Apunts d'Aritmètica

Marc Masdeu

4 de febrer de 2020

Índex

1 Primers i congruències (∼6h)

1.1 Divisibilitat

Teorema 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 1.2 (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 1.3. *Es té:*

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

Observem que, com a conseqüència, també obtenim

$$\gcd(a, b + at) = \gcd(a, b) \quad \forall t \in \mathbb{Z}.$$

Aquesta observació ens permet calcular el màxim comú divisor entre dos nombres de manera ràpida. Comencem amb un exemple:

Exemple 1.4. 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:

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

També és fàcil de veure que

Lema 1.5. *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 1.6. *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 1.7 (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 1.8. *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 1.9 (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 1.7. 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 1.10 (Euclides)**.** *Hi ha infinits primers.*

Demostració. Donats primers $p_1, p_2, \ldots, p_n$, 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 1.11 (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 $\sqrt{m}$.

```
def garbell(n):
    if n <= 2:
        return []
    P = [2] # El primer més petit és el 2
    if n == 3:
        return P
    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

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

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

Proposició 1.12 (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 1.13. *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 d'anells, podem parlar del nucli $\ker m_a$. Fixem-nos que, com que $\gcd(a,m) = 1$, la Proposició 1.12 ens garanteix

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

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

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

$$ax + my = 1.$$

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

Remarca 1.15. *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 1.16. 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

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

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 1.17. *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 $a/gx \equiv b/g \pmod{n/g}$. □

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 1.18 (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 $\#H = \mathrm{ord}(a) \mid \#G = \varphi(n)$. Per tant, $a^{\varphi(n)}$ és la identitat a G, com voliem veure. □

Corol·lari 1.19 (Petit teorema de Fermat)**.** *Si p és un primer i $p \nmid a$, aleshores*

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

1.3.3 El teorema dels residus xinesos

Teorema 1.20. *Si $m_1, \ldots, m_k$ són enters coprimers entre si, 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 1.21. *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 és té solució perquè $\gcd(m, n) = 1$, tal i com hem vist a la Proposició 1.17.

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 1.20). 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 dels residus xinesos pels grups d'unitats.

Lema 1.22. *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 dels residus xinesos.

Per veure l'exhaustivitat, observem que el teorema dels residus xinesos 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 1.9) 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 1.23. *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 1.24. *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 1.25. *En general, és difícil calcular $\varphi(n)$ eficientment sense conèixer una factorització de n. Per exemple, si $n = pq$ és el producte 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 1.26. *Per a tot $n \geq 1$ es té:*

$$\sum_{1 \leq d | n} \varphi(d) = n$$

Demostració. 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 $k \geq 0$. Els divisors de p^k són de la forma p^r amb $0 \leq r \leq k$, i per tant:

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

□

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

$$g = ax + by. \tag{1}$$

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

Exemple 1.28. 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":

```
def xgcd(a,b):
    signe_a, signe_b = a.sign(), b.sign()
    a, b = a.abs(), b.abs()
    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, signe_a * x, signe_b * y
```

Demostració (de la Proposició 1.27). 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 $a_n, \ldots$ 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 1.29. *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 $x = a + (b-a)xm = ayn + bxm$. 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 $ax = b \pmod{m}$:

```
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 $\mathbb{Z}/m\mathbb{Z}$:

```
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 hauriem d'evitar fer $r-1$ multiplicacions (que és com probablement hem apres a calcular a^r). En l'exemple següent veiem com podem fer-ho més ràpidament.

Exemple 1.30. 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 $\mathbb{Z}/m\mathbb{Z}$.

```
def exponentiate(a,r,m):
    result = 1
    powers = a % m
    if r < 0:
        r = -r
        powers = invers_mod(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 1.31. 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:

```
def exponentiate_reverse(a,r,m):
    if r < 0:
        r = -r
        a = invers_mod(a,m)
    result = 1
    for bit in reversed(r.bits()):
        result = result**2 % m
        if bit == 1:
            result = (result * a) % m
    return result
```

1.5 Diffie–Hellman i RSA

Els algoritmes que hem vist fins ara ens permeten descriure protocols clàssics en la criptografia.

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 primer p. Es treballarà amb el grup cíclic $G = (\mathbb{Z}/p\mathbb{Z})^\times$. Alice i Bob fixen també un generador $g \in G$, que a l'igual que p serà públic. El protocol funciona de la manera següent:

1. L'Alice escull un enter a l'atzar $1 < a < p-1$, i envia la quantitat $A = g^a \bmod p$ a en Bob.

2. En Bob, per la seva banda, escull un enter a l'atzar $1 < b < p-1$, i envia la quantitat $B = g^b \bmod p$ a l'Alice.

3. Alice i Bob calculen respectivament $S = B^a \bmod p$ i $S = A^b \bmod p$. Observem que les dues quantitats són iguals a $g^{ab} \pmod p$, que serà el secret compartit.

Primer de tot, observem que els càlculs involucrats es poden fer de manera eficient gràcies a l'exponenciació modular. Per trobar un generador g, 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 2019, 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 RSA

En aquest cas, 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. Per fer-ho, cada usuari receptor 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 $(\varphi(N), d)$.

Suposem ara que Alice vol enviar un missatge a 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 Alice calcula $c = m^{e_B} \bmod N_B$, que serà el missatge xifrat. Quan Bob ho rebi, 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 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 1.25). 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 250 decimals.

[1] S'entén la comunitat acadèmica.

[2] Almenys al 2019.

2 Corbes el·líptiques (∼9h)

2.1 Definició i llei de grup

Definició 2.1. Una *corba el·líptica* sobre un cos K és una equació de la forma

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

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 2.2. *Si la característica de K és diferent de 2, aleshores es pot fer un canvi afí de variables que permet escriure E de forma*

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

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

$$\Delta_E = -16(4a^3 + 27b^2).$$

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

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

Quan $Z = 0$, obtenim com a solució el punt projectiu $\mathcal{O} = (0 : 1 : 0)$, que anomenarem *punt a l'infinit* d'E.

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

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

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 2.3. *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 ja sabem que interseca de manera triple amb $\mathcal{O}$.

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.

□

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 $\ell_{R,\mathcal{O}}$.

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

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

L'associativitat d'aquesta operació es pot veure de diferents maneres, però fer-ho ens duria massa lluny. Més endavant en donarem alguna indicació. Així, el conjunt de punts K-definits d'E adquireix una estructura addicional: és un grup abelià.

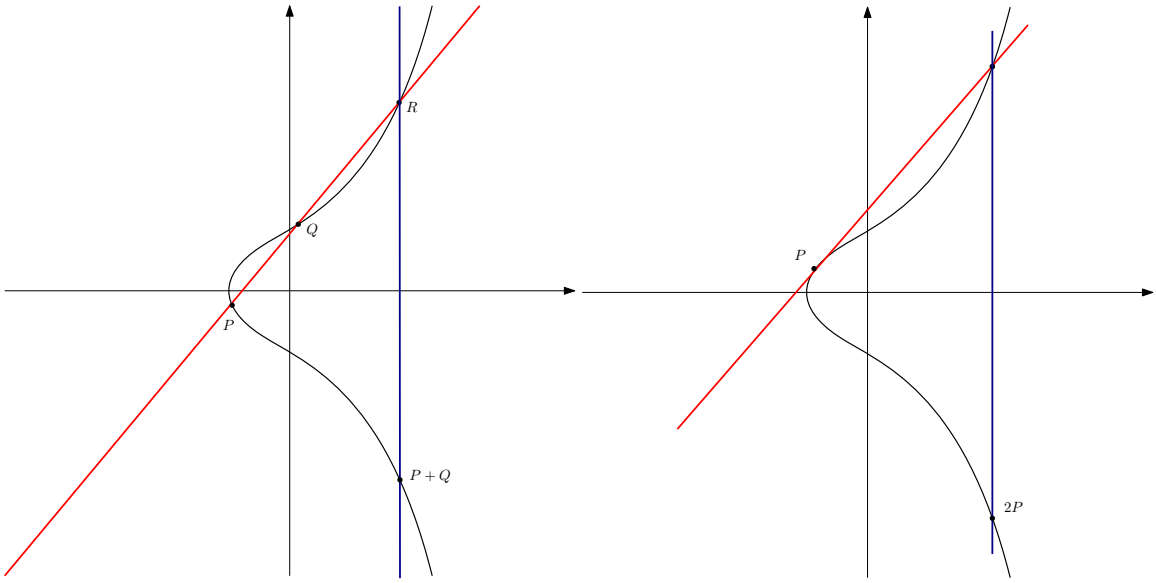

Figura 1: Suma de dos punts a E

2.1.1 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 $P_1 = \mathcal{O}$ o $P_2 = \mathcal{O}$ 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

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{si } P_1 \neq P_2, \\ \frac{3x^2 + 2a_2x + a_4}{2y} & \text{si } P_1 = P_2. \end{cases}$$

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`. El següent codi ens demostra la següent proposició.

Proposició 2.4. *1. Si P, Q, R satisfan que els elements*

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

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

2. Si P, Q satisfà que els elements

$$\{P, -P, 2P, -2P, Q, \mathcal{O}\}$$

són tots ells diferents, aleshores

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

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

$$2(2P) = P + 3P.$$

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

```
S.<a2,a4,a6,x1,x2,x3,y1,y2,y3> = PolynomialRing(QQ,8)
I = S.ideal([y1^2-(x1^3 + a2*x1^2 + a4*x1 + a6), \
             y2^2-(x2^3 + a2*x2^2 + a4*x2 + a6), \
             y3^2-(x3^3 + a2*x3^2 + a4*x3 + a6)])
P = (x1,y1)
Q = (x2,y2)
R = (x3,y3)

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

```
def double(P):
    s1 = (3*P[0]**2 + 2*a2 *P[0] + a4) / (2 * P[1])
    xPQ = s1^2 - 2*P[0]
    yPQ = -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 2.5. *Per a qualssevol punts P, Q i R d'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 2.6. *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 2.7. *La llei de grup definida anteriorment és associativa. Per tant, defineix un grup abelià.*

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

2.2 Punts de torsió, punts racionals

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

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

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

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

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 2.8 (Nagell–Lutz (1935, 1937))**.** *Sigui E una corba el·líptica amb equació*

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

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

1. *$x, y \in \mathbb{Z}$, i*
2. *$y = 0$ o $y^2 \mid \Delta_E$.*

Remarca 2.9. *La condició $a, b \in \mathbb{Z}$ sempre es pot aconseguir satisfer, fent un canvi de variables de la forma $(x', y') = (u^2 x, u^3 y)$ amb un $u \in \mathbb{Q}$ adequat.*

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 2.10 (Mazur, 1978)**.** *Sigui E una corba el·líptica definida a $\mathbb{Q}$. Aleshores*

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

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 2.11 (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[3] per calcular-lo, encara que hi ha mètodes que funcionen bastant bé.

2.2.1 Altures

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

Definició 2.12. 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 2.13. *Per cada $M > 0$, $\{P \in E(\mathbb{Q}) \mid h(P) \leq M\}$ és un conjunt finit.*

Lema 2.14. *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 2.15. *Hi ha una constant C tal que*

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

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

Teorema 2.16. *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,

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

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 $E(\mathbb{Q})_{\leq M}$. □

2.2.2 La versió dèbil del teorema de Mordell

Ens hem reduït a demostrar el següent resultat.

Teorema 2.17 (Mordell–Weil dèbil)**.** *El quocient $E(\mathbb{Q})/2E(\mathbb{Q})$ és finit.*

Remarca 2.18. *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

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

Remarca 2.19. *En general, $E[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ per a tot m, però no ho veurem aquí.*

Suposarem, d'ara en endavant, que $E[m] \subset E(K)$.

Per cada punt $P \in E(K)$, escollim $Q \in E(\bar{K})$ 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

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

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 $m(Q - R) = P - P = \mathcal{O}$ i, per tant, $Q - R \in E[m]$. Com que $E[m] \subseteq E(K)$, aleshores

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

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

Remarca 2.20. *Recordem que hem suposat que $E(K)$ conté $E[m]$. En general, $E[m]$ és finit (només ho hem vist per $m = 2$) i per tant 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 2.21. *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 $m(\sigma_2(Q) - Q) = \sigma_2(P) - P = \mathcal{O}$, 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 $\sigma(Q) - Q = \mathcal{O}$ 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 $\sigma(Q) - Q = \mathcal{O}$ 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 d'el 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. Si a més $E[m]$ és finit (per exemple, en el cas $m = 2$ ja ho sabem) aleshores el grup d'homomorfismes entre aquests dos grups finits serà necessàriament finit i haurem demostrat el teorema.

Lema 2.22. *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:

$$P = \sigma(P) = \sigma(2Q) = 2\sigma(Q) = 2(-Q) = -P,$$

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.

2.2.3 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 $x(2Q)$ 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,e_1,e_2')
T.<x> = PolynomialRing(SR)
F = x*(x-e_1)*(x-e_2)
g = (4*F*(e_1 + e_2 - 2*x) +
    (3*x^2-2*(e_1+e_2)*x+e_1*e_2)**2) -
    alpha*4*F
show(g.roots())
```

Veiem que les arrels són de la forma

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

Remarca 2.23. *També podem resoldre l'equació $g(x) = 0$ a mà: escrivim*

$$g(x) = (x^2 + Ax + B)^2 - (Cx)^2,$$

amb A, B, C a determinar. Igualant coeficients veiem que una solució és

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

Per tant,

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

i fent servir la fórmula quadràtica arribem a les solucions desitjades.

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

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

Aquesta expressió la podem reescriure com

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

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 2.24. *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. Primer, deixem com a exercici veure que si $(x, y) \in E(\mathbb{Q})$, aleshores $x = m/e^2$ i $y = n/e^3$ amb $m, n, e \in \mathbb{Z}$ i $\gcd(e, m) = \gcd(e, n) = 1$. Per fer-ho, s'escriu $x = m/M$ i $y = n/N$, i de l'equació d'E es dedueix que $N^2 = M^3$ (veient per separat les dues divisibilitats).

Sabem doncs que $(x, y) = (m/e^2, n/e^2)$ amb $\gcd(m, e) = \gcd(n, e) = 1$. Volem estudiar la part lliure de quadrats de l'enter m. Substituint-ho a l'equació d'E i netejant denominadors 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

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

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 ens dona una quantitat finita d'extensions $\mathbb{Q}(\sqrt{\alpha})$, però també hem de tractar amb $\mathbb{Q}(\sqrt{\alpha - e_1})$. 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 $\mathbb{Q}(\sqrt{\alpha - e_1})$ i per tant també per les possibilitats d'L_P. Així, el compost de tots els L_P és una extensió finita.

2.3 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 2.25. 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:

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

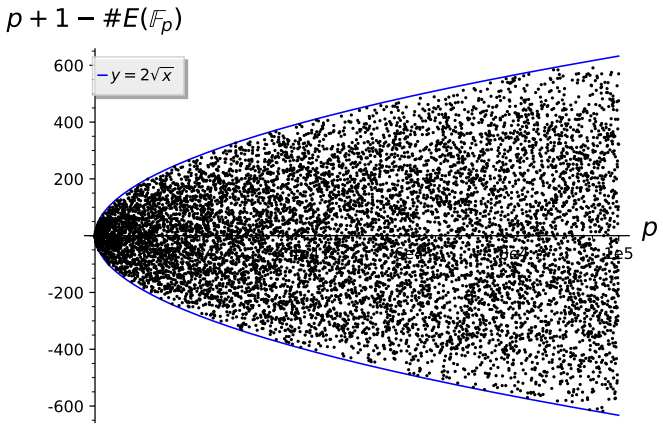

Figura 2: Il·lustració del Teorema de Hasse per la corba $E\colon y^2 = x^3 - x + 1$

Teorema 2.26 (Teorema de Hasse)**.** *Si E és una corba el·líptica definida sobre $\mathbb{F}_q$, aleshores*

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

En la demostració del teorema anterior, és crucial estudiar la isogènia següent (les aplicacions entre corbes el·líptiques que són algebraiques i que a més preserven l'estructura de grup s'anomenen *isogènies*):

Definició 2.27. Sigui $E/\mathbb{F}_q$ una corba el·líptica. L'*endomorfisme de Frobenius* és la isogènia

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

Remarca 2.28. *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

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

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 $\mathbb{F}_q$.

Idea de la demostració del Teorema de Hasse. Es basa en tres fets fonamentals, la demostració dels quals ometrem.

1. A cada isogènia $\varphi \in \mathrm{End}(E)$ se li pot assignar un grau $\deg(\varphi)$.
2. $\deg(\phi_E) = q$ i $\deg([m]) = m^2$ per a tot $m \in \mathbb{Z}$,
3. La isogènia $\phi_E - 1$ té nucli de tamany $\deg(\phi_E - 1)$, i
4. $\deg\colon \mathrm{End}(E) \to \mathbb{Z}$ és una forma quadràtica.

La desigualtat de Cauchy–Schwartz diu aleshores que donades isogènies φ_1 i φ_2 es té

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

Aplicant aquesta desigualtat a $\varphi_1 = \phi_E$ i $\varphi_2 = [1]$ obtenim el resultat, ja que $\#E(\mathbb{F}_q) = \#\ker(\phi_E - 1) = \deg(\phi_E - 1)$. □

Proposició 2.29. *Sigui $E/\mathbb{F}_q$ una corba el·líptica, i escrivim $a = q + 1 - \#E(\mathbb{F}_q)$. Aleshores ϕ_E satisfà*

$$\phi_E^2 - a\phi_E + q = 0.$$

Remarca 2.30. *La proposició diu que per a tot punt $P = (x, y) \in E(\bar{\mathbb{F}}_q)$, es té*

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

Aquí, recordem que les operacions $-$ $+$ i $\cdot$ es corresponen a la llei de grup.

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 $\#E(\mathbb{F}_q)$. Considerem el polinomi $X^2 - aX + q$, on $a = q + 1 - \#E(\mathbb{F}_q)$, que té discriminant $a^2 - 4q \leq 0$ pel Teorema de Hasse. Per tant, les seves arrels $\alpha, \beta \in \mathbb{C}$ són complexes conjugats, i el seu producte és q, per tant $|\alpha| = |\beta| = \sqrt{q}$.

Teorema 2.31. *Sigui E una corba el·líptica definida sobre $\mathbb{F}_q$. Aleshores,*

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

2.4 Criptografia amb corbes el·líptiques

2.4.1 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[4] 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 $p = 1550031797834347859248576414813139942411$ (131 bits). En canvi, des del 2005 es pot (amb tècniques molt avançades i amb molt d'esforç computacional) resoldre el logaritme discret 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 comprable 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 $\mathbb{F}_p^\times$.

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

2.4.2 ElGamal amb corbes el·líptiques

Una variant del protocol de Diffie–Hellman ens permet establir un sistema de xifrat de clau pública basat en el logaritme discret. El descriurem de manera uniforme per un grup $G = \mathbb{F}_q^\times$ o $G = E(\mathbb{F}_q)$.

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

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

Fixem-nos que la part de preparació s'assembla molt al que fa l'Alice amb 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 $Y^a = g^{ay} = A^y$), 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 $A = g^a$, i això és precisament el problema de Diffie–Hellman, que estem assumint igual de difícil que el problema del logaritme discret.

2.5 Comptatge de punts

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,

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

Suposem també que $p > 3$ (en cas contrari, és molt fàcil determinar $E(\mathbb{F}_p)$), i escrivim E en la forma

$$E\colon y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{F}_p.$$

Per cada $a \in \mathbb{F}_p$, definim

$$\chi(a) = \begin{cases} 0 & \text{si } a = 0, \\ +1 & \text{si } a \in (\mathbb{F}_p^\times)^2, \\ -1 & \text{si } a \in \mathbb{F}_p^\times \smallsetminus (\mathbb{F}_p^\times)^2. \end{cases}$$

Aleshores, observem que

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

i per tant tenim una formula tancada per t:

$$t = \sum_{x \in \mathbb{F}_p} \chi(x^3 + Ax + B).$$

A la secció següent veurem una manera eficient de calcular $\chi(x)$ per qualsevol $x \in \mathbb{F}_p$. Tot i així, si p és molt gran (de manera que ens sigui útil en criptografia) no podrem recórrer[5] tots els elements de $\mathbb{F}_p$.

2.5.1 L'algoritme d'Schoof

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.

Recordem que l'endomorfisme de Frobenius

$$\phi \colon E \to E, \quad (x, y) \mapsto (x^p, y^p)$$

satisfà l'equació quadràtica

$$\phi^2 - t\phi + q = 0.$$

Sigui $P = (x, y) \in E(K)$, on $K/\mathbb{F}_p$ és una extensió qualsevol. Aleshores

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

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.

[5] 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}.

Remarca 2.32. *Fixem-nos que l'enter t no es pot extreure directament de $[t]$, ja que si (x, y) té ordre N, aleshores (x^p, y^p) també (per què?), i per tant $[t+kN](x^p, y^p) = [t](x^p, y^p)$ per a tot k. Així, només podem determinar t mòdul N.*

La idea de Schoof consisteix en determinar $t \pmod{\ell}$ per suficients primers ℓ petits, i després reconstruir t 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 2.33.

$$t \bmod 2 = \begin{cases} 1 & \text{si } x^3 + Ax + B \text{ és irreductible a } \mathbb{F}_p, \\ 0 & \text{altrament.} \end{cases}$$

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 és $(\alpha, 0)$ on α és una arrel de $x^3 + Ax + B$). Ara bé, com que p és senar tenim

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

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 2.34. *Considerem els polinomis $\psi_m \in \mathbb{F}_p[x, y]$,*

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

Aleshores per a tot primer senar $\ell < p$, $\psi_\ell \in \mathbb{F}_p[x, y^2]$ i, si substituim $y^2 = x^3 + Ax + B$ obtenim un polinomi en x de grau $\frac{\ell^2-1}{2}$. A més,

$$P \in E(\bar{\mathbb{F}}_p)[\ell] \setminus \{\mathcal{O}\} \iff \psi_\ell(x(P)) = 0.$$

Corol·lari 2.35. *Per tot primer ℓ, 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, hi ha $1 + 2\deg(\psi_\ell) = \ell^2$ punts a $E[\ell]$. Com que tot $P \in E[\ell]$ satisfà $\ell P = \mathcal{O}$, necessàriament $E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$. □

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 $D = \alpha^3 + A\alpha + B$.

La següent millora ens permet treballar al cos K, sense afegir una arrel de D. Considerem la corba

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

Aleshores l'isomorfisme

$$\tau \colon E \to E^D, \quad (x, y\delta) \mapsto (Dx, D^2y), \quad \delta = \sqrt{D}$$

ens permet realitzar totes les operacions a $E^D(K)$. Observem que

$$\begin{aligned}
\tau((\alpha, \delta)) &= (D\alpha, D^2), \\
\tau((\alpha^p, \delta^p)) &= (D\alpha^p, D^{\frac{p+3}{2}}), \\
\tau((\alpha^{p^2}, \delta^{p^2})) &= (D\alpha^{p^2}, D^{\frac{p^2+3}{2}}).
\end{aligned}$$

Per tant, l'equació (2) és equivalent a la següent equació a E^D:

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

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 $O(\ell^2 \log q) = O(\log^3 q)$. 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 $O(\log^{5+\epsilon} p)$. Millores posteriors de Elkies i Atkin permeten calcular $\#E(\mathbb{F}_p)$ amb temps $O(\log^{4+\epsilon} p)$.

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

```
def t_mod(A, B, p, ell):
    pmod = p % ell
```

```
    if pmod > ell / 2: pmod -= ell
    R.<t> = PolynomialRing(GF(p))
    if ell == 2: return 1 if (t^3+A*t+B).is_irreducible() else 0
    h = E.division_polynomial(ell,t,0).factor()[0][0]
    K.<a> = FiniteField(p^h.degree(), modulus = h)    # K = F[x]/(h(x))
    D = a^3 + A * a + B
    E = EllipticCurve([A*D^2, B*D^3])
    P = E([D*a,D^2])
    phi_P = E([D * a^p, D^((p+3)//2)])
    phi2_P = E([D * a^(p^2), D^((p^2+3)//2)])
    LHS = phi2_P + pmod * P; RHS = E(0)
    for t in xrange((ell+1)//2):
        if LHS ==  RHS: return t
        elif LHS == -RHS: return -t
        RHS += phi_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))
    t = CRT(traces, S) # Fem servir el Teorema Xinès dels Residus
    return t if t < M / 2 else t-M
```

3 La llei de reciprocitat quadràtica (∼5h)

3.1 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 3.1. 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*.

Òbviament, si $a \equiv a' \pmod{p}$ aleshores a és un residu quadràtic mòdul p si i només si a' ho és.

Exemple 3.2. 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 3.3. 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 produce 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 3.4. *Si p és un primer senar, l'aplicació $\psi\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}, \quad a \mapsto \left(\frac{a}{p}\right)$ 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

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

□

3.2 LRQ i demostració

Durant el segle XVIII, els 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 $a = 5$ podem fer una taula com la que apareix a la Taula 3.2. Fixem-nos que sembla que

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

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 3.2. 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 3: 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 3.5 (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.

3.2.1 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 3.6 (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 3.7. *Si p és un primer senar, aleshores*

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

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

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

Veurem ara que $\tau^p \equiv \zeta^p + \zeta^{-p} \equiv \epsilon(p)\tau \pmod{p}$:

Cas $p \equiv \pm 1 \pmod 8$ **(** $\iff \epsilon(p) = 1$**):** En aquest cas, $\tau^p \equiv \zeta + \zeta^{-1} \equiv \tau \pmod p$.

Cas $p \equiv \pm 3 \pmod 8$ **(** $\iff \epsilon(p) = -1$**):** En aquest cas, $\tau^p \equiv \zeta^3 + \zeta^{-3} \equiv -\tau \pmod p$.

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

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

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

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 3.8. *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

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

□

Definició 3.9. La *suma de Gauss* associada a un element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ és

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

Lema 3.10. *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 3.11. *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 és el següent resultat.

Proposició 3.12. *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 $p-1$).

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

□

Demostració del Teorema 3.5. Si escrivim $p^* = (-1)^{\frac{p-1}{2}}p$, aleshores fixem-nos que

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

Per tant, per demostrar la LRQ ens cal veure que

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

Per acabar, haurem de treballar a $\mathbb{Z}[\zeta_p]/(q)$, que és un anell de característica q. Aleshores, pel criteri d'Euler,

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

Ara 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 de l'expressió

$$\gamma_1 \left(\frac{p^*}{q}\right) \equiv \gamma_1 \left(\frac{q}{p}\right) \pmod{q}$$

per obtenir el resultat.

□

3.3 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 el símbol és el de Legendre. Observem que si m és un primer senar, aleshores aquesta definició coincideix amb el símbol de Legendre.

Lema 3.13. *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 3.14. *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

$$\{1, 4, 6, 9, 10\}.$$

Teorema 3.15 (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,

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

Exemple 3.16. Suposem que volem saber si 7411 és un quadrat mòdul 9283. Primer hauriem 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 $1872 = 2^4 \cdot 3^3 \cdot 13$. En canvi, fent servir el símbol de Jacobi només hem de treure les potències de 2:

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

3.4 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 $\delta^2 = D$.

Per tant, podem suposar que $p \equiv 1 \pmod 4$. Donarem ara un algoritme probabilístic per trobar δ. 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

$$\varphi\colon R \to \mathbb{F}, \quad a + b\sqrt{D} \mapsto a + b\delta$$

(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 $\mathbb{F}_p^\times$ té $p - 1$ elements, necessàriament $u + v\delta \in \{0, 1, -1\}$. Per tant, si $v \neq 0$ aleshores

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

Podem provar aquestes tres possibilitats i trobarem δ. Si $v = 0$, triem un altre $z \in \mathbb{F}_p^\times$ i repetim el procés.

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

4 Primalitat i factorització (∼10h)

4.1 Primalitat

4.1.1 El "test" de Wilson

Proposició 4.1 (Teorema de Wilson)**.** *Un enter $p > 1$ és primer si i només si*

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

Demostració. Si p no és primer, prenem $\ell \mid p$ un factor primer de p. Tenim, per una banda, que $\ell \mid (p-1)!$, i també que $\ell \mid p \mid (p-1)! + 1$. Però aleshores $\ell \mid 1$, que és una contradicció.

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

$$(p-1)! = \prod_{x=1}^{p-1} x$$

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

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

4.1.2 Fermat i Miller–Rabin

Definició 4.2. Un enter compost senar n s'anomena *pseudoprimer en base b* si $\gcd(b, n) = 1$ i $b^{n-1} \equiv 1 \pmod{n}$.

Observem que n és pseudoprimer en bases b_1 i b_2, aleshores també ho és en les bases $b_1 b_2$ i $b_1 b_2^{-1}$ (on l'invers el fem mòdul n).

Lema 4.3. *Si n no és pseudoprimer en una base $(b \in \mathbb{Z}/n\mathbb{Z})^\times$, aleshores n no ho és en com a mínim la meitat de les possibles bases b.*

Demostració. Sigui $\{b_1, \ldots, b_s\}$ el conjunt de les bases en les quals n és pseudoprimer. Sigui $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ una base en la qual n no és pseudoprimer. Aleshores $\{bb_1, \ldots, bb_s\}$ és un conjunt de s residus tals que n no és pseudoprimer en aquelles bases. □

Definició 4.4. 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 4.5. *Sigui n un primer compost.*

1. *Si n no és lliure de quadrats, aleshores n no és de Carmichael.*
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. [6] □

Per evitar els problemes amb els nombres de Carmichael, suposem que n sigui un pseudoprimer en base b. Per tant,

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

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

Definició 4.6. Escrivim un enter compost $n = 2^s t + 1$, amb t senar. Direm que n és pseudoprimer fort en base $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ si $b^t \equiv 1 \pmod{n}$ o hi ha algun r amb $0 \leq r < s$ tal que

$$b^{2^r t} \equiv -1 \pmod{n}.$$

[6] **FIXME:** Vegeu els problemes per entregar.

Proposició 4.7. *Un enter compost n és pseudoprimer fort per com a molt el 25% de les possibles bases $1 \leq b < n$.*

Per la demostració ens caldran dos lemes previs:

Lema 4.8. *Sigui G un grup cíclic amb m elements. Aleshores*

$$G[k] = \{x \in G \mid x^k = 1\}$$

té ordre $\gcd(k, m)$.

Lema 4.9. *Sigui p un primer senar, i escrivim $p = 1 + 2^{s't'}$ amb t' senar. Aleshores*

$$\#\{x \in \mathbb{F}_p^\times \mid x^{2^s t} \equiv 1 \pmod{p}\} = \begin{cases} 2^s \gcd(t, t') & si\ s < s', \\ 0 & si\ s \geq s'. \end{cases}$$

Demostració. Fixem un generador g de $\mathbb{F}_p^\times$ i escrivim $x = g^j$ amb $0 \leq j < 1$. Aleshores l'equació que ha de satisfer x es tradueix a

$$2^s tj \equiv \frac{p-1}{2} \equiv s^{s'-1}t' \pmod{2^{s'}t}.$$

Veiem que no hi ha solucions si $s < s'$. En canvi, si $s \geq s'$, aleshores dividim per $2^s d$ (amb $d = \gcd(t, t')$) i obtenim el resultat. □

Demostració (de la Proposició 4.7). La demostració es divideix en 3 casos.

Cas 1: n no és lliure de quadrats. Suposem que $p^2 \mid n$ per algun primer senar p. Veurem que en aquest cas n és pseudoprimer (dèbil) per com a molt un 25% de bases. Fem servir que $(\mathbb{Z}/p^2\mathbb{Z})^\times$ és cíclic, de tamany $p(p-1)$. Si b és una base per la qual n és presudoprimer, aleshores $b^{n-1} \equiv 1 \pmod{p^2}$ i per tant l'ordre de b divideix $n-1$. El nombre de possibilitats per un tal b és doncs

$$d = \gcd(p(p-1), n-1).$$

Com que $p \mid n$, aleshores $p \nmid n-1$ i per tant $d \leq p-1$. Per tant, la proporció de b's és

$$\leq \frac{p-1}{p^2-1} = \frac{1}{p+1} \leq \frac{1}{4}.$$

Cas 2: $n = pq$ és producte de dos primers.
[7]

□

[7] **FIXME:** Acabar-la

Remarca 4.10. *Només hi ha un pseudoprimer fort en 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 b 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 decideix que n és compost. Així:

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

Una possible implementació del 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):
        b = ZZ.random_element(1, n)
        if not es_pseudoprimer_fort(n, b):
            return False
    return True
```

El test de Miller–Rabin no dona una manera de demostrar la primalitat de n, llevat de comprovar més de 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 4.11. *Suposem GRH. Si* n *és un enter compost senar, aleshores hi ha alguna base* $b < 2\log^2 n$ *tal que* n *no és pseudoprimer fort en base* b.

4.1.3 Test de Lucas

Aquest test es basa en la següent afirmació.

Proposició 4.12. *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 $p \mid n-1$

$$a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}.$$

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 4.13. 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

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

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*.

```
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):
            b += 1
    return True
```

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.

4.3 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. Per exemple, f pot ser un polinomi amb coeficients enters i, 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 $x_j \equiv x_k \pmod{d}$, i aleshores

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

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 4.14. *Sigui S un conjunt de d elements, i sigui $\lambda > 0$ 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 $\ell = 1 + \lfloor\sqrt{2\lambda d}\rfloor$.*

La proporció de parelles (f, x_0) per les quals $x_0, x_1, \dots x_\ell$ són tots diferents és $< e^{-\lambda}$.

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 $\ell > \sqrt{2d\lambda}$, obtenim el resultat. □

Corol·lari 4.15. *L'algoritme ρ de Pollard troba, amb probabilitat més gran que $1 - e^{-\lambda}$ un factor no trivial de n en $O(\sqrt[4]{n})$ passos.*

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

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 4.16. *Siguin k_0 i j_0 dos índexs 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, depent de λ) 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).

4.3.1 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 4.17. Donat $B > 0$, diem que un enter k és B-potència-suau si per a tot primer p,

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

El mètode és el següent:

1. Triem un enter m que sigui múltiple de tots (o quasi tots) els enters menors que alguna fita B. Per exemple, podem triar $m = B!$, o bé $m = \gcd\{1, 2, 3, \ldots, B\}$.
2. Triem un enter a l'atzar $a \in \{2, \ldots, m-2\}$.
3. Calculem $a^m \pmod n$ fent servir exponenciació modular.
4. Calculem $d = \gcd(a^m - 1 \bmod n, n)$ fent servir l'algoritme d'Euclides.
5. Si $1 < d < n$, ja hem trobat un divisor no trivial de n. Si no, tornem a començar amb un altre a o un altre m.

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

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

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

Remarca 4.18. *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.*

4.3.2 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 4.19. Imaginem que hem pres $B = 20$, i que n és $59 \cdot 101 = 5959$. Aleshores

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

no són B-potència-suaus. En canvi,

$$59 - 2 = 57 = 3 \cdot 19, \quad 101 - 2 = 99 = 9 \cdot 11$$

sí que són B-potència-suaus. Per tant, 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 com

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

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 kP pensant E com una corba definida a $\mathbb{Z}/n\mathbb{Z}$. Per fer-ho, calculem:
$$2^{\alpha_2}P, 3^{\alpha_3}(2^{\alpha_2}P), \ldots, kP.$$

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 4.20 (Lenstra)**.** *Si assumim com a certes algunes conjectures estàndard, el nombre d'operacions de bit necessàries per factoritzar n és*[8]
$$O\left(e^{\sqrt{(1+\varepsilon)\log n \log\log n}}\right)$$

```
def factor_lenstra(n, intents = 100):
    from sage.rings.finite_rings.finite_field_prime_modn \
        import FiniteField_prime_modn as GFmodn
    import re # Per tractar amb expressions regulars
    R = GFmodn(n,check=False)
    Bound = 10000
    primes_up_to_bound = prime_range(Bound)

    for _ in xrange(intents):
        Q = EllipticCurve([R.random_element(),1])([0,1])
        try:
            for ell in primes_up_to_bound:
                Q *= ell**ZZ(floor(RR(B).log(ell)))
        except ZeroDivisionError as e:
            return ZZ(re.search(r'\d+', str(e)).group()).gcd(n)
```

4.4 Bases de factors

4.4.1 El mètode de Fermat

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

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

Exemple 4.21. Suposem que volem factoritzar $n = 200819$. Si calculem

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

podem escriure

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

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).

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

Lema 4.22. *Hi ha una correspondència bijectiva*

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

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

Exemple 4.23. 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 $\sqrt{kn}$.

4.4.2 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 4.24. 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 4.25. 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 4.26. Prenem $B = \{-1, 2, 3\}$ i $n = 4633$. Aleshores

$$67^2 \bmod n = -144 = -1 \cdot 2^4 \cdot 3^2, \quad 68^2 \bmod n = -9 = -1 \cdot 3^2, \quad 69^2 \bmod n = 128 = 2^7,$$

i 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 4.27. 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 $J \subset \{1, \ldots, n\}$ tenim

$$\sum_{j \in J} v_{b_j} = 0,$$

aleshores

$$(\prod_{j \in J} b_j)^2 \equiv (\prod_{j \in J} p_j^{r_j}) \pmod{n},$$

on els exponents r_j s'obtenen fàcilment de la factorització de cadascun dels b_j mod n involucrats.

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 $b^2 \bmod n$ 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.

4.5 Fraccions continuades

Pel què hem vist fins ara, volem trobar enters b tals que $b^2 \bmod N$ 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

$$[\,a_0; a_1, a_2, \ldots, a_k\,] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \quad + \cfrac{1}{a_k}}}}$$

Lema 4.28. *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 4.29. *La successió $(a_i)_{i\geq 0}$ és finita si i només si $x \in \mathbb{Q}$.*

Demostració. Si la successió és finita aleshores per algun $i \geq 0$ tindrem $x_i = 0$ i, per tant,

$$x = [\,a_0; a_1, \ldots, a_i\,] \in \mathbb{Q}.$$

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 4.30. 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:

$$\begin{array}{lll} p_0 = a_0, & p_1 = a_0a_1 + 1, & p_n = a_np_{n-1} + p_{n-2} \ (n \geq 2) \\ q_0 = 1, & q_1 = a_1, & q_n = a_nq_{n-1} + q_{n-2} \ (n \geq 2). \end{array}$$

Proposició 4.31. *1. La n-èssima convergent és p_n/q_n.*

2. Per a tot $n \geq 0$, es té

$$p_{n+1}q_n - p_nq_{n+1} = (-1)^n. \tag{3}$$

Demostració. Es fa fàcilment per inducció. □

Corol·lari 4.32. *La n-èssima convergent té forma reduïda p_n/q_n.*

Demostració. De l'Equació (3) veiem per inducció que $\gcd(p_n, q_n) = 1$. □

Proposició 4.33. *Per a tot $x \in \mathbb{R}$, es té*

$$\lim_{n\to\infty} \frac{p_n}{q_n} = x.$$

Demostració. Si a l'Equació (3) dividim per q_nq_{n+1} obtenim

$$\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_nq_{n+1}}.$$

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,

$$\begin{aligned} x - \frac{p_n}{q_n} &= \frac{p_n\frac{1}{x_n} + p_{n-1}}{q_n\frac{1}{x_n} + q_{n-1}} - \frac{p_n}{q_n} \\ &= \frac{p_{n-1}q_n - p_nq_{n-1}}{q_n(q_n/x_n + q_{n-1})} = \frac{(-1)^n}{q_n(q_n/x_n + q_{n-1})}. \end{aligned}$$

Prenent el valor absolut, obtenim

$$\begin{aligned} \left| x - \frac{p_n}{q_n} \right| = \frac{1}{q_n(q_n/x_n + q_{n-1})} &< \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} \\ &= \frac{1}{q_nq_{n+1}} \end{aligned}$$

Com que $q_n \to \infty$, obtenim el resultat. □

La demostració de la proposició anterior ens permet veure la següent estimació.

Corol·lari 4.34. *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 4.35. *Sigui $x > 1$. Aleshores*

$$\left| q_n^2 x^2 - p_n^2 \right| < 2x$$

Demostració. Escrivim

$$|q_n^2 x^2 - p_n^2| = q_n^2 |x - p_n/q_n||x + p_n/q_n| < q_n^2 \frac{1}{q_n q_{n+1}} (2x + \frac{1}{q_n q_{n+1}}).$$

Restant $2x$, obtenim

$$\begin{aligned} |q_n^2 x^2 - p_n^2| - 2x &< 2x(-1 + q_n/q_{n+1} + \frac{1}{2x q_{n+1}}) \\ &< 2x \left(-1 + \frac{q_n}{q_{n+1}} + \frac{1}{q_{n+1}} \right) \\ &< 2x(-1 + \frac{q_{n+1}}{q_{n+1}}) < 0. \end{aligned}$$

□

Corol·lari 4.36. *Sigui $N > 1$ un enter que no sigui un quadrat perfecte, i siguin p_n/q_n les convergents de $\sqrt{N}$. Aleshores*

$$|p_n^2 \mod N| < 2\sqrt{N}.$$

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.

```
def es_B_suau(n,B):
    m = n
    v = []
    for p in B:
        if p == -1:
```

```
            val, m = m.sign(), m.abs()
        else:
            val = 0
            while m % p == 0:
                m /= p
                val += 1
        v.append(val)
    return v if  m == 1 else False

def frac_continuada_sqrt(n):
    F.<s> = QuadraticField(n)
    v = F.embeddings(RDF)[0]
    if v(s) < 0:
        v = F.real_embeddings()[1]
    b0 = 1
    b = v(s).floor()
    a = b
    x = s - a
    yield b
    while True:
        xinv = 1 / x
        a =  v(xinv).floor()
        x = xinv - a
        b, b0 = a * b + b0, b
        yield b

def factor_fraccions_continuades(n,B):
    M = frac_continuada_sqrt(n)
    relations = []
    relation_matrix = Matrix(GF(2),0,len(B),0)
    while relation_matrix.rank() < len(B):
        x = M.next()
        if 2*x > n:
            x -= n
        y = x^2 % n
        if 2*y > n:
            y -= n
        if gcd(y,n) > 1:
```

```
            return g
        vec = es_B_suau(y,B)
        if vec:
            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(r[0]^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] ==
                    assert ap % 2 == 0
                    y0 *= p^(ap // 2)
                g = gcd(x0-y0,n)
                if g > 1 and g < n:
                    return g
```

Acabem aquesta § amb un resultat interessant sobre fraccions continuades, encara que no ens serveixi directament per factoritzar.

Exemple 4.37. Calculem la fracció continuada del valor $x = \sqrt{7} = 2.64575131106459\ldots$. Comencem amb

$$a_0 = \lfloor \sqrt{7} \rfloor = 2, \quad x_0 = \sqrt{7} - 2 = 0.64575131106459\ldots.$$

Després calculem

$$\frac{1}{x_0} = \frac{1}{\sqrt{7}-2} = \frac{2+\sqrt{7}}{3} = 1.54858377035486\ldots.$$

d'on obtenim

$$a_1 = 1, \quad x_1 = \frac{-1+\sqrt{7}}{3} = 0.54858377035486\ldots.$$

Ara calculem

$$\frac{1}{x_1} = \frac{3}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{2} = 1.82287565553230\ldots$$

i obtenim

$$a_2 = 1, \quad x_2 = \frac{\sqrt{7}-1}{2} = 0.82287565553230\ldots.$$

El terme següent és $1/x_2 = \frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3} = 1.21525043702153\ldots$ que dona

$$a_3 = 1, \quad x_3 = \frac{\sqrt{7}-2}{3} = 0.21525043702153.$$

Seguidament, calculem $1/x_3 = \frac{3}{\sqrt{7}-2} = \sqrt{7}+2 = 4.64575131106459\ldots$, cosa que resulta en

$$a_4 = 4, \quad x_4 = \sqrt{7}-2 = 0.64575131106459\ldots$$

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 4.38. Suposem que $x \in \mathbb{R}$ té fracció continuada

$$x = [\,3; 5, 3, 5, 3, 5, 3, \ldots\,]$$

Aleshores podem escriure

$$x = 3 + \frac{1}{5 + \frac{1}{x}},$$

d'on obtenim

$$3 + \frac{x}{5x+1} = x \implies \frac{16x+3}{5x+1} = x,$$

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 4.39. *Un real x té una fracció continuada periòdica 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 $\alpha = [\, a_{n+1}; a_{n+2}, \dots]$. Aleshores tenim que

$$\alpha = [\, a_{n+1}; \dots, a_{n+h}, \alpha\,].$$

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

$$x = [\, a_0; a_1, \dots, a_n, \alpha\,] = \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \; + \cfrac{1}{a_n + \cfrac{1}{\alpha}}}}},$$

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 $x = [\, a_0; a_1, \dots]$, definim r_n com la cua $[\, a_n; a_{n+1}, \dots]$, de tal manera que $x = [\, a_0; a_1, \dots, a_{n-1}, r_n\,]$ 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

$$\begin{aligned}
[\, a_0; \dots, a_{n-1}, r_n\,] &= [\, a_0; \dots, a_{n-1}, a_n, \dots, a_{n+h-1}, r_{n+h}\,] \\
&= [\, a_0; \dots, a_{n-1}, a_n, \dots, a_{n+h-1}, r_n\,] \\
&= [\, a_0; \dots, a_{n-1}, a_n, \dots, a_{n+h-1}, a_n, \dots, a_{n+h-1}, r_{n+h}\,] \\
&= [\, a_0; \dots, a_{n_1}, \overline{a_n, \dots, a_{n+h-1}}\,].
\end{aligned}$$

De l'expressió $x = [\, a_0; a_1, \dots, a_{n-1}, r_n\,]$ tenim

$$x = \frac{r_n p_{n-1} + p_{n-2}}{r_n q_{n-1} + q_{n-2}}.$$

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

$$\begin{aligned}
A_n &= a p_{n-1}^2 + b p_{n-1} q_{n-1} + c q_{n-1}^2 \\
B_n &= 2a p_{n-1} p_{n-2} + b(p_{n-1} q_{n-2} + p_{n-2} q_{n-1}) + 2c q_{n-1} q_{n-2} \\
C_n &= a p_{n-2}^2 + b p_{n-2} q_{n-2} + c q_{n-2}^2.
\end{aligned}$$

Ens hem de fixar que $A_n, B_n, C_n \in \mathbb{Z}$ i que $C_n = A_{n-1}$. A més, resulta que

$$B_n^2 - 4A_nC_n = (b^2 - 4ac)(p_{n-1}q_{n-2} - q_{n-1}p_{n-2})^2 = b^2 - 4ac.$$

De la desigualtat

$$\left| x - \frac{p_{n-1}}{q_{n-1}} \right| < \frac{1}{q_{n-1}q_n} < \frac{1}{q_{n-1}^2}$$

obtenim

$$p_{n-1} = xq_{n-1} + \frac{\delta}{q_{n-1}}, \quad |\delta| < 1.$$

Aleshores podem calcular

$$A_n = 2ax\delta + a\frac{\delta^2}{q_{n-1}^2} + b\delta,$$

i per tant

$$|A_n| = \left| 2ax\delta + a\frac{\delta^2}{q_{n-1}^2} + b\delta \right| < 2|a||x| + |a| + |b|.$$

D'això en deduïm que A_n només pot prendre un nombre finit de valors, i també $C_n = A_{n-1}$. Finalment, com que B_n satisfà $B_n^2 = 4A_nC_n + b^2 - 4ac$, també només pot prendre un nombre finit de valors. Així, hi ha un nombre finit de possibilitats per r_n. □

4.5.1 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 3.4).

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 són B-potència-suau.

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 4.40. *Si es tria B adequadament (en funció de n) s'obté un algoritme que factoritza en*

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

operacions.

```
def garbell(k0, k1, B, n):
    llista = [[x, x*x -n] for x in srange(k0,k1)]

    for p in B:
        if p == -1:
            continue
        nmodp = n % p
        x0 = GF(p)(nmodp).sqrt()
        x1 = (-x0).lift()
        x0 = x0.lift()
        for r in [x0, x1]:
            for i in sxrange((r-k0) % p, len(llista), p):
                while llista[i][1] % p == 0:
                    llista[i][1] /= p
    return [(x,x*x - n) for x,y in llista if y == 1]

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)
            assert ap % 2 == 0
            y0 *= p^(ap // 2)
        g = gcd(x0 - y0,n)
        if g > 1 and g < n:
            return g
```

4.6 Algoritmes pel logaritme discret

4.6.1 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 b, 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,... 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 $\{r_{p,i}\}_{i=0,\dots p-1}$.

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, $y_2^{\frac{n}{p}} = 1$ i es té

$$y_1^{\frac{n}{p^2}} = b^{x_1 \frac{n}{p}} = r_{p,x_1}.$$

...

Pas (i): Calculem $y_i = y_{i-1} b^{-p x_{i-1}}$ i calculem

$$y_i^{\frac{n}{p^{i+1}}} = r_{p,x_i}.$$

4.6.2 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.

4.6.3 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 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 $\mathcal{B} = \{-1, 2, 3, 5, 7, 11, \ldots, B\}$.
2. Per $k = 1, 2, 3, \ldots$ intentem factoritzar $b^k \pmod{p}$ en la base $\mathcal{B}$. (només tindrem èxit si $b^k \pmod{p}$ és B-suau).
3. Per cada factorització correcta

   $$b^k = \prod_{\ell \in \mathcal{B}} \ell^{\alpha_\ell},$$

   afegim una relació $(k, \alpha_0, \alpha_1, \ldots)$.
4. Quan tinguem $\#B$ relacions independents, podem trobar (mitjançant àlgebra lineal) els logaritmes discrets de tots els elements de $\mathcal{B}$. Per cada $\ell \in \mathcal{B}$, 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 $\mathcal{B}$-suau.
2. Quan trobem un t tal que

$$b^t y = \prod_{\ell \in \mathcal{B}} \ell^{\beta_\ell},$$

podem retornar

$$i(y) = -t + \sum_{p\ell \in \mathcal{B}} \beta_\ell i(\ell).$$

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 poden aplicar a grups cíclics més generals, i el que permet que el logaritme discret en corbes el·líptiques sigui més difícil que a $\mathbb{F}_q^\times$.

A Projectes de Sage

A.1 Com factoritza un polinomi mòdul diferents primers

En aquest projecte s'estudia la factorització d'un polinomi fixat 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).

Comenceu estudiant polinomis quadràtics, i vegeu quins tipus apareixen, i quantes vegades. El fenòmen que descobrim l'hauriem de poder demostrar.

Després es pot continuar per polinomis cúbics i veure si podem veure algun patró. Es pot seguir amb polinomis de grau més alt.

A.2 Estudi del nombre de punts d'una corba algebraica segons el primer

En aquest projecte, estudiarem corbes de la forma $f(x, y, z) = 0$, on $f \in \mathbb{Z}[x, y, z]$ és un polinomi homogeni. Podem comptar els punts mòdul diferents primers, així com els punts a $\mathbb{F}_{p^k}$ on $k \geq 1$ va canviant. Escrivim

$$N_f(p, k) = \#\{(x : y : z) \in \mathbb{P}^2(\mathbb{F}_{p^k}) \mid f(x, y, z) = 0\}.$$

El tipus de preguntes que ens podem fer:

- Com creix $N_f(p, 1)$ respecte p? Depen de f, aquest creixement?
- Podem veure termes de segon ordre en el creixement de $N_f(p, 1)$? Aquests, depenen d'alguna manera del polinomi f (o del seu grau)?
- Fixeu f i un primer p, i trobeu una fórmula recursiva per $N_f(p, k)$ que us permeti trobar $N_f(p, k)$ per a tot k a partir dels valors corresponents per $k = 1, 2, \ldots, k_0$ (on k_0 dependrà del grau d'f però no de p).

A.3 Nombre de punts mòdul p per corbes el·líptiques: variació I

Estudieu la distribució de $\#E(\mathbb{F}_p)$, i després la de

$$\frac{p+1-\#E(\mathbb{F}_p)}{2\sqrt{p}}$$

per diverses corbes el·líptiques. Dibuixeu histogrames dels resultats, i intenteu identificar les distribucions resultants. Compareu en particular el resultat que obteniu per aquestes dues corbes:

$$E_0 \colon y^2 + y = x^3 - x^2,$$
$$E_1 \colon y^2 + y = x^3.$$

A.4 Nombre de punts mòdul p per corbes el·líptiques: variació II

Donada una corba el·líptica E definida sobre $\mathbb{Q}$, definim la funció

$$C_E(x) = \prod_{p \leq x} \frac{\#E(\mathbb{F}_p)}{p}, \quad x \in \mathbb{R}_{>0}.$$

Estudieu el comportament assimptòtic de C_E ($x \to \infty$) per diverses corbes el·líptiques. Per exemple, considereu les corbes:

$$E_0 \colon y^2 + y = x^3 - x^2,$$
$$E_1 \colon y^2 + y = x^3 - x,$$
$$E_2 \colon y^2 + y = x^3 + x^2 - 2x,$$
$$E_3 \colon y^2 + y = x^3 - 7x + 6.$$

B Exposicions orals

1. Caracteritzar quins primers es poden expressar com a suma de dos quadrats.
2. Demostracions "Euclidianes" de l'existència d'infinits primers en algunes successions aritmètiques.
3. Demostració topològica de la infinitud dels primers (Fustenberg).
4. El postulat de Bertrand: per a tot $n \geq 1$, $[n, 2n] \cap \{\text{primers}\} \neq \emptyset$.
5. El teorema de Mill: $\exists A$ tal que $\lfloor A^{3^n} \rfloor$ és primer per a tot n.
6. La irracionalitat de π fent servir fraccions contínues (Lakzkovich).
7. La irracionalitat de e i d'$e^2 + re$ per a tot $r \in \mathbb{Q}$ fent servir fraccions contínues.
8. L'equació de Pell, i la seva solució amb fraccions contínues.
9. L'estructura de grup de $(\mathbb{Z}/m\mathbb{Z})^\times$.
10. La sèrie $\sum_{p \text{ primer}} \frac{1}{p}$ és divergent.
11. El teorema dels nombres primers (sense demostració).
12. El "primer cas" de l'Últim Teorema de Fermat.
13. Els nombres p-àdics: definició, el lema de Hensel.
14. El principi de Hasse.
15. Teorema d'Schnirelmann: si A té densitat (d'Schnirelmann) positiva, existeix una k tal que tot nombre natural és suma de com a molt k nombres de A.
16. Prime gaps, la història.
17. La conjectura de Goldbach, i remarques sobre la demostració versió dèbil (ternària).
18. Conjunts de Sidon, i la construcció de Ruzsa.

C Problemes per entregar

1. Sigui p un nombre primer. Direm que $\alpha \in \mathbb{F}_p^\times$ és una arrel primitiva si genera el grup $\mathbb{F}_p^\times$.

   (a) Sigui p un nombre primer de la forma $p = 2^{2^k} + 1$ per algun k (primers de Fermat). Demostreu que el conjunt d'arrels primitives a $\mathbb{F}_p$ és igual al conjunt d'elements de $\mathbb{F}_p$ que no són quadrats.

   (b) Sigui q un primer tal que $p = 4q + 1$ també és primer. Demostreu que el conjunt d'arrels primitives a $\mathbb{F}_p$ és igual al conjunt d'elements que no són quadrats ni el seu quadrat és -1.

   (c) Trobeu totes les arrels primitives a $\mathbb{F}_{13}$, $\mathbb{F}_{29}$, $\mathbb{F}_{149}$.

   (d) Demostreu que el nombre d'arrels primitives de $\mathbb{F}_p$ és igual a $\varphi(\varphi(p))$.

   (e) Demostreu que si $p > 3$ és un nombre primer, el producte de totes les arrels primitives de $\mathbb{F}_p$ és igual a 1.

   (f) Demostreu que si $p \geq 3$ és un nombre primer, la suma de totes les arrels primitives de $\mathbb{F}_p$ és congruent a $\mu(p-1) \pmod p$, on $\mu(n)$ és la funció de Möbius, que val 1 si n és producte d'un nombre parell de primers diferents, -1 si n és producte d'un nombre senar de primers diferents, i 0 si no (o sigui n és divisible per un quadrat > 1).

   (Pista per e) i f): Demostreu que

   $$\prod_{\alpha \text{ arrel primitiva a } \mathbb{F}_p} (x - \alpha) = \Phi_{p-1}(x),$$

   on $\Phi_n(x)$ és el polinomi ciclotòmic enèssim.

2. Parametrització de corbes i varietats.

   (a) Calculeu una fórmula que determini les solucions racionals de l'equació $ax^2 + by^2 = a + b$ en (x, y), en funció del paràmetres a i b.

   (b) Calculeu una fórmula que determini les solucions racionals de l'equació $x^2 + y^2 + z^2 = 1$ en (x, y, z). Per fer-ho, podeu utilitzar la projecció estereogràfica $\pi(x, y, z) = (s, t)$ a partir del punt $(0, 0, -1)$, i trobeu una descripció explícita del punt (x, y, z) en funció del punt (s, t) del pla.

   (c) Feu el mateix que l'apartat (b) però amb l'equació $x_1^2 + x_2^2 + \cdots + x_n^2 = 1$.

(d) Comproveu que les solucions racionals de l'equació $x^3 + y^3 + z^3 = 1$ venen donades donant valors racionals (s, t) a les fórmules

$$x(s,t) = \frac{3t - \frac{1}{3}(s^2+st+t^2)^2}{t(s^2+st+t^2) - 3}$$

$$y(s,t) = \frac{3s + 3t + \frac{1}{3}(s^2+st+t^2)^2}{t(s^2+st+t^2) - 3}$$

$$z(s,t) = \frac{-3 - (s^2+st+t^2)(s+t)}{t(s^2+st+t^2) - 3}.$$

3. (a) Demostreu que si $n \geq 2$ i $k \geq 1$ són enters, aleshores $(n-1)$ sempre divideix $(n^k - 1)$, però que $(n-1)^2$ divideix $(n^k - 1)$ si i només si $(n-1)$ divideix k.

   (b) Demostreu que n divideix $(n-1)! + 1$ si i només si n és un nombre primer.

   (c) Demostreu que $(n-1)! + 1 = n^k$ per un cert nombre k si i només si $n = 2, 3$ o 5.

4. Un nombre enter n no primer s'anomena un nombre de Carmichael si per a tot nombre enter a coprimer amb n tenim que

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

   (a) Demostreu que un nombre enter n es de Carmichael si i només si n és compost i divideix $a^n - a$ per a tot enter a.

   (b) Demostreu que per a tot $n \geq 2$ enter, el nombre d'elements a de $\mathbb{Z}/n\mathbb{Z}$ tals que $a^{n-1} = 1$ és exactament igual a

$$\prod_{p|n,\ p \text{ primer}} \gcd(p-1, n-1)$$

   (c) Demostreu que un nombre compost m es de Carmichael si és lliure de quadrats i $(p-1)$ divideix $(m-1)$ per a tot primer p que divideix m.

   (d) Trobeu tots els nombres de Carmichael entre 2 i 3000.

5. Considereu la funció φ d'Euler (o sigui, $\varphi(n)$ és igual al nombre d'elements invertibles a l'anell $\mathbb{Z}/n\mathbb{Z}$).

(a) Trobeu tots els nombres n tals que $\varphi(n) = 1$, i tots els nombres n tals que $\varphi(n) = 2$.

(b) Trobeu tots els nombres n tals que $\varphi(n) = 24$.

(c) Trobeu l'enter positiu més petit a tal que no hi ha cap enter n amb $\varphi(n) = a$, el més petit tal que té exactament 2 solucions, exactament 3 solucions i exactament 4 solucions.

(d) Demostreu que, si $\gcd(m, n) > 1$, aleshores $\varphi(nm) > \varphi(n)\varphi(m)$.

(e) Demostreu que, si $m \mid n$, aleshores $\varphi(m) \mid \varphi(n)$.

(f) Demostreu que $n \mid \varphi(a^n - 1)$ per a tot $a > 1$.

6. Sigui p un nombre primer senar.

(a) Sigui A el producte de tots els residus quadràtics mòdul p (els residus quadràtics mòdul p són els elements de $\mathbb{F}_p^\times$ que són quadrats). Demostreu que

$$A \equiv (-1)^{(p+1)/2} \pmod{p}.$$

(b) Demostreu que si $p \equiv 1 \pmod 4$, aleshores la suma de tots el nombres r, $1 \leq r \leq p-1$ que són residus quadràtics és igual a $p(p-1)/4$.

(c) Sigui a un nombre enter no divisible per p. Considerem el conjunt

$$S_a = \{\overline{na} \in \mathbb{F}_p \ : \ n \in \{1, 2, \ldots, (p-1)/2\}\},$$

i el conjunt S'_a format pels elements $\bar{r}$ de S_a tals que $r > p/2$, on r és l'únic nombre enter tal que $1 \leq r \leq p-1$, i $r \equiv \bar{r} \pmod p$. Demostreu que

$$\prod_{r \in S_a} r = (-1)^{|S'_a|} \prod_{s \in S_1} s$$

i deduïu que $\left(\frac{a}{p}\right) = (-1)^{|S'_a|}$.

7. Sigui m un enter positiu senar. Podem escriuré així $m = p_1 \ldots p_s$ on els p_i són primers senars, no necessàriament diferents. Es defineix el **símbol de Jacobi** com:

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{s} \left(\frac{a}{p_i}\right).$$

(a) Demostreu que si a és primer amb m, aleshores l'aplicació $\mu_a\colon\ :\mathbb{Z}/m\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$ definida com $x\mapsto ax$ és un automorfisme (i.e. és bijectiva i morfisme de grups).

(b) Denotem per $\left[\frac{a}{m}\right]$ el signe de la permutació donada per l'aplicació μ_a a $\mathbb{Z}/m\mathbb{Z}$. Demostreu que si $m=m_1m_2$, aleshores

$$\left[\frac{a}{m}\right]=\left[\frac{a}{m_1}\right]\left[\frac{a}{m_2}\right].$$

(c) Demostreu que per a tot m senar i a primer amb m tenim que

$$\left[\frac{a}{m}\right]=\left(\frac{a}{m}\right).$$

(d) Siguin m i n dos enters senars positius i primer entre si. Si escollim com a representant de cada element de $\mathbb{Z}/m\mathbb{Z}$ un enter $0\le a<m$, i també representants $0\le b<n$ dels elements de $\mathbb{Z}/n\mathbb{Z}$, demostreu que tenim tres bijeccions naturals $L,M,N\colon\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/(mn)\mathbb{Z}$ donades per L la bijecció que ens determina el teorema xinès, $N(a,b)=an+b$ i $M(a,b)=bm+a$.

(e) Demostreu que per a tot $b\in\mathbb{Z}/m\mathbb{Z}$, el signe de la permutació $\sigma_b\colon\mathbb{Z}/m\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$ que envia $\sigma_b(a)=a+b$ és sempre 1. Comproveu que la composició de $L^{-1}N$ és igual a l'aplicació $(\sigma_b\circ\mu_n)\times i\colon\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ donada $((\sigma_b\circ\mu_n)\times i)(a,b)=(na+b,b)$. Idem amb $L^{-1}M$ i $i\times(\sigma_a\circ\mu_m)$.

(f) Demostreu que el signe de la permutació de $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ donada per la bijecció $N^{-1}M$ és $(-1)^{(m-1)(n-1)/4}$. Per fer-ho podeu fer servir el fet que el signe d'una permutació τ d'un conjunt X totalment ordenat és igual a -1 elevat al nombre d'inversions de τ: parelles $(a,b)\in X^2$ tals que $a<b$ i $\tau(b)<\tau(a)$, i demostrar que si posem l'ordre lexicogràfic a $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$, el nombre d'inversions és $\binom{m}{2}\binom{n}{2}$.

(g) Deduïu de $(L^{-1}N)(N^{-1}M)=L^{-1}M$ la Llei de reciprocitat quadràtica per al símbol de Jacobi: Si $(m,n)=1$, aleshores

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

8. Direm que un nombre és k-compost si es divisible per com a mínim k-nombres primers diferents. Per exemple, 24 es 2-compost però no és 3-compost, i $210=2\cdot3\cdot5\cdot7$ es k-compost per a $k=2,3,4$.

(a) Trobeu 3 nombres consecutius cadascun d'ells 3-compost.

(b) Demostreu que per a tot $k \geq 2$ i per a tot n existeixen n nombres consecutius tots ells k-compostos.

(c) Un nombre enter n no és lliure de quadrats si hi ha algun nombre primer p tal que p^2 divideix n. Doneu tres nombres consecutius que no siguin lliures de quadrats. Demostreu per a tot $m \geq 2$ existeixen m nombres consecutius que no són lliures de quadrats.

(d) Hi ha m nombres consecutius lliures de quadrats per a a tot $m \geq 2$?

(e) Per a tot $k \geq 1$, hi ha m nombres consecutius que no siguin k-compostos per a a tot $m \geq 2$?

9. (a) Demostreu que hi ha exactament 4 anells commutatius (amb unitat) no isomorfs dos a dos amb 4 elements. Descriviu-los.

(b) Més en general, demostreu que si p és un nombre primer, hi ha exactament 4 anells commutatius (amb unitat) no isomorfs dos a dos amb p^2 elements. (Indicació: Demostreu que un anell amb p^2 elements, o bé és isomorf a $\mathbb{Z}/p^2\mathbb{Z}$, o bé és un $\mathbb{Z}/p\mathbb{Z}$ espai vectorial de dimensió 2).

(c) Podeu dir quants anells commutatius amb 6 elements hi ha, mòdul isomorfia?

10. Considerem una aplicació $d : \mathbb{Z} \to \mathbb{Z}$ tal que $d(p) = 1$ per a tot nombre primer p, i que $d(nm) = nd(m) + md(n)$ per a qualssevol enters n i m.

(a) Demostreu que $d(n) = 0$ si i només si $n = 0$ o ± 1.

(b) Demostreu que $d(-n) = -d(n)$.

(c) Demostreu que si $n = \prod_{i=1}^{s} p_i^{r_i}$ és la factorització amb producte de nombres enters, on p_i són nombres primers diferents, $r_i \geq 1$, aleshores

$$d(n) = n \sum_{i=1}^{s} \frac{r_i}{p_i}.$$

(i per tant d està únicament determinada).

(d) Sigui p és un nombre primer. Definim $v_p(n) = k$ si p^k és la màxima potència de p que divideix un enter n. Demostreu que si $0 < v_p(n) < p$, aleshores $v_p(d(n)) = v_p(n) - 1$, però, en canvi, si $v_p(n) = p$, aleshores $v_p(d(n)) \geq p$.

(e) Demostreu que n és lliure de quadrats si i nomes si $\gcd(n, d(n)) = 1$.

(f) Demostreu que $n = d(n)$ si i nomes si $n = \pm p^p$ per un nombre primer p.

(g) Demostreu que no hi ha solucions de $d(n) = a$ per a $a = 2, 3$ i 11. Trobeu totes les solucions de $d(a) = 4, 5$ i 6.

11. Considerem un nombre primer $p \geq 3$, i definim els enters a_k (depenent de p) que verifiquen la següent igualtat de polinomis en x amb coeficients a $\mathbb{Z}$:

$$\prod_{j=1}^{p-1}(x-j) = \sum_{k=0}^{p-1} a_k x^k.$$

(a) Demostreu que $p \mid a_k$ per a $1 \leq k \leq p-2$. (Indicació: treballeu a $\mathbb{F}_p$).

(b) Calculeu explícitament a_0, i demostreu que

$$a_1 = -(p-1)! \sum_{j=1}^{p-1} \frac{1}{j}.$$

(c) Demostreu que si $p \geq 5$, aleshores $p^2 \mid a_1$. (Indicació: substituïu x per p a l'equació definitoria dels a_k).

(d) Utilitzeu l'apartat anterior per a demostrar que si $p \geq 5$, aleshores

$$\sum_{j=1}^{p-1} \frac{1}{j} \equiv 0 \pmod{p^2}$$

(pensant l'igualtat a $\mathbb{F}_p$ o, si ho preferiu, que el numerador de la part esquerra de l'equació és divisible per p^2).

(e) Demostreu que si $p \geq 5$, aleshores

$$\sum_{j=1}^{p-1} \frac{1}{j^2} \equiv 0 \pmod{p}.$$

12. Considereu la funció φ d'Euler (o sigui, $\varphi(n)$ és igual al nombre d'elements invertibles a l'anell $\mathbb{Z}/n\mathbb{Z}$).

(a) Demostreu que si k i a són enters positius, amb $a \geq 2$, i $m = a^k - 1$, aleshores k és l'ordre de a mòdul m.

(b) Demostreu que si k i a són enters positius, amb $a \geq 2$, aleshores $k \mid \varphi(a^n - 1)$.

(c) Demostreu que si $p \mid \varphi(m)$ però $p \nmid m$, aleshores hi ha com a mínim un nombre q primer amb $q \mid m$ i $q \equiv 1 \pmod{p}$.

(d) Demostreu que per a tot nombre primer p, hi ha infinits nombres primers q tals que $q \equiv 1 \pmod{p}$.

13. Diem que un polinomi irreductible i mònic $q(x)$ de $\mathbb{F}_p[x]$, on p és un nombre primer, és primitiu si la classe de x a $\mathbb{F}_p[x]/q(x)$ és primitiva (i.e. té ordre exactament $p^d - 1$, on d és el grau de $q(x)$).

(a) Demostreu que un polinomi de la forma $x^d + a \in \mathbb{F}_p[x]$ no pot ser mai primitiu.

(b) Demostreu que si $p = 2$ i $2^d - 1$ és un primer (s'anomenen de Mersene), aleshores tot polinomi $q(x) \in \mathbb{F}_2[x]$ monic i irreductible és primitiu.

(c) Demostreu que el nombre de polinomis irreductibles, primitius i mònics de grau $d > 1$ a $\mathbb{F}_p[x]$ és exactament $\frac{\varphi(p^d-1)}{d}$, on φ és la funció φ d'Euler.

(d) Un trinomi primitiu és un polinomi de la forma $q(x) = x^d + ax^s + b \in \mathbb{F}_p[x]$, que és irreductible i primitiu. Demostreu que si $p = 2$, un trinomi $x^d + x^s + 1 \in \mathbb{F}_2[x]$ és primitiu si i només si la recurrència $z_n = z_{n-d} + z_{n-s} \pmod 2$ té periode $t = 2^d - 1$, i és el màxim posible (el periode és t si $z_n = z_{n+t}$ per a tot n, i $t > 0$ és el més petit que ho compleix).

(e) Calculeu tots els polinomis primitius per a $p = 2$ i $n = 2, 3, 4$, $p = 3$, $n = 2, 3$, i $p = 5$, $n = 2$.

14. Direm que un polinomi $p(x) \in \mathbb{Q}[x]$ pren valors enters si per a tot $n \in \mathbb{Z}$ es té $p(n) \in \mathbb{Z}$. Denotem per $\mathbb{Z}\{x\}$ el conjunt de polinomis que pren valors enters.

(a) Demostreu per a tot $n \in \mathbb{Z}_{\geq 1}$, el polinomi

$$b_n(x) = \frac{1}{n!} \prod_{i=0}^{n-1} (x - i)$$

pren valors enters. Definim $b_0(x) = 1$.

(b) Donat un polinomi $p(x) \in \mathbb{Q}[x]$, definim $\Delta(p(x)) = p(x+1) - p(x)$. Demostreu que si $p(x) \in \mathbb{Z}\{x\}$, aleshores $\Delta(p(x)) \in \mathbb{Z}\{x\}$. Demostreu que $\Delta(b_n(x)) = b_{n-1}(x)$ per a tot $n \geq 1$.

(c) Demostreu que $Z\{x\}$ és un subanell de $\mathbb{Q}[x]$.

(d) Demostreu que si un polinomi $p(x)$ és combinació lineal entera

$$p(x) = \sum_{n=0}^{r} a_n b_n(x)$$

amb $a_n \in \mathbb{Z}$ per a tot n, aleshores $p(x) \in \mathbb{Z}\{x\}$, i a més $a_n = \Delta^n(p(x))(0)$.

(e) Demostreu, utilitzant l'apartat anterior, que tot polinomi de $\mathbb{Z}\{x\}$ és combinació lineal entera dels $p_n(x)$, i per tant que

$$\mathbb{Z}\{x\} = \bigoplus_{n=0}^{\infty} \mathbb{Z}b_n(x).$$

15. Una funció $f : \mathbb{Z}_{\geq 1} \to \mathbb{C}$ és multiplicativa si $f(ab) = f(a)f(b)$ per a tot a i b primers entre si.

(a) Demostreu que la funció $d(n)$ que compta el nombre de divisors de n és multiplicativa.

(b) Demostreu que la funció $\sigma(n) = \sum_{d|n} d$, suma de divisors de n, és multiplicativa.

(c) Demostreu que si f és multiplicativa, la següent funció també ho és:

$$\widehat{f}(n) = \sum_{d|n} f(d).$$

(d) Determineu explicitament $\widehat{f}$ per a $f(n) = 1$ (constant igual a 1), $f(n) = \chi_1(n)$ (la funció que val 1 si $n = 1$, i 0 si no), $f(n) = n$ (la funció identitat) i $f = \varphi(n)$ (la funció d'Euler).

(e) Sigui $\mu(n)$ la funció definida com $\mu(n) = 0$ si n és divisible per algun quadrat, $\mu(n) = 1$ si n té exactament un nombre parell de divisors primers i $\mu(n) = -1$ si en té un nombre senar. Demostreu que

$$f(n) = \sum_{d|n} \mu(d)\widehat{f}(n/d)$$

(Pista: feu-ho primer per la funció $\chi_1(n)$ que val 0 per a tot $n > 0$, $\chi_1(1) = 1$.)

(f) Demostreu que si $F(x)$ és una funció de $[1, \infty]$ als reals $\mathbb{R}$, i

$$G(x) = \sum_{1 \leq d \leq x} F(x/d)$$

per a tot $x \geq 1$, aleshores

$$F(x) = \sum_{1 \leq d \leq x} \mu(d)G(x/d)$$

per a tot $x \geq 1$.

(g) Demostreu que, per a tot $x \geq 2$,

$$\left| \sum_{1 \leq n \leq x} \frac{\mu(n)}{n} \right| \leq 1.$$

Per a demostrar-ho podeu fer els següents passos:

i. Proveu que $\sum_{d \leq x} \mu(d) \lfloor \frac{x}{d} \rfloor = 1$ per a tot $x \geq 1$ enter.

ii. Proveu que

$$\left| \sum_{d \leq x} \mu(d) \left(\frac{x}{d} - \lfloor \frac{x}{d} \rfloor \right) \right| \leq x - 1.$$

iii. Deduïu que

$$x \left| \sum_{d \leq x} \frac{\mu(d)}{d} \right| \leq x$$

16. Definim inductivament els polinomis ciclotòmics $\Phi_n(x)$ per a $n \geq 1$ enter com $\Phi_1(x) = x - 1$ i

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\ d<n} \Phi_d(x)}$$

(a) Demostreu que $\Phi_{2n}(x) = \Phi_n(-x)$ si n és senar.

(b) Demostreu que $\Phi_{p^m}(x) = \Phi_p(x^{p^{m-1}})$.

(c) Demostreu que $\Phi_n(x) = \Phi_q(x^{n/q})$ si

$$q = \mathrm{rad}(n) = \prod_{p|n,\ p \text{ primer}} p.$$

(d) Demostreu que si p i q son primers diferents, aleshores $\Phi_p(x)$ i $\Phi_{pq}(x)$ tenen tots els coeficients iguals a 0, 1 o -1.

(e) Demostreu que si n és divisible com a molt per a dos primers senars diferents, aleshores $\Phi_n(x)$ té tots els coeficients iguals a 0, 1 o -1.

(f) Calculeu $\Phi_{105}(x)$ i comproveu que té algun coefficient diferent de 0 i ± 1.

17. Sigui $\lfloor x \rfloor$ la part entera inferior d'un nombre real (o sigui, el nombre enter més gran més petit que x).

Definim, donat un nombre real, les successions $r_0 = x$, $a_0 = \lfloor r_0 \rfloor$, i per $n \geq 1$, si $r_{n-1} = a_{n-1}$, parem la successió, i si no

$$r_n = \frac{1}{r_{n-1} - a_{n-1}} \quad \text{i} \quad a_n = \lfloor r_n \rfloor .$$

Denotem per $x = [a_0; a_1, a_2, a_3, \cdots]$ l'expansió de x en fracció continua.

(a) Demostreu que x és racional si i només si existeix un n tal que $r_n = a_n$.

(b) Donat un nombre real $x = [a_0; a_1, a_2, a_3, \cdots]$, considerem els nombres racionals

$$q_n = [a_0; a_1, a_2, a_3, \cdots, a_n]$$

per a cada $n \geq 0$. Siguin h_n i k_n el numerador i denominador de q_n. Demostreu que

$$h_n = a_n h_{n-1} + h_{n-2} \text{ i que } k_n = a_n k_{n-1} + k_{n-2}.$$

(c) Demostreu que

$$k_n h_{n-1} - k_{n-1} h_n = (-1)^n \text{ i } \frac{h_n}{k_n} - \frac{h_{n-1}}{k_{n-1}} = \frac{(-1)^{n+1}}{k_n k_{n-1}}.$$

(d) Per a $n \geq 1$ i $x = [a_0; a_1, a_2, a_3, \cdots]$ real, sigui $x_n = [a_n; a_{n+1}, a_{n+2}, a_{n+3}, \cdots]$. Demostreu que per a tot $n \geq 1$,

$$x = \frac{h_n x_{n+1} + h_{n-1}}{k_n x_{n+1} + k_{n-1}}$$

(e) Diem que $x = [a_0; a_1, a_2, a_3, \cdots]$ és una fracció continua eventualment periòdica si existeixen $d \geq 1$ i $n_0 \geq 0$ tal que $x_{n+d} = x_n$ per a tot $n \geq n_0$. Demostreu que per $x = \sqrt{2}$, per $\sqrt{3}$ i per $\sqrt{5}$, la fracció continua és eventualment periòdica.

(f) Demostreu que si la fracció continua de x és periòdica amb periode 1 o 2, aleshores x és arrel d'un polinomi mònic de grau com a molt 2 amb coeficients racionals.

(g) Demostreu que si la fracció continua de x és eventualment periòdica, aleshores x és arrel d'un polinomi mònic de grau com a molt 2 amb coeficients racionals. *Comentari:* El recíproc és cert però molt més difícil de demostrar.

18. Sigui $\lfloor x \rfloor$ la part entera inferior d'un nombre real (o sigui, el nombre enter més gran més petit que x). Donat un nombre primer p, i un enter n, sigui $v_p(n)$ la màxima potencia de p que divideix n.

(a) Demostreu que si $x_i \in \mathbb{R}$ per a $i = 1, \ldots, n$, aleshores

$$\sum_{i=1}^{n} \lfloor x_i \rfloor \leq \left\lfloor \sum_{i=1}^{n} x_i \right\rfloor .$$

(b) Demostreu que

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

(c) Demostreu que si $m = a_1 + \cdots + a_n$, amb $a_i \in \mathbb{Z}_{\geq 0}$, i p és un nombre primer, aleshores

$$v_p(m!) \geq \sum_{i=1}^{n} v_p(a_i!).$$

Deduïu que

$$\frac{m!}{a_1! \cdots a_n!} \in \mathbb{Z}_{\geq 1}.$$

(d) Demostreu que si $a \in \mathbb{Z}$, aleshores el nombre $\frac{1}{2a-1}\binom{2a}{a}$ és enter.

(e) Demostreu que si a i $b \in \mathbb{Z}$, aleshores el nombre següent és enter:

$$\frac{(2a)!(2b)!}{a!b!(a+b)!}$$

(f) Demostreu que

$$N! > \left(\frac{N}{e}\right)^N$$

(Indicació: $e^N > N^N/N!$), i deduïu, junt amb b), que

$$\sum_{p \leq N} \frac{\log(p)}{p-1} > \log(N) - 1,$$

el que prova que hi ha infinits primers d'una altra manera.

19. Sigui $\lfloor x \rfloor$ la part entera inferior d'un nombre real (o sigui, el nombre enter més gran més petit que x). Donat un nombre primer p, i un enter n, sigui $v_p(n)$ la màxima potencia de p que divideix n.

(a) Demostreu que

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

(b) Demostreu que per a tot $n \geq a \geq 0$,

$$v_p(n!) \geq v_p(a!) + v_p((n-a)!).$$

(c) Demostreu que si $\frac{2n}{3} < p \leq n$ és un nombre primer, aleshores

$$v_p(\binom{2n}{n}) = 0.$$

(d) Demostreu que si $\sqrt{2n} < p \leq n$ és un nombre primer, aleshores

$$v_p(\binom{2n}{n}) \leq 1.$$

(e) Demostreu que per a tot nombre enter n, si prenem

$$P_n = \{p \text{ nombres primers } \mid n+2 \leq p \leq 2n+1\}$$

aleshores

$$\prod_{p \in P_n} p \leq \binom{2n+1}{n} < 4^n.$$

(f) Deduïu de tot això que si n és prou gran, aleshores sempre hi ha un nombre primer p amb $n \leq p < 2n$. (Indicació: considereu $\binom{2n}{n}$).

20. Sigui $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$ un morfisme de grups. Denotarem per $\chi(n) = \chi(\bar{n})$ si $\bar{n} \neq 0$ és la classe de n mòdul p, i $\chi(n) = 0$ si $\bar{n} = 0$. L'anomenarem caràcter de Dirichlet mòdul p. Diem que $\chi = 1$ si $\chi(a) = 1$ per a tot $a \in \mathbb{F}_p^*$.

(a) Demostreu que $\chi(n) = \left(\frac{n}{p}\right)$ és un caràcter de Dirichlet.

(b) Si χ i χ' són caràcters de Dirichlet mòdul p, demostreu que $\chi\chi'$ (definit com $(\chi\chi')(a) = \chi(a)\chi'(a)$) també ho és.

(c) Demostreu que $\sum_{a \in \mathbb{F}_p} \chi(a) = 0$ si i només si $\chi \neq 1$.

(d) Sigui $\psi = e^{2\pi i/p} \in \mathbb{C}$ una arrel primitiva p-èssima de 1. Definim la suma de Gauss de χ com

$$G(\chi) = \sum_{a \in \mathbb{F}_p} \chi(a)\psi^a.$$

Calculeu $G(\chi)$ si $\chi = 1$, si χ és el caràcter modul 5 determinat dient que $\chi(2) = i = \sqrt{-1}$, i si χ és el caràcter modul 7 determinat dient que $\chi(3) = \omega = e^{\pi i/3}$..

(e) Si χ i χ' són caràcters de Dirichlet mòdul p, definim

$$J(\chi, \chi') = \sum_{a \in \mathbb{F}_p} \chi(a)\chi'(1-a).$$

Demostreu que si χ, χ' i $\chi\chi'$ són $\neq 1$, aleshores

$$J(\chi, \chi')G(\chi\chi') = G(\chi)G(\chi').$$

(f) Demostreu que si $\chi \neq 1$, aleshores $\|G(\chi)\| = \sqrt{p}$ com a número complex.

21. L'objectiu d'aquest problema és demostrar que per a tota base $b > 1$, hi ha infinits enters $n > 1$ no primers que són pseudoprimers per la base b. Recordem que n és pseudoprimer per a la base b si $b^{n-1} \equiv 1 \pmod{n}$.

(a) Dóna un exemple d'un pseudoprimer n no primer en la base 2. Demostra que si n és pseudoprimer no primer en la base 2, aleshores $2^n - 1$ també ho és.

(b) Més en general, demostra que si n és pseudoprimer no primer en la base b, i $\gcd(b-1, n) = 1$, aleshores l'enter $N = (b^n - 1)/(b - 1)$ també ho és, i $N > n$.

(c) Aplica l'apartat anterior per a demostrar que hi ha infinits pseudoprimers no primers en la base $b = 2, 3, 5$.

(d) Sigui $b > 1$ un enter i p un nombre primer tal que p no divideix $b^3 - b$. Sigui $n = (b^{2p} - 1)/(b^2 - 1)$.

i. Demostra que n és un enter, i que no és primer.

ii. Demostra que $2p$ divideix $n - 1$.

iii. Demostra que n és pseudoprimer en la base b.

(e) Conclou demostrant l'objectiu.

22. Sigui $P_n = 2 \cdot 3 \cdot 5 \cdots p_n$ és producte de tots els n primers nombres primers, on p_n denota el enèssim nombre primer. L'objectiu es demostrar que el primer p_{n+1} és l'únic nombre enter positiu m tal que

$$1 < 2^m \left(\sum_{d|P_n} \frac{\mu(d)}{2^d - 1} - \frac{1}{2} \right) < 2,$$

on $\mu(d)$ és la funció de Möbius que val 1 si d és producte d'un nombre parell de primers diferents, -1 si és producte d'un nombre senar de primers diferents, i 0 si no (o sigui, és divisible per algun nombre > 1 al quadrat).

(a) Definim la següent distribució de probabilitat als enters positius $n \geq 1$: $p(n) = 2^{-n}$. Demostreu que la probabilitat $q(d)$ que un enter a l'atzar sigui divisible per d amb aquesta distribució és

$$q(d) = \sum_{n=1}^{\infty} p(nd) = \frac{1}{2^d - 1}.$$

(b) Demostreu ara que la probabilitat $c(m)$ que un nombre enter a l'atzar sigui coprimer amb m és

$$c(m) = \sum_{d|m} \frac{\mu(d)}{2^d - 1},$$

utilitzant l'anomenat principi d'inclusió-exclusió.

(c) Demostreu directament que

$$c(P_n) = \sum_{\gcd(m,P_n)=1} p(m) = \frac{1}{2} + \frac{1}{2^{p_{n+1}}} + \sum_{i \in I_n} \frac{1}{2^i}, \quad \text{on } I_n \subset \mathbb{Z}_{i > p_{n+1}}.$$

(d) Demostreu que

$$2^{m-p_{n+1}} < 2^m \left(c(P_n) - \frac{1}{2} \right) < 2^{m-p_{n+1}+1}$$

i deduïu-ne el resultat.

(e) Doneu una fòrmula per p_n utilitzant això i la funció $\lfloor\ \rfloor$ "part entera per sota".

(f) Una altra fòrmula "fàcil" per $\pi(n)$, el nombre de primers menors que n és la següent:

$$\pi(n) = \sum_{j=2}^{n} \left(1 + \left\lfloor \frac{2 - \sum_{i=1}^{j} \left(\left\lfloor \frac{j}{i} \right\rfloor - \left\lfloor \frac{j-1}{i} \right\rfloor \right)}{j} \right\rfloor \right)$$

i. Demostreu primer que

$$d(j) = \sum_{i=1}^{j} \left(\left\lfloor \frac{j}{i} \right\rfloor - \left\lfloor \frac{j-1}{i} \right\rfloor \right)$$

és el nombre de divisors de j.

ii. Demostreu ara que

$$F(j) = 1 + \left\lfloor \frac{2 - d(j)}{j} \right\rfloor = \begin{cases} 1 & \text{si } j \text{ és primer,} \\ 0 & \text{si } j \text{ és compost.} \end{cases}$$

iii. Deduïu la fórmula per $\pi(n)$.

23. A la classe de problemes hem analitzat l'algoritme de Karatsuba per la multiplicació d'enters. Aquest exercici estudia una generalització d'aquest algoritme. Considerem dos nombres positius x, y, cadascun de kn bits per certs enters k i n (si el nombre de bits no és un múltiple de k, podem afegir zeros). Escrivim x i y en base $B = 2^n$ (notem que en aquesta base tant x com y tindran exactament k dígits), de manera que $x = \sum_{i=0}^{k-1} y_i B^i$ i $y = \sum_{i=0}^{k-1} y_i B^i$. Considerem els polinomis $p(t) = \sum_{i=0}^{k-1} x_i t^i$ i $q(t) = \sum_{i=0}^{k-1} y_i t^i$.

(a) Trobeu una relació entre els polinomis $p(t)$, $q(t)$ i el producte xy.

(b) Trobeu una fórmula semblant a la de l'algoritme de Karatsuba que dóni els coeficients de $p(t)q(t)$ en termes dels valors de p i q en els punts

$$\infty, 0, \pm 1, \pm 2, \ldots \pm (k-2), k-1.$$

(c) En el cas $k = 3$, compteu el nombre de sumes i productes d'enters de n bits que cal fer en aquest cas per obtenir el producte de x i y.

(d) Doneu un algoritme recursiu aprofitant aquesta idea (per $k = 3$) i estimeu el nombre d'operacions de bit que cal per multiplicar enters de N bits.

(e) A la vista del resultat obtingut, podeu conjecturar quin és el nombre d'operacions de bit aproximat que calen amb k arbitrari?

(f) Compareu el resultats amb l'algoritme *schoolbook* i amb l'algoritme de *Karatsuba*.

24. Sigui $n \geq 2$ un nombre enter. Denotem per

$$s_m(n) = \sum_{k=1}^{m} k^n.$$

Donat un nombre enter $n \geq 2$, denotem P_n el conjunt de primers que el divideix.

(a) Demostreu que si $n = p$ un nombre primer, aleshores $s_{n-1}(n-1) \equiv -1 \pmod{n}$.

(b) Demostreu que si p és un primer, aleshores $s_{p-1}(n-1) = \sum_{k=1}^{p-1} k^{n-1}$ és $\equiv -1 \pmod{p}$ si $p-1$ divideix a $n-1$, i és $\equiv 0 \pmod{p}$ si no.

(c) Demostreu que $s_{n-1}(n-1) \equiv -1 \pmod{n}$ si i només si per a tot $p \in P_n$ tenim que $p(p-1)$ divideix $\frac{n}{p} - 1$.

(Indicació: proveu que si p divideix n, $s_{n-1}(n-1) = \sum_{k=1}^{n-1} k^{n-1}$ és $\equiv -\frac{n}{p} \pmod{p}$ si $p-1$ divideix a $n-1$, i és $\equiv 0 \pmod{p}$ si no).

(d) Trobeu 2 nombres enters no primers n tals que per a tot $p \in P_n$ tenim que $p-1$ divideix $\frac{n}{p} - 1$.

(e) Trobeu 2 nombres enters no primers n tals que per a tot $p \in P_n$ tenim que p divideix $\frac{n}{p} - 1$.

(f) Demostreu que n compleix que per a tot $p \in P_n$, p divideix $\frac{n}{p} - 1$ si i només si

$$\sum_{p \in P_n} \frac{1}{p} - \prod_{p \in P_n} \frac{1}{p} \in \mathbb{Z}_{\geq 1}.$$

(g) Demostreu que un nombre senar i lliure de quadrats que compleixi la propietat anterior ha de tenir com a mínim 9 divisors primers diferents.

(h) Proveu amb l'ajuda de l'ordinador què no hi ha cap nombre senar lliure de quadrats menor que 10^{12} que compleixi la propietat anterior (es sospita que no n'hi ha cap, però no es coneix).

25. Definim els polinomis de Bernoulli $B_n(x)$ com els coeficients del desenvolupament en serie de la funció

$$\frac{ze^{zx}}{e^z - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{z^n}{n!},$$

i els nombres de Bernoulli $B_n = B_n(0)$.

Definim

$$s_m(n) = \sum_{k=1}^{m} k^n.$$

(a) Demostreu que

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}.$$

(b) Demostreu que

$$s_m(n) = \frac{1}{m+1}(B_{m+1}(n+1) - B_{m+1}).$$

(c) Demostreu que

$$\sum_{k=0}^{n} \binom{n+1}{k} B_k = 0.$$

(d) Demostreu que $B_n = 0$ per a tot n senar.

(e) Demostreu que per a tot n,

$$B_{2n} + \sum_{(p-1)|2n} \frac{1}{p} \in \mathbb{Z}.$$

(f) Demostreu que per a tot nombre primer p, i n i m no divisibles per $p-1$ però $n \equiv m \pmod{p-1}$, aleshores

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \pmod{p}$$

26. Un número enter n és abundant si la suma dels seus divisors és més gran que $2n$ (recordem que un nombre és perfecte si la suma dels seus divisors és igual a $2n$).

(a) Proveu que tot múltiple positiu d'un nombre abundant és abundant.

(b) Proveu que tot múltiple positiu de un nombre perfecte fora d'ell mateix és abundant.

(c) Comproveu que tot nombre de la forma $6m + 20$, $6m + 12$ i $6m + 40$ per $m > 1$ i $12m + 20$ per $m \geq 1$, són suma de dos nombres abundants.

(d) Proveu que tot nombre parell més gran que 46 és suma de dos nombres abundants, veient que els casos anteriors cobreixen tots aquests nombres parells.