Ejercicios de Curvas elípticas sobre cuerpos finitos

Popayán - Esquela CIMPA 2023

August 2, 2023

1 Ecuación (general) de Weierstrass

- Considere la ecuación (general) de Weierstrass: $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ donde $a_1, a_2, a_3, a_4, a_6 \in K$ cuerpo.
- Muestre que si K tiene una característica diferente de 2, la transformación afín

$$\begin{cases} x \longmapsto x \\ y \longmapsto y - (a_1x + a_3)/2 \end{cases}$$

  mapea la ecuación (general) de Weierstrass en una de las formas $y^2 = x^3 + b_2x^2 + b_4x + b_6$. Calcule b_2, b_4, b_6 en términos de a_1, a_2, a_3, a_4, a_6.
- Muestre que si K tiene una característica diferente de 3, la transformación afín

$$\begin{cases} x \longmapsto x - a_2/3 \\ y \longmapsto y \end{cases}$$

  mapea la ecuación de Weierstrass: $y^2 = x^3 + b_2x^2 + b_4x + b_6$ en una de las formas $y^2 = x^3 + c_4x + c_6$. Calcule c_4, c_6 en términos de b_2, b_4, b_6.
- Suponga que la característica de K es 2 y considere la ecuación de Weierstrass: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
  - Si $a_1 \neq 0$, demuestre que la transformación

$$\begin{cases} x \longmapsto a_1^2x + a_3/a_1 \\ y \longmapsto a_1^3y + (a_1^2a_4 + a_3^2)/a_1^3 \end{cases}$$

    asigna la ecuación anterior a lo siguiente: $y^2 + xy = x^3 + b_2x^2 + b_6$. También pruebe que lo anterior no es singular si y solo si $b_6 \neq 0$.
  - Si $a_1 = 0$, demuestre que la transformación

$$\begin{cases} x \longmapsto x + a_2 \\ y \longmapsto y \end{cases}$$

    asigna la ecuación anterior a lo siguiente: $y^2 + b_3x = x^3 + b_4x + b_6$. También pruebe que lo anterior no es singular si y solo si $b_3 \neq 0$.
  - Muestre que una curva definida por $y^2 + xy = x^3 + b_2x^2 + b_6$ ($b_6 \neq 0$) tiene un único punto de orden 2 mientras que $y^2 + b_3x = x^3 + b_4x + b_6$ ($b_3 \neq 0$) no tiene puntos de orden 2.
  - Enumere todas las posibles ecuaciones de Weierstrass no singulares (simplificadas) sobre $\mathbb{F}_2$ y para cada uno de ellos calcular el grupo de puntos racionales sobre $\mathbb{F}_2$. Calcular, cuando sea posible, las isogenias entre las curvas anteriores.
- Considere la transformación afín:

$$\begin{cases} x = u^2x' + r \\ y = u^3y' + su^2x' + t \end{cases}$$

  dónde: $u \in K^*, r, s, t \in K$.
  - Muestre que mapea una ecuación general de Weierstrass en otra ecuación de Weierstass;
  - Muestre que cualquier transformación afín entre las ecuaciones de Weierstrass tiene la forma anterior;
  - Muestre que la transformación anterior es un isomorfismo entre los respectivos grupos de puntos racionales.
- Clasificar todas las posibles clases de isomorfismos de curvas elípticas sobre $\mathbb{F}_3$.

2 Polinomios de división

Considerar

$$\begin{cases} \psi_0 = 0, \quad \psi_1 = 1, \\ \psi_2 = 2y, \\ \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2, \\ \psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \\ \vdots \\ \psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ por } m \geq 2, \\ \psi_{2m} = \left(\frac{\psi_m}{2y}\right) \cdot (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ por } m \geq 3. \end{cases}$$

El polinomio ψ_n se llama **polinomio n–ésimo de división**. El objetivo de estos problemas es establecer las propiedades básicas de estos polinomios.

1. Verificar la identidad
$$[n](x,y) = \left(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2(x)}, \frac{\psi_{2n}(x,y)}{2\psi_n^4(x)}\right)$$
por $n = 1, 2, 3$.

2. Establecer $y^2 = x^3 + Ax + B$ y mostrar que $\psi_{2m+1} \in \mathbb{Z}[x, A, B]$ y $\psi_{2m} \in 2y\mathbb{Z}[x, A, B]$.

3. Demostrar la identidad
$$\psi_n = \begin{cases} nx^{(n^2-1)/2} + \cdots & \text{si } n \text{ es impar;} \\ y(nx^{(n^2-4)/2} + \cdots) & \text{si } n \text{ es par.} \end{cases}$$

4. Muestre que si E está definido sobre K, entonces $\psi_n^2, \frac{\psi_{2n}}{y}, \psi_{2n+1}$, están todos en $K[x]$.

5. Demuestra que las raíces de ψ_{2n+1} son las coordenadas x de los puntos de $E[2n+1] \setminus \{\infty\}$, donde $E[2n+1]$ es el subgrupo de torsión $(2n+1)^{\text{th}}$ de E. De manera similar, las raíces de ψ_{2n}/y son las coordenadas x de los puntos de $E[2n] \setminus E[2]$.