Curvas elípticas

155. Para cada $m \in \mathbb{Q}$ considérese la intersección de la circunferencia unidad con la recta de pendiente m que pasa por $(1,0)$ y utilícese esta construcción para probar que las curvas $Y = 0$ y $X^2 + Y^2 = 1$ son birracionalmente equivalentes.

156. Usando el problema anterior, dar una fórmula para todos los pares de números racionales que pueden ser catetos de un triángulo rectángulo de hipotenusa 1.

157. Reducir la curva elíptica $E : Y^2 + 4XY = 3X^3 + 5X^2 + 1$ a su forma canónica.

158. Hallar la forma canónica de la curva elíptica $U^3 + V^3 = 1$ empleando el cambio $X = (3U + 3V)^{-1}$, $Y = (U - V)(6U + 6V)^{-1}$.

159. Sea $E : Y^2 = P(X)$ con $P(X) = X^3 + AX + B$. Demostrar que E es una curva elíptica si y sólo si $\mathrm{mcd}(P', P) = 1$. Deducir que E es una curva elíptica si y sólo si $4A^3 + 27B^2 \neq 0$.

160. Sean $P = (1,1)$, $Q = (-1,3)$, $R = (-1,-3)$ puntos de la curva elíptica $E : Y^2 = X^3 - 5X + 5$. Hallar $P + Q$, $P - Q$ y $2P + Q + R$.

161. Considérense $P = (-1,1)$ y $Q = (1,2)$ puntos de la curva elíptica $E : Y^2 = X^3 + X/2 + 5/2$. Hallar $2P$ y $2Q$.

162. Sea la curva elíptica $E : Y^2 = X^3 + 17$ y los puntos $P = (-2,3)$, $Q = (2,5)$. Calcular $P + Q$ y $3P$.

163. Hallar el orden de $P = (-3,2)$ en la curva elíptica $E : Y^2 + 2(X+1)Y = X^3 - X^2 - 2X + 26$.

164. Calcular el orden de $P = (2,3)$ en la curva elíptica $E : Y^2 = X^3 + 1$.

165. Si E es una curva elíptica y $m \in \mathbb{Z}^+$, se define $E[m] = \{P \in E \ : \ mP = O\}$. Comprobar que $E[m]$ es un grupo. Hallar una curva elíptica tal que $E[2] = \{O\}$. ¿A qué grupo es isomorfo $E[2]$ si consideramos E definida sobre $\mathbb{C}$ en vez de sobre $\mathbb{Q}$?

166. Fermat probó que $z^2 = x^4 + y^4$ no tiene soluciones enteras $xyz \neq 0$. Deducir de ello que el grupo de Mordell-Weil de $E : Y^2 = X^4 + 1$ es isomorfo a $\mathbb{Z}_3$. (Nota: Como se verá en un problema posterior, E es realmente una curva elíptica. Para este ejercicio no es necesario reducirla a su forma canónica).

167. La ecuación $E : \ Y^2 = X^3 + AX + B$ define una curva elíptica en $\mathbb{F}_p$ (esto es, $\mathbb{Z}_p$ con estructura de cuerpo) siempre que $X^3 + AX + B$ no tenga raíces dobles módulo p. Estas curvas elípticas sobre $\mathbb{F}_p$ también tienen una ley de grupo definida con las mismas fórmulas que en $\mathbb{Q}$ pero usando las operaciones de $\mathbb{F}_p$. Demostrar que el grupo de Mordell-Weil es un grupo abeliano de a lo más $2p + 1$ elementos. *Indicación*: Dar todos los posibles valores a X.

168. Hallar el grupo de Mordell-Weil de $E: Y^2 = X^3 + 2$ en $\mathbb{F}_5$. Calcular la suma de $(2,0)$ y $(3,2)$.

169. Sabiendo que la curva elíptica $E: Y^2 = X^3 + X + 1$ sobre $\mathbb{F}_{103}$ tiene 87 puntos (contando también O), hallar el número de puntos de $E_d: dY^2 = X^3 + X + 1$ donde $103 \not| d$. *Indicación*: Distínganse dos casos según d sea o no sea residuo cuadrático módulo 103.

170. Sea N_p el orden del grupo de Mordell-Weil de una curva elíptica sobre $\mathbb{F}_p$. La *desigualdad de Hasse* es un profundo resultado que afirma que $|N_p - p - 1| < 2\sqrt{p}$. Comprobar esta desigualdad para $E: Y^2 = X^3 + X + 1$ con $p = 5$ y $p = 7$.

171. Sea $E: Y^2 = X^4 + 2\alpha X^2 + \beta$, con $\beta \neq 0, \alpha^2$. Demostrar, reduciéndola a su forma canónica con el cambio $U = X^2 + Y + \alpha$, $V = X(X^2 + Y + \alpha)$, que E es una curva elíptica. Concluir que $Y^2 = (1 + aX^2)(1 + bX^2)$ también lo es para $0 < a < b$.

172. Sea $S(d_1, d_2) = \{(x, y, z) \in \mathbb{Z}^3 \ : \ x^2 - d_1 y^2 = 1, \ z^2 - d_2 y^2 = 1\}$ con $d_1, d_2 \in \mathbb{Z}^+$ distintos. Utilizando el teorema de Siegel, el problema anterior y que $(x, y, z) \in S(d_1, d_2)$ implica $(xz)^2 = (1 + d_1 y^2)(1 + d_2 y^2)$, demostrar que $|S(d_1, d_2)| < \infty$.