Práctica

1. Sea $\mathcal{C}$ una cúbica en el plano proyectivo dada por la ecuación homogénea:

$$y^2z = x^3 + axz^2 + bz^3.$$

   (a) Verificar que hay un único punto en el infinito: $\mathcal{O} = (0 : 1 : 0)$. $\mathcal{O}$ es un punto no singular de $\mathcal{C}$ y además es un punto de inflexión.

   (b) Probar que la curva $\mathcal{C}$ es no singular si y sólo si $4a^3 + 27b^2 \neq 0$

   (c) Si $4a^3 + 27b^2 = 0$, encuentre los puntos singulares de $\mathcal{C}$ y decida de qué tipo de singularidades se trata (cúspide o un nodo). Pruebe que, en estos casos, $\mathcal{C}$ es parametrizable y encuentre una parametrización.

2. Probar que

   (a) $y^2 - xy + 2y = x^3 + 2x^2$ tiene un punto de orden 7;

   (b) $y^2 + 7xy - 6y = x^3 - 6x^2$ tiene un punto de orden 8.

3. Sea $P = (x, y)$ un punto de la cúbica

$$y^2 = x^3 + ax + b$$

   .

   (a) Sabemos que la coordenada x del punto $2P$ está dada por

$$x(2P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4y^2}.$$

   Derivar una fórmula similar para la coordenada y de $2P$ en términos de x e y.

   (b) Encontrar polinomios $\psi_3(x)$ y $\psi_4(x)$ cuyas raíces sean las x-coordenadas de los puntos P de orden 3 y de orden 4, respectivamente.
   sugerencia: $3P = \mathcal{O}$ puede escribirse $2P = -P$ y $4P = \mathcal{O}$ si y sólo si $y(P) = 0$ o $y(2P) = 0$.

   (c) Encuentre todos los puntos de orden 3 y de orden 4 de la curva $y^2 = x^3 + 1$.

4. Sea $\mathcal{C}$ una cúbica no singular, dada por la ecuación usual

$$y^2 = f(x) = x^3 + ax + b.$$

Probar que:

$$\frac{d^2y}{dx^2} = \frac{2f''(x)f(x) - f'(x)^2}{4yf(x)} = \frac{\psi_3(x)}{4yf(x)}$$

y deducir que un punto $P \in \mathcal{C}$ es un punto de orden 3 si y sólo si $P \neq \mathcal{O}$ y P es un punto de infexión de la cúbica.

5. Sean $p \geq 2$ primo y $\mathcal{C}$ la cúbica

$$\mathcal{C} : y^2 = x^3 + px.$$

Encuentre todos los puntos de torsión en $\mathcal{C}(\mathbb{Q})$.

6. Encontrar el grupo de puntos de torsión de las siguientes cúbicas:

   (a) $y^2 = x^3 + 1$
   (b) $y^2 = x^3 - 4x$
   (c) $y^2 = x^3 - 43x + 166$
   (d) $y^2 = x(x-1)(x+2)$
   (e) $y^2 = x(x+1)(x+4)$
   (f) $y^2 = x(x+81)(x+256)$

7. Sea $\mathcal{C}$ la curva elíptica $y^2 = x^3 + ax$, $a \in \mathbb{Z}$. Sea $p \equiv 3(4)$ primo y $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Probar que $|\mathcal{C}(\mathbb{F}_p)| = p + 1$.

   Sugerencia: observar que $f(x) = x^3 + ax$ es una función impar y que -1 no es residuo cuadrático módulo p. Cuente el número de puntos.

8. Sea $\mathcal{C}$ la curva elíptica $y^2 = x^3 + ax$, $a \in \mathbb{Z}$ libre de potencias cuartas. Sea T el grupo de puntos de torsión de $\mathcal{C}(\mathbb{Q})$.

   (a) Probar que $|T| \mid 4$.
   (b) Probar que T está dado por:

$$T = \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{si } a = 4 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{si } -a \text{ es un cuadrado en } \mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} & \text{sino} \end{cases}$$

9. Sea p un primo impar y sea $\mathcal{C}$ la curva elíptica

$$y^2 = x^3 - p^2x.$$

Probar que el rango r de $\mathcal{C}(\mathbb{Q})$ satisface:

$$\begin{array}{ll} r \leq 2 & \text{si } p \equiv 1(8) \\ r = 0 & \text{si } p \equiv 3(8) \\ r \leq 1 & \text{si } p \equiv 5, 7(8) \end{array}$$