Problemes d'Aritmètica. Llista 3

1. Considera una corba el·líptica $L = \mathbb{R}(X)[y]/(y^2 - x^3 - ax - b)$, amb $a, b \in \mathbb{R}$.
   a) Determina que han de complir els coeficients (a, b) per tal que $E_L(\mathbb{R})$ sigui connexa. Quantes components connexes pot tenir?
   b) Descriu geomètricament (al pla real) els punts d'ordre 2 d'una corba el·líptica donada.
   c) Descriu geomètricament els punts d'ordre 3.

2. Sigui K un cos de característica arbitrària, i

$$L = K(X)[y]/(y^2 + a_1Xy + a_3y - X^3 - a_2X^2 - a_4X - a_6)$$

   una corba el·líptica sobre K, comproveu que la definció de la suma al conjunt $E_L(K)$ té sentit, és a dir, que donats $P, Q \in E_L(K)$, llavors $P + Q \in E_L(K)$. Trobeu les fórmules explícites per $-P$, $2P$ i $P + Q$.

3. Descriu el grup abstracte de punts $E_L(\mathbb{F}_3)$, on $\mathbb{F}_3$ és el cos de 3 elments, per les corbes el·líptiques $L = \mathbb{F}_3(X)[y]/F(X, y)$ on $F(X, y)$ és:

$y^2 - X^3 + X + 1$	$y^2 - X^3 + X^2 + 1$	$y^2 - X^3 - X^2 + 1$	$y^2 - X^3 - X$
$y^2 - X^3 + X$	$y^2 - X^3 + X^2 - 1$	$y^2 - X^3 - X^2 - 1$	$y^2 - X^3 + X - 1$

4. Donat $P = (x, y) \in E_L(\mathbb{Q})$ on $L = \mathbb{Q}(X)[y]/(y^2 - X^3 - c)$, demostreu que aleshores

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3}\right)$$

   també és una solució. Comproveu que aquesta fórmula es correspon a la operació $-2P$ respecte la operació suma de la corba el·líptica (aquesta fórmula va ser descoberta per Claude Gaspar Bachet de Méziriac (1581-1638)).

5. Considera la corba el·líptica $L = \mathbb{Q}(X)[y]/(y^2 - X^3 + 4X - 16)$. Comproveu que el punt $P = (0, 4) \in E_L(\mathbb{Q})$ és d'ordre 5. Podeu calcular $2P, 3P$ i $4P$. Quina figura geomètrica formen (en el pla real)?

6. Tradicionalment es diu que un nombre natural $n > 0$ (lliure de quadrats) és congruent si hi ha un triangle rectangle amb costats racionals tal que n és igual a la seva àrea.

   Per exemple 6 és congruent ja que és l'àrea del triangle rectangle amb costats $3, 4$ i 5; i 5 també ho és, ja que és l'àrea del triangle rectangle amb costats $\frac{3}{2}$, $\frac{20}{3}$ i $\frac{41}{6}$. Si denotem (a, b, h) els costats d'un triangle amb àrea n amb, $A < b < h =$ hipotenusa, demostreu que aleshores $x = \frac{n(a+h)}{b}$ és la coordenada x d'una solució de la corba $E_n : y^2 = x^3 - n^2x$.

   a) Quina és la coordenada y? Recíprocament, demostreu que un punt (x, y) de E_n amb $y \neq 0$ ens determina un triangle rectangle amb àrea n.
   b) Comproveu que els punts que ens donen les solucions d'abans per a $n = 6$ i 5 tenen ordre inifinit.
   c) Es pot demostrar que $1, 2, 3$ i 4 no són congruents, calculant explícitament els punts racionals de la corba E_n corresponent.
   d) Demostreu que $E_{m^2n}(\mathbb{Q}) \cong E_n(\mathbb{Q})$ si n i $m \in \mathbb{Z}$, i per tant m^2 mai és congruent per a $m \in \mathbb{Z}$.
   e) Demostreu, finalment, que $n = 7, 13, 14, 15$ i 20 són congruents. Compte, que n'hi ha un d'aquests que és més difícil que els altres!

7. Sigui k un cos. Considereu el conjunt S de solucions de l'equació $Y^2Z = X^3$ en el pla projectiu $\mathbb{P}^2(k)$.
   a) Comproveu que S és igual a les solucions de la forma $[x : y : 1]$ i el punt $\infty = [0 : 1 : 0]$.
   b) Demostreu que la corba donada per l'equació $y^2 - x^3 = 0$ és singular en el punt $(0, 0)$ i enlloc més.
   c) Demostreu que l'aplicació $\varphi : k \to S_0 := S \setminus \{[0 : 0 : 1]\}$ donada per $t \mapsto \left[t : 1 : t^3\right]$ (o, en coordenades afins, per $t \mapsto \left(\frac{1}{t^2}, \frac{1}{t^3}\right)$), és una bijecció.
   d) Demostreu que la operació suma dels punts de les corbes el·líptiques ens dóna també una operació a S_0, i que a través de φ correspon a la suma (usual) de k.

8. Sigui k un cos. Considereu el conjunt $E_L(k)$ amb $L = k(X)[y]/(y^2 - X^3 - X^2)$. Demostreu que l'aplicació $\psi : E_L(k) \to K^*$ donada per

$$\psi(P) = \begin{cases} \frac{y-x}{y+x} & \text{si } P \neq \mathcal{O} \\ 1 & \text{si } P = \mathcal{O} \end{cases}$$

   és un morfisme de grups bijectiu.