenen *irreductibles*). Per tant, en aquest anell no es compleix l'anàleg del teorema fonamental de l'aritmètica.

El resultat clau que ens caldrà per demostrar aquest teorema és el següent.

Teorema 1.2.3 — Euclides. Sigui p és un primer i $a,b \in \mathbb{Z}$. Aleshores

$$p \mid ab \implies p \mid a \text{ o } p \mid b.$$

Demostració. Si $p \mid a$ ja estem. Si no, aleshores $\gcd(p,a) = 1$. Per tant, $\gcd(pb,ab) = b$. Ara observem que $p \mid pb$ i $p \mid ab$, i per tant $p \mid \gcd(pb,ab) = b$. ■

Ara ja podem demostrar el teorema fonamental de l'aritmètica.

Demostració del Teorema 1.2.1. Primer veiem l'existència, per inducció en $n \geq 1$. Si $n = 1$ ja estem (producte buit). Pel cas general, si n és primer ja estem (producte d'un sol terme), i si no, aleshores es pot escriure $n = ab$ amb $a, b < n$. Per hipòtesi d'inducció, tant a com b són producte de primers, i per tant n també ho és.

Per veure la unicitat, suposem que tenim dues factoritzacions

$$n = p_1 \cdots p_r = q_1 \cdots q_s,$$

amb els p_i's i q_j's primers. Observem que p_1 divideix $q_1 \cdot (q_2 \cdots q_s)$. Aleshores, o bé $p_1 = q_1$ o bé $p_1 \mid q_2 \cdots q_s$. Continuant, podem veure que $p_1 = q_j$ per algun j. Per tant, podem cancel·lar p_1 de la primera expressió i q_j de la segona. Obtenim que

$$n/p_1 = p_2 \cdots p_r = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s.$$

Per inducció sobre n, aquestes dues factoritzacions de n/p_1 són iguals, i per tant les dues factoritzacions de n també ho són. ■

Tal i com hem vist a la primera part de la demostració, escriure una factorització en primers és fàcil si sabem trobar un primer que divideixi n (o un factor no trivial). Aquest problema no és gens fàcil de fer quan n és gran, i més endavant veurem la importància que aquest fet té per la criptografia.

El teorema fonamental de l'aritmètica ens porta a pensar que hi hauria d'haver molts primers, si amb ells s'han de poder construir tots els naturals. En efecte, tenim el següent resultat famós.

Teorema 1.2.4 — Euclides. Hi ha infinits primers.

Demostració. Donats primers p_1, p_2, …, p_n, construirem un primer p_{n+1} diferent de tots els anteriors: considerem

$$N = p_1 p_2 \cdots p_n + 1,$$

i sigui q un primer que divideixi a N. Aleshores $q \mid N$ i, si q fos un dels p_i, aleshores q també dividiria a $p_1 p_2 \cdots p_n = N - 1$. Però això voldria dir que q dividiria a $N - (N-1) = 1$, que no pot ser. Per tant, q és un primer que no apareix a la llista, i podem definir $p_{n+1} = q$. Com que aquest procés es pot repetir indefinidament, hi ha infinits primers. ■

També ens podem preguntar si podem trobar molts primers entre els termes d'una successió aritmètica donada. Concretament, si a i r són dos enters positius, podem considerar els enters de la forma $a + rx$, amb $x \geq 0$. Òbviament, si $g = \gcd(a, r) > 1$, tindrem $g \mid a + rx$ i per tant com a molt hi haurà un primer en el conjunt $\{a + rx \mid x \geq 0\}$. En canvi, tenim el següent resultat, del qual no tindrem temps de fer la demostració.

Teorema 1.2.5 — Dirichlet. Siguin a, r dos enters coprimers. Aleshores hi ha infinits primers de la forma $a + rx$, amb $x \in \mathbb{Z}$.

Si ens interessa enumerar els primers, podem fer servir l'anomenat *garbell d'Eratòstenes*, que ens dona tots els primers menors que un enter donat n. Es tracta d'anar traient de la llista tots els múltiples de p, on p és el primer element de la llista (que forçosament haurà de ser primer). Només cal mirar fins a $\sqrt{n}$, ja que si un enter m no és primer, aleshores necessàriament ha de tenir un factor primer menor que $\sqrt{m}$.

Algoritme 1.2.1 Retorna una llista dels primers menors que n

```
def garbell(n):
    if n <= 2:
        return []
    elif n == 3:
        return [2]
    else:
        P = [2] # El primer més petit és el 2
        X = range(3,n,2) # Inicialitzem amb els senars < n.
        p = X[0]
        while p * p <= n:
            P.append(p)
            X = [x for x in X if x % p != 0]
            p = X[0]
        P += X
        return P
```

1.3 Els enters mòdul n

Donat un enter positiu n, considerarem el morfisme d'anells

$$\text{red}\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad a \mapsto a \bmod n.$$

Direm que $a \equiv b \pmod{n}$ si $\text{red}(a) = \text{red}(b)$ (com a elements de $\mathbb{Z}/n\mathbb{Z}$). És a dir, si $n \mid a-b$.

Proposició 1.3.1 — Cancel·lativitat. Si $\gcd(c,n) = 1$ i $ac \equiv bc \pmod{n}$, llavors $a \equiv b \pmod{n}$.

Demostració. Farem servir el teorema fonamental de l'aritmètica: suposem que n divideix $ac - bc = (a-b)c$ i $\gcd(c,n) = 1$. Aleshores, si una potència d'un primer p divideix exactament a n (que escriurem $p^k \parallel n$), necessàriament $p^k \parallel (a-b)$ (ja que $p \nmid c$). Per tant, $n \mid (a-b)$, que és equivalent a $a \equiv b \pmod{n}$. ■

1.3.1 Inversos mòdul n

Considerem el grup d'unitats $(\mathbb{Z}/n\mathbb{Z})^\times$ de l'anell $\mathbb{Z}/n\mathbb{Z}$. Ens interessa saber quins elements de $\mathbb{Z}/n\mathbb{Z}$ són unitats.

Proposició 1.3.2 Si $\gcd(a,n) = 1$, aleshores l'aplicació

$$m_a\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto ax$$

és una bijecció.

Demostració. Com que m_a és un morfisme de grups (amb la suma), podem parlar del nucli $\ker m_a$. Fixem-nos que, com que $\gcd(a,n) = 1$, la Proposició 1.3.1 ens garanteix

$$ax \equiv 0 \pmod{n} \implies x \equiv 0 \pmod{n},$$

i per tant $\ker m_a = \{0\}$, i m_a és injectiva. Com que els conjunts de sortida i d'arribada són finits i iguals, necessàriament m_a és exhaustiva. ■

Corol·lari 1.3.3 — Unitats de $\mathbb{Z}/n\mathbb{Z}$. El grup d'unitats de $\mathbb{Z}/n\mathbb{Z}$ és

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n) = 1\}.$$

Demostració. Si $\gcd(a,n) = 1$, aleshores la proposició anterior (de fet, l'exhaustivitat d'm_a) ens garanteix l'existència d'un element x tal que $ax \equiv 1 \pmod{n}$, és a dir que a és invertible a $\mathbb{Z}/n\mathbb{Z}$.

Recíprocament, si $x \in \mathbb{Z}$ satisfà $ax \equiv 1 \pmod{n}$, aleshores existeix $y \in \mathbb{Z}$ tal que

$$ax + ny = 1.$$

Suposem que $d \mid a$ i $d \mid n$. Per l'equació anterior, $d \mid ax + ny = 1$, i per tant $d = 1$. Concloem que $\gcd(a,n) = 1$. ■

Remarca 1.3.4 Fixem-nos que si $a \in \mathbb{Z}/n\mathbb{Z}$ té sentit parlar de $\gcd(a,n)$, pensant en $\gcd(\hat{a},n)$ on $\hat{a}$ és un enter qualsevol tal que $\mathrm{red}(\hat{a}) = a$. Si prenem un altre aixecament $\hat{a} + tn$, aleshores $\gcd(\hat{a} + tn, n) = \gcd(\hat{a}, n)$, i per tant no depèn de quin hem triat.

Donarem un nom al cardinal d'aquest grup finit.

Definició 1.3.5 La funció φ *d'Euler* assigna a un enter positiu n el valor

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{1 \leq a \leq n \mid \gcd(a,n) = 1\}.$$

Per exemple, $\varphi(p) = p - 1$ si p és primer i, de fet, és fàcil de veure que, per tot $k \geq 1$,

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

Més endavant veurem com determinar $\varphi(n)$ en general, si coneixem la factorització d'n en producte de primers.

El que hem desenvolupat fins aquí ens permet resoldre totes les equacions lineals mòdul n.

Proposició 1.3.6 L'equació $ax \equiv b \pmod{n}$ té solució si i només si $\gcd(a,n) \mid b$.

Demostració. Sigui $g = \gcd(a,n)$. Si x és una solució de $ax \equiv b \pmod{n}$, aleshores $n \mid ax - b$. Com que $g \mid a$ i $g \mid n$, aleshores $g \mid b$.

Recíprocament, suposem que $g \mid b$. Aleshores $g \mid a$, $g \mid b$, i $g \mid n$. Per tant, $n \mid (ax - b)$ si i només si

$$\frac{n}{g} \mid \left(\frac{a}{g}x - \frac{b}{g}\right).$$

Però ara $\gcd(a/g, n/g) = 1$ i, per tant, es té una solució de $a/g\,x \equiv b/g \pmod{n/g}$. ■

1.3.2 El petit teorema de Fermat i el teorema d'Euler

Recordem un teorema bàsic de la teoria de grups, conegut com el teorema de Lagrange: si G és un grup finit aleshores l'ordre de qualsevol subgrup $H \subseteq G$ divideix l'ordre de G. Això ens servirà per demostrar dos teoremes atribuits a Euler i Fermat:

Teorema 1.3.7 — Euler. Sigui $\gcd(a,n) = 1$. Aleshores

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

Demostració. Considerem $G = (\mathbb{Z}/n\mathbb{Z})^\times$, i $H = \langle a \rangle \subseteq G$. Aleshores el teorema de Lagrange ens diu que $\#H = \mathrm{ord}(a) \mid \#G = \varphi(n)$. Per tant, $a^{\varphi(n)}$ és la identitat a G, com volíem veure. ■

Corol·lari 1.3.8 — Petit teorema de Fermat. Si p és un primer i $p \nmid a$, aleshores

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

Remarca 1.3.9 Observem que el recíproc no és cert. Per exemple, $2^{340} \equiv 1 \pmod{341}$ i $341 = 11 \cdot 31$. En aquest cas, però, es compleix $3^{340} \equiv 56 \pmod{341}$. Ens podem plantejar, doncs si és cert que si n és compost aleshores podem trobar un enter a coprimer amb n tal que $a^{n-1} \not\equiv 1 \pmod{n}$. Això tampoc és cert, i als nombres que incompleixen aquest principi (per exemple $561 = 3 \cdot 11 \cdot 17$) se'ls anomena *nombres de Carmichael*. Més endavant n'estudiarem algunes de les seves propietats.

1.3.3 El teorema de Wilson

El següent resultat ens dona una caracterització dels primers en termes de congruències.

Proposició 1.3.10 — Teorema de Wilson. Un enter $n > 1$ és primer si i només si

$$(n-1)! \equiv -1 \pmod{n}.$$

Demostració. Suposem primer que la congruència és certa però que n no és primer. Prenem llavors un factor primer $\ell \mid n$ de n. Tenim, per una banda, que $\ell \mid (n-1)!$, i també que $\ell \mid n \mid (n-1)!+1$. Però aleshores $\ell \mid 1$, que és una contradicció.

D'altra banda, si $n > 2$ és primer (per $n = 2$ ho podem verificar directament), aleshores fixem-nos que els factors que apareixen en el producte

$$(n-1)! = \prod_{a=1}^{n-1} a$$

són representants de tots els elements de $(\mathbb{Z}/n\mathbb{Z})^\times$. En particular, per cada a que apareix en el producte també apareix $b \equiv a^{-1} \pmod{n}$, que es cancel·larà. L'única manera que aquests dos termes no es cancel·lin és si $b = a$, és a dir si $a^2 \equiv 1 \pmod{n}$, i això només passa per $a = 1$ i $a = n-1$. Per tant, tenim $(n-1)! \equiv n-1 \equiv -1 \pmod{n}$, com volíem demostrar. ■

Fixem-nos que no és un mètode pràctic per decidir si n és primer, ja que per calcular el factorial de $n-1$ calen prop de n operacions. Més endavant veurem altres mètodes que ens permetran demostrar que un nombre és compost, o bé donar-nos molta seguretat sobre el fet que és primer (si ho és).

1.3.4 El teorema xinès dels residus

Teorema 1.3.11 Si $m_1, \ldots, m_k$ són enters coprimers dos a dos, aleshores el morfisme d'anells

$$\mathbb{Z}/(m_1 \cdots m_k)\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}, \quad a \mapsto (a \bmod m_1, \ldots, a \bmod m_k)$$

és un isomorfisme.

La demostració d'aquest teorema es redueix fàcilment, com veurem, al cas $k = 2$. En aquest cas, podem veure que el teorema es diu el següent:

Proposició 1.3.12 Siguin $m, n \in \mathbb{Z}$ enters amb $\gcd(m,n) = 1$. Aleshores, donats $a, b \in \mathbb{Z}$, el

sistema d'equacions

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

té solució, que és única mòdul mn.

Demostració. Busquem x de la forma

$$x = a + tm,$$

per algun t tal que $a + tm \equiv b \pmod{n}$. Aquesta equació té solució perquè $\gcd(m,n) = 1$, tal i com hem vist a la Proposició 1.3.6.

Per veure la unicitat, considerem dues solucions x i y. Aleshores $z = x - y$ és divisible per n i m. Com que $\gcd(m,n) = 1$, tenim $nm \mid z$, i per tant $z \equiv 0 \pmod{mn}$, d'on tenim que $x \equiv y \pmod{mn}$. ■

Demostració (del Teorema 1.3.11). Farem inducció en $k \geq 1$, on el cas $k = 1$ és trivial. Considerarem $k \geq 2$. Per veure l'exhaustivitat cal trobar, donats $a_1, \ldots, a_k$, un enter $x \in \mathbb{Z}$ tal que

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

Aplicant la proposició anterior, el conjunt de solucions de les dues primeres equacions és el mateix que el conjunt de solucions de

$$x \equiv a_{12} \pmod{m_1 m_2},$$

on a_{12} és la solució proporcionada per la Proposició. Per tant, ens reduïm al sistema

$$\begin{aligned} x &\equiv a_{12} \pmod{m_1 m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

que té una solució única mòdul $m_1 m_2 \cdots m_k$, per hipòtesi d'inducció. ■

Tenim una versió del teorema xinès dels residus pels grups d'unitats.

Lema 1.3.13 Si $m_1, \ldots, m_k$ són enters coprimers entre si, aleshores el morfisme de grups

$$(\mathbb{Z}/(m_1 \cdots m_k)\mathbb{Z})^\times \to (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})^\times, \quad a \mapsto (a \bmod m_1, \ldots, a \bmod m_k)$$

és un isomorfisme.

Demostració. Si $\gcd(a, m_1 \cdots m_k) = 1$, aleshores $\gcd(a, m_i) = 1$ per a tot $i = 1, \ldots, k$. Per tant, l'aplicació està ben definida.

La injectivitat és automàtica, pel fet que es tracta de la restricció del morfisme d'anells del teorema xinès dels residus.

Per veure l'exhaustivitat, observem que el teorema xinès dels residus ens garanteix, donats $a_i \in \mathbb{Z}/m_i\mathbb{Z}$, un element $a \in \mathbb{Z}/(m_1 \cdots m_k)\mathbb{Z}$ que tal que $a \pmod{m}_i = a_i$. Ara bé, si sabem que $\gcd(a_i, m_i) = 1$ per a tot i, aleshores $\gcd(a, m_i) = 1$ per a tot i, i d'aquí obtenim (pel Teorema 1.2.3) que $\gcd(a, m) = 1$. ■

En teoria de nombres, una funció f s'anomena *multiplicativa* si $f(mn) = f(m)f(n)$ sempre i quan $\gcd(m,n) = 1$. Si $f(mn) = f(m)f(n)$ per a tot m,n aleshores s'anomena *completament multiplicativa*.

Corol·lari 1.3.14 La funció φ d'Euler és multiplicativa: si $\gcd(m,n) = 1$, aleshores

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

Demostració. Només cal prendre cardinalitats en el lema anterior. ■

Com a conseqüència de la multiplicativitat de φ, podem donar una fórmula per $\varphi(n)$ en termes de la factorització de n.

Proposició 1.3.15 Sigui $n \geq 1$ un enter que factoritza com $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Aleshores

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1).$$

Remarca 1.3.16 En general, és difícil calcular $\varphi(n)$ eficientment sense conèixer una factorització de n. Per exemple, si $n = pq$ és el producte de dos primers, aleshores la informació que ens dona saber $\varphi(n)$ ens permet calcular la factorització de n de manera molt ràpida: considerem el polinomi $X^2 - 2sX + n$, on $s = \frac{n+1-\varphi(n)}{2}$. Aquest polinomi té p i q com a arrels, que podem trobar calculant:

$$p, q = s \pm \sqrt{s^2 - n}.$$

La funció φ també satisfà una propietat que ens serà útil més endavant.

Proposició 1.3.17 Per a tot $n \geq 1$ es té:

$$\sum_{\substack{d \geq 1 \\ d \mid n}} \varphi(d) = n$$

Demostració 1 (fent servir teoria de grups). Observem que per a tot d, $\varphi(d)$ és el nombre de generadors d'un grup cíclic d'ordre d. Considerem doncs un grup cíclic G d'ordre n. Diem que dos elements $x, y \in G$ estan relacionats si $\langle x \rangle = \langle y \rangle$. El nombre d'elements a la classe de x és $\varphi(d)$ si x té ordre d, i G té un únic subgrup d'ordre d per cada divisor $d \mid n$, d'on obtenim la fórmula. ■

Demostració 2 (elemental). Anomenem $f(n)$ al terme de l'esquerra, i volem veure que $f(n) = n$. Primer veurem que f és multiplicativa: considerem enters coprimers m i n. Donat un enter k, denotem per $\Delta(k)$ el conjunt dels seus divisors positius. Aleshores es té una bijecció $\Delta(m) \times \Delta(n) \to \Delta(mn)$, donada per $(d_1, d_2) \mapsto d_1 d_2$ (comproveu-ho). Per tant:

$$\begin{aligned} f(mn) &= \sum_{d \in \Delta(mn)} \varphi(d) = \sum_{d_1 \in \Delta(m)} \sum_{d_2 \in \Delta(n)} \varphi(d_1 d_2) \\ &= \sum_{d_1 \in \Delta(m)} \sum_{d_2 \in \Delta(n)} \varphi(d_1)\varphi(d_2) \\ &= \sum_{d_1 \in \Delta(m)} \varphi(d_1) \sum_{d_2 \in \Delta(n)} \varphi(d_2) = f(m)f(n). \end{aligned}$$

Per tant, només cal comprovar que $f(p^k) = p^k$ per a tot primer p i tot $k \geq 1$. Els divisors de p^k són de la forma p^r amb $0 \leq r \leq k$, i per tant:

$$f(p^k) = \sum_{r=0}^{k} \varphi(p^r) = 1 + \sum_{r=1}^{k} (p-1)p^{r-1} = p^k.$$

■

1.4 Mètodes efectius per inversos i exponenciació

El primer que veurem és com es pot trobar de manera efectiva l'invers d'un element a mòdul n, és a dir, com resoldre l'equació $ax \equiv 1 \pmod{n}$, suposant que $\gcd(a,n) = 1$. L'eina clau ens la dona el que es coneix com la identitat de Bézout.

Proposició 1.4.1 — Identitat de Bézout. Siguin $a, b \in \mathbb{Z}$ i $g = \gcd(a,b)$. Aleshores existeixen $x, y \in \mathbb{Z}$ tals que

$$g = ax + by. \tag{1.1}$$

Com que la demostració es pot fer constructiva, començarem amb un exemple, que podrem convertir en un algoritme que ens proporcioni la demostració.

■ **Exemple 1.4.2** Prenem $a = 120$, $b = 53$. Ja veiem que $\gcd(a,b) = 1$, però el que farem serà aplicar l'algoritme d'Euclides i aprofitar tota la informació que ens dona:

$$\begin{aligned}
120 &= \underline{2} \cdot 53 + 14 \\
53 &= \underline{3} \cdot 14 + 11 \\
14 &= \underline{1} \cdot 11 + 3 \\
11 &= \underline{3} \cdot 3 + 2 \\
3 &= \underline{1} \cdot 2 + 1
\end{aligned}$$

Ara aprofitem les equacions anteriors, per escriure:

$$\begin{aligned}
14 &= 120 - 2 \cdot 53 \\
11 &= 53 - 3 \cdot 14 = 53 - 3 \cdot (120 - 2 \cdot 53) = -3 \cdot 120 + 7 \cdot 53 \\
3 &= 14 - 1 \cdot 11 = (120 - 2 \cdot 53) - 1 \cdot (-3 \cdot 120 + 7 \cdot 53) = 4 \cdot 120 - 9 \cdot 53 \\
2 &= 11 - 3 \cdot 3 = (-3 \cdot 120 + 7 \cdot 53) - 3 \cdot (4 \cdot 120 - 9 \cdot 53) = -15 \cdot 120 + 34 \cdot 53 \\
1 &= 3 - 1 \cdot 2 = (4 \cdot 120 - 9 \cdot 53) - 1 \cdot (-15 \cdot 120 + 34 \cdot 53) = 19 \cdot 120 - 43 \cdot 53.
\end{aligned}$$

Fixem-nos que podem rescriure les igualtats anteriors fent servir "coordenades" respecte la parella $(120, 53)$:

$$\begin{aligned}
14 &= (1,0) - \underline{2} \cdot (0,1) = (1,-2) \\
11 &= (0,1) - \underline{3} \cdot (1,-2) = (-3,7) \\
3 &= (1,-2) - \underline{1} \cdot (-3,7) = (4,-9) \\
2 &= (-3,7) - \underline{3} \cdot (4,-9) = (-15,34) \\
1 &= (4,-9) - \underline{1} \cdot (-15,34) = (19,-43)
\end{aligned}$$

Observem que els nombres subratllats són justament els quocients que hem anant obtenint en les divisions successives. ■

L'exemple anterior ens dona la idea de l'algoritme conegut com "algoritme d'Euclides extès":

Algoritme 1.4.1 Donats $a, b > 0$, retorna enters g, x i y satisfent $g = \gcd(a,b)$ i $ax + by = g$

```
def xgcd(a,b):
    x, y, r, s = 1, 0, 0, 1
    while b:
        q, c = a.quo_rem(b)
        a, b, r, s, x, y = b, c, x - q * r, y - q * s, r, s
    return a, x, y
```

Demostració (de la Proposició 1.4.1). Demostrarem que l'algoritme és correcte. Denotem els valors inicials per $a_0, b_0, r_0, s_0, x_0, y_0$ i els valors després de n iteracions per $a_n, b_n, r_n, s_n, x_n, y_n$. Podem suposar que $a_0, b_0 \geq 0$, i veurem per inducció que a cada iteració es té que

$$\begin{aligned} a_n &= ax_n + by_n \\ b_n &= ar_n + bs_n \\ \gcd(a_n, b_n) &= \gcd(a,b) \end{aligned}$$

Fixem-nos que el cas $n = 0$ és trivial. Ara bé:

1. $a_{n+1} = b_n$, $x_{n+1} = r_n$, $y_{n+1} = s_n$, i per tant (1) es redueix a observar que $b_n = ar_n + bs_n$, per hipòtesi d'inducció.
2. $b_{n+1} = c = a_n - qb_n$, i $r_{n+1} = x_n - qr_n$, $s_{n+1} = y_n - qs_n$. Per tant, (2) es redueix a observar que

$$\begin{aligned} ar_{n+1} + bs_{n+1} &= a(x_n - qr_n) + b(y_n - qs_n) \\ &= ax_n + by_n - q(ar_n + bs_n) \\ &= a_n - qb_n = b_{n+1}. \end{aligned}$$

3. Per hipòtesi d'inducció, tenim $\gcd(a_n, b_n) = \gcd(a,b)$. Aleshores:

$$\begin{aligned} \gcd(a_{n+1}, b_{n+1}) &= \gcd(b_n, a_n - qb_n) \\ &= \gcd(b_n, a_n) = \gcd(a,b). \end{aligned}$$

Quan l'algoritme acaba, $b_n = 0$ i per tant $\gcd(a,b) = \gcd(a_n, 0) = a_n$. A més, $a_n = ax_n + by_n$, i per tant $x = x_n$ i $y = y_n$ satisfan la identitat que busquem. ■

Remarca 1.4.3 Fixem-nos que la solució del teorema xinès dels residus es troba invertint m mòdul n, i per tant es basa en última instància en l'algoritme d'Euclides extès. Més concretament, com que $\gcd(m,n) = 1$, podem trobar enters x, y tals que

$$xm + yn = 1.$$

Aleshores podem definir $z = a + (b-a)xm = ayn + bxm$. Fixem-nos que:

$$ayn + bxm \equiv ayn \equiv a(1 - xm) \equiv a \pmod{m},$$

i

$$ayn + bxm \equiv bxm \equiv b(1 - yn) \equiv b \pmod{n}.$$

Fent servir la identitat de Bézout, és molt fàcil donar un algoritme per resoldre $ax = b \pmod{m}$:

Algoritme 1.4.2 Donats a, b i m retorna x satisfent $ax \equiv b \pmod{m}$

```
def resol_equacio_lineal(a,b,m):
    g, x, y = xgcd(a, m) # g = a * x + m * y
    q, r = b.quo_rem(g)
    if r != 0:
        raise ValueError("L'equació no té solució")
    else:
        return q * x
```

En particular, podem calcular inversos a $\mathbb{Z}/m\mathbb{Z}$:

Algoritme 1.4.3 Donats a i m coprimers, retorna a^* satisfent $aa^* \equiv 1 \pmod{m}$

```
def invers_mod(a,m):
    return resol_equacio_lineal(a,1,m)
```

El segon objectiu que ens proposem en aquesta secció és el de, donats enters a, r i m, calcular la quantitat $a^r \pmod{m}$. Com que ja sabem calcular inversos, suposarem que $r > 0$. Aleshores, podem suposar d'entrada que: $m \geq 2$ i que $0 \leq a \leq m$.

La manera naïf de calcular $a^r \pmod{m}$ consistiria en calcular primer a^r i després reduir mòdul m. Si r és gran, però, això ens faria treballar amb nombres molt grans (nombres amb r vegades el nombre de dígits d'a), mentre que el resultat és petit (busquem un nombre menor que m). Per tant, a cada operació ens interessa reduir el resultat parcial mòdul m.

L'altre problema que tenim és que, si r és gran, aleshores hauríem d'evitar fer $r-1$ multiplicacions (que és com probablement hem après a calcular a^r). En l'exemple següent veiem com podem fer-ho més ràpidament.

■ **Exemple 1.4.4** Suposem que volem calcular a^{25}. Observem que $25 = 16+8+1 = 2^4+2^3+1$. Per tant,

$$a^{25} = a^{2^4+2^3+1} = a^{2^4} \cdot a^{2^3} \cdot a = (((a^2)^2)^2)^2 \cdot ((a^2)^2)^2 \cdot a.$$

Aleshores, podem obtenir el resultat calculant primer a^2, després $a^4 = (a^2)^2$, després $a^8 = (a^4)^2$, després $a^{16} = (a^8)^2$ i, finalment $a^{25} = a^{16} \cdot a^8 \cdot a$ s'obté fent dos productes de les quantitats prèvies. En total, hem elevat al quadrat 4 vegades i hem fet 2 multiplicacions al final: aquestes 6 multiplicacions són bastant menys que les 24 que haurien calgut per obtenir el resultat de manera naïf. ■

Donem un algoritme que calcula $a^r \pmod{m}$ amb $O(\log(r))$ multiplicacions a $\mathbb{Z}/m\mathbb{Z}$.

Algoritme 1.4.4 Calcula $a^r \pmod m$, versió inicial

```
def exponentiate(a,r,m):
    result = 1
    powers = a % m
    while r:
        if r % 2 == 1:
            result = (result * powers) % m
        powers = powers ** 2 % m
        r //= 2
    return result
```

Podem estalviar espai llegint els bits al revés. Vegem primer un exemple

■ **Exemple 1.4.5** Escrivim

$$a^{25} = a^{16+8+1} = a^{16+8} \cdot a = (a^4 \cdot a^2)^4 \cdot a = (((a^2 \cdot a)^2)^2)^2 \cdot a.$$

En aquest cas, amb una sola variable podem anar desant el resultat parcial. ■

Obtindrem la següent funció:

Algoritme 1.4.5 Calcula $a^r \pmod m$, versió millorada

```
def exponentiate_reverse(a,r,m):
    result = 1
    for bit in reversed(r.bits()):
        result = result**2 % m
        if bit == 1:
            result = (result * a) % m
    return result
```

1.5 Aplicacions a la criptografia

Els algoritmes que hem vist fins ara ens permeten descriure protocols clàssics en la criptografia. Un d'aquests (RSA) porta dècades utilitzant-se a la pràctica.

1.5.1 Diffie–Hellman

L'intercanvi de claus de Diffie–Hellman funciona de la manera següent. Les dues parts, Alice i Bob, fixen un grup cíclic G, de cardinal N. Alice i Bob fixen també un generador $g \in G$, que a l'igual que G (i N) també serà públic. El protocol funciona de la manera següent:

1. Alice escull un enter a l'atzar $1 < a < N$, i envia la quantitat $A = g^a$ a Bob.
2. Bob, per la seva banda, escull un enter a l'atzar $1 < b < N$, i envia la quantitat $B = g^b$ a l'Alice.
3. Alice i Bob calculen respectivament $S_a = B^a$ i $S_b = A^b$. Observem que els dos elements són iguals a $S = g^{ab} \in G$, que serà el secret compartit.

Primer de tot, observem que els càlculs involucrats es poden fer de manera eficient gràcies a l'exponenciació modular, si tenim una manera eficient de calcular en G.

Un possible exemple de grup cíclic que funciona en aquest cas és $G = (\mathbb{Z}/p\mathbb{Z})^\times$ i $N = p-1$ (on p és un primer). En aquest cas, per trobar un generador g de manera fàcil, el que es fa és triar

un primer p de la forma $p = 2q+1$ amb q primer, i així per veure que $g \neq \pm 1$ té ordre $p-1$ només cal comprovar (mitjançant exponenciació modular) que $g^q \equiv -1 \pmod{p}$.

Fixem-nos que un observador Eve que tingui accés a tota la comunicació sap els valors de $g^a \pmod{p}$ i $g^b \pmod{p}$. El *problema de Diffie–Hellman* consisteix a calcular $g^{ab} \pmod{p}$ donats $g^a \pmod{p}$ i $g^b \pmod{p}$. Al 2021, no coneixem[1] cap algoritme que resolgui aquest problema sense resoldre el *problema del logaritme discret*: donats A i g, trobar a tal que $g^a \equiv A \pmod{p}$.

1.5.2 El xifrat ElGamal

Una variant del protocol de Diffie–Hellman ens permet establir un sistema de xifrat de clau pública basat en el logaritme discret.

Preparació: Cada usuari tria un grup cíclic $G = \langle g \rangle$ de tamany N. Seguidament, tria un enter $2 < s < N$ i calcula $K = g^s$. La clau pública de l'Alice serà la tupla (G, N, g, K), i la clau secreta serà s.

Xifrat: Suposem que l'Alice vol enviar un missatge $m \in G$ a en Bob, que té clau pública (G, N, g, K_B). L'Alice tria un enter a l'atzar, $2 < y < N$, i calcula $Y = g^y$ i també $Z = mK_B^y$. Aleshores envia a en Bob la tupla (Y, Z).

Desxifrat: Per recuperar el missatge, en Bob calcula $Y^{-s}Z$. Observem que

$$Y^{-s}Z = g^{-sy}mg^{sy} = m.$$

Fixem-nos que la part de preparació s'assembla molt al que fa l'Alice en el protocol Diffie–Hellman, mentre que la part de xifrat s'assembla al que faria en Bob, amb la diferència que la part "secreta" y va canviant a cada missatge. Aleshores la part "pública" Y permet acordar un secret comú (que seria $Y^s = g^{sy} = K_B^y$), i que és justament el secret que s'ha fet servir per emmascarar el missatge m.

Si un possible atacant que tingui accés a la comunicació vol recuperar el missatge m a partir de (Y, Z), haurà de trobar el secret a partir de $Y = g^y$ i de $K_B = g^s$, i això és precisament el problema de Diffie–Hellman, que estem assumint igual de difícil que el problema del logaritme discret.

1.5.3 El xifrat RSA

Com en el cas anterior, es tracta d'establir un protocol que permeti a qualsevol usuari d'escriure un missatge xifrat de manera que només el receptor pretés el pugui desxifrar.

Preparació: Cada usuari escull dos primers grans p i q, i calcula el producte $N = pq$ i $\varphi(N) = (p-1)(q-1)$. Aleshores tria un enter $1 < e < \varphi(n)$, i fent servir l'algoritme que hem vist abans calcula el seu invers mòdul $\varphi(n)$: calcula d amb $de \equiv 1 \pmod{\varphi(n)}$. Així, cada usuari té una clau pública (N, e) i una clau privada $(\varphi(N), d)$.

Xifrat: Suposem ara que l'Alice vol enviar un missatge a en Bob, que té clau pública (N_B, e_B). Podem suposar que el missatge està codificat com un enter $1 < m < N_B$ coprimer amb N_B. Aleshores l'Alice calcula $c = m^{e_B} \bmod N_B$, que serà el missatge xifrat.

Desxifrat: Per recuperar el missatge, en Bob calcula $c^{d_B} \bmod N_B$.

Vegem que

$$c^{d_B} \equiv m^{e_B d_B} \equiv m^{1+t\varphi(N_B)} \equiv m \pmod{N_B},$$

i per tant en Bob pot desxifrar el missatge. Sense saber quant val $\varphi(N_B)$, no es pot trobar d_B a partir de e_B i, per tant, la seguretat del sistema rau en la dificultat de factoritzar N_B (vegeu la Remarca 1.3.16). Més endavant veurem algoritmes per factoritzar enters, però els millors mètodes són sub-exponencials, fet que els fa inviables[2] per certs nombres de més de 260 decimals.

[1] S'entén la comunitat acadèmica.

[2] Almenys al 2020! El febrer de 2020 un equip de 6 matemàtics va aconseguir factoritzar l'RSA-250, que té 250 dígits decimals.

2. La llei de reciprocitat quadràtica

2.1 Residus quadràtics i el símbol de Legendre

L'objectiu d'aquesta secció és estudiar les solucions d'equacions quadràtiques mòdul un primer p. Concretament, ens fixarem en l'equació $x^2 \equiv a \pmod{p}$.

Definició 2.1.1 Sigui p un primer. Diem que un enter a no divisible per p és un *residu quadràtic mòdul* p si a és un quadrat mòdul p. Si no, direm que a és un *no-residu quadràtic mòdul* p.

Observem que, si $a \equiv a' \pmod{p}$ aleshores a és un residu quadràtic mòdul p si i només si a' ho és. Per tant, donat p és fàcil donar una llista de tots els residus quadràtics mòdul p.

■ **Exemple 2.1.2** L'1 és l'únic residu quadràtic tant mòdul 2 com mòdul 3. Els residus quadràtics mòdul 5 són l'1 i el 4, perquè $1^2 \equiv 1$, $2^2 \equiv 4$, i $3^2 \equiv (-2)^2$, $4^2 \equiv (-1)^2$.

Els residus quadràtics mòdul 7 són $\{1,2,4\}$.

Els residus quadràtics mòdul 11 són $\{1,3,4,5,9\}$. ■

Introduim una notació que va bé per parlar d'aquest concepte.

Definició 2.1.3 El *símbol de Legendre* es defineix, donats un primer **senar** p i un enter a, com

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

Si a i b són residus quadràtics, posem $a \equiv x^2 \pmod{p}$ i $b \equiv y^2 \pmod{p}$, aleshores és clar que $ab \equiv (xy)^2 \pmod{p}$ i, per tant ab també és un residu quadràtic. De manera semblant, si $a \equiv x^2 \pmod{p}$ i $ab \equiv y^2 \pmod{p}$, aleshores $b \equiv (x^{-1}y)^2 \pmod{p}$, del que en deduïm que el producte d'un residu amb un no-residu és un no-residu. El següent lema ens diu que el producte de dos no-residus és un residu.

Lema 2.1.4 Si p és un primer senar, l'aplicació $\psi\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$, $a \mapsto \left(\frac{a}{p}\right)$ és un morfisme de grups exhaustiu.

Demostració. Fem servir que $G = (\mathbb{Z}/p\mathbb{Z})^\times$ és cíclic. El nucli de l'aplicació ψ el formen els quadrats, un subgrup (normal) H d'índex 2. Per tant ψ és la composició de

$$G \twoheadrightarrow G/H \cong \{\pm 1\}.$$

■

2.2 LRQ i demostració

Durant el segle XVIII, diversos matemàtics es van preguntar si hi havia una manera senzilla de predir com es comporta $\left(\frac{a}{p}\right)$ quan variava p. Per exemple, quan $a = 5$ obtenim la Taula 2.1.

p	7	**11**	13	17	**19**	23	**29**	**31**	37	**41**	43	47
$\left(\frac{5}{p}\right)$	-1	**1**	-1	-1	**1**	-1	**1**	**1**	-1	**1**	-1	-1
$p \bmod 5$	2	**1**	3	2	**4**	3	**4**	**1**	2	**1**	3	2

Taula 2.1: Taula de $\left(\frac{5}{p}\right)$ per diversos primers.

Fixem-nos que sembla que el símbol $\left(\frac{5}{p}\right)$ només depengui de si $p \equiv 1,4 \pmod 5$ o no. En canvi, si fem el mateix amb $a = 7$ obtenim la Taula 2.2. Ara observem que no sembla d'entrada que

p	11	13	17	**19**	23	**29**	**31**	**37**	41	43	**47**	**53**	**59**	61
$\left(\frac{7}{p}\right)$	-1	-1	-1	**1**	-1	**1**	**1**	**1**	-1	-1	**1**	**1**	**1**	-1
$p \bmod 7$	4	6	3	**5**	2	**1**	**3**	**2**	6	1	**5**	**4**	**3**	5

Taula 2.2: Taula de $\left(\frac{7}{p}\right)$ per diversos primers.

hi hagi una relació tan senzilla. En canvi, per $a = 11$ tornem a observar el mateix comportament que per $a = 5$ (quant val $\left(\frac{9}{p}\right)$?). El teorema següent explica aquest fenòmen de manera molt precisa.

Teorema 2.2.1 — Llei de Reciprocitat Quadràtica de Gauss. Siguin p i q dos primers senars. Aleshores

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right) = \begin{cases} +\left(\frac{q}{p}\right) & p \equiv 1 \pmod 4 \text{ o } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & p \equiv 3 \pmod 4 \text{ i } q \equiv 3 \pmod 4 \end{cases}.$$

A més,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4, \end{cases} \quad \left(\frac{2}{p}\right) = \begin{cases} +1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8. \end{cases}$$

Fixem-nos que, si posem $p = 5$, el teorema anterior ens dona que

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & p \equiv 1,4 \pmod 5, \\ -1 & p \equiv 2,3 \pmod 5. \end{cases}$$

En canvi, si $p=7$, el signe $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}=(-1)^{\frac{q+1}{2}}$ depèn de com sigui q mòdul 4. Com que $\left(\frac{q}{7}\right)$ depèn de q mòdul 7, la quantitat $\left(\frac{7}{q}\right)$ depèn de q mòdul 28. De fet,

$$\left(\frac{7}{p}\right)=\begin{cases}1 & p\equiv 1,3,9,19,25,27 \pmod{28}\\ -1 & p\equiv 5,11,13,15,17,23 \pmod{28}\\ 0 & p=7.\end{cases}$$

La LRQ també ens permet calcular ràpidament els símbols de Legendre: per exemple, suposem que volem saber si 211 és un quadrat mòdul 653.

Com que $653\equiv 1 \pmod 4$,

$$\left(\frac{211}{653}\right)=\left(\frac{653}{211}\right),$$

i com que $653\equiv 20 \pmod{211}$,

$$\left(\frac{653}{211}\right)=\left(\frac{20}{211}\right)=\left(\frac{4\cdot 5}{211}\right)=\left(\frac{4}{211}\right)\left(\frac{5}{211}\right)=\left(\frac{5}{211}\right).$$

Com que $5\equiv 1 \pmod 4$,

$$\left(\frac{5}{211}\right)=\left(\frac{211}{5}\right)=\left(\frac{1}{5}\right)=1.$$

Concloem que 211 és un quadrat mòdul 653, però fixem-nos que aquest càlcul no ens permet dir quin és x tal que $x^2\equiv 211 \pmod{653}$ (solució: $118^2\equiv 211 \pmod{653}$).

Fixem-nos que per dur a terme el càlcul anterior cal factoritzar ($20=4\cdot 5$). Per nombres molt grans això seria un problema, però hi ha una generalització del símbol de Legendre (anomenat símbol de Jacobi) que solventa aquest problema.

2.2.1 Demostració de la LRQ

Sigui p un primer senar, i a un enter no divisible per p. El primer resultat que ens caldrà dona una manera eficient de calcular $\left(\frac{a}{p}\right)$, i ens servirà també per la demostració de la LRQ.

Proposició 2.2.2 — Criteri d'Euler.

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

Demostració. Si $a\equiv x^2 \pmod p$, aleshores

$$a^{\frac{p-1}{2}}\equiv x^{p-1}\equiv 1 \pmod p,$$

pel petit teorema de Fermat. Considerem ara la factorització

$$x^{p-1}-1=(x^{\frac{p-1}{2}}-1)(x^{\frac{p-1}{2}}+1).$$

El polinomi $x^{p-1}-1$ té com a molt $p-1$ arrels a $\mathbb{Z}/p\mathbb{Z}$. Com que tots els elements de $(\mathbb{Z}/p\mathbb{Z})^\times$ en són arrel, en deduïm que té exactament $p-1$ arrels. Aquestes s'han de dividir en arrels de cadascun dels factors. Com que la meitat d'elements (els quadrats) són arrel del primer factor, l'altra meitat (els no-quadrats) han de ser arrels del segon factor, i per tant si a és un no-quadrat,

$$a^{\frac{p-1}{2}}+1\equiv 0 \pmod p,$$

com voliem veure. ■

Observem que la proposició anterior demostra la fórmula per $\left(\frac{-1}{p}\right)$. Vegem ara la fórmula per $\left(\frac{2}{p}\right)$.

Proposició 2.2.3 Si p és un primer senar, aleshores

$$\left(\frac{2}{p}\right) = \varepsilon(p) = \begin{cases} +1 & p \equiv \pm 1 \pmod 8, \\ -1 & p \equiv \pm 3 \pmod 8. \end{cases}$$

Demostració. Considerem l'anell $R = \mathbb{Z}[\zeta]/(p)$ amb $\zeta = \zeta_8$. Pel criteri d'Euler,

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

i per tant serà útil trobar una arrel quadrada de 2 mòdul p. Fixem-nos que $\zeta^4 + 1 = 0$, o $\zeta^2 + \zeta^{-2} = 0$. Per tant, si escrivim $\tau = \zeta + \zeta^{-1}$, tenim

$$\tau^2 = (\zeta + \zeta^{-1})^2 = 2.$$

Deduïm que

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

Observem que, com que R és de característica p, tenim $\tau^p \equiv \zeta^p + \zeta^{-p} \pmod p$. Tenint en compte que $\zeta^8 = 1$, veiem que aquesta quantitat només depèn de $p \mod 8$, i coincideix amb $\varepsilon(p)\tau$.

Per tant, $\tau\left(\frac{2}{p}\right) \equiv \varepsilon(p)\tau \pmod p$ i, multiplicant per τ, obtenim

$$2\left(\frac{2}{p}\right) \equiv 2\varepsilon(p) \pmod p.$$

Com que p és senar, trobem finalment $\left(\frac{2}{p}\right) = \varepsilon(p)$. ■

Donat un primer p, denotarem per ζ_p el nombre complex $\zeta_p = e^{\frac{2\pi i}{p}}$. Recordem una propietat coneguda de ζ_p:

Lema 2.2.4 Es té, per a tot $a \in \mathbb{Z}$,

$$\sum_{n=0}^{p-1} \zeta_p^{an} = \begin{cases} p & p \mid a, \\ 0 & p \nmid a. \end{cases}$$

Demostració. Si $p \mid a$, aleshores $\zeta_p^a = 1$ i el resultat és obvi. En cas contrari, $\zeta_p^a \neq 1$, i per tant la suma geomètrica val

$$\sum_{n=0}^{p-1} \zeta_p^{an} = \frac{\zeta_p^{ap} - 1}{\zeta_p^a - 1} = 0.$$

■

Definim una suma semblant a l'anterior, però modificant el signe d'alguns dels seus termes.

Definició 2.2.5 La *suma de Gauss* associada a un element $a \in (\mathbb{Z}/p\mathbb{Z})$ és

$$\gamma_a = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{an}.$$

Lema 2.2.6 La suma de Gauss γ_0 val 0.

Demostració. Com que $\gamma_0 = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right)$ i hi ha la meitat d'elements que són residus quadràtics i la meitat que no ho són, la suma dels residus és 0. ■

Lema 2.2.7 Per a tot enter a, es té $\gamma_a = \left(\frac{a}{p}\right) \gamma_1$.

Demostració. Pel lema anterior, podem assumir que $p \nmid a$. Aleshores:

$$\left(\frac{a}{p}\right) \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{an} = \sum_{n=0}^{p-1} \left(\frac{an}{p}\right) \zeta_p^{an} = \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta_p^{m} = \gamma_1,$$

on hem fet servir que multiplicar per a permuta els elements de $\mathbb{Z}/p\mathbb{Z}$. El resultat s'obté multiplicant per $\left(\frac{a}{p}\right)$. ■

La base de la demostració de la Llei de reciprocitat quadràtica és el següent resultat.

Proposició 2.2.8 Per tot enter a coprimer amb p, es té que

$$\gamma_a^2 = (-1)^{\frac{p-1}{2}} p.$$

Demostració. Pel lema anterior, podem suposar que $a = 1$. Fixem-nos que, pel criteri d'Euler,

$$\gamma_a \gamma_{-a} = \left(\frac{a}{p}\right) \gamma_1 \left(\frac{-a}{p}\right) \gamma_1 = \left(\frac{-1}{p}\right) \gamma_1^2 = (-1)^{\frac{p-1}{2}} \gamma_1^2.$$

Per tant, caldrà veure que $\gamma_a \gamma_{-a} = p$. Per fer-ho, calculem (totes les sumes recorren els enters entre 1 i $p-1$).

$$\sum_a \gamma_a \gamma_{-a} = \sum_{a,m,n} \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) \zeta_p^{an-am} = \sum_{n,m} \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) \sum_a \zeta^{a(n-m)} = \sum_n p \left(\frac{n}{p}\right)^2 = p(p-1).$$

■

Demostració del Teorema 2.2.1. Treballarem a $\mathbb{Z}[\zeta_p]/(q)$, que és un anell de característica q. No hem aconseguit una arrel quadrada de p, sinó de $p^* = (-1)^{\frac{p-1}{2}} p$. Per tant, buscarem una formula per $\left(\frac{p^*}{q}\right)$ fent servir el criteri d'Euler:

$$\left(\frac{p^*}{q}\right) = (p^*)^{\frac{q-1}{2}} \equiv \gamma_1^{q-1} \pmod{q}.$$

Calculem

$$\gamma_1^q \equiv \left(\sum_n \left(\frac{n}{p}\right) \zeta_p^n\right)^q \equiv \sum_n \left(\frac{n}{q}\right) \zeta_p^{qn} \equiv \gamma_q \equiv \gamma_1 \left(\frac{q}{p}\right) \pmod{q}.$$

Com que γ_1 és invertible a $\mathbb{Z}[\zeta_p]/(q)$, podem simplificar γ_1 i obtenim

$$\left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod{q}.$$

Com que a R es pot distingir 1 de -1, d'aquesta congruència en deduïm la igualtat $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$. Per acabar, fixem-nos que

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

i per tant hem demostrat la LRQ. ■

2.3 El símbol de Jacobi

Donats un enter a i un *enter senar positiu* m, definim $\left(\frac{a}{m}\right) = \prod_{p^k \| m} \left(\frac{a}{p}\right)^k$, on en el producte de la dreta fem servir el símbol de Legendre. Observem que si m és un primer senar, aleshores aquesta definició coincideix amb el símbol de Legendre.

Lema 2.3.1 1. Si $a \equiv b \pmod{m}$ aleshores $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.
2. $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$ per a qualssevol a, b i qualsevol enter senar positiu m.
3. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$ per a qualsevol a i qualssevol enters senars positius m i n.

Remarca 2.3.2 Notem que si $\left(\frac{a}{m}\right) = -1$ aleshores a no és un quadrat mòdul m (ja que no ho és mòdul p per algun primer p que divideix m a una potència senar). Però en canvi, si $\left(\frac{a}{m}\right) = 1$ no podem deduir que a sigui un quadrat mòdul m. Per exemple, $\left(\frac{2}{15}\right) = 1$, però els quadrats mòdul 15 són $\{1,4,6,9,10\}$.

Per acabar, veiem que també es té una versió de la Llei de reciprocitat quadràtica.

Teorema 2.3.3 — Llei de Reciprocitat Quadràtica pel símbol de Jacobi. Siguin m i n dos enters positius senars i coprimers entre si. Aleshores

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right).$$

A més,

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} = \begin{cases} +1 & m \equiv 1 \pmod 4 \\ -1 & m \equiv 3 \pmod 4 \end{cases}, \quad \left(\frac{2}{m}\right) = \begin{cases} 1 & m \equiv \pm 1 \pmod 8 \\ -1 & m \equiv \pm 3 \pmod 8. \end{cases}$$

Demostració. Per la primera part, escrivim $m = \prod_i p_i$ i $n = \prod_j q_j$, amb p_i i q_j possiblement repetits. Aleshores

$$\left(\frac{m}{n}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right) = \prod_{i,j} \varepsilon(p_i,q_j) \left(\frac{q_j}{p_i}\right) = \left(\frac{n}{m}\right) \prod_{i,j} \varepsilon(p_i,q_j).$$

N'hi ha prou, doncs, amb trobar una fórmula per $\prod \varepsilon(p_i,q_j)$.

$$\varepsilon(p_i,q_j) = \prod_{i \equiv 3 \pmod 4} \prod_{j \equiv 3 \pmod 4} (-1).$$

Ara bé, fixem-nos que

$$\prod_{j\equiv 3 \pmod 4} (-1) = \begin{cases} 1 & m \equiv 1 \pmod 4 \\ -1 & m \equiv 3 \pmod 4 \end{cases}$$

i d'aquí obtenim la fórmula. Les lleis suplementàries es demostren de manera similar. ■

■ **Exemple 2.3.4** Suposem que volem saber si 7411 és un quadrat mòdul 9283. Primer hauríem de veure que els dos són primers (sí que ho són). Aleshores, com que els dos són $\equiv 3 \pmod 4$ obtenim

$$\left(\frac{7411}{9283}\right) = -\left(\frac{9283}{7411}\right) = -\left(\frac{1872}{7411}\right).$$

Si només fem servir el símbol de Legendre, ara hem de factoritzar $1872 = 2^4 \cdot 3^2 \cdot 13$. En canvi, fent servir el símbol de Jacobi només hem de treure les potències de 2:

$$\begin{aligned} -\left(\frac{1872}{7411}\right) &= -\left(\frac{2^4}{7411}\right)\left(\frac{117}{7411}\right) = -\left(\frac{7411}{117}\right) \\ &= -\left(\frac{40}{117}\right) = -\left(\frac{2}{117}\right)\left(\frac{5}{117}\right) = \left(\frac{5}{117}\right) = \left(\frac{117}{5}\right) = \left(\frac{2}{5}\right) = -1. \end{aligned}$$

A més, com que el resultat és -1, ja sabem que 7411 no és un quadrat mòdul 9283, encara que no haguem comprovat que són primers. ■

2.4 Aplicació: arrels quadrades mòdul p

En aquesta secció ens plantegem el problema de trobar les solucions d'una equació quadràtica $ax^2+bx+c=0$ a $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, amb $p \geq 3$ primer. De la fórmula quadràtica se'n despren que n'hi ha prou amb saber trobar l'arrel quadrada de $D = b^2-4ac$, si en té. Fent servir la llei de reciprocitat quadràtica, hem vist que podem determinar ràpidament si D és un quadrat, però que no obtenim informació sobre com trobar $\delta \in \mathbb{F}$ tal que $\delta^2 = D$.

Recordem que, si D és un quadrat, aleshores $D^{\frac{p-1}{2}} \equiv 1 \pmod p$. Per tant, $D^{\frac{p+1}{2}} \equiv D \pmod p$. Observem aleshores que, si $\frac{p+1}{2}$ és parell ($\iff p \equiv 3 \pmod 4$), aleshores $\delta = D^{\frac{p+1}{4}}$ satisfà $\delta^2 = D$.

A partir d'ara, doncs, suposarem que $p \equiv 1 \pmod 4$. Veurem dos algoritmes probabilístics per trobar δ.

2.4.1 Un primer algoritme

Considerem l'anell $R = \mathbb{F}_p[x]/(x^2-D)$, i escrivim $\sqrt{D}$ per la classe de x a R. Considerem el morfisme d'anells $\varphi\colon R \to \mathbb{F}_p$ que envia $a+b\sqrt{D} \mapsto a+b\delta$ (fixem-nos que encara no hem trobat δ, però en tot cas sabem que existeix).

Ara, triem un element $z \in \mathbb{F}_p^\times$ a l'atzar, i calculem (fent servir exponenciació eficient) la quantitat

$$(1+z\sqrt{D})^{\frac{p-1}{2}} = u+v\sqrt{D} \in R.$$

Com que $\varphi(u+v\sqrt{D}) = (1+\varphi(z)\delta)^{\frac{p-1}{2}}$ i $\#\mathbb{F}_p^\times = (p-1)$, necessàriament $u+v\delta \in \{0,1,-1\}$. Per tant, si $v \neq 0$ (si $v=0$, triem un altre $z \in \mathbb{F}_p^\times$ i repetim el procés), aleshores

$$\delta \in \{-u/v, (1-u)/v, (-1-u)/v\}.$$

Podem provar aquestes tres possibilitats i trobarem δ.

Algoritme 2.4.1 Donat D i un primer p, troba (si existeix) una arrel quadrada de D a $\mathbb{F}_p$.

```
def troba_arrel_quadrada(D, p):
    if (p+1) % 4 != 0: return D^((p+1)//4)
    R.<alpha> = GF(p)['x'].quotient(x^2-D)
    v = 0
    while v == 0:
        u, v = ((1 + GF(p).random_element() * alpha)^ZZ((p-1) / 2)).list()
    root = -u / v
    if root^2 == D: return root
    vinv = 1 / v
    root += vinv
    if root^2 == D: return root
    return root - 2 * vinv
```

2.4.2 L'algoritme de Cipolla

Treballarem també amb un anell de la forma $R = \mathbb{F}_p[x]/(x^2 - u)$, però l'arrel que adjuntarem no serà l'arrel de D, que ja sabem que és un quadrat, sino una que ens garanteixi que R és un cos. Concretament, hem de trobar $t \in \mathbb{F}_p$ tal que $u = t^2 - D$ sigui un no-quadrat a $\mathbb{F}_p$. La meitat de les possibles t funcionaran, perquè la meitat de residus són no-quadrats.

Teorema 2.4.1 Sigui $\delta = (t + \sqrt{u})^{\frac{p+1}{2}} \in R$. Aleshores:
1. $\delta^2 = D$, i
2. $\delta \in \mathbb{F}_p$.

Demostració. Primer calculem quant val $\sqrt{u}^p$: $\sqrt{u}^p = \sqrt{u}\sqrt{u}^{p-1} = \sqrt{u}u^{\frac{p-1}{2}} = -\sqrt{u}$, on a l'última igualtat hem fet servir el criteri d'Euler i el fet que u és un no-quadrat. Aleshores, per veure (1), calculem a R, que és de característica p, i recordem que $t \in \mathbb{F}_p$:

$$\delta^2 = (t + \sqrt{u})^{p+1} = (t + \sqrt{u})(t^p + \sqrt{u}^p) = (t + \sqrt{u})(t - \sqrt{u}) = t^2 - u = D.$$

Per veure (2), observem que el polinomi $x^2 - D$ té com a molt dues arrels en qualsevol cos. Hem vist que $\pm\delta$ són dues arrels quadrades, i sabem que $x^2 - D$ té dues arrels a $\mathbb{F}_p \subset R$ (perquè estem suposant que D és un quadrat a $\mathbb{F}_p$). Per tant, $\pm\delta$ han de ser les arrels que busquem a $\mathbb{F}_p$. ■

Com que podem calcular δ amb exponenciació modular a R, obtenim un algoritme per trobar l'arrel quadrada de D. Obtenim el següent algoritme.

Algoritme 2.4.2 Donat D i un primer p, troba (si existeix) una arrel quadrada de D a $\mathbb{F}_p$.

```
def troba_arrel_quadrada(D, p):
    assert legendre_symbol(D, p) == 1
    Fp = GF(p)
    u = 0
    while legendre_symbol(u, p) != -1:
        t = Fp.random_element()
        u = t^2 - D
    S.<x> = Fp['x']
    R.<w> = S.quotient(x^2 - u)
    return Fp(((t + w)^( (p+1) // 2)).lift())
```

3. Corbes el·líptiques

3.1 Definició i llei de grup

Definició 3.1.1 Una *corba el·líptica* sobre un cos K és una equació de la forma

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

on $a_1, a_2, a_3, a_4, a_6 \in K$ són tals que

$$\Delta_E = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \neq 0,$$

amb

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \text{ i} \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

Remarca 3.1.2 Si la característica de K és diferent de 2 i 3, aleshores es pot fer un canvi afí de variables que permet escriure E de forma

$$E: y^2 = x^3 + ax + b, \quad a, b \in K.$$

En aquest cas, el discriminant Δ_E té una expressió més senzilla:

$$\Delta_E = -16(4a^3 + 27b^2) = 16\,\mathrm{disc}(x^3 + ax + b).$$

Podem pensar una corba el·líptica E com un cert subconjunt de $\mathbb{P}^2$. En aquest cas cal considerar l'equació homogènia ($x = X/Z$, $y = Y/Z$)

$$E: Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Quan $Z = 0$, obtenim com a solució el punt projectiu $\mathscr{O} = (0:1:0)$, que anomenarem *punt a*

l'infinit d'E.

Donat un cos $L \supseteq K$, el conjunt de *punts definits a* L és

$$E(L) = \{(x,y) \in L \times L \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathscr{O}\}.$$

La importància de les corbes el·líptiques en la teoria de nombres prové del fet que el conjunt de punts $E(L)$ ve dotat d'una estructura de grup abelià. Ens serà útil el següent lema geomètric:

Lema 3.1.3 Tota recta interseca E en tres punts, si els comptem amb multiplicitat.

A més, si dos d'aquests punts tenen coordenades a una extensió L, també les hi té el tercer punt.

Demostració. Considerem una recta genèrica a $\mathbb{P}^2$, donada per l'equació

$$\alpha X + \beta Y + \gamma Z = 0, \quad \alpha, \beta, \gamma \in L.$$

Si $\alpha = \beta = 0$, aleshores es tracta de la recta a l'infinit, que interseca de manera triple amb $\mathscr{O}$ com podem comprovar fàcilment.

Suposem doncs que $\alpha \neq 0$ o $\beta \neq 0$, i per tant podem treballar amb la forma no-homogènia

$$\alpha x + \beta y + \gamma = 0.$$

Si $\alpha \neq 0$, aleshores substituint $x = \frac{-1}{\alpha}(\gamma + \beta y)$ a l'equació d'E obtenim un polinomi en y de grau 3, i per tant 3 solucions. També, si $\beta \neq 0$, substituint $y = \frac{-1}{\beta}(\gamma + \alpha x)$ s'obté un polinomi en x de grau 3 i, per tant les tres solucions.

Suposem que dos dels punts d'intersecció tenen coordenades a L. Notem que, per veure que un punt té coordenades a L només cal veure que o bé la seva coordenada x o bé la y és de L, ja que l'altra coordenada també ho serà fent servir l'equació de la recta. En els polinomis anteriors, que estan definits a K (en x o en y) el producte de les tres arrels és el terme constant i, per tant, és de $K \subseteq L$. Si dues de les arrels són d'L, aleshores la tercera també ho és.

■

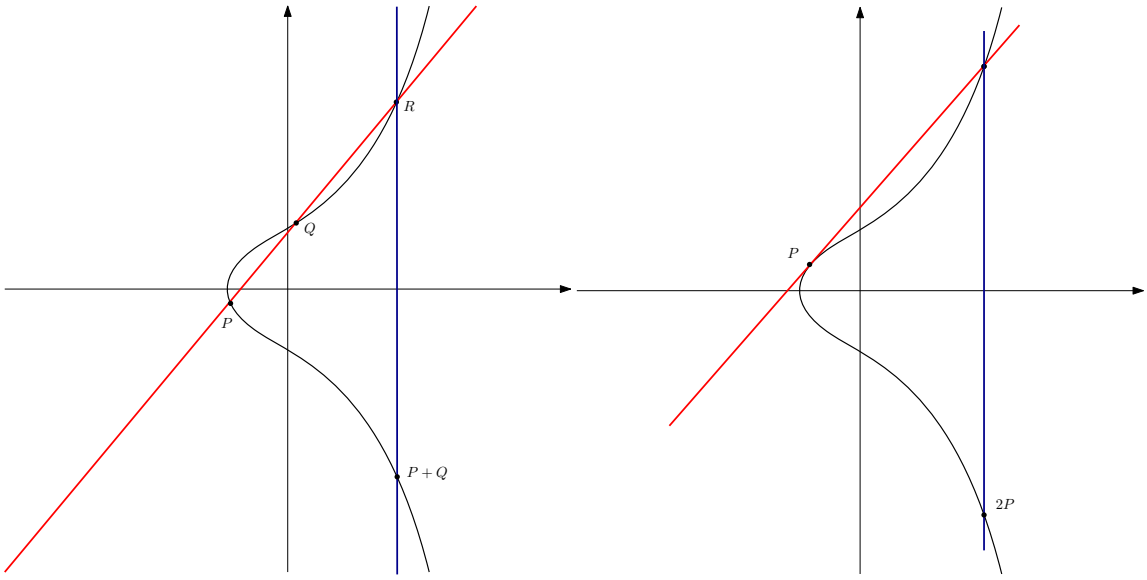

Figura 3.1: Suma de dos punts a E

Donats dos punts $P, Q \in E(K)$, considerem la recta que $\ell_{P,Q}$ que passa per P i Q (en cas que $P = Q$, aleshores $\ell_{P,P}$ serà la recta tangent a E que passa per P).

La recta $\ell_{P,Q}$ interseca en un altre punt $R \in E(K)$. Finalment, definim $P+Q$ com el tercer punt d'intersecció de la recta $\ell_{R,\mathscr{O}}$.

Òbviament aquesta operació és commutativa, i és fàcil veure que el punt de l'infinit $\mathscr{O}$ és l'element neutre.

Definim $-P$ com el tercer punt d'intersecció de la recta $\ell_{\mathscr{O},P}$. Per definició, $\ell_{P,-P} = \ell_{\mathscr{O},P}$, i per tant el punt R és justament $\mathscr{O}$. Ara, si prenem la recta tangent a E que passa per $\mathscr{O}$, obtenim la recta de l'infinit $\{z=0\}$, que talla E només a $\mathscr{O}$ (intersecció triple). Per tant, concloem que $P+(-P)=\mathscr{O}$.

L'associativitat d'aquesta operació no es veu tan trivialment, i en deixem la demostració per més endavant. Així, el conjunt de punts K-definits d'E adquireix una estructura addicional: és un grup abelià.

3.1.1 La llei de grup en coordenades

Donats punts $P_1=(x_1,y_1)$ i $P_2=(x_2,y_2)$ d'E, volem calcular $P_3=(x_3,y_3)=P_1+P_2$. Fixem-nos que, si $P_1=\mathscr{O}$ o $P_2=\mathscr{O}$ aleshores el resultat és clar. També si $P_2=-P_1$. Per tant, suposarem que aquest no és el cas. Per simplificar les fórmules, treballarem amb el model

$$y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

En aquest cas, fixem-nos que si $P=(x,y)$ aleshores $-P=(x,-y)$.

La recta ℓ_{P_1,P_2} té equació $y=\lambda(x-x_1)+y_1$, on

$$\lambda = \begin{cases} \frac{y_2-y_1}{x_2-x_1} & \text{si } P_1 \neq P_2, \\ \frac{3x_1^2+2a_2x_1+a_4}{2y_1} & \text{si } P_1 = P_2. \end{cases}$$

Substituint-ho a l'equació d'E, obtenim un polinomi de grau 3 en x, del qual ens fixarem en el terme de grau 2, que és $a_2-\lambda^2$. Aquest terme es correspon a $-(x_1+x_2+x_3)$ i, per tant, podem aïllar

$$x_3 = \lambda^2 - a_2 - x_1 - x_2.$$

La coordenada y de P_3 és l'oposat del punt d'intersecció que acabem de calcular. Per tant, obtenim:

$$y_3 = \lambda(x_1-x_3) - y_1.$$

Aquestes formules ens permeten verificar l'associativitat de la suma ajudant-nos de Sage.

Proposició 3.1.4 1. Si P,Q,R satisfan que els elements

$$\{P,-P,Q,-Q,R,-R,P+Q,-(P+Q),(Q+R),-(Q+R),\mathscr{O}\}$$

són tots ells diferents, aleshores $P+(Q+R)=(P+Q)+R$.

2. Si P,Q satisfà que els elements $\{P,-P,2P,-2P,Q,\mathscr{O}\}$ són tots ells diferents, aleshores

$$2P+Q = P+(P+Q).$$

3. Si $P \in E(K)$, aleshores

$$2(P+Q) = P+(Q+(P+Q)).$$

Demostració. El següent codi en Sage verifica les equacions algebraiques que es corresponen a cada igualtat.

```
S.<a1, a2, a3, a4,a6, x1, x2, x3,y1,y2,y3> = PolynomialRing(QQ, 11)
I = S.ideal([y1^2 + a1*x1*y1 + a3*y1 -(x1^3 + a2*x1^2 + a4*x1 + a6), \
             y2^2 + a1*x2*y2 + a3*y2 - (x2^3 + a2*x2^2 + a4*x2 + a6), \
             y3^2 + a1*x3*y3 + a3*y3 -(x3^3 + a2*x3^2 + a4*x3 + a6)])
P, Q, R = (x1,y1), (x2,y2), (x3,y3)

def add(P,Q):
    s1 = (Q[1]-P[1]) / (Q[0]-P[0])
    xPQ = s1^2 + a1 *s1 - a2 - P[0] - Q[0]
    yPQ = -a1 * xPQ -a3 - P[1] + s1*(P[0] - xPQ)
    return (xPQ, yPQ)

def double(P):
    s1 = (3*P[0]**2 + 2*a2 *P[0] -a1*P[1]+ a4) / (2 * P[1] + a1*P[0] + a3)
    xPQ = s1^2 + s1*a1 - a2 - 2*P[0]
    yPQ = -a1 * xPQ -a3 - P[1] + s1*(P[0] - xPQ)
    return (xPQ, yPQ)

A = add( add(P, Q), R )
B = add(P, add(Q, R) )
print( (A[0] - B[0]).numerator() in I and (A[1] - B[1]).numerator() in I )

A = add(double(P),Q)
B = add(P,add(P,Q))
print( (A[0] - B[0]).numerator() in I and (A[1] - B[1]).numerator() in I )

A = double(add(P,Q))
B = add(P,add(Q,add(P,Q)))
print( (A[0] - B[0]).numerator() in I and (A[1] - B[1]).numerator() in I )
```

■

Lema 3.1.5 Per a qualssevol punts P, Q i R de la corba E, es satisfà:

1. $(P+Q)-Q=P$.
2. $P+R=Q+R \iff P=Q$.
3. $2P+Q=P+(P+Q)$.

Demostració. La primera afirmació es comprova amb la definició de suma, fent servir que la recta simètrica a $\ell_{P,Q}$ és la recta $\ell_{P+Q,-Q}$.

La segona afirmació segueix de la primera: si $P+R=Q+R$, aleshores $P=(P+R)-R=(Q+R)-R=Q$.

Finalment, per comprovar l'última afirmació primer cal veure-la quan Q és $\mathcal{O}$ o $\pm P$, i en aquests casos és fàcil comprovar-ho pel què hem vist fins ara. Si $2P=\mathcal{O}$ també és fàcil, així com quan $Q=-2P$. El cas $Q=2P$ i el cas general són precisament els que s'han comprovat amb Sage. ■

Corol·lari 3.1.6 Per a qualssevol punts P i Q d'E, es satisfà:

1. $((P+Q)+P)+Q=2(P+Q)$.
2. $P+(Q-(P+Q))=\mathcal{O}$.

Amb aquests resultats, podem demostrar ja l'associativitat de la suma.

Teorema 3.1.7 La llei de grup definida anteriorment és associativa. Per tant, defineix un grup abelià.

Demostració. Els casos on $\mathscr{O} \in \{P, Q, R\}$ són obvis. Els casos especials queden coberts amb el lema i corol·lari anteriors, i el cas general s'ha comprovat amb `Sage`. ■

3.2 Punts de torsió, punts racionals

Donada una corba el·líptica E definida sobre un cos K, definim el subgrup de torsió com

$$E(K)_{\text{tors}} = \{P \in E(K) \mid nP = \mathscr{O}, \text{ per algun } n \geq 1\}.$$

També definim, per cada $n \geq 1$, el subgrup

$$E[n](K) = \{P \in E(K) \mid nP = \mathscr{O}\},$$

de manera que

$$E(K)_{\text{tors}} = \bigcup_{n \geq 1} E[n](K).$$

Més endavant també ens convindrà escriure $E[n] = E[n](\bar{K})$.

El següent resultat, que no demostrarem aquí, ens dona una manera de trobar tots els punts de torsió d'una corba el·líptica definida sobre $\mathbb{Q}$.

Teorema 3.2.1 — Nagell–Lutz (1935, 1937). Sigui E una corba el·líptica amb equació

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{Z}.$$

Si $P = (x, y)$ pertany a $E(\mathbb{Q})_{\text{tors}}$, aleshores:

1. $x, y \in \mathbb{Z}$, i
2. $y = 0$ o $y^2 \mid -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = \Delta_E/16$.

Remarca 3.2.2 Fent un canvi de variables de la forma $(x', y') = (u^2x + r, u^3y)$, amb un $u \in \mathbb{Q}^\times$ i $r \in \mathbb{Q}$ adequats, es pot aconseguir sempre que a, b, c siguin enters.

Remarca 3.2.3 Observem que el recíproc no és cert. Per exemple, el punt $P = (1, 1)$ de la corba $y^2 = x^3 - 16x + 16$ té ordre infinit. De fet, si P fos torsió aleshores $2P$ també ho seria, però $2P = (161/4, 2033/8)$, que no té coordenades enteres.

■ **Exemple 3.2.4** Considerem la corba el·líptica

$$E : y^2 = x^3 - 15x + 22$$

Calculem $\Delta_E/16 = 6912/16 = 2^4 \cdot 3^3$. Per tant, els possibles valors de y tals que y^2 divideixi $\Delta_E/16$ són, llevat de signe, $1, 2, 4, 3, 6, 12$. Comprovant totes les possibilitats, obtenim $\{(-1, \pm 6), (3, \pm 2)\}$. Comprovem que els múltiples de $P = (-1, 6)$ són

P	$2P$	$3P$	$4P$	$5P$	$6P$
$(-1, 6)$	$(3, -2)$	$(2, 0)$	$(3, 2)$	$(-1, -6)$	$\mathscr{O}_E$

Per altra banda, les arrels racionals de $x^3 - 15x + 22$ han de ser divisors de 22, és a dir que x hauria de ser, llevat de signe $1, 2, 11, 22$. Comprovant totes les possibilitats, obtenim el punt de 2-torsió $(2,0)$ que ja havíem vist abans.

Per tant, deduïm que $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z}$, generat per $(-1,6)$. ∎

Bastants anys més tard, Barry Mazur va demostrar un teorema molt més difícil, que ens diu l'estructura d'$E(\mathbb{Q})_{\text{tors}}$ de manera precisa.

Teorema 3.2.5 — Mazur, 1978. Sigui E una corba el·líptica definida a $\mathbb{Q}$. Aleshores

$$E(\mathbb{Q})_{\text{tors}} \cong \begin{cases} \mathbb{Z}/N\mathbb{Z} & 1 \leq N \leq 10, \text{ o } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} & 1 \leq N \leq 4. \end{cases}$$

A més, tots els 15 possibles subgrups de torsió es donen.

El següent teorema fou demostrat per Louis Mordell el 1922, i dedicarem unes quantes pàgines a la seva demostració.

Teorema 3.2.6 — Mordell, 1922. El grup $E(\mathbb{Q})$ està generat per un nombre finit de punts.

Gràcies al teorema de classificació dels grups abelians finitament generats, en deduïm que

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r, \quad r \geq 0.$$

L'enter r s'anomena el *rang de Mordell–Weil* d'$E(\mathbb{Q})$, i avui en dia no hi ha cap algoritme[1] per calcular-lo, encara que hi ha mètodes que funcionen bastant bé.

3.2.1 Altures

Volem definir l'"altura" d'un racional, de manera que hi hagi finits racionals d'altura fixada.

Definició 3.2.7 L'*altura* d'un racional $\frac{a}{b} \in \mathbb{Q}$ és

$$h(a/b) = \log \max\{|a|, |b|\}, \quad \text{si } \gcd(a,b) = 1.$$

Si $P = (x,y) \in E(\mathbb{Q})$, l'*altura* de P és $h(P) = h(x)$, l'altura de la seva coordenada-x. També escriurem $h(\mathcal{O}) = 0$.

Remarca 3.2.8 Per cada $M > 0$, el conjunt $E(\mathbb{Q})_{\leq M} = \{P \in E(\mathbb{Q}) \mid h(P) \leq M\}$ és finit.

Lema 3.2.9 Sigui $Q_0 \in E(\mathbb{Q})$. Hi ha una constant $C(Q_0)$ tal que

$$h(P + Q_0) \leq 2h(P) + C(Q_0), \quad \forall P \in E(\mathbb{Q}).$$

Lema 3.2.10 Hi ha una constant C tal que

$$h(2P) \geq 4h(P) - C, \quad \forall P \in E(\mathbb{Q}).$$

Teorema 3.2.11 Si $E(\mathbb{Q})/2E(\mathbb{Q})$ és finit, aleshores $E(\mathbb{Q})$ és finitament generat.

Demostració. Siguin $Q_1, \ldots, Q_t$ representants del quocient $E(\mathbb{Q})/2E(\mathbb{Q})$. Per tant, donat $P = P_0 \in E(\mathbb{Q})$, podem escriure $P_0 = Q_{i_0} + 2P_1$, amb $P_1 \in E(\mathbb{Q})$. Repetint l'argument amb P_1, podem escriure $P_1 = Q_{i_1} + 2P_2$. Per tant,

$$P = Q_{i_0} + 2P_1 = Q_{i_0} + 2Q_{i_1} + 4P_2.$$

[1] Per algoritme volem dir un programa d'ordinador el qual podem garantir que acabi en temps finit.

Després de n iteracions d'aquest argument, obtenim

$$P = Q_{i_0} + 2Q_{i_1} + 4Q_{i_2} + \cdots + 2^{n-1}Q_{i_{n-1}} + 2^n P_n$$

Calculem ara l'altura de P_j, per cada j. Si escrivim $\bar{C} = \max\{C(Q_1), \ldots C(Q_t)\}$, tenim

$$h(P - Q_i) \leq 2h(P) + C(Q_i) \leq 2h(P) + \bar{C}.$$

Aleshores,

$$4h(P_j) \leq h(2P_j) + C = h(P_{j-1} - Q_{i_{j-1}}) + C \leq 2h(P_{j-1}) + \bar{C} + C.$$

Per tant, escrivint $M = \bar{C} + C$, tenim

$$h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{M}{4} = \frac{3}{4}h(P_{j-1}) - \frac{1}{4}\left(h(P_{j-1}) - M\right).$$

D'aquí en traiem:

$$\text{Si } h(P_{j-1}) \geq M, \text{ aleshores } h(P_j) \leq \frac{3}{4}h(P_{j-1}).$$

Per tant, si observem la successió de punts $P_0, P_1, P_2, \ldots$, si tenen altura més gran que M, aleshores la seva altura cada vegada es fa més petita (tendint a zero). Aleshores hi ha algun índex n tal que $P_n \in E(\mathbb{Q})_{\leq M} = \{P \in E(\mathbb{Q}) \mid h(P) \leq M\}$.

Concloem que tot punt $P \in E(\mathbb{Q})$ es pot escriure com a combinació lineal entera dels punts $Q_1, \ldots Q_t$ i dels finits punts de $E(\mathbb{Q})_{\leq M}$. ■

3.2.2 La versió dèbil del teorema de Mordell

Ens hem reduït a demostrar el següent resultat.

Teorema 3.2.12 — Mordell–Weil dèbil. El quocient $E(\mathbb{Q})/2E(\mathbb{Q})$ és finit.

Remarca 3.2.13 De fet, el teorema de Mordell–Weil afirma que, donat un cos de nombres K i un enter $m \geq 2$, el quocient $E(K)/mE(K)$ és finit. Encara que la idea de la demostració és la mateixa, alguns dels ingredients que apareixen en aquest cas més general fan servir eines més avançades que preferim no introduir.

Primer ens cal estudiar el grup de 2-torsió $E[2]$. Fixem-nos que $2P = \mathcal{O}$ si i només si $P = \mathcal{O}$ o $P = (x, 0)$. Per tant, els punts no trivials de 2-torsió es corresponen amb les arrels de $x^3 + ax + b$. Així, $E[2]$ té ordre 4. Com que és un grup d'exponent 2, en deduïm que

$$E[2] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

En general, fixem-nos que $E[m]$ té exponent m (és a dir, tot element $P \in E[m]$ té ordre divisor de m). De fet, $E[m]$ és isomorf a $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ per a tot m. Demostrem aquí una versió més dèbil d'aquest fet, que no ens diu l'estructura de $E[m]$.

Proposició 3.2.14 Per a tot $m \geq 2$, el grup $E[m] = E[m](\bar{K})$ és finit.

Demostració. Podem suposar (ja que K és de característica zero) que E té per equació $y^2 = x^3 + Ax + B$ amb $A, B \in K$. Fent inducció en m, és fàcil veure que l'aplicació "multiplicar per m" s'escriu, en coordenades, $(x, y) \mapsto \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ per certs polinomis $u, v, s, t \in K[x]$.

Per tant, $m(x, y) = \mathcal{O}$ si, i només si, $v(x) = 0$ (si i només si $t(x) = 0$). Com que $v(x)$ té un nombre finit d'arrels, hi ha un nombre finit de possibles coordenades-x pels punts d'$E[m]$ i d'aquí en deduïm el resultat. ■

Per cada punt $P \in E(K)$, escollim $Q = (x,y) \in E(\bar{K})$ tal que $mQ = P$, i definim $L_P = K(x,y)$ com la mínima extensió de K que conté les coordenades x i y de Q. Definim també L com la clausura normal de la composició de totes les extensions L_P.

Considerem l'aplicació

$$\phi_P \colon \mathrm{Gal}(L/K) \to E[m], \quad \phi_P(\sigma) = \sigma(Q) - Q.$$

Observem que

$$m(\sigma(Q) - Q) = m\sigma(Q) - mQ = \sigma(mQ) - mQ = \sigma(P) - P = \mathscr{O},$$

i per tant $\phi_P(\sigma) \in E[m]$.

Ens agradaria veure que l'aplicació ϕ_P no depèn del punt Q triat. Per això, ens caldrà suposar que:

Hipòtesi: $E[m] \subseteq E(K)$.

Si R és una altre punt tal que $mR = P$, aleshores es té $m(Q-R) = P - P = \mathscr{O}$ i, per tant, $Q - R \in E[m]$. Com que $E[m] \subseteq E(K)$, aleshores

$$(\sigma(Q) - Q) - (\sigma(R) - R) = \sigma(Q-R) - (Q-R) = (Q-R) - (Q-R) = \mathscr{O}.$$

Per tant, ϕ_P només depèn de P, i no pas del punt $Q \in E(L)$ tal que $mQ = P$.

Remarca 3.2.15 Recordem que hem suposat que $E(K)$ conté $E[m]$. Com que $E[m]$ és finit, aquesta hipòtesi es pot satisfer canviant K per una extensió K' més gran, i que podem suposar de Galois. És fàcil veure que si el teorema de Mordell–Weil dèbil és cert per $E(K')$ amb $K' \supseteq K$ aleshores també és cert per $E(K)$: el nucli de l'aplicació

$$E(K)/mE(K) \to E(K')/mE(K')$$

és el conjunt

$$(E(K) \cap mE(K'))/mE(K) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(K'/K), E[m]), \quad P \mapsto \phi_P,$$

i el grup de la dreta és finit perquè tant $\mathrm{Gal}(K'/K)$ com $E[m]$ ho són.

Proposició 3.2.16 Sigui K un cos de nombres, i suposem que $E[m] \subset E(K)$. Aleshores l'assignació $P \mapsto \phi_P$ indueix una injecció

$$\phi \colon E(K)/mE(K) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L/K), E[m]).$$

Demostració. Ens cal veure:

1. Per cada $P \in E(K)$, l'aplicació ϕ_P és un morfisme de grups.
2. $\ker\phi = mE(K)$.

Calculem $\phi_P(\sigma_1\sigma_2) - \phi_P(\sigma_1) - \phi_P(\sigma_2)$, on $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/K)$:

$$\begin{aligned}\phi_P(\sigma_1\sigma_2) - \phi_P(\sigma_1) - \phi_P(\sigma_2) &= (\sigma_1\sigma_2)(Q) - Q - \sigma_1(Q) + Q - \sigma_2(Q) + Q \\ &= \sigma_1(\sigma_2(Q) - Q) - (\sigma_2(Q) - Q).\end{aligned}$$

Com que $m(\sigma_2(Q) - Q) = \sigma_2(P) - P = \mathscr{O}$, tenim que $\sigma_2(Q) - Q \in E[m] \subseteq E(K)$ i, per tant és invariant per σ_1.

Calculem ara $\ker\phi$. Òbviament, si $P \in mE(K)$, podem triar $Q \in E(K)$ tal que $mQ = P$, i aleshores $\sigma(Q) - Q = \mathscr{O}$ per a tot $\sigma \in \mathrm{Gal}(L/K)$. Per tant, $mE(K) \subseteq \ker\phi$.

Per acabar, doncs, cal veure que $\ker\phi \subseteq mE(K)$. Per tant, suposem que $P \in E(K)$ és tal que $\sigma(Q) - Q = \mathscr{O}$ per a tot $\sigma \in \mathrm{Gal}(L/K)$. Això vol dir que $Q \in E(K)$, i per tant $P = mQ \in mE(K)$. ∎

La proposició que hem demostrat permet veure el quocient que ens interessa com un subgrup del grup $\mathrm{Hom}(\mathrm{Gal}(L/K), E[m])$. Si podem demostrar que L/K és una extensió finita, aleshores $\mathrm{Gal}(L/K)$ serà un grup finit. Com que $E[m]$ també és finit aleshores el grup d'homomorfismes entre aquests dos grups finits serà necessàriament finit i haurem demostrat el teorema.

Lema 3.2.17 Si $P \notin E(K)[2]$, aleshores $L_P = K(x(Q))$.

Demostració. Prenem $\sigma \in \mathrm{Gal}(\bar{K}/K(x))$ i volem veure que $\sigma(y) = y$. Com que $\sigma(x) = x$, per l'equació d'E es té $\sigma(y)^2 = y^2$, és a dir $\sigma(y) = \pm y$. Suposem, per arribar a contradicció, que $\sigma(y) = -y$. Aleshores $\sigma(Q) = -Q$. Per tant:

$$P = \sigma(P) = \sigma(mQ) = m\sigma(Q) = m(-Q) = -P,$$

i això només pot passar si P és de 2-torsió. ■

A partir d'ara ens centrarem en el cas $K = \mathbb{Q}$ i $m = 2$, ja que la demostració en el cas més general és notablement més complicada.

3.2.3 Demostració de la finitud de $L/\mathbb{Q}$

Com que $E[2] \subseteq E(\mathbb{Q})$, fent un canvi de variables podem assumir que E té equació de la forma

$$y^2 = x(x-e_1)(x-e_2), \quad e_1, e_2 \in \mathbb{Q}.$$

La fórmula per la duplicació es simplifica, en aquest cas, a

$$x(2Q) = \frac{x^4 - 2e_1e_2x + e_1^2e_2^2}{4y^2}.$$

Sense pèrdua de generalitat, podem restringir-nos a punts $P \in E(\mathbb{Q}) \setminus E[2]$, ja que només obviem un nombre finit de punts. Si $P = (\alpha, \beta) \in E(\mathbb{Q})$, els punts Q tals que $2Q = P$ hauran de satisfer que $x(2Q) = \alpha$. Com que $y^2 = x(x-e_1)(x-e_2)$, això equival a que $x(Q)$ satisfaci l'equació

$$g(x) = x^4 - 4\alpha x^3 + (4\alpha(e_1+e_2) - 2e_1e_2)x^2 - 4e_1e_2\alpha x + e_1^2e_2^2 = 0.$$

El següent codi de Sage ens permet trobar les seves arrels:

```
var('alpha,e1,e2')
x = SR['x'].gen()
F = x * (x - e1) * (x - e2)
g = (4*F*(e1 + e2 - 2*x) + (3*x^2-2*(e1+e2)*x+e1*e2)**2)- alpha*4*F
show(g.roots())
```

Veiem que les arrels són de la forma

$$\alpha \pm \sqrt{(\alpha-e_1)(\alpha-e_2)} \pm \sqrt{2\alpha^2 - e_1\alpha - e_2\alpha \pm 2\alpha\sqrt{(\alpha-e_1)(\alpha-e_2)}}.$$

Remarca 3.2.18 També podem resoldre l'equació $g(x) = 0$ a mà, amb el que es coneix com el mètode de Ferrari. Escrivim

$$g(x) = (x^2 + Ax + B)^2 - C^2x^2, \quad \text{amb } A, B, C \text{ a determinar.}$$

Aleshores podem factoritzar $g(x)$ com

$$g(x) = (x^2 + (A+C)x + B)(x^2 + (A-C)x + B),$$

i fent servir la fórmula quadràtica trobem totes les solucions. En el nostre cas, igualant coeficients

veiem que una solució és

$$(A,B,C) = (-2\alpha, e_1e_2, 2\sqrt{(\alpha-e_1)(\alpha-e_2)}).$$

Veurem ara que es té $L_P \subseteq L_\alpha = \mathbb{Q}(\sqrt{\alpha-e_1}, \sqrt{\alpha-e_2})$. Només ens cal veure que

$$2\alpha^2 - e_1\alpha - e_2\alpha \pm 2\alpha\sqrt{(\alpha-e_1)(\alpha-e_2)} \in (L_\alpha^\times)^2$$

Aquesta expressió la podem reescriure com

$$2\alpha^2 - e_1\alpha - e_2\alpha \pm 2\alpha\sqrt{(\alpha-e_1)(\alpha-e_2)} = \left(\sqrt{\alpha(\alpha-e_1)} \pm \sqrt{\alpha(\alpha-e_2)}\right)^2,$$

i per tant només ens cal veure que $\sqrt{\alpha} \in L_\alpha$. Fent servir l'equació d'E, tenim

$$\sqrt{\alpha(\alpha-e_1)(\alpha-e_2)} = \sqrt{\alpha}\sqrt{\alpha-e_1}\sqrt{\alpha-e_2} = \pm\beta \in \mathbb{Q},$$

i per tant $\sqrt{\alpha}$ pertany a L_α.

Per acabar, només hem de veure que el compost de tots els L_α és una extensió finita.

Lema 3.2.19 Si $E\colon y^2 = x^3 + ax^2 + bx$ amb $a,b \in \mathbb{Z}$, aleshores les coordenades-x dels punts d'$E(\mathbb{Q})$ només prenen un nombre finit de valors, mòdul quadrats.

Demostració. Suposem que $(x,y) \in E(\mathbb{Q})$, i escrivim $x = m/M$ i $y = n/N$ en fraccions reduïdes. Si substituïm a l'equació d'E i netegem denominadors, obtenim

$$n^2M^3 = N^2m(m^2 + amM + bM^2).$$

Si $p^r \parallel M^3$, aleshores $p \nmid m$ i $p \nmid m^2 + amM + bM^2$. Per tant, obtenim $p^r \mid N^2$. Recíprocament, si $p^r \parallel N^2$, aleshores $p^r \mid n^2M^3$ i, com que $p \nmid n$, obtenim $p^r \mid M^3$. En conclusió, $N^2 = M^3 = e^6$ i per tant podem escriure $x = m/e^2$ i $y = n/e^3$ amb $m,n,e \in \mathbb{Z}$ i $\gcd(e,m) = \gcd(e,n) = 1$.

Volem doncs estudiar la part lliure de quadrats de l'enter m. Simplificant l'equació anterior obtenim

$$n^2 = m(m^2 + ame^2 + be^4).$$

Per tant, el producte de la dreta és un quadrat, i si escrivim $g = \gcd(m, m^2 + ame^2 + be^4)$, aleshores

$$n^2 = g^2m_1m_2, \text{ amb } \gcd(m_1,m_2) = 1,$$

d'on en deduïm que m_1 i m_2 són quadrats. Per tant, $m = gr^2$ i per tant l'enter g és un múltiple de la part lliure de quadrats d'm.

Com que $g \mid m$, aleshores $g \mid be^4$. Com que $\gcd(g,e) = 1$, obtenim $g \mid b$. Per tant, els possibles g són divisors de b, i d'aquests n'hi ha un nombre finit. ■

El lema anterior aplicat a la nostra corba E ens dona una quantitat finita d'extensions $\mathbb{Q}(\sqrt{\alpha})$, però també hem de tractar amb $\mathbb{Q}(\sqrt{\alpha-e_1})$ i $\mathbb{Q}(\sqrt{\alpha-e_2})$. Considerem la corba el·líptica

$$E'\colon y^2 = x(x+e_1)(x+e_1-e_2).$$

Si $(\alpha,\beta) \in E(\mathbb{Q})$, aleshores $(\alpha-e_1,\beta) \in E'(\mathbb{Q})$. Per tant, aplicant el lema a E' obtenim també un nombre finit de possibilitats per $\mathbb{Q}(\sqrt{\alpha-e_1})$. Podem repetir l'argument amb

$$E''\colon y^2 = x(x+e_2)(x+e_2-e_1),$$

que ens donarà un nombre finit de possibilitats per $\mathbb{Q}(\sqrt{\alpha-e_2})$ i per tant també per les possibilitats d'L_P. Així, el compost de tots els L_P és una extensió finita.

3.3 Isogènies

En aquesta secció introduïm els morfismes entre corbes el·líptiques, que s'anomenen isogènies. Recordem que una corba el·líptica té dues estructures fonamentals: en primer lloc té una estructura algebraica, perquè ve donada per una equació polinomial. Però també té una llei de grup, és a dir una estructura de grup abelià (per cada extensió L/K, de fet). Voldrem morfismes que tinguin en compte aquestes dues estructures.

Definició 3.3.1 Una *isogènia* entre corbes el·líptiques E_1 i E_2 definides sobre un cos K és una aplicació $\phi\colon E_1(\bar{K}) \to E_2(\bar{K})$, donada per funcions racionals en les coordenades, i que envia $\mathcal{O}_{E_1}$ a $\mathcal{O}_{E_2}$.

Expliquem primer què vol dir que $\phi\colon E_1(\bar{K}) \to E_2(\bar{K})$ vingui donada per funcions racionals. Volem dir que existeixen $u(X,Y)$ i $v(X,Y)$ elements de $K(X,Y)$ (el cos de fraccions $K[X,Y]$) tals que

$$(x,y) \in E_1(\bar{K}) \implies (u(x,y),v(x,y)) \in E_2(\bar{K}).$$

Una altra manera de pensar-ho és com un cert morfisme d'anells. Donada una corba E/K amb equació $y^2 = f(x)$, el seu *anell de funcions regulars* es defineix com $K[E] = \frac{K[x,y]}{(y^2-f(x))}$, i el seu *cos de funcions* $K(E) = \mathrm{Frac}(K[E])$ és el cos de fraccions de $K[E]$.

Ara suposem que E_1 i E_2 tenen, respectivament, equacions $y^2 = f(x)$ i $y^2 = g(x)$. Aleshores donar ϕ és equivalent a donar una morfisme d'anells

$$\phi^*\colon K[E_2] \to K[E_1], \quad (\phi^* h) = h(u(x,y),v(x,y)).$$

Remarca 3.3.2 Es pot demostrar que aquestes dues condicions impliquen el fet (sorprenent?) que si $\phi\colon E_1 \to E_2$ és una isogènia, aleshores $\phi(P+Q) = \phi(P)+\phi(Q)$ per a tot $P,Q \in E(\bar{K})$. És per això que no ho hem demanat com axioma, sinó que només hem hagut de demanar que dugui el neutre $\mathcal{O}_{E_1}$ d'E_1 al neutre d'E_2.

El morfisme ϕ^* indueix un morfisme entre els corresponents cossos de funcions que, si $\phi \neq 0$, és una injecció

$$\phi^*\colon K(E_2) \hookrightarrow K(E_1).$$

Definició 3.3.3 El *grau* d'una isogènia $\phi\colon E_1 \to E_2$ és el grau de l'extensió de cossos $\phi^*(K(E_2)) \subseteq K(E_1)$.

Lema 3.3.4 Siguin E_1 i E_2 corbes el·líptiques amb equacions de Weierstrass curtes, i sigui $\phi\colon E_1 \to E_2$ una isogènia. Aleshores podem trobar $u(x),v(x),s(x),t(x) \in K[x]$, amb $\gcd(u,v) = \gcd(s,t) = 1$, tals que

$$\phi(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$$

La quadrupla de polinomis (u,v,s,t) s'anomenarà la *forma normal* de ϕ.

Corol·lari 3.3.5 Si $\phi \neq 0$, aleshores $\ker\phi \subseteq E_1(\bar{K})$ és finit.

Demostració. De la forma normal de ϕ, podem veure que un punt $P = (x,y) \in E_1(\bar{K})$ és del nucli de ϕ si, i només si, $v(x) = 0$ o $t(x) = 0$. Però un polinomi en una variable sempre té un nombre finit de solucions, i per tant hi ha un nombre finit de possibilitats per la coordenada x. Per cada x fixada, només hi ha dues possibilitats per la coordenada y, d'on n'obtenim la finitud. ■

Proposició 3.3.6 Si $\phi\colon E_1 \to E_2$ té forma normal donada per (u,v,s,t), aleshores $\deg(\phi) = \max\{\deg(u),\deg(v)\}$.

■ **Exemple 3.3.7** Considerem $E_1\colon y^2 = f_1(x) = x^3-2x+1$ i $E_2\colon y^2 = f_2(x) = x^3-7x-6$. Considerem l'aplicació $\phi\colon E_1 \to E_2$ definida com

$$(x,y) \mapsto \phi(x,y) = (\sigma(x),\tau(x)y) = \left(\frac{x^2-x+1}{x-1}, \frac{x^2-2x}{x^2-2x+1}y\right).$$

Podem comprovar que $\tau(x)^2y^2 - \sigma(x)^3 + 7\sigma(x) + 6 = \tau(x)^2 f_1(x) - \sigma(x)^3 + 7\sigma(x) + 6 = 0$ a $K[x,y]$. Per veure la imatge del punt de l'infinit i del punt $(1,0)$ hem de passar-ho a coordenades projectives i fer servir l'equació de la corba E_1 per obtenir polinomis que no s'anulin a la vegada. Per exemple, podem calcular que, mòdul l'equació d'E_1, tenim:

$$\frac{x^2-x+1}{x-1} = \frac{y^2(x-1)+x(x^2+x-1)}{y^2}, \qquad \frac{x^2-2x}{x^2-2x+1} = \frac{y^4-(x^2+x-1)^2}{y^4}.$$

Això ens permet reescriure les equacions de ϕ en coordenades projectives com:

$$\phi(x:y:z) = \left(y^3(x-z)+xy(x^2+xz-z^2) : y^4-(x^2+xz-z^2)^2 : y^3z\right).$$

Observem que els tres polinomis són homogenis de grau 4, per tant podem evaluar ϕ a $(0:1:0)$ fent servir aquesta fórmula i obtenim $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ (i per tant ϕ és una isogènia). Deixem com exercici fer el mateix pel punt $(1,0)$, que també resulta tenir imatge $\mathcal{O}_{E_2}$. En deduïm que $\ker\phi$ té tamany 2.

Com que la tenim posada en forma normal, el grau de ϕ és 2. ■

■ **Exemple 3.3.8** Sigui E una corba el·líptica. Evidentment, la identitat Id_E és una isogènia, que habitualment s'escriu $[1]$. També l'aplicació $P \mapsto -P$ (que ve donada per $(x,y) \mapsto (x,-y)$ si E ve donada per una equació $y^2 = f(x)$) és una isogènia, que anomenem $[-1]$. Ja hem vist que l'aplicació $[2]\colon E \to E$ que envia P a $2P$ és una isogènia: ve donada per les aplicacions racionals

$$(x,y) \mapsto \left(\frac{x^4-2ax^2-8bx+a^2}{4y^2}, \frac{x^6+5ax^4+20bx^3-5a^2x^2-4abx-a^3-8b^2}{8y^3}\right).$$

Més generalment, per qualsevol enter m es té la isogènia $[m]$ que envia $P \mapsto mP$. ■

Sigui $E/\mathbb{F}_q$ una corba el·líptica. Observem que si $(x,y) \in E(\bar{\mathbb{F}}_q)$ satisfà l'equació de la corba, posem $y^2 = x^3+ax+b$, aleshores

$$(y^q)^2 = (y^2)^q = (x^3+ax+b)^q = (x^q)^3 + a^qx^q + b^q = (x^q)^3 + ax^q + b,$$

on hem fet servir que q és una potència de p (i p és la característica del cos), el teorema del "binomi del Batxillerat" i el fet que a i b són de $\mathbb{F}_q$. Això ens permet considerar una isogènia pròpia del fet que estem en característica finita.

Definició 3.3.9 L'*endomorfisme de Frobenius* és la isogènia

$$\phi_E\colon E \to E, \quad (x,y) \mapsto (x^q,y^q).$$

Remarca 3.3.10 Donada una corba el·líptica E, denotem per $\mathrm{End}(E)$ l'anell d'endomorfismes d'E, format per les isogènies d'E a E i pel 0 (alguns autors no consideren l'aplicació 0 com una isogènia, nosaltres ho remarcarem sempre per evitar confusió). La suma ve definida per $(\phi+\psi)(P) = \phi(P)+\psi(P)$, i el producte per la composició. En general, es tracta d'un anell no

commutatiu. Tot i així, observem que

$$\phi \circ [m] = [m] \circ \phi, \quad \phi \in \mathrm{End}(E), \quad m \in \mathbb{Z}.$$

La remarca anterior té una conseqüència interessant. Si $\phi \in \mathrm{End}(E)$ és una isogènia i $m \geq 1$ és un enter, aleshores ϕ indueix un endomorfisme ϕ_m del grup $E[m]$. Si m és invertible a K (K té característica 0 o coprimera amb m), aleshores $E[m] \cong \mathbb{Z}/m \oplus \mathbb{Z}/m$, i per tant ϕ_m ve donada (després de triar una base) per una matriu a $M_2(\mathbb{Z}/m\mathbb{Z})$. Per tant, té sentit parlar del determinant de ϕ_m.

Teorema 3.3.11 Per a tot $m \geq 1$ invertible a K, es té la congruència

$$\deg(\phi) \equiv \det(\phi_m) \pmod{m}.$$

Acabem amb una propietat que necessitarem més endavant.

Corol·lari 3.3.12 L'aplicació $\deg\colon \mathrm{End}(E) \to \mathbb{Z}$ és una forma quadràtica. És a dir,

1. $\deg(n\phi) = n^2 \deg(\phi)$ per a tot $n \in \mathbb{Z}$, i $\phi \in \mathrm{End}(E)$, i
2. L'aplicació $(\phi, \psi) \mapsto \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$ és bilineal.

Demostració. Apliquem la proposició anterior, observant que el determinant, vist com una aplicació $M_2(\mathbb{Z}) \to \mathbb{Z}$, és una forma quadràtica. Aleshores obtenim el resultat mòdul m, per a tot $m \geq 1$. Per obtenir igualtat en comptes de congruència, fem tendir m a infinit. ■

Proposició 3.3.13 — Desigualtat de Cauchy–Schwartz. Donades isogènies φ_1 i φ_2 es té

$$|\deg(\varphi_1 - \varphi_2) - \deg(\varphi_1) - \deg(\varphi_2)| \leq 2\sqrt{\deg(\varphi_1)\deg(\varphi_2)}.$$

Demostració. Considerem l'aplicació bilineal, simètrica i definida positiva (φ, ψ) del corol·lari anterior. Fixem-nos que és definida positiva perquè $(\varphi, \varphi) = 2\deg(\varphi) \geq 0$. Aleshores el resultat que volem demostrar és equivalent a $(\varphi, \psi)^2 \leq (\varphi, \varphi)(\psi, \psi)$. Aquesta desigualtat s'obté fent servir bilinealitat repetidament per calcular

$$((\psi, \psi)\varphi - (\varphi, \psi)\psi, (\psi, \psi)\varphi - (\varphi, \psi)\psi) \geq 0.$$

■

3.4 Corbes sobre cossos finits

En aquesta secció tractarem amb corbes el·líptiques E definides sobre un cos finit $\mathbb{F}_q$ de $q = p^r$ elements, per cert primer p i $r \geq 1$.

Fixem-nos que òbviament $E(\mathbb{F}_q)$ és finit. De fet, com a molt es tenen $2q+1$ punts: el punt de l'infinit, i per cada tria d'x obtenim un polinomi en y de grau 2, que com a molt té dues arrels. Podem afinar l'anàlisi una mica més: per cada valor d'x, el polinomi quadràtic té o bé zero o dues solucions, i si cadascun dels casos es dona amb la mateixa freqüència obtindríem uns $q+1$ punts.

■ **Exemple 3.4.1** Considerem la corba el·líptica

$$E\colon y^2 = x^3 - x + 1.$$

Com que $\Delta_E = -2^4 \cdot 23$, podem considerar la corba mòdul diferents primers, excepte 2 i 23. Si escrivim $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$, obtenim la taula següent:

p	3	5	7	11	13	17	19	29	31	37
$\#E(\mathbb{F}_p)$	7	8	12	10	19	14	22	37	35	36
$a_p(E)$	-3	-2	-4	2	-5	4	-2	-7	-3	2

Taula 3.1: Nombre de punts d'$E(\mathbb{F}_p)$ al variar p.

Podem fer la taula molt més gran (per $p \leq 10^5$) i representar el resultat en una gràfica com la següent. Obtindrem el següent resultat curiós:

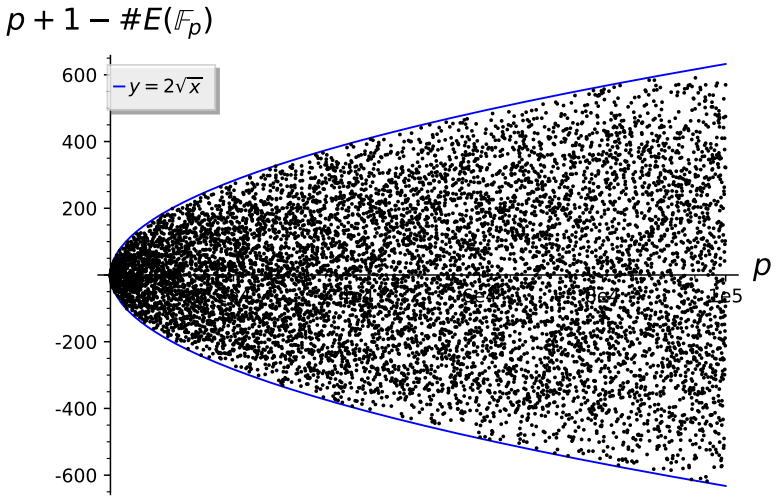

Figura 3.2: Il·lustració del Teorema de Hasse per la corba $E\colon y^2 = x^3 - x + 1$

■

El que s'observa a la gràfica s'expressa en forma de teorema:

Teorema 3.4.2 — Teorema de Hasse. Si E és una corba el·líptica definida sobre $\mathbb{F}_q$, aleshores

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

Idea de la demostració. Recordem la isogènia de Frobenius ϕ_E. Observem que $E(\mathbb{F}_q) = \ker(\phi_E - 1)$, i per tant ens interessa calcular $\#\ker(\phi_E - 1)$. Aplicarem la desigualtat de Cauchy–Schwartz a $\varphi_1 = \phi_E$ i $\varphi_2 = [1]$. De la forma normal de ϕ_E veiem que $\deg(\phi_E) = q$. Per altra banda, resulta que $\deg(\phi_E - 1) = \#\ker(\phi_E - 1)$. Observem aleshores que $\#E(\mathbb{F}_q) = \#\ker(\phi_E - 1) = \deg(\phi_E - 1)$, i per tant obtenim directament el resultat. ■

Proposició 3.4.3 Sigui $E/\mathbb{F}_q$ una corba el·líptica. Aleshores ϕ_E satisfà

$$\phi_E^2 - a\phi_E + q = 0, \text{ on } a = q + 1 - \#E(\mathbb{F}_q).$$

Demostració. Considerem l'endomorfisme $f = \phi_E^2 - a\phi_E + q$, que volem veure que és 0. Com ja hem vist, f indueix una aplicació lineal $f_m \in \mathrm{End}(E[m])$, per a tot $m \geq 1$. Si m és coprimer amb q, aleshores $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. Del fet que ϕ_E té grau q, que $\phi_E - 1$ té grau $\#E(\mathbb{F}_q)$, i que $\det(\phi_m)) \equiv \deg(\phi) \pmod{m}$ en deduïm, evaluant el polinomi característic de ϕ_m a 1, que $\mathrm{tr}(\phi_m) \equiv a \pmod{m}$. Per tant, $f_m \equiv 0 \pmod{m}$, i això vol dir que el nucli de f conté $E[m]$. Com que m es pot fer arbitràriament gran, concloem que f té nucli infinit. Per tant, $f = 0$, com volíem veure. ■

Remarca 3.4.4 La proposició diu que per a tot punt $P=(x,y)\in E(\bar{\mathbb{F}}_q)$, es té

$$(x^{q^2},y^{q^2})-a\cdot(x^q,y^q)+q\cdot(x,y)=\mathscr{O}_E.$$

El següent teorema ens dona una manera fàcil de calcular $\#E(\mathbb{F}_{q^n})$ si la corba E està definida sobre $\mathbb{F}_q$ i sabem calcular $\#E(\mathbb{F}_q)$. Per enunciar-lo, ens cal considerar les arrels α,β del polinomi X^2-aX+q, on $a=q+1-\#E(\mathbb{F}_q)$.

Lema 3.4.5 Les arrels α i β del polinomi X^2-aX+q són o bé les dues iguals o bé complexos conjugats. En tot cas, satisfan $|\alpha|=|\beta|=\sqrt{q}$.

Demostració. Pel Teorema de Hasse, el polinomi X^2-aX+q té discriminant $a^2-4q\leq 0$. Si aquest discriminant és 0 (i per tant q és un quadrat) aleshores $X^2-aX+q=(X\pm\sqrt{q})^2$. Si $a^2-4q<0$, aleshores α i β són complexos conjugats i el seu producte és q. Per tant, tenim $|\alpha|=|\beta|=\sqrt{q}$. ■

Teorema 3.4.6 Sigui E una corba el·líptica definida sobre $\mathbb{F}_q$. Aleshores,

$$\#E(\mathbb{F}_{q^n})=q^n+1-\alpha^n-\beta^n,\quad \forall n\geq 1.$$

Demostració. Definim $s_i=\alpha^i+\beta^i$. Per altra banda, observem que el polinomi $X^{2i}-s_iX^i+q^i$ es pot escriure com $(X^i-\alpha^i)(X^i-\beta^i)$. Sabem que el primer factor és múltiple de $X-\alpha$ i el segon és múltiple de $X-\beta$ i, per tant, el polinomi $X^{2i}-s_iX^i+q^i$ és un múltiple de X^2-aX+q. Això implica que ϕ_E^n satisfà el polinomi $X^2-s_nX+q^n$. Si pensem ara en E com una corba sobre $\mathbb{F}_{q^n}$ i apliquem la proposició anterior, obtenim que ϕ_E^n també satisfà $X^2-t_nX+q^n$, on $t_n=q^n+1-\#E(\mathbb{F}_{q^n})$. Per tant, satisfà la seva diferència, és a dir: $(t_n-s_n)\phi_E^n=0$. Com que ϕ_E^n no és zero, n'extreiem que $s_n=t_n$, que és el que volíem veure. ■

Remarca 3.4.7 El teorema anterior ens dona una manera recursiva de calcular $\#E(\mathbb{F}_{q^n})$ sense treballar amb nombres complexos ni amb arrels quadrades. Si escrivim $s_i=\alpha^i+\beta^i$, observem que $s_0=2$ i $s_1=a$, i es demostra directament que

$$s_{n+1}=\alpha^{n+1}+\beta^{n+1}=(\alpha+\beta)(\alpha^n+\beta^n)-\alpha\beta(\alpha^{n-1}+\beta^{n-1})=as_n-qs_{n-1},\quad n\geq 2.$$

3.5 Criptografia amb corbes el·líptiques

3.5.1 Diffie–Hellman amb corbes el·líptiques

Recordem que el protocol de Diffie–Hellman fa servir l'operació de grup a $\mathbb{F}_p^\times$, que és un grup cíclic, per establir una clau comuna entre Alice i Bob. Podem canviar el grup $\mathbb{F}_p^\times$ pel grup generat per un punt $P\in E(\mathbb{F}_q)$. Denotem per N l'ordre del punt P (fixem-nos que $N\simeq q$, pel teorema de Hasse). Això resulta en el següent protocol (compareu-lo amb la §1.5.1).

1. L'Alice escull un enter a l'atzar $1<a<N$, i envia el punt $Q_A=aP\in E(\mathbb{F}_q)$ a en Bob.
2. En Bob, per la seva banda, escull un enter a l'atzar $1<b<N$, i envia el punt $Q_B=bP\in E(\mathbb{F}_q)$ a l'Alice.
3. L'Alice i en Bob calculen respectivament aQ_B i bQ_A. Observem que els dos punts calculats són iguals a abP, que serà el secret compartit.

En aquest cas, també es creu que *problema de Diffie–Hellman per corbes el·líptiques (ECDHP)* i el *problema del logaritme discret per corbes el·líptiques (ECDLP)* són equivalents. Òbviament, la seguretat del sistema depèn de l'ordre N del punt P escollit, i per tant ens interessarà trobar corbes el·líptiques $E/\mathbb{F}_q$ tals que $\#E(\mathbb{F}_q)$ sigui divisible per un primer gran.

Per altra banda, l'algoritme més potent per resoldre el logaritme discret a $\mathbb{F}_q^\times$, que s'anomena "Index Calculus", no té anàleg a $E(\mathbb{F}_q)$. Això fa que per solucionar el logaritme discret a $E(\mathbb{F}_q)$ només es tinguin disponibles els algoritmes que funcionen per grups cyclic genèrics. Conseqüentment, un sistema criptogràfic basat en l'ECDLP pugui assolir la mateixa seguretat que un sistema basat en el DLP treballant amb un cos finit de cardinal molt menor.

La companyia Certicom[2] té diferents reptes de resoldre el logaritme discret en corbes el·líptiques, i ofereix 20.000$ a qui trobi el logaritme discret d'un punt concret d'una corba E definida sobre $\mathbb{F}_p$, on $p = 155003179783434785924857641481313994241 1$ (131 bits). En canvi, des del 2005 es pot (amb tècniques molt avançades i amb molt d'esforç computacional) resoldre el logaritme discret a $\mathbb{F}_p^\times$ per primers d'aquest tamany. De fet, es pot fer per primers de fins a 180 bits. Es considera que la seguretat en corbes el·líptiques obtinguda amb primers d'uns 160 bits és comparable a l'obtinguda a $\mathbb{F}_p^\times$ amb primers de 1024 bits, mentre que amb només 256 bits s'obté la seguretat corresponent a 4096 bits de $\mathbb{F}_p^\times$.

3.5.2 ElGamal amb corbes el·líptiques

El xifrat ElGamal també es pot dur a terme amb corbes el·líptiques. Aprofitarem per descriure l'algoritme per un grup $G = \mathbb{F}_q^\times$ o $G = E(\mathbb{F}_q)$. En el cas $G = \mathbb{F}_q^\times$ recuperaríem l'algoritme de la §1.5.2

Preparació: Cada usuari (posem Alice) tria un element $g \in G$ d'ordre N suficientment gran. Seguidament, tria un enter $2 < a < N$ i calcula $A = g^a$. La clau pública de l'Alice serà la tupla (G, g, A), i la clau secreta serà a.

Xifrat: Suposem que en Bob vol enviar un missatge $m \in G$ a l'Alice. En Bob tria un enter a l'atzar, $2 < y < N$, i calcula $Y = g^y \in G$ i també $Z = mA^y$. Aleshores envia a Alice la tupla (Y, Z).

Desxifrat: Per recuperar el missatge, Alice calcula $Y^{-a}Z$. Observem que

$$Y^{-a}Z = g^{-ay}mg^{ay} = m.$$

3.6 Comptatge de punts: l'algoritme de Schoof

En aquest apartat volem estudiar el problema de determinar, donada una corba $E/\mathbb{F}_p$, el nombre de punts $\#E(\mathbb{F}_p)$. Ja sabem que, pel Teorema de Hasse,

$$\#E(\mathbb{F}_p) = p + 1 - a, \quad \text{amb } |a| \leq 2\sqrt{p}.$$

Suposem també que $p > 3$ (en cas contrari, és molt fàcil determinar $E(\mathbb{F}_p)$), i escrivim E en la forma $E\colon y^2 = x^3 + Ax + B$, amb $A, B \in \mathbb{F}_p$. Recordem el símbol de Legendre, que podem pensar que pren arguments a $\mathbb{F}_p$:

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{si } x = 0, \\ +1 & \text{si } x \in (\mathbb{F}_p^\times)^2, \\ -1 & \text{si } x \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2. \end{cases}$$

Aleshores, observem que

$$\#E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + Ax + B}{p}\right)\right) = 1 + p + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{p}\right),$$

[2] https://www.certicom.com/content/certicom/en/the-certicom-ecc-challenge.html

i per tant tenim una formula tancada per a:

$$a = -\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+Ax+B}{p}\right).$$

Ja hem vist dues maneres de calcular $\left(\frac{x}{p}\right)$ de manera eficient, per qualsevol x fixat. Tot i així, si p és molt gran (que sigui útil en criptografia) no podrem recórrer[3] tots els elements de $\mathbb{F}_p$.

El 1985, R. Schoof va donar el primer algoritme que calculava $\#E(\mathbb{F}_p)$ amb un nombre d'operacions polinomial en $\log(p)$, fet que va permetre d'utilitzar les corbes el·líptiques en la criptografia de manera pràctica. Seguidament veurem les idees principals de l'algoritme d'Schoof.

A la Remarca 3.4.4 hem vist que si $P=(x,y)\in E(K)$, on $K/\mathbb{F}_p$ és una extensió qualsevol, aleshores

$$(x^{p^2},y^{p^2})+[p](x,y)=[a](x^p,y^p). \tag{3.1}$$

La quantitat de l'esquerra es pot calcular de manera eficient, fent servir exponenciació modular pel primer terme, i l'anàleg de l'exponenciació modular per corbes el·líptiques pel segon.

Remarca 3.6.1 Fixem-nos que l'enter a no es pot extreure directament de $[a]$ actuant en punt qualsevol, ja que si (x,y) té ordre N, aleshores (x^p,y^p) també (per què?), i per tant $[a+kN](x^p,y^p)=[a](x^p,y^p)$ per a tot k. Així, el punt (x,y) només permet determinar a mòdul N.

La idea de Schoof consisteix en determinar $a \pmod{\ell}$ per suficients primers ℓ petits, i després reconstruir a fent servir el teorema xinès dels residus. Per exemple, per determinar $\#E(\mathbb{F}_p)$ amb $p\simeq 10^{71}$ n'hi ha prou amb considerar $2<\ell<100$. Afegint-hi els 5 primers que hi ha fins a $\ell<115$ ja podem determinar $\#E(\mathbb{F}_p)$ amb $p\simeq 10^{91}$, i amb dos primers més (127, 131) ja podem arribar a $p\simeq 10^{100}$.

Fem primer el cas $\ell=2$.

Lema 3.6.2 L'enter a és parell si, i només si, x^3+Ax+B té arrels a $\mathbb{F}_p$.

Demostració. Recordem que x^3+Ax+B factoritza a $\mathbb{F}_p$ si i només si $E(\mathbb{F}_p)$ té un element d'ordre 2, que serà de la forma $(\alpha,0)$ on α és una arrel de x^3+Ax+B. Ara bé, com que p és senar tenim

$$\#E(\mathbb{F}_p)=p+1-a\equiv a \pmod 2,$$

i $E(\mathbb{F}_p)$ té un element d'ordre 2 si i només si $\#E(\mathbb{F}_p)$ és parell. ■

Així, considerem ara un primer ℓ senar, i ens cal trobar un punt d'ordre ℓ. No podem esperar que aquest punt estigui definit a $\mathbb{F}_p$, i per tant en general haurem de considerar extensions $K/\mathbb{F}_p$.

Teorema 3.6.3 Considerem els polinomis $\psi_m\in\mathbb{Z}[x,y]$,

$$\begin{aligned}
&\psi_1=1,\quad \psi_2=2y,\quad \psi_3=3x^4+6Ax^2+12Bx-A^2,\\
&\psi_4=4y(x^6+5Ax^4+20Bx^3-5A^2x^2-4ABx-8B^2-A^3),\\
&\psi_{2m+1}=\psi_{m+2}\psi_m^3-\psi_{m-1}\psi_{m+1}^3, && (m\geq 2),\\
&\psi_{2m}=\frac{\psi_m}{2y}(\psi_{m+2}\psi_{m-1}^2-\psi_{m-2}\psi_{m+1}^2), && (m\geq 3).
\end{aligned}$$

[3] En l'actualitat es fan servir primeres d'entre 50 i 80 xifres decimals, i cal tenir en compte que un ordinador actual trigaria l'edat de l'univers a recórrer els enters entre 1 i 10^{27}.

Aleshores per a tot primer senar $\ell \neq p$, es té $\psi_\ell \pmod p \in \mathbb{F}_p[x,y^2]$ i, si substituim $y^2 = x^3 + Ax + B$ obtenim un polinomi en x de grau $\frac{\ell^2-1}{2}$. A més, $P \in E(\bar{\mathbb{F}}_p)[\ell] \setminus \{\mathscr{O}\} \iff \psi_\ell(x(P)) = 0$.

Corol·lari 3.6.4 Per tot primer $\ell \neq p$, es té $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$.

Demostració. Els punts d'$E[\ell] = E(\bar{\mathbb{F}}_p)[\ell]$ són de la forma (α,β) on α és una arrel de ψ_ℓ. Per tant, $\#E[\ell] = 1 + 2\deg(\psi_\ell) = \ell^2$. Com que tot $E[\ell]$ té exponent ℓ, necessàriament $E[\ell] = (\mathbb{Z}/\ell\mathbb{Z})^2$. ■

Si prenem $K/\mathbb{F}_p$ un cos on ψ_ℓ tingui alguna arrel α, aleshores podem considerar el punt de ℓ-torsió $P = (\alpha, \sqrt{D}) \in E(K(\sqrt{D}))$, on $D = \alpha^3 + A\alpha + B$. Per tant, per determinar $a \bmod \ell$ caldrà calcular múltiples de P en el grup $E[\ell](K(\sqrt{D}))$. Fixem-nos que aquest cos té un grau gran $(\ell^2 - 1)$, i per tant les operacions seran molt costoses si ℓ es fa moderadament gran.

Podem treballar al cos K, sense afegir una arrel de D: considerem la corba

$$E^D : y^2 = x^3 + AD^2x + BD^3.$$

Aleshores, si escrivim $\delta = \sqrt{D}$, tenim un isomorfisme $\tau : E \to E^D$ que envia (x,y) a $\tau(x,y) = (Dx, \delta^3 y)$, i que ens permet realitzar totes les operacions a $E^D(K)$. Fixem-nos que si D és un quadrat, aleshores E és isomorfa a E (via τ) però en general l'isomorfisme està definit sobre una extensió de grau 2. En tot cas, observem que

$$\tau((\alpha,\delta)) = (D\alpha, D^2), \quad \tau((\alpha^p,\delta^p)) = (D\alpha^p, D^{\frac{p+3}{2}}), \quad \tau((\alpha^{p^2},\delta^{p^2})) = (D\alpha^{p^2}, D^{\frac{p^2+3}{2}}).$$

Per tant, l'equació (3.1) és equivalent a la següent equació a E^D:

$$(D\alpha^{p^2}, D^{\frac{p^2+3}{2}}) + [p](D\alpha, D^2) = [a](D\alpha^p, D^{\frac{p+3}{2}}).$$

Acabem la secció amb una implementació en Sage de l'algoritme d'Schoof.

Algoritme 3.6.1 Donats E i primers p i ℓ, calcula $p+1-\#E(\mathbb{F}_p)$ mòdul ℓ.

```
def t_mod(A, B, p, ell):
    pmod = p % ell
    if pmod > ell / 2:
        pmod -= ell
    A = GF(p)(A)
    B = GF(p)(B)
    t = PolynomialRing(GF(p), 't').gen()
    if ell == 2:
        return 1 if (t^3+A*t+B).is_irreducible() else 0
    E0 = EllipticCurve([0,0,0,A,B])
    h = E0.division_polynomial(ell,t,0).factor()[0][0]
    K.<r> = FiniteField(p^h.degree(), modulus = h)    # K = F[x]/(h(x))
    D = r^3 + A * r + B
    E = EllipticCurve([A*D^2, B*D^3])
    P = E([D*r, D^2])
    phi_P = E([D * r^p, D^((p+3)//2)])
    phi2_P = E([D * r^(p^2), D^((p^2+3)//2)])
    LHS = phi2_P + pmod * P; RHS = E(0)
    for a in range((ell+1) // 2):
        if LHS ==  RHS: return a
        elif LHS == -RHS: return -a
        RHS += phi_P
```

Algoritme 3.6.2 Donats E i p, calcula $p+1-\#E(\mathbb{F}_p)$.

```
def Schoof(A, B, p): # y^2 = x^3 + Ax + B
    M = 1; ell = 1; S = []; traces = []
    while M <= 4*RR(p).sqrt():
        ell = next_prime(ell); S.append(ell); M *= ell
        traces.append(t_mod(A, B, p, ell))
    a = CRT(traces, S) # Fem servir el Teorema Xinès dels Residus
    return a if a < M / 2 else a - M
```

Finalment, vegem la complexitat d'aquest algoritme. Els polinomis ψ_ℓ tenen grau $O(\ell^2) = O(\log^2 p)$. Per tant, els elements de l'extensió K tenen tamany $O(\ell^2 \log p) = O(\log^3 p)$. Per calcular α^p i α^{p^2} calen $O(\log p)$ operacions a K, i per tant en total $O((\log p)(\log^3 p)^2)$, és a dir $O(\log^7 p)$. Com que això s'ha de fer per $O(\log p)$ primers (pel Teorema dels Nombres Primers), en total calen $O(\log^8 p)$ operacions de bit. Si es poden fer operacions a K de manera més ràpida (per exemple fent servir transformades de Fourier) es pot reduir la complexitat a $O(\log^{5+\varepsilon} p)$. Millores posteriors de Elkies i Atkin permeten calcular $\#E(\mathbb{F}_p)$ amb temps $O(\log^{4+\varepsilon} p)$.

4. Primalitat i factorització

4.1 Primalitat

En aquesta secció estudiarem diferents algoritmes que ens permeten decidir si un enter n és primer. És el que es coneix com *tests de primalitat*.

4.1.1 El test de Fermat

El primer test pràctic que analitzem es basa en explotar el petit Teorema de Fermat. Sabem que si n és primer aleshores per tot enter a amb $\gcd(a,n) = 1$ es té $a^{n-1} \equiv 1 \pmod{n}$. Donarem un nom als nombres compostos que es comporten com a primers des del punt de vista d'aquest resultat.

Definició 4.1.1 Un enter compost senar n s'anomena *pseudoprimer en base a* si $\gcd(a,n) = 1$ i $a^{n-1} \equiv 1 \pmod{n}$.

Observem que n és pseudoprimer en bases a i b, aleshores també ho és en les bases ab i ab^{-1} (on l'invers el fem mòdul n).

Lema 4.1.2 Si n no és pseudoprimer en una base $(a \in \mathbb{Z}/n\mathbb{Z})^\times$, aleshores n no ho és en com a mínim la meitat de les possibles bases a.

Demostració. Sigui $\{a_1,\dots,a_s\}$ el conjunt de les bases en les quals n és pseudoprimer. Sigui $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ una base en la qual n no és pseudoprimer. Aleshores $\{aa_1,\dots,aa_s\}$ és un conjunt de s residus tals que n no és pseudoprimer en aquelles bases. ■

Definició 4.1.3 Un enter compost n és *de Carmichael* si n és pseudoprimer en totes les bases $b \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Els primers nombres de Carmichael són $561 = 3\cdot 11\cdot 17$, $1105 = 5\cdot 13\cdot 17$, $1729 = 7\cdot 13\cdot 19$,... Per tant, donat un enter senar n, si triem k bases b i trobem que

$$b^{n-1} \equiv 1 \pmod{n}$$

per a cadascuna de les bases b, podem deduir que o bé n és de Carmichael, o bé n és primer amb probabilitat $1-2^{-k}$.

La següent proposició (sobretot la segona part) ens pot donar una idea de com de difícil és de trobar nombres de Carmichael.

Proposició 4.1.4 Sigui n un primer compost.
1. Si n és de Carmichael, aleshores n és lliure de quadrats.
2. Si n és lliure de quadrats, aleshores n és de Carmichael si i només si $p-1 \mid n-1$ per tot $p \mid n$.

Demostració. Per veure (1), escrivim $n = p^t m$ amb $t \geq 2$ i p primer no dividint m. El teorema xinès dels residus ens permet trobar un enter a tal que $a \equiv 1+p \pmod{p^t}$ i $a \equiv 1 \pmod{m}$. Aleshores a és coprimer amb n (per què?) i , com que n és de Carmichael, $a^n \equiv a \pmod{n}$. En particular, calculant mòdul p^2 (que divideix n) tenim $(1+p)^n \equiv 1+p \pmod{p^2}$, però $(1+p)^n \equiv 1+np \equiv 1 \pmod{p^2}$. Per tant $p \equiv 0 \pmod{p^2}$, que és una contradicció.

Per demostrar (2), suposem que n és de Carmichael i considerem un primer $p \mid n$. Triem un enter b que tingui ordre $p-1$ mòdul p, i pel teorema xinès dels residus trobem un a tal que $a \equiv b \pmod{p}$ i $a \equiv 1 \pmod{n/p}$. Aleshores, calculant mòdul p arribem a que $b^{n-1} \equiv 1 \pmod{p}$ i per tant $p-1 \mid n-1$. De manera recíproca, si suposem que $p-1 \mid n-1$ per a tot $p \mid n$, aleshores si a és coprimer amb n i $p \mid n$ també tindrem $p \nmid a$ i, per tant, $a^{p-1} \equiv 1 \pmod{p}$. La hipòtesi ens diu que $a^{n-1} \equiv 1 \pmod{p}$. Com que això passa per a tot p i n és lliure de quadrats, deduïm que $a^{n-1} \equiv 1 \pmod{n}$, com volíem veure. ■

Corol·lari 4.1.5 Si n és un nombre de Carmichael, aleshores és producte de com a mínim tres primers.

Demostració. Suposem, per arribar a contradicció, que $n = pq$ és producte de només dos primers, amb $p < q$. Treballem mòdul $(q-1)$, i sabem que $n-1 \equiv 0 \pmod{q-1}$. Però $n = pq$ i $q \equiv 1 \pmod{q-1}$, per tant $0 \equiv n-1 \equiv pq-1 \equiv p-1 \pmod{q-1}$. D'aquí en treiem que $q-1$ divideix $p-1$, que és una contradicció amb el fet que $p < q$. ■

4.1.2 El test de Solovay-Strassen

Podem millorar el test de Fermat amb el que hem après al capítol anterior. D'entrada, si n és primer aleshores sabem que per a tot a coprimer amb n es té

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

Això ens donaria un altre test, però malauradament també hi ha nombres anàlegs al de Carmichael que passen aquest test sense ser primers. El primer exemple és $n = 1729 = 7 \cdot 13 \cdot 19$.

L'existència del símbol de Jacobi ens permet millorar aquest test. Sabem que, si n és primer, aleshores es satisfà el criteri d'Euler: per a tot $1 < a < n$,

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}. \tag{4.1}$$

Tenim maneres eficients de calcular els dos costats de la igualtat: exponenciació modular per una banda, i la llei de reciprocitat quadràtica per l'altra. Per tant, per cada a obtenim un test que potencialment ens pot certificar que n és compost.

Definició 4.1.6 Un enter a és un testimoni d'Euler (per la no-primalitat de n) si $\gcd(a,n) > 1$ o bé no satisfà l'Equació (4.1).

L'avantatge d'aquest criteri és que no hi ha àngels dels nombres de Carmichael. De fet, veurem que si n és compost trobarem molts testimonis d'Euler coprimers amb n.

Teorema 4.1.7 — Solovay–Strassen. Sigui $n > 1$ un compost senar. Aleshores existeix un testimoni d'Euler amb $\gcd(a,n) = 1$.

Demostració. Primer suposem que $n = p_1 p_2 \cdots p_r$ sigui lliure de quadrats. Sigui b un no-quadrat mòdul p_1, i sigui a un enter menor que n i satisfent (gràcies al teorema xinès dels residus):

$$a \equiv b \pmod{p_1}$$
$$a \equiv 1 \pmod{p_2 \cdots p_r}.$$

Sabem que $a \neq 1$, perquè $b \not\equiv 1 \pmod{p_1}$. Cap dels p_i divideix a, i per tant $\gcd(a,n) = 1$. D'altra banda, per la definició d'a és evident que $\left(\frac{a}{n}\right) = -1$. Suposem que no fos un testimoni d'Euler. Aleshores tindríem $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$. Mirant l'equivalència mòdul p_2, obtindrem $1 \equiv -1 \pmod{p_2}$, contradicció.

Ara suposem que $n = p^2 n'$. Com abans, construïm $1 < a < n$, amb $\gcd(a,n) = 1$ i satisfent

$$a \equiv (1+p) \pmod{p^2}$$
$$a \equiv 1 \pmod{n'}.$$

Per obtenir una contradicció, elevem al quadrat l'Equació (4.1) i obtenim que $a^{n-1} \equiv 1 \pmod{n}$. Però mòdul p^2 podem calcular:

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

Per tant, obtindríem $(n-1)p \equiv 0 \pmod{p^2}$, i per tant $n - 1 \equiv 0 \pmod{p}$, que és una contradicció amb el fet que p divideix n. ■

Corol·lari 4.1.8 Sigui $n > 1$ un compost senar. Aleshores més de la meitat dels enters $1 < a < n$ són testimonis d'Euler.

Demostració. Considerem el grup $G = (\mathbb{Z}/n\mathbb{Z})^\times$ de les unitats mòdul n, i definim

$$H = \left\{ a \in G \mid \left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \right\}.$$

Observem que H és un subgrup de G, ja que els dos membres de la igualtat que defineix H són multiplicatius. El teorema de Solovay–Strassen ens demostra que $H \neq G$, i per tant H és un subgrup propi de G. Per tant, $\#H \leq \frac{\#G}{2} < \frac{n-1}{2}$. ■

Algoritme 4.1.1 Test de Solovay–Strassen

```
def solovay_strassen(n, t=10):
    # Assumim que n és senar i més gran que 2
    R = Zmod(n)
    m = (n-1) // 2
    for _ in range(t):
        a = ZZ.random_element(2, n)
        if gcd(a, n) > 1:
            return False # n és compost
        if Mod(a, n)^m != jacobi_symbol(a,n):
            return False # n és compost
    return True # n és primer amb probabilitat 1-2^-t
```

4.1.3 El test de Miller–Rabin

Suposem que n sigui un pseudoprimer en base a. Per tant,

$$a^{n-1} \equiv 1 \pmod{n}.$$

La idea és que si anem fent arrels quadrades d'aquesta igualtat i n és primer, anirem trobant 1 fins que al final trobarem un -1. Si això no passa, aleshores deduirem que n és compost.

Definició 4.1.9 Escrivim un enter compost $n = 2^e k + 1$, amb k senar. Direm que n és pseudoprimer fort en base $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ si $a^k \equiv 1 \pmod{n}$ o hi ha algun i amb $0 \leq i < e$ tal que

$$a^{2^i k} \equiv -1 \pmod{n}.$$

Teorema 4.1.10 — Miller, Monier. Un enter compost n és pseudoprimer fort per com a molt el 25% de les possibles bases $1 \leq a < n$.

Demostració. Primer de tot, estudiem el cas on $n = p^\alpha$ és una potència d'un primer. Recordem que, en aquest cas, el grup $(\mathbb{Z}/n\mathbb{Z})^\times$ és cíclic d'ordre $(p-1)p^{\alpha-1}$. Si n és pseudoprimer fort en base a, aleshores $a^{p-1} \equiv 1 \pmod{n}$: per la definició, és clar que $a^{n-1} \equiv 1 \pmod{n}$. Per tant, l'ordre d'$a$ és un divisor de $\gcd(\varphi(n), n-1)$. Com que $\varphi(n) = (p-1)p^{\alpha-1}$ i $p-1$ divideix a $n-1$ i p no divideix a $n-1$, $\gcd(\varphi(n), n-1) = p-1$. Com que hi ha exactament $p-1$ elements que satisfacin aquesta congruència, obtindrem que hi ha com a molt la proporció

$$\frac{p-1}{(p-1)p^{\alpha-1}} = \frac{1}{p^{\alpha-1}}$$

de bases dolentes. Per $n = 9$ comprovem a mà que el teorema és cert, i per per tot altre n la quantitat $\frac{1}{p^{\alpha-1}}$ és menor que $1/4$, com volíem.

A partir d'ara, podem suposar que n és divisible per com a mínim dos primers. Escrivim, com abans, $n = 2^e k + 1$ amb k senar. Sigui i_0 l'enter més gran en el conjunt $\{0, 1, \ldots, e-1\}$ tal que hi ha alguna base a_0 satisfent $a_0^{2^{i_0}} \equiv -1 \pmod{n}$. Definim els següents subconjunts de $(\mathbb{Z}/n\mathbb{Z})^\times$:

$$F = \{a \colon a^{n-1} \equiv 1 \pmod{n}\},$$
$$H = \{a \colon a^{2^{i_0} k} \equiv \pm 1 \pmod{n}\}.$$

Podem comprovar fàcilment que les bases per les quals n és pseudoprimer fort pertanyen a tots dos, i que tenim les següent inclusions:

$$H \subseteq F \subseteq (\mathbb{Z}/n\mathbb{Z})^\times.$$

També és fàcil de veure que F i H són subgrups de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Primer de tot, vegem que H és sempre un subgrup propi d'F, trobant un element $a \in F \setminus H$. Escollim $p \mid n$, i escrivim $n = pn'$ amb $n' > 1$. Pel teorema xinès dels residus, podem trobar una classe a satisfent $a \equiv a_0 \pmod{p}$ i $a \equiv 1 \pmod{n'}$. Aleshores, recordant que k és senar, tenim

$$a^{2^{i_0} k} \equiv a_0^{2^{i_0} k} \equiv (-1)^k \equiv -1 \pmod{p}.$$

D'altra banda, mòdul n' tenim la congruència

$$a^{2^{i_0} k} \equiv 1^{2^{i_0} k} \equiv 1 \pmod{n'}.$$

Per tant, $a^{2^{i_0} k}$ no pot ser ni 1 ni -1 mòdul n, i per tant a no pertany a H. D'altra banda, comprovem que

$$a^{2^{i_0+1} k} \equiv 1 \pmod{n},$$

i per tant $a^{n-1} \equiv 1 \pmod{n}$, cosa que demostra que a pertany a F.

Això ja ens demostra que com a molt hi ha un 50% de bases per les quals n no és pseudoprimer fort: com que $H \neq (\mathbb{Z}/n\mathbb{Z})^\times$, el subgrup H té índex com a mínim 2. Hem de treballar una mica més per reduir aquesta fita al 25%. Observem, però que si n no és de Carmichael aleshores $F \neq (\mathbb{Z}/n\mathbb{Z})^\times$ (tautològicament). Com que ja hem vist que en general $F \neq H$, obtenim

$$H \subsetneq F \subsetneq (\mathbb{Z}/n\mathbb{Z})^\times$$

i per tant $\#H/(n-1) < \frac{\#H}{\#\mathbb{Z}/n\mathbb{Z})^\times} \leq 1/4$.

Podem doncs assumir que n és de Carmichael i que, per tant, és divisible per com a mínim 3 primers. Escrivim $n = p_1 \cdots p_r$ amb $r \geq 3$. Introduïm el següent subgrup:

$$G = \{a \colon a^{2^{i_0}k} \equiv \pm 1 \pmod{p}, \quad \forall p \mid n\}.$$

Observem que $H \subseteq G \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$. Veurem que $[G\colon H] = 2^{r-1} \geq 4$. Considerem l'aplicació

$$f \colon G \to \prod_{i=1}^{r} \{\pm 1\}, \quad a \mapsto (a^{2^{i_0}k} \bmod p_i)_{i=1,\ldots,r}.$$

És obvi que f és un morfisme de grups. Sigui $K = \ker f$, un subgrup de H. Observem que la imatge de H és $f(H) = \{(1,1,\ldots,1),(-1,-1,\ldots,-1)\}$, un grup d'ordre 2. Per tant $[H\colon K] = 2$. D'altra banda, si veiem que f és exhaustiva aleshores G/K tindrà ordre 2^r, i per tant:

$$[G\colon H] = \frac{[G\colon K]}{[H\colon K]} = \frac{2^r}{2} = 2^{r-1} \geq 2^2 = 4.$$

Per acabar, doncs, n'hi ha prou amb veure que f és exhaustiva. Donat un element qualsevol $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r)$ de $\prod_{i=1}^{r}\{\pm\}$, definim a mitjançant el teorema xinès dels residus de manera que

$$a \equiv \begin{cases} a_0 \pmod{p_i} & \text{si } \varepsilon_i = -1, \\ 1 \pmod{p_i} & \text{si } \varepsilon_i = 1. \end{cases}$$

Aleshores és fàcil de veure que $f(a) = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r)$, com volíem. ■

Remarca 4.1.11 Només hi ha un pseudoprimer fort respecte les bases $2,3,5,7$ per $n \leq 2.5 \cdot 10^{10}$, que és $n = 3215031751$.

El test de Miller–Rabin consisteix en triar unes quantes bases i comprovar si n és pseudoprimer fort en totes les bases triades. Si es dona el cas, es decideix que n és primer; i si per alguna base no passa el test es té una demostració que n és compost. Així, tenim:

$$\text{Prob}(\text{error} \mid n \text{ primer}) = 0, \quad \text{Prob}(\text{error} \mid n \text{ compost}) < 4^{-k}.$$

Veiem tot seguit una possible implementació del test de Miller–Rabin.

Algoritme 4.1.2 Test de Miller–Rabin

```
def es_pseudoprimer_fort(n,base):
    s = 0
    t = n - 1
    while t % 2 == 0:
        s += 1
        t /= 2
    #En aquest punt es compleix que 2^s * t == n - 1
    bt = Mod(base,n)^t
    if bt == 1:
        return True
    while bt != -1:
        if s == 0:
            return False
        bt ^= 2
        s -= 1
    return True

def es_primer_miller_rabin(n,k):
    for _ in xrange(k):
        a = ZZ.random_element(1, n)
        if not es_pseudoprimer_fort(n, a):
            return False
    return True
```

El test de Miller–Rabin no dona una manera de demostrar la primalitat de n, llevat de comprovar més d'una quarta part de les bases, que és impràctic. Tot i així, si assumim una generalització de la hipòtesi de Riemann (coneguda com a GRH per funcions-L de Dirichlet) aleshores tenim:

Proposició 4.1.12 Suposem GRH. Si n és un enter compost senar, aleshores hi ha alguna base $a < 2\log^2 n$ tal que n no és pseudoprimer fort en base a.

Aquesta proposició dona lloc a un algoritme polinomial que determina si n és primer o no, subjecte a una conjectura no provada. És a dir, deixaríem de creure una probabilitat per passar a creure en una conjectura.

4.1.4 El test de Lucas

Aquest test es basa en la següent observació.

Proposició 4.1.13 Sigui $n > 1$ un natural. Aleshores n és primer si i només si hi ha algun enter a, amb $1 < a < n$, tal que $a^{n-1} \equiv 1 \pmod{n}$, i tal que per a tot primer $p \mid n-1$ satisfà $a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$.

Demostració. Si n és primer, aleshores $\mathbb{F}_n^\times$ és cíclic d'ordre $n-1$, i si a és un generador, es compleixen les dues condicions. Recíprocament, si $a^{n-1} \equiv 1 \pmod{n}$, aleshores $\gcd(a,n) = 1$. La segona condició ens diu que l'ordre d'a a $(\mathbb{Z}/n\mathbb{Z})^\times$ és exactament $n-1$, i això només pot passar si n és primer. ■

■ **Exemple 4.1.14** Vegem que 103 és primer fent aquest test. Com que $102 = 2 \cdot 3 \cdot 17$, hem de trobar a tal que

$$a^{102} \equiv 1, \quad a^6 \not\equiv 1, \quad a^{34} \not\equiv 1, \quad a^{51} \not\equiv 1 \pmod{103}$$

Amb $a = 2,3,4$ no funciona, però amb $a = 5$ obtenim

$$a^{102} \equiv 1, \quad a^6 \equiv 72, \quad a^{34} \equiv 56, \quad a^{51} \equiv 102 \pmod{103}.$$

■

■ **Exemple 4.1.15** Vegem que $n = 134369$ és primer fent aquest test. Observem que $134368 = 2^5 \cdot 13 \cdot 17 \cdot 19$. Comprovem que 3 satisfà $3^{n-1} \equiv 1 \pmod{n}$, i

$$3^{\frac{n-1}{2}} \equiv 134368, \quad a^{\frac{n-1}{13}} \equiv 17862, \quad 3^{\frac{n-1}{17}} \equiv 73312, \quad 3^{\frac{n-1}{19}} \equiv 103556 \pmod{134369}.$$

Per tant, concloem que n és primer. ■

L'avantatge del test de Lucas és que, si podem factoritzar completament $n-1$, obtenim una demostració de la primalitat de n. Per demostrar que els factors primers de $n-1$ són de fet primers, podem aplicar de nou el test de Lucas, i si fem aquest procés de manera recursiva arribem a una demostració incondicional de la primalitat de n, que és fàcilment verificable. El conjunt de dades involucrades en aquesta cadena s'anomena *certificat de primalitat de Pratt*.

Algoritme 4.1.3 Test de Lucas

```
def test_lucas(n,a, trust = 100):
    verbose('Test de Lucas amb n = %s i base = %s'%(n,a))
    if Mod(a,n)^(n-1) != 1:
        return False
    primers_dubtosos = []
    for p,_ in ZZ(n-1).factor(): # Això pot ser molt lent!
        if p > trust:
            primers_dubtosos.append(p)
        verbose('Provant p = %s...'%p)
        if Mod(a,n)^((n-1) // p) == 1:
            return False
        verbose(' ... OK.')
    for p in primers_dubtosos:
        b = 2
        while not test_lucas(p, b, trust): # Crida recursiva
            b += 1 # Sabem que acabarà, perquè 'factor' funciona
    return True
```

4.1.5 El test de Pocklington

El problema principal del test de Lucas és que requereix la factorització de $n-1$, que pot ser molt costosa. El següent test relaxa aquesta condició, i també ens dona un certificat. Escrivim $n-1 = AB$ amb $\gcd(A,B) = 1$. Farem servir el següent teorema.

Teorema 4.1.16 — Pocklington. Si per tot factor $p \mid A$, existeix un enter a_p tal que

1. $a_p^{n-1} \equiv 1 \pmod{n}$, i
2. $\gcd(a_p^{\frac{n-1}{p}} - 1, n) = 1$,

aleshores per tot primer $q \mid n$ es té $q \equiv 1 \pmod{A}$.

Demostració. Suposem $p^e \parallel A$, i escrivim $b_p = a_p^{\frac{n-1}{p^e}}$. Aleshores tenim

$$b_p^{p^e} \equiv a_p^{n-1} \equiv 1 \pmod{q}, \quad b_p^{p^{e-1}} \equiv a_p^{\frac{n-1}{p}} \not\equiv 1 \pmod{q}.$$

Per tant, l'ordre de b_p a $(\mathbb{Z}/q\mathbb{Z})^\times$ és exactament p^e. Per tant, en deduïm que $p^e \mid q-1$. Això és cert per cada $p^e \parallel A$, i per tant obtenim $A \mid q-1$, com volíem. ■

Corol·lari 4.1.17 Amb les hipòtesis del teorema, si a més tenim $A > B$ aleshores n és primer.

Demostració. El teorema ens diu que, per tot primer $q \mid n$, tenim $q-1 \geq A$. Com que $A > B$ i $AB = n-1$, tenim $A > \sqrt{n}$. Per tant, $q > \sqrt{n}$. Però si n fos compost hauria de tenir un divisor primer $\leq \sqrt{n}$, i arribem a una contradicció. ■

▪ **Exemple 4.1.18** Considerem $n = 2,175,282,177,377$. Calculem fàcilment la factorització parcial de $n-1$:

$$n-1 = 2^5 \cdot 7^2 \cdot 11^3 \cdot 1,042,297.$$

No intentem factoritzar l'últim factor $B = 1,042,297$ (que de fet és $1,009 \cdot 1033$), ja que $A = 2^5 \cdot 7^2 \cdot 11^3 = 2,087,008 > B$.

Comprovem que $a_2 = 3$, $a_7 = 3$ i $a_{11} = 2$ satisfan les hipòtesis del teorema, i per tant n és primer. ▪

El següent algoritme comprova que n és primer fent servir un certificat que consisteix en una llista de primers `plist` amb enters a_p corresponents donats per `alist`.

Algoritme 4.1.4 Test de Pocklington

```
def test_pocklington(n, plist, alist):
    A = 1
    for a, p in zip(alist, plist):
        if not ZZ(p).is_prime(): # Hauríem de comprovar-ho recursivament!
            return False
        A *= p^((n-1).valuation(p))
        if Mod(a,n)^(n-1) != 1:
            return False
        if gcd(Mod(a,n)^((n-1)/p) -1, n) != 1:
            return False
    if A * A > n-1:
        return True
    return False
```

4.2 Algoritmes de factorització

D'entre els mètodes per determinar la primalitat de n, només el mètode del garbell ens dona un factor de n si aquest és compost. Els altres mètodes ens diran que n és compost, sense donar-nos cap informació dels factors de n. En aquesta § veurem mètodes que intenten trobar un factor no trivial de n quan ja sabem que aquest existeix.

4.2.1 ρ de Pollard

Per aplicar aquest mètode, hem de triar una aplicació $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ que sigui fàcil d'evaluar. Més endavant ens convindrà que f sigui un polinomi amb coeficients enters; de fet, una tria usual és $f(x) = x^2 + 1$.

Triem també, a l'atzar, un element $x_0 \in \mathbb{Z}/n\mathbb{Z}$. Definim una successió a $\mathbb{Z}/n\mathbb{Z}$ de manera recursiva, com

$$x_1 = f(x_0), x_2 = f(x_1) = f(f(x_0)), \ldots, x_{j+1} = f(x_j), \quad j \geq 0.$$

La idea és que aquesta successió també defineix una successió a $\mathbb{Z}/d\mathbb{Z}$ on $d \mid n$ és un divisor propi de n. En algun moment, es donarà el fet que $x_j \equiv x_k \pmod{d}$ (amb $j \neq k$), i aleshores

$$d \mid \gcd(x_j - x_k, n) \mid n.$$

Per tant, si calculem els màxims comuns divisors entre les diferències dels termes i el nostre n, en algun moment trobarem un divisor propi. Ens cal, però, una estimació de quants termes haurem de considerar per arribar a una tal coincidència.

Proposició 4.2.1 Sigui S un conjunt de d elements, i sigui $0 < \varepsilon < 1$ real. Donada una parella (f, x_0) on $f\colon S \to S$ i $x_0 \in S$, definim la successió $x_{j+1} = f(x_j)$. Definim també $\ell = 1 + \lfloor \sqrt{-2d\log(\varepsilon)} \rfloor$.

La proporció de parelles (f, x_0) per les quals $x_0, x_1, \ldots x_\ell$ són tots diferents és $< \varepsilon$.

■ **Exemple 4.2.2** Per exemple, per més de la meitat de les possibles tries (f, x_0) en un conjunt S de tamany 1000, trobarem una repetició entre els primers 38 termes. Pel 99% de les possibles parelles (f, x_0) trobarem una repetició entre els primers 96 termes. ■

Demostració. Hi ha $d^d \cdot d = d^{d+1}$ parelles (f, x_0) possibles. D'entre elles, si volem que els primers ℓ termes siguin tots diferents, aleshores hi ha d possibilitats per x_0, $d-1$ possibilitats per x_1, i així fins a $d - \ell$ possibilitats per x_ℓ. Aleshores, cal definir encara f per la resta de termes. Així, obtenim una proporció de

$$\frac{d^{d-\ell} \prod_{j=0}^{\ell} (d-j)}{d^{d+1}} = \prod_{j=1}^{\ell} \left(1 - \frac{j}{d}\right).$$

Prenent el logaritme i fent servir que per $x \in (0,1)$ es té que $\log(1-x) < -x$, obtenim

$$\log\left(\prod_{j=1}^{\ell} \left(1 - \frac{j}{d}\right)\right) < -\sum_{j=1}^{\ell} \frac{j}{d} = \frac{-\ell(\ell+1)}{2d} < -\frac{\ell^2}{2d}.$$

Com que $\ell > \sqrt{-2d\log(\varepsilon)}$, obtenim el resultat. ■

Corol·lari 4.2.3 L'algoritme ρ de Pollard troba, amb probabilitat més gran que $1 - \varepsilon$, un factor no trivial de n en $O(\sqrt[4]{n})$ passos, on la constant implícita depèn d'ε.

Demostració. Com que n té un factor no trivial $d < \sqrt{n}$, el terme ℓ de l'enunciat de la proposició és $O\left(\sqrt{-\log(\varepsilon)}\sqrt[4]{n}\right)$. ■

Fixem-nos que en el pas k, després de calcular x_k caldria realitzar k gcd's. Per fer-ho ràpid, podem aprofitar la següent observació:

Lema 4.2.4 Suposem que f ve donada per un polinomi amb coeficient enters, i siguin k_0 i j_0 dos índexos tals que $x_{k_0} \equiv x_{j_0} \pmod{d}$. Aleshores $x_k \equiv x_j \pmod{d}$ per a tot (k, j) tals que $k - j = k_0 - j_0$.

Demostració. Escrivim $j = j_0 + t$ i $k = k_0 + t$, amb $t \geq 0$. Aleshores podem fer inducció en t, fent servir que si $x_{j-1} \equiv x_{k-1} \pmod{d}$ aleshores $x_j = f(x_{j-1}) \equiv f(x_{k-1}) = x_k \pmod{d}$. ■

Aleshores, en l'algoritme modificat calculem, a cada pas:

$$x_k = f(x_{k-1}), \quad y_k = x_{2k} = f(f(y_{k-1})).$$

Si calculem $\gcd(y_k - x_k, n) = \gcd(x_{2k} - x_k, n)$, en el pas on $k = |j_0 - k_0|$ la diferència d'índexos és la mateixa i, per tant, detectarem el divisor d.

Una altra millora que es pot fer a l'algoritme per estalviar el càlcul de molts gcd és el de calcular, per cada iteració, $z = \prod_{k=k_0}^{k_0+100}(x_{2k} - x_k)$, i seguidament calcular $\gcd(z, n)$. Així, canviem 100 càlculs de gcd per 99 multiplicacions i un sol càlcul de gcd. Pot passar que $\gcd(z, n)$ sigui n, i aleshores simplement podem refer el càlcul dels 99 termes que ens hem saltat, tot esperant que algun d'ells ens doni un factor no trivial.

Com que es pot calcular el gcd fent $O(\log^3(n))$ operacions de bits, aquest algoritme troba (amb probabilitat alta, depenent de ε) un factor no trivial en $O(\sqrt[4]{n}\log^3 n)$ operacions de bits (recordem que el garbell d'Eratòstenes requereix $O(\sqrt{n}\log^2 n)$ operacions).

```
def pollard_rho(n):
    R = Zmod(n)
    x = R.random_element()
    y = x
    g = 1
    while g == 1 or g == n:
        x, y = x^2 + 1, (y^2 + 1)^2 + 1
        g = gcd((x-y).lift(), n)
    return g
```

4.2.2 Mètode $(p-1)$ de Pollard

Suposem donat un primer n compost, i ens proposem trobar un factor no trivial de n. El mètode $(p-1)$ de Pollard funciona bé quan algun dels primers p que divideixen n (que no coneixem) satisfà que cap dels divisors primers de $p-1$ no són grans.

Definició 4.2.5 Donat $B > 0$, diem que un enter k és B-potència-suau si per a tot primer p,

$$p^e \mid k \implies p^e \leq B.$$

El mètode és el següent:

1. Fixem una fita B i definim (però no calculem explícitament) k_B com
$$k_B = \prod_{\ell \leq B} \ell^{\alpha_\ell}, \quad \alpha_\ell = \lfloor \log B / \log \ell \rfloor$$
2. Triem un enter a l'atzar $a \in \{2, \ldots, k_B - 2\}$.
3. Calculem $c = a^{k_B} \bmod n$ fent servir exponenciació modular.
4. Si $1 < \gcd(c-1, n) < n$, ja hem trobat un divisor no trivial de n. Si no, tornem a començar amb un altre a o una altra B.

Suposem que $p \mid n$ és un primer tal que $p-1$ és B-potència suau. Aleshores, k_B és un múltiple de $p-1$ i, pel petit teorema de Fermat, tenim

$$a^{k_B} \equiv 1 \pmod{p}.$$

Per tant $p \mid \gcd(a^{k_B}-1, n)$. Pot passar que el gcd resulti en n, que passarà si $a^{k_B} \equiv 1 \pmod{n}$. En cas contrari, l'algoritme retorna un divisor no trivial.

Remarca 4.2.6 Només un 15% dels primers en l'interval $[10^{15}, 10^{15}+10000]$ satisfan que $p-1$ és 10^6-potència-suau. Això fa que aquest mètode sigui bastant limitat.

Algoritme 4.2.1 Factorització amb el mètode $(p-1)$ de Pollard

```
def factor_pollard_pm1(n, B = 100):
    while True:
        a = Zmod(n).random_element()
        for i in range(2, B + 1): # Calculem a^(B!)
            a = a^i
        g = gcd(a.lift()-1, n)
        if g > 1 and g < n:
            return g
        else:
            B *= 2
```

4.2.3 El mètode de Lenstra

Com hem vist, el problema amb el mètode $p-1$ de Pollard és que si resulta que tots els factors primers $p \mid n$ són tals que $p-1$ té factors grans, aleshores el mètode no funcionarà. El *mètode de Lenstra*, també conegut com el *mètode de factorització amb corbes el·líptiques* es basa en canviar els grups $(\mathbb{Z}/p\mathbb{Z})^\times$ pel grup de punts $E(\mathbb{F}_p)$ d'una corba el·líptica. Com que E podrà variar, tindrem molts més grups dels quals podem esperar que algun tingui ordre potència-suau.

■ **Exemple 4.2.7** Imaginem que hem pres $B = 12$, i que $n = 59 \cdot 101 = 5959$. Aleshores

$$59-1 = 58 = 2 \cdot 29, \quad 101-1 = 100 = 4 \cdot 25$$

no són B-potència-suaus. En canvi,

$$101-2 = 99 = 9 \cdot 11$$

sí que és B-potència-suau. De fet, la corba el·líptica amb equació $y^2 = x^3 + 744x + 1$ té 99 punts mòdul 101. Per tant, ja veiem que tindrem més possibilitats d'èxit si podem canviar $p-1$ per $p \pm s$ per algun s. ■

El mètode per trobar un divisor propi $d \mid n$ depèn, com en el mètode $p-1$ de Pollard, d'un paràmetre inicial B, que podem anar augmentant progressivament.

1. Definim (però no calculem explícitament) k_B com

$$k_B = \prod_{\ell \le B} \ell^{\alpha_\ell}, \quad \alpha_\ell = \lfloor \log B / \log \ell \rfloor$$

2. Triem un enter a de manera aleatòria, i considerem la corba el·líptica $E\colon y^2 = x^3 + ax + 1$ i un punt $P = (0,1) \in E(\mathbb{Q})$.

3. Calculem $d = \gcd(4a^3 + 27, n)$. Si $d > 1$, hem trobat un factor propi de n (si $d < n$), o bé triem una altre a. Si $d = 1$, continuem.
4. Intentem calcular $k_B P$ pensant E com una corba definida a $\mathbb{Z}/n\mathbb{Z}$. Per fer-ho, calculem:

$$2^{\alpha_2}P, 3^{\alpha_3}(2^{\alpha_2}P), \ldots, k_B P.$$

5. Si en algun dels passos anteriors no podem fer una divisió mòdul n (fent servir l'algoritme d'Euclides), és perquè la quantitat que volem invertir no és coprimera amb n, i això ens donarà un factor.
6. Tornem al pas 1 fins que funcioni.

Teorema 4.2.8 — Lenstra. Si assumim com a certes algunes conjectures estàndard, el nombre d'operacions de bit necessàries per factoritzar n és[a]

$$O\left(e^{\sqrt{(1+\varepsilon)\log n \log\log n}}\right)$$

[a] Cal assumir també que n no sigui divisible ni per 2 ni per 3 i que no sigui una potència perfecta.

Algoritme 4.2.2 Factorització de Lenstra

```
def factor_lenstra(n, intents = 100, B = 10000):
    R = Zmod(n)
    import re # Per tractar amb expressions regulars
    for i in range(intents):
        Q = EllipticCurve([R.random_element(),1])([0,1])
        try:
            for ell in prime_range(B):
                Q *= ell^ZZ(floor(RR(B).log(ell)))
        except ZeroDivisionError as e:
            return ZZ(re.search(r'\d+', str(e)).group()).gcd(n)
```

4.2.4 Bases de factors: l'algoritme de Dixon

El mètode de Fermat

Comencem amb un exemple senzill, conegut des dels temps de Fermat.

■ **Exemple 4.2.9** Suposem que volem factoritzar $n = 200819$. Si calculem

$$\lceil \sqrt{n} \rceil = \lceil 448.1283\ldots \rceil = 449$$

podem escriure

$$449^2 = 200819 + 782, \quad 450^2 = 200819 + 1681, \ldots$$

Fixem-nos ara que $1681 = 41^2$ és un quadrat perfecte. Per tant,

$$200819 = 450^2 - 41^2 = (450+41)(450-41) = 491 \cdot 409,$$

i hem obtingut una factorització de 200819 (caldria comprovar que 491 i 409 són primers, però això només requeriria comprovar que no són divisibles per cap primer ≤ 19). ■

El mètode que hem fet servir a l'exemple anterior es basa en el següent fet trivial:

Lema 4.2.10 Hi ha una correspondència bijectiva

$$\{\text{ factoritzacions } n=ab,\ a\geq b>0\}\longleftrightarrow\{\text{ representacions } n=t^2-s^2,\ t\geq 0, s\geq 0\},$$

donada per $(t,s)=(\frac{a+b}{2},\frac{a-b}{2})$ i $(a,b)=(t+s,t-s)$.

■ **Exemple 4.2.11** Factoritzem ara $n=141467$. Si provem pels enters $\lceil\sqrt{n}\rceil=377$ i els següents $(378,379,380,381,382,\ldots)$ ens adonem que cap d'aquests és un quadrat perfecte. Però en canvi, podem provar

$$t=\lceil\sqrt{3n}\rceil=652,653,\ldots$$

i de seguida trobarem $655^2-3\cdot 141467=68^2$. Per tant, obtenim $3n=(655+68)(655-68)=723\cdot 587$. Si fem $\gcd(n,723)=241$ obtenim un factor no trivial de n. ■

El mètode de l'exemple anterior s'anomena *Fermat generalitzat*. Ha funcionat per $n=141467$ perquè hi ha una factorització $n=ab$ amb $b\simeq 3a$. En general, si $n=ab$ amb $b\simeq ka$, podrem aplicar el mètode amb enters propers a $\sqrt{kn}$.

L'algoritme de Dixon

Podem repensar el mètode de Fermat generalitzat com el problema de trobar parelles (t,s) tals que $t^2-s^2=kn$ per algun k. Dit d'altra manera, estem buscant parelles (t,s) amb $t^2\equiv s^2 \pmod n$ (i amb $t\neq\pm s \pmod n$). Si aconseguim trobar una d'aquestes parelles, aleshores $\gcd(n,t+s)$ ens donarà un factor propi de n.

■ **Exemple 4.2.12** Com que $118^2\equiv 25=5^2 \pmod{4633}$, trobem factors

$$\gcd(4633,118+5)=41,\quad \gcd(4633,118-5)=113,$$

i resulta que $4633=41\cdot 113$. ■

D'ara en endavant anomenarem *residu reduït* l'enter entre $-n/2$ i $n/2$ en la classe de $a \pmod n$. Escriurem $a \bmod n$ per denotar aquest residu.

Definició 4.2.13 Una *base de factors* és un conjunt de primers (i aquí -1 també es compta com a primer)

$$B=\{p_1=-1,p_2,\ldots,p_h\}.$$

Un enter k és un *B-nombre mòdul n* si $k^2 \bmod n$ es pot escriure com a producte d'elements de B (potser amb repetició).

■ **Exemple 4.2.14** Prenem $B=\{-1,2,3\}$ i $n=4633$. Aleshores

$$67^2 \bmod n=-144=-1\cdot 2^4\cdot 3^2,\quad 68^2 \bmod n=-9=-1\cdot 3^2,\quad 69^2 \bmod n=128=2^7.$$

Veiem que 67, 68 i 69 són B-nombres mòdul n. En canvi, 66 no ho és perquè $66^2 \bmod n=-277$. ■

En la situació de l'exemple anterior, fixem-nos que

$$(67\cdot 68)^2\equiv(2^2\cdot 3^2)^2 \pmod n.$$

És a dir, que $77^2\equiv 36^2 \pmod n$ (perquè $67\cdot 68\equiv -77 \pmod n$), i d'aquí podem obtenir el factor no trivial $\gcd(77+36,4633)=113\mid 4633$.

Fixem-nos que a cada B-nombre b li podem associar un vector $v_b\in\mathbb{F}_2^{\#B}$, corresponent als exponents mòdul 2 de la factorització de $b^2 \bmod n$.

■ **Exemple 4.2.15** Seguint amb $n = 4633$ i $B = \{-1,2,3\}$, podem calcular

$$v_{67} = (1,0,0), \quad v_{68} = (1,0,0), \quad v_{69} = (0,1,0).$$

■

Per obtenir una factorització, ens cal trobar prou enters b de manera que el conjunt $\{v_{b_1}, \ldots, v_{b_h}\}$ sigui linealment dependent a $\mathbb{F}_2^{\#B}$. En particular, si $h > \#B$ això ja ho tindrem garantit, encara que pot ser que trobem una relació amb menys vectors. Una relació de dependència donarà lloc a una factorització, de la següent manera: si per cert subconjunt $J \subset \{1,\ldots,h\}$ tenim $\sum_{j\in J} v_{b_j} = 0$, aleshores obtindrem la congruència

$$\left(\prod_{j\in J} b_j\right)^2 \equiv \left(\prod_{i=1}^{\#B} p_i^{r_i}\right)^2 \pmod{n},$$

on els exponents r_i s'obtenen fàcilment de la factorització de cadascun dels b_j^2 mod n involucrats: escrivim $\beta_j = b_j^2 \bmod n$, i aleshores

$$r_i = \frac{1}{2}\sum_{j\in J} v_{p_i}(\beta_j).$$

Si triem enters b mòdul n a l'atzar, obtenim el que es coneix com l'algoritme de Dixon. També els podem triar de manera que b^2 mod n sigui petit (perquè així la probabilitat que b sigui un B-nombre serà més alta. La manera com s'aconsegueix això dona lloc per una banda a l'algoritme basat en fraccions continuades, i per altra al garbell quadràtic.

4.2.5 Fraccions continuades

Hem vist que per dur a terme l'algoritme de Dixon ens cal trobar enters b tals que b^2 mod N sigui petit (comparat amb N). Les fraccions continuades donen una manera de trobar bons candidats b.

Donat un real x, definim les successions (possiblement finites) $(a_i)_{i\geq 0}$ i $(x_i)_{i\geq 0}$ com:

$$\begin{aligned} a_0 &= \lfloor x \rfloor, & x_0 &= x - a_0 \\ a_1 &= \left\lfloor \frac{1}{x_0} \right\rfloor, & x_1 &= \frac{1}{x_0} - a_1 \\ a_{i+1} &= \left\lfloor \frac{1}{x_i} \right\rfloor, & x_{i+1} &= \frac{1}{x_i} - a_{i+1}, \quad (i \geq 1). \end{aligned}$$

Si en algun moment $x_{i-1} = \pm 1$, aleshores $x_i = 0$ i la successió serà finita. Donats reals a_i, fem servir la notació

$$[a_0; a_1, a_2, \ldots, a_k] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; + \cfrac{1}{a_k}}}}$$

Lema 4.2.16 Per a tot $x \in \mathbb{R}$ i per a tot $i \geq 0$, es té $x = [a_0; a_1, a_2, \ldots, a_i + x_i]$.

Demostració. Per $i = 0$ és clar: $[a_0 + x_0] = a_0 + x_0 = a_0 + x - a_0 = x$. Suposem-ho cert per $i \geq 0$. De la definició, i fent servir que $a_{i+1} + x_{i+1} = 1/x_i$, tenim

$$[a_0; a_1, \ldots, a_i, a_{i+1} + x_{i+1}] = [a_0; a_1, \ldots, a_i + x_i].$$

Per tant, el resultat és cert per inducció. ■

Proposició 4.2.17 La successió $(a_i)_{i\geq 0}$ és finita si i només si $x \in \mathbb{Q}$.

Demostració. Una direcció és fàcil: si la successió és finita aleshores per algun $i \geq 0$ tindrem $x_i = 0$ i, per tant, $x = [a_0; a_1, \ldots, a_i]$, que és un nombre racional.

Suposem doncs que x és racional, i vegem que la successió és finita. Fixem-nos que en aquest cas $x_i \in \mathbb{Q}$ per a tot $i \geq 0$ (ho veiem fàcilment per inducció). També veiem fàcilment que $0 \leq x_i < 1$. Escrivim doncs $x_i = r_i/s_i$ amb $r_i < s_i$, i veurem que $(s_i)_{i\geq 0}$ és estrictament decreixent. Això farà que en algun moment s_i hagi de ser 1 i aleshores $x_i = 0$. Per veure que $s_{i+1} < s_i$, hem de calcular el denominador de x_{i+1}:

$$x_{i+1} = \frac{1}{x_i} - a_{i+1} = \frac{1 - x_i a_{i+1}}{x_i} = \frac{s_i - r_i a_{i+1}}{r_i}.$$

Per tant, $s_{i+1} \leq r_i < s_i$, com voliem. ■

Suposem ara que x no és racional i que, per tant, té una fracció continuada infinita.

Definició 4.2.18 Si $x \in \mathbb{R} \setminus \mathbb{Q}$, la n-èssima convergent és el nombre racional $[a_0; a_1, \ldots, a_n]$.

Definim successions $(p_n)_{n\geq 0}$ i $(q_n)_{n\geq 0}$ recursivament:

$$\begin{aligned} &p_0 = a_0, && p_1 = a_0 a_1 + 1, && p_n = a_n p_{n-1} + p_{n-2} \quad (n \geq 2) \\ &q_0 = 1, && q_1 = a_1, && q_n = a_n q_{n-1} + q_{n-2} \quad (n \geq 2). \end{aligned}$$

Proposició 4.2.19 Sigui $x \in \mathbb{R} \setminus \mathbb{Q}$.

1. Per a tot $n \geq 0$, es té la identitat

$$p_{n+1} q_n - p_n q_{n+1} = (-1)^n. \tag{4.2}$$

2. La n-èssima convergent és p_n/q_n, i està en forma reduïda.

Demostració. Per inducció es veu fàcilment (1), i que la n-èssima convergent és p_n/q_n. Aleshores de l'Equació (4.2) obtenim $\gcd(p_n, q_n) = 1$ i, per tant, p_n/q_n és una fracció reduïda. ■

Proposició 4.2.20 Per a tot $x \in \mathbb{R} \setminus \mathbb{Q}$, es té $\lim_{n\to\infty} \frac{p_n}{q_n} = x$.

Demostració. Si a l'Equació (4.2) dividim per $q_n q_{n+1}$ obtenim

$$\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n q_{n+1}}.$$

Com que els $(q_n)_{n\geq 1}$ són estrictament creixents, veiem que les convergents formen una successió de Cauchy. Per trobar el límit, observem que podem escriure

$$x = [a_0; \ldots, a_{n+1} + x_{n+1}] = \frac{p_n \frac{1}{x_n} + p_{n-1}}{q_n \frac{1}{x_n} + q_{n-1}}.$$

Per tant,

$$x - \frac{p_n}{q_n} = \frac{p_n \frac{1}{x_n} + p_{n-1}}{q_n \frac{1}{x_n} + q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n-1} q_n - p_n q_{n-1}}{q_n (q_n/x_n + q_{n-1})} = \frac{(-1)^n}{q_n (q_n/x_n + q_{n-1})}.$$

Prenent el valor absolut, obtenim

$$\left|x-\frac{p_n}{q_n}\right| = \frac{1}{q_n(q_n/x_n+q_{n-1})} < \frac{1}{q_n(a_{n+1}q_n+q_{n-1})} = \frac{1}{q_nq_{n+1}}$$

Com que $q_n \to \infty$, obtenim el resultat. ■

La demostració de la proposició anterior ens permet veure la següent estimació.

Corol·lari 4.2.21 Per a tot $n \geq 0$, es té $\left|x-\frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$.

La següent proposició ens permet estudiar com de bones són les aproximacions racionals que obtenim amb les convergents.

Proposició 4.2.22 Si $x > 1$, aleshores $|q_n^2x^2 - p_n^2| < 2x$.

Demostració. Escrivim

$$|q_n^2x^2-p_n^2| - 2x = q_n^2|x-p_n/q_n||x+p_n/q_n| - 2x < \frac{q_n}{q_{n+1}}\left(2x+\frac{1}{q_nq_{n+1}}\right) - 2x = \star$$

Reordenant, obtenim la cadena de desigualtats

$$\star < 2x\left(-1+\frac{q_n}{q_{n+1}}+\frac{1}{2xq_{n+1}}\right) < 2x\left(-1+\frac{q_n}{q_{n+1}}+\frac{1}{q_{n+1}}\right) < 2x(-1+\frac{q_n+1}{q_{n+1}}) < 0.$$

■

Corol·lari 4.2.23 Sigui $N > 1$ un enter que no sigui un quadrat perfecte, i siguin p_n/q_n les convergents de $\sqrt{N}$. Aleshores

$$|p_n^2 \bmod N| < 2\sqrt{N}.$$

Demostració. Apliquem la proposició anterior a $x = \sqrt{N}$. ■

Per tant, veiem que els termes de la successió $(p_n)_{n\geq 0}$ ens proporcionen bons candidats per obtenir B-nombres a l'hora de factoritzar un enter N. El següent algoritme calcula successivament aquests termes.

Algoritme 4.2.3 Càlcul de la fracció continuada d'$\sqrt{n}$.

```
def frac_continuada_sqrt(n):
    F.<s> = NumberField(x^2 - n)
    v = F.hom([RealField(2 * len(n.bits()))(n).sqrt()])
    b0 = 1
    b = v(s).floor()
    a, x = b, s - b
    yield b
    while True:
        xinv = 1 / x
        a =  v(xinv).floor()
        x = xinv - a
        b, b0 = a * b + b0, b
        yield b
```

Tal i com hem dit, ens cal una manera eficient de determinar si un enter és B-suau, que eviti la factorització d'aquest.

Algoritme 4.2.4 Factorització per fraccions continuades.

```
def factor_fraccions_continuades(n,B):
    rvalues = []
    rvecs = Matrix(ZZ,0,len(B),0) # Relacions trobades
    rvecs_mod2 = Matrix(GF(2),0,len(B),0) # El mateix, però mòdul 2
    for x in frac_continuada_sqrt(n):
        if 2 * x > n: x -= n
        y = x^2 % n
        if 2 * y > n: y -= n
        if gcd(y,n) > 1: # Molt improbable
            return g
        vec = es_B_suau(y,B)
        if vec: # Hem tingut sort: x^2 mod n és B-suau
            rel = Matrix(ZZ, 1, len(B), vec)
            rvecs = rvecs.stack(rel)
            rvecs_mod2 = rvecs_mod2.stack(rel)
            rvalues.append(x)
            for v in rvecs_mod2.kernel().basis():
                v = v.lift() # Són 0 o 1, els volem com a enters
                x0 = prod(r^i for r,i in zip(rvalues,v))
                y0 = prod(p^(ap // 2) for p, ap in zip(B, v * rvecs))
                g = gcd(x0 - y0, n)
                if g > 1 and g < n:
                    return g
```

Algoritme 4.2.5 Determina si un enter és B-suau.

```
def es_B_suau(n,B):
    v = []
    for p in B:
        if p == -1:
            val, n = n.sign(), n.abs()
        else:
            val = n.valuation(p)
            n //= p^val
        v.append(val)
    return v if n == 1 else False
```

Acabem aquesta § amb un resultat interessant sobre fraccions continuades, encara que no ens serveixi directament per factoritzar.

■ **Exemple 4.2.24** Calculem la fracció continuada del valor $x = \sqrt{7} = 2.64575131106459\ldots$. Comencem amb

$$a_0 = \lfloor \sqrt{7} \rfloor = 2, \quad x_0 = \sqrt{7} - 2 = 0.64575131106459\ldots.$$

Seguim calculant:

$$\begin{aligned}
\frac{1}{x_0} &= \frac{1}{\sqrt{7}-2} = \frac{2+\sqrt{7}}{3} = 1.548583\ldots && \rightsquigarrow a_1 = \mathbf{1}, \quad x_1 = \frac{-1+\sqrt{7}}{3} = 0.548583\ldots \\
\frac{1}{x_1} &= \frac{3}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{2} = 1.82287\ldots && \rightsquigarrow a_2 = \mathbf{1}, \quad x_2 = \frac{\sqrt{7}-1}{2} = 0.82287\ldots \\
\frac{1}{x_2} &= \frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3} = 1.21525\ldots && \rightsquigarrow a_3 = \mathbf{1}, \quad x_3 = \frac{\sqrt{7}-2}{3} = 0.21525. \\
\frac{1}{x_3} &= \frac{3}{\sqrt{7}-2} = \sqrt{7}+2 = 4.6457513\ldots && \rightsquigarrow a_4 = \mathbf{4}, \quad x_4 = \sqrt{7}-2 = 0.6457513\ldots
\end{aligned}$$

Observem que $x_4 = x_0$ i que, per tant $a_{n+4} = a_n$ i $x_{n+4} = x_n$ per a tot $n \geq 4$. Per tant la fracció continuada és periòdica:

$$\sqrt{7} = [2;1,1,1,4,1,1,1,4,1,1,1,4,\ldots] = [2;\overline{1,1,1,4}]$$

■

■ **Exemple 4.2.25** Suposem que $x \in \mathbb{R}$ té fracció continuada $x = [3;5,3,5,3,5,3,\ldots]$. Aleshores podem escriure

$$x = 3 + \frac{1}{5+\frac{1}{x}} \Longrightarrow 3 + \frac{x}{5x+1} = x \Longrightarrow \frac{16x+3}{5x+1} = x,$$

és a dir $5x^2 - 15x - 3 = 0$, que té arrels $\frac{15\pm\sqrt{285}}{10}$. Fixem-nos que $x > 0$, i per tant $x = \frac{15+\sqrt{285}}{10}$. ■

El comportament dels exemples anteriors és més general, i de fet podem caracteritzar per quins reals obtenim fraccions continuades periòdiques.

Teorema 4.2.26 Un real x té una fracció continuada periòdica (infinita) si i només si x satisfà un polinomi de grau dos amb coeficients racionals.

Demostració. Ja hem caracteritzat els racionals i les fraccions continuades finites, per tant podem assumir que la fracció continuada és infinita (i que x no és racional).

Primer, suposem que

$$x = [a_0;a_1,\ldots,a_n,\overline{a_{n+1},\ldots,a_{n+h}}].$$

Escrivim $\alpha = [a_{n+1};a_{n+2},\ldots]$. Aleshores tenim que $\alpha = [a_{n+1};\ldots,a_{n+h},\alpha]$. Per tant,

$$\alpha = \frac{\alpha p_{n+h} + p_{n+h-1}}{\alpha q_{n+h} + q_{n+h-1}}.$$

D'aquí en deduïm que α satisfà un polinomi quadràtic. Com que

$$x = [a_0;a_1,\ldots,a_n,\alpha] = a_0 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \cfrac{1}{\alpha}}},$$

veiem que $x \in \mathbb{Q}(\alpha)$ i, com que $x \notin \mathbb{Q}$ obtenim que x també satisfà un polinomi quadràtic.

Suposem ara que x satisfà $ax^2+bx+c = 0$, amb $a,b,c \in \mathbb{Z}$ i $a \neq 0$. Si $x = [a_0;a_1,\ldots]$, definim r_n com la cua $[a_{n+1};a_{n+2},\ldots]$, de tal manera que $x = [a_0;a_1,\ldots,a_n,r_n]$ per tot $n \geq 0$. Veurem que

r_n només pren un conjunt finit de valors. Aleshores, si $r_{n+h} = r_n$ per algun $n \geq 0$ i algun $h > 0$, tindrem

$$\begin{aligned}[a_0;\ldots,a_n,r_n] &= [a_0;\ldots,a_n,a_{n+1},\ldots,a_{n+h},r_{n+h}]\\ &= [a_0;\ldots,a_n,a_{n+1},\ldots,a_{n+h},r_n]\\ &= [a_0;\ldots,a_n,a_{n+1},\ldots,a_{n+h},a_{n+1},\ldots,a_{n+h},r_{n+h}]\\ &= [a_0;\ldots,a_n,\overline{a_{n+1},\ldots,a_{n+h}}].\end{aligned}$$

De l'expressió $x = [a_0;a_1,\ldots,a_n,r_n]$ tenim $x = \frac{r_n p_n + p_{n-1}}{r_n q_n + q_{n-1}}$. Si substituïm aquesta expressió a l'equació quadràtica, i agrupem els termes en r_n obtenim $A_n r_n^2 + B_n r_n + C_n = 0$, amb

$$\begin{aligned}A_n &= ap_n^2 + bp_n q_n + cq_n^2\\ B_n &= 2ap_n p_{n-1} + b(p_n q_{n-1} + p_{n-1}q_n) + 2cq_n q_{n-1}\\ C_n &= ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2.\end{aligned}$$

Ens hem de fixar que $A_n, B_n, C_n \in \mathbb{Z}$ i que $C_n = A_{n-1}$. Veurem que aquests valors estan fitats (independentment de n). Això implica que prenen un conjunt finit de valors i, per tant les arrels r_n dels polinomis quadràtics $A_n X^2 + B_n X + C_n$ també prenen un conjunt finit de valors. Escriurem $f(X) = aX^2 + bX + c$ i, per tot n, escriurem també $\theta_n = p_n/q_n$ la n-èssima convergent.

Per fitar A_n, observem que $A_n = q_n^2 f(\theta_n)$. Aleshores:

$$|f(\theta_n) = |f(\theta_n) - f(x)| = |f'(\xi)||x - \theta_n| < \frac{1}{q_n^2}M, \quad M = \max_{\xi\in[x-1,x+1]} |f'(\xi)|.$$

Per tant $|A_n| < M$ i $|C_n| = |A_{n-1}| < M$. Passem ara a fitar $|B_n|$. Escrivim $B_n = q_n q_{n-1} F(\theta_n, \theta_{n-1})$, on $F(X,Y) = aXY + b\frac{X+Y}{2} + c$. Observem que $F(X,X) = f(X)$, i fàcilment veiem també que

$$f(X) - F(X,Y) = (2ax+b)\frac{X-Y}{2} = f'(X)\frac{X-Y}{2}.$$

Per tant,

$$f(\theta_n) - F(\theta_n, \theta_{n-1}) = \frac{1}{2}(\theta_n - \theta_{n-1})f'(\theta_n).$$

Prenent valors absoluts, obtenim

$$|f(\theta_n) - F(\theta_n, \theta_{n-1})| \leq \frac{f'(\theta_n}{2q_n q_{n-1}} \leq \frac{M}{2q_n q_{n-1}}.$$

Aplicant la desigualtat triangular i la fita anterior, concloem que

$$|F(\theta_n, \theta_{n-1}| \leq \frac{M}{2q_n q_{n-1}} + \frac{M}{q_n^2} < \frac{3M}{2q_n q_{n-1}}.$$

Per tant $|B_n| < 3M$. ■

Remarca 4.2.27 Una manera alternativa de veure B_n pot prendre només un conjunt finit de valors (un cop hem vist que A_n i C_n ho fan) és calcular directament (i tediosa)

$$B_n^2 - 4A_n C_n = (b^2 - 4ac)(p_n q_{n-1} - q_n p_{n-1})^2 = b^2 - 4ac.$$

Per tant, $B_n = b^2 - 4ac + 4A_n C_n$ només pren un conjunt finit de valors.

4.2.6 El garbell quadràtic

Recordem que volem trobar B-nombres, és a dir x's tals que $x^2 \mod n$ sigui B-suau. El mètode de les fraccions continuades ens dona bons candidats fent servir les convergents de $\sqrt{N}$. Una alternativa és considerar molts candidats $x = \lceil\sqrt{n}\rceil, \lceil\sqrt{n}\rceil + 1, \lceil\sqrt{n}\rceil + 2, \ldots$ i trobar una manera molt ràpida de distingir quins d'ells són B-nombres.

Primer de tot, com que $x \simeq \sqrt{n}$, aleshores $x^2 \mod n = x^2 - n$. Per tant, no ens caldrà fer cap divisió per reduir mòdul n.

Segon, sigui $p \leq B$. Aleshores $p \mid x^2 - n \iff x^2 \equiv n \pmod{p}$. Considerarem doncs una base de factors formada només per primers p tals que n sigui un quadrat mòdul p. Per cadascun d'aquests primers, ja sabem que només hem de mirar $x \equiv a_1, a_2 \pmod{p}$ (on a_1 i a_2 són arrels de n mod p, que podem calcular fàcilment tal i com hem vist a la Secció 2.4). Així, podem construir una taula on a la fila i hi desem les quantitats $x = \lceil\sqrt{n}\rceil + i$ i $x^2 - n$, amb $0 \leq i \leq X$ (per alguna fita X).

Per cada $p \leq B$ amb $\left(\frac{n}{p}\right) = 1$, dividim les entrades $x^2 - n$ de les files $i \equiv a_1, a_2 \pmod{p}$ per p tantes vegades com sigui possible. A l'acabar, aquelles files on haguem obtingut un 1 són precisament les que es corresponen a B-nombres.

Algoritme 4.2.6 Factorització pel garbell quadràtic

```
def factor_garbell_quadratic(n, Bmax, inc):
    B = [-1,2] + [p for p in prime_range(3,Bmax) \
                    if legendre_symbol(n,p) == 1]
    x = RR(n).sqrt().floor()
    relations = []
    relation_matrix = Matrix(GF(2),0,len(B),0)
    k0 = x
    while relation_matrix.rank() < len(B):
        llista_garbellada = garbell(k0, k0 + inc, B, n)
        k0 += inc
        for x, y in llista_garbellada:
            vec = es_B_suau(y,B)
            rel = Matrix(GF(2),1,len(B),[GF(2)(a) for a in vec])
            relation_matrix = relation_matrix.stack(rel)
            relations.append((x,vec))
        for v in relation_matrix.kernel().basis():
            vlist = v.list()
            x0 = prod(ZZ(r[0])^ZZ(i) for r,i in zip(relations,vlist))
            y0 = 1
            for j, p in enumerate(B):
                ap = sum(r[1][j] for k, r in enumerate(relations) \
                                 if vlist[k] == 1)
                y0 *= p^(ap // 2)
            g = gcd(x0 - y0,n)
            if g > 1 and g < n:
                return g
```

Algoritme 4.2.7 Garbella un interval

```
def garbell(k0, k1, B, n):
    N = k1 - k0
    llista = [[x, x*x - n] for x in range(k0, k1)]
    for p in B:
        if p == -1: continue
        x0 = GF(p)(n).sqrt()
        x1 = (-x0).lift()
        x0 = x0.lift()
        for i in range((x0-k0) % p, N, p) + range((x1-k0) % p, N, p):
            llista[i][1] = llista[i][1].prime_to_m_part(p)
    return [(x, x*x - n) for x,y in llista if y == 1]
```

El nombre d'operacions que ens caldran per fer aquest procés és $O(X\sum_{p\leq B}\frac{1}{p}) = O(X\log\log B)$. Per tant, per a cada valor hi hem d'invertir $O(\log\log B)$ operacions, en comptes de les $O(B)$ necessàries sense fer el garbell.

Proposició 4.2.28 Triant B adequadament (en funció de n) s'obté un algoritme que factoritza en

$$O\left(e^{(1+\varepsilon)\sqrt{\log n\log\log n}}\right) \text{ operacions.}$$

4.3 Algoritmes pel logaritme discret

4.3.1 Pohlig–Hellman

Aquest algoritme funciona bé quan $G = \langle b\rangle$ té ordre n divisible només per primers petits. Donat $y \in G$, l'objectiu és trobar $x \in \mathbb{Z}/n\mathbb{Z}$ tal que $b^x = y$.

El primer pas consisteix en calcular les arrels p-èssimes de 1, per cada divisor primer $p \mid n$. Definim doncs

$$r_{p,j} = b^{j\frac{n}{p}}, \quad j = 0,1,\ldots,p-1.$$

Observem que només és factible calcular i emmagatzemar aquestes quantitats si els primers p són relativament petits.

Fixem-nos també en que, si es té una factorització $n = \prod_p p^\alpha$, només cal trobar $x \pmod{p^\alpha}$ per cada $p \mid n$ i després calcular x fent servir el teorema dels residus xinesos.

Fixem doncs un primer $p \mid n$, i volem trobar

$$x \equiv x_0 + x_1 p + \cdots + x_{\alpha-1}p^{\alpha-1} \pmod{p^\alpha}, \quad 0 \leq x_i < p.$$

L'algoritme ens permet calcular $x_0, x_1, x_2, \ldots$ pas a pas.

Pas 0: Definim $y_0 = y$, i calculem $y_0^{\frac{n}{p}}$, que és una arrel p-èssima de 1 perquè $y^n = 1$. per tant,

$$y^{\frac{n}{p}} = (b^x)^{\frac{n}{p}} = b^{x_0\frac{n}{p}} = r_{p,x_0}.$$

És a dir x_0 s'obté de mirar en quina posició es troba la quantitat $y^{\frac{n}{p}}$ en la taula $\{r_{p,i}\}_{i=0,\ldots p-1}$.

Pas 1: Canviem y per $y_1 = yb^{-x_0}$, que té logaritme discret $x - x_0 = x_1 p + \cdots x_{\alpha-1}p^{\alpha-1}$. Per tant, $y_1^{\frac{n}{p}} = 1$ i es té $y_1^{\frac{n}{p^2}} = b^{x_1\frac{n}{p}} = r_{p,x_1}$.

$(\cdots)$

Pas i: Definim $y_i = y_{i-1}b^{-p^{i-1}x_{i-1}}$ i calculem $y_i^{\frac{n}{p^{i+1}}} = r_{p,x_i}$.

4.3.2 Rho de Pollard

Aquest és un anàleg del mètode amb al mateix nom per factoritzar. Es tracta de trobar parelles de la forma $b^i y^j$ amb suficients i, j. Suposem que en algun moment tenim $b^i y^j = b^{i'} y^{j'}$, amb $j - j'$ invertible mòdul N. Aleshores, existeix un enter r que satisfà $r(j-j') \equiv 1 \pmod{N}$, i per tant tenim

$$b^{r(i'-i)} = y^{r(j-j')} = y^{1+kN} = y,$$

i haurem calculat el logaritme discret de y en la base b.

Per trobar les parelles $(b^i y^j, b^{i'} y^{j'})$, es consideren tres successions (x_n, i_n, j_n), de tal manera que $x_n = b^{i_n} y^{j_n}$. Es pot inicialitzar la successió a $(1,0,0)$, i aleshores definir la resta de termes de manera recursiva $x_{n+1} = f(x_n)$, on f és:

$$f(x) = \begin{cases} bx & x \in S_0 \\ yx & x \in S_1 \\ x^2 & x \in S_2, \end{cases}$$

amb $G = S_0 \cup S_1 \cup S_2$ una partició en tres conjunts. Aquesta funció anirà donant nous elements de G de manera més o menys aleatòria. Fixem-nos que si $x = b^i y^j$, aleshores $f(x) = b^{i'} y^{j'}$ amb

$$(i', j') = \begin{cases} (i+1, j) & x \in S_0 \\ (i, j+1) & x \in S_1 \\ (2i, 2j) & x \in S_2. \end{cases}$$

(Fixem-nos que les parelles les considerem sempre mòdul N). De la mateixa manera que quan factoritzàvem, podem calcular els termes (x_n, i_n, j_n) i (x_{2n}, i_{2n}, j_{2n}) a la n-èssima iteració, i comparar-los.

Aquest algoritme troba el logaritme discret en $O(\sqrt{N})$ iteracions i és, per tant, un mètode exponencial.

4.3.3 Càlcul d'índexs

Aquest algoritme ens permet calcular el logaritme discret a $\mathbb{F}_p^\times$, on p és un primer gran. Hi ha modificacions que ens permeten calcular-lo també a $\mathbb{F}_q^\times$ (amb q una potència d'un primer), però aquí ens centrarem en el primer cas.

Com sempre, suposem donat un generador b de $\mathbb{F}_p^\times$, i $y \in \mathbb{F}_p^\times$. Volem trobar $x \pmod{p-1}$ tal que $b^x = y$. La clau de l'algoritme radica en el fet que si $b^{x_1} = y_1$ i $b^{x_2} = y_2$, aleshores $b^{x_1+x_2} = y_1 y_2$. Per tant, per exemple si poguéssim factoritzar y (com a enter) simplificariem el problema. Això serà molt difícil de fer en general, però potser podem factoritzar $b^t y \pmod{p}$, i aleshores també guanyem.

L'algoritme funciona de la següent manera.

Precomputació

1. Triem una base de factors $\mathscr{B} = \{-1, 2, 3, 5, 7, 11, \ldots, B\}$.
2. Per $k = 1, 2, 3, \ldots$ intentem factoritzar $b^k \pmod{p}$ en la base $\mathscr{B}$ (només tindrem èxit si $b^k \pmod{p}$ és B-suau).
3. Per cada factorització correcta

$$b^k = \prod_{\ell \in \mathscr{B}} \ell^{\alpha_\ell},$$

afegim una relació $(k, \alpha_{-1}, \alpha_2, \alpha_3, \ldots)$.

4. Quan tinguem $\#\mathscr{B}$ relacions independents, podem trobar (mitjançant àlgebra lineal) els logaritmes discrets de tots els elements de $\mathscr{B}$. Per cada $\ell \in \mathscr{B}$, denotarem per $i(\ell)$ l'enter tal que $b^{i(\ell)} = \ell$.

Logaritme discret

1. Per diferents exponents $t = 1, 2, \ldots$ veiem si $b^t y \pmod{p}$ és $\mathscr{B}$-suau.
2. Quan trobem un t tal que

$$b^t y = \prod_{\ell \in \mathscr{B}} \ell^{\beta_\ell},$$

podem retornar $i(y) = -t + \sum_{\ell \in \mathscr{B}} \beta_\ell i(\ell)$.

Això ens dona un mètode sub-exponencial, però observem que es basa en l'existència de primers a $\mathbb{Z}$. Això fa que aquest tipus d'algoritmes no es puguin aplicar a grups cíclics més generals, i el que permet que el logaritme discret en corbes el·líptiques sigui més difícil que a $\mathbb{F}_q^\times$.

Exposicions orals

1. Demostracions “Euclidianes” de l’existència d’infinits primers en successions aritmètiques.

   Prime Numbers in certian arithmetic progressions. Ram Murty and Nithum Thain
2. El teorema de Schur: $\{p$ primer tal que $p \mid f(n) \neq 0\}$ és infinit, per a tot $f(x) \in \mathbb{Z}[x]$.

   Aigner, M. and Ziegler, G. “Proofs from The Book”
3. El teorema d’aproximació de Dirichlet i aplicació a la solució de l’equació de Pell.

   `http://www-personal.umich.edu/~hlm/math475/pell.pdf`
4. El teorema dels nombres primers (sense demostració).

   Apostol, T. “Introduction to Analytic Number Theory”, Chapters 4 and 13
5. El “primer cas” de l’Últim Teorema de Fermat: p és regular i $x^p + y^p = z^p \implies p \mid xyz$.

   Marcus, D. “Number Fields”
6. Els nombres p-àdics: definició, i el lema de Hensel.

   Gouvea, F. “p-adic numbers: An Introduction”
7. El principi de Hasse local-global: teorema de Minkowski.

   Serre, J.-P. “A course in arithmetic”
8. El principi de Hasse local-global: l’exemple de Selmer.

   `https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf`
9. El Teorema d’Schnirelmann.

   `http://jonismathnotes.blogspot.com/2015/04/schnirelmann-density-and-warings-problem.html`
10. Primalitat és a la classe "P": el test de primalitat AKS.

    `https://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf`
11. Prime gaps, la història.

    `https://dms.umontreal.ca/~andrew/CurrentEventsArticle.pdf`
12. La conjectura de Goldbach, i remarques sobre la demostració de la versió dèbil (ternària).

    Helfgott, H. “The ternary Goldbach conjecture is true”
13. Conjunts de Sidon, i la construcció de Ruzsa.

    Rusza, I. “Solving a linear equation in a set of integers I”
14. Carreres de primers.

    `https://dms.umontreal.ca/~andrew/PDF/PrimeRace.pdf`

15. L'enunciat de la conjectura ABC, i una justificació heurística.

    https://terrytao.wordpress.com/2012/09/18/the-probabilistic-heuristic-justification-of-the-abc-conjecture/

16. La conjectura ABC implica Fermat assimptòtic.

    http://www.ams.org/notices/200210/fea-granville.pdf

17. El teorema dels 15 de Conway–Schneeberger.

    M.Bhargava "On the Conway-Schneeberger Fifteen Theorem"https://www.maths.ed.ac.uk/~v1ranick/books/dublin.pdf

18. L'altura canònica en corbes el·líptiques i el regulador.

    Silverman, J. "The arithmetic of elliptic curves", capítol VIII.9

19. Criptografia basada en isogènies.

    https://eprint.iacr.org/2011/506.pdf

20. El xifrat TRUEncrypt i els atacts coneguts.

    https://www.ntru.org/f/hps98.pdf

21. Signatura digital amb RSA.

    http://cacr.uwaterloo.ca/hac/about/chap11.pdf, pg. 433

22. Xifrat (parcialment) homomòrfic: el xifrat de Pailler.

    https://en.wikipedia.org/wiki/Paillier_cryptosystem

23. L'equació de S-unitats i el teorema de Siegel.

    Hindry, M. and Silverman, J. "Diophantine Approximation", Theorem D.8.1

24. La multiplicació de Karatsuba, anàlisi de la complexitat.

    https://en.wikipedia.org/wiki/Karatsuba_algorithm

25. El teorema de Cayley–Bacharach. Aplicació a la llei de grup d'una corba el·líptica.

    https://staff.math.su.se/shapiro/UIUC/DingPlaneCurves.pdf

26. La funció L d'una corba el·líptica, i la conjectura de Birch i Swinnerton-Dyer.

    https://www.claymath.org/sites/default/files/birchswin.pdf

27. L'enunciat del teorema de modularitat de corbes el·líptiques.

    http://www.ams.org/notices/199911/comm-darmon.pdf

28. La demostració del teorema de Nagell–Lutz.

    Silverman, J., Tate, J. "Rational Points on Elliptic Curves"

29. Teorema de Szemerédi, Teorema de Green–Tao i la conjectura d'Erdös sobre progressions aritmètiques.

    https://en.wikipedia.org/wiki/Szemer%C3%A9di%27s_theorem

30. Sistemes recobridors: definicions i algun exemple (amb demostració)

    http://maths.nju.edu.cn/~zwsun/Cover.pdf

31. El teorema dels 6 exponencials i la conjectura dels 4 exponencials: enunciats i alguna conseqüència.

    https://en.wikipedia.org/wiki/Six_exponentials_theorem

Projectes de Sage

.1 Com factoritza un polinomi mòdul diferents primers, variació 1

En aquest projecte s'estudia la factorització d'un polinomi irreductible amb coeficients enters, mòdul diferents primers. Donat un polinomi $f(x) \in \mathbb{Z}[x]$, definim el seu tipus de factorització mòdul p de la manera següent: suposem que la imatge $\bar{f}(x) \in \mathbb{F}_p[x]$ factoritza com

$$\bar{f}(x) = \bar{f}_1(x)^{e_1} \cdots \bar{f}_g(x)^{e_g} \in \mathbb{F}_p[x],$$

on $\deg \bar{f}_i(x) = d_i$. Aleshores direm que f té tipus de factorització $(d_1^{e_1}, \ldots, d_g^{e_g})$ (on l'ordre no importa). Per exemple, un polinomi de grau 2 pot tenir tipus (2), (1^2) o $(1,1)$ (no posem els exponents si són 1).

Escriviu un programa que, donat un polinomi irreductible, calculi el tipus de factorització mòdul tots els primers fins una fita donada. Direm que un enter positiu M és el *mòdul* d'aquest polinomi si el tipus de factorització mòdul p depèn de la classe de p mòdul M, i M és el menor enter amb aquesta propietat.

Comenceu estudiant polinomis quadràtics, i vegeu quins tipus apareixen. Calculeu el mòdul de qualsevol polinomi quadràtic. Això s'hauria de poder demostrar, fent servir el què hem vist a classe.

Després continueu estudiant els polinomis cúbics. Escriviu un programa que intenti trobar el mòdul d'un polinomi. Podeu trobar exemples de polinomis cúbics amb mòdul i d'altres sense?.

Seguiu amb polinomis de grau més alt. Podeu estudiar els polinomis ciclotòmics (tenen mòdul? quins tipus de factorització apareixen?).

Donat un polinomi irreductible, sabrieu predir si té mòdul o no, a partir d'informació que podeu trobar a `lmfdb.org`?

.2 Com factoritza un polinomi mòdul diferents primers, variació 2

En aquest projecte s'estudia la factorització d'un polinomi irreductible amb coeficients enters, mòdul diferents primers. Donat un polinomi $f(x) \in \mathbb{Z}[x]$, definim el seu tipus de factorització

mòdul p de la manera següent: suposem que la imatge $\bar{f}(x) \in \mathbb{F}_p[x]$ factoritza com

$$\bar{f}(x) = \bar{f}_1(x)^{e_1} \cdots \bar{f}_g(x)^{e_g} \in \mathbb{F}_p[x],$$

on $\deg \bar{f}_i(x) = d_i$. Aleshores direm que f té tipus de factorització $(d_1^{e_1}, \ldots, d_g^{e_g})$ (on l'ordre no importa). Per exemple, un polinomi de grau 2 pot tenir tipus (2), (1^2) o $(1,1)$ (no posem els exponents si són 1).

Escriviu un programa que, donat un polinomi irreductible, calculi el tipus de factorització mòdul tots els primers fins una fita donada.

Ens interessa veure com es reparteixen els primers entre els diferents tipus de factorització. Observeu quina proporció de primers hi ha en cadascuna de les tres classes per polinomis de grau 2.

Després continueu estudiant els polinomis cúbics. Hauríeu de veure diferent comportament depenent del polinomi que trieu.

Seguiu amb polinomis de grau més alt. Intenteu predir quines proporcions trobareu, a partir d'informació que trobeu a `lmfdb.org`. Trobareu molts casos interessants amb grau 6.

.3 Formes quadràtiques representant primers

Considereu una forma quadràtica

$$f(x,y) = ax^2 + bxy + cy^2, \quad \Delta = b^2 - 4ac,$$

i suposem que és definida positiva (és a dir, $\Delta = -D < 0$ i $a > 0$). Dibuixeu els punts

$$R_M = \{(x,y) \in \mathbb{Z}^2 \,:\, |f(x,y)| < M\} \subseteq \mathbb{C},$$

per una constant M que anireu fent gran. Què observeu en la distribució d'aquests punts? Estudieu les coordenades polars d'aquests punts $(x,y) = \rho e^{i\theta}$. En particular, feu histogrames amb els valors de θ.

Podeu formular alguna conjectura? Veieu diferents comportaments quan varieu la forma f?

.4 Nombre de punts mòdul p per corbes el·líptiques

Donada una corba el·líptica E definida sobre $\mathbb{Q}$, definim la funció

$$C_E(x) = \prod_{p \le x} \frac{\#E(\mathbb{F}_p)}{p}, \quad x \in \mathbb{R}_{>0}.$$

Estudieu el comportament assimptòtic de C_E $(x \to \infty)$ per diverses corbes el·líptiques. Per exemple, considereu les corbes:

$$\begin{aligned}
&E_0 \colon y^2 + y = x^3 - x^2,\\
&E_1 \colon y^2 + y = x^3 - x,\\
&E_2 \colon y^2 + y = x^3 + x^2 - 2x,\\
&E_3 \colon y^2 + y = x^3 - 7x + 6.
\end{aligned}$$

Hauríeu de veure un comportament molt diferenciat entre E_0 i la resta d'exemples. Intenteu comparar $C_E(x)$ amb $K\log(x)^n$ per alguna constant K i algun enter $n \ge 0$. Què pot ser que n ens digui sobre la corba E? Hauríeu de poder trobar la resposta consultant la web `lmfdb.org`.