Aritmética de Curvas Elípticas

2do. Cuatrimestre 2006

Guía 1

Por K denotaremos un cuerpo (no necesariamente algebraicamente cerrado).

(1) Sea $\mathcal{C} \subset \mathbb{P}^2$ la curva dada por la ecuación $x^2 + y^2 = z^2$. Probar (a mano) que la función:

$$\phi : \mathcal{C} \mapsto \mathbb{P}^1, \qquad \phi = [x + z, y]$$

es un morfismo definido en todos los puntos.

(2) Sea $\mathcal{C}/K$ una cúbica no singular en $\mathbb{P}^2$ (i.e. esta dada por un polinomio homogéneo de grado 3 sin puntos singulares) con un punto $P \in \mathbb{P}^2(K)$.
- Probar que $(\mathcal{C}, P)$ es una curva elíptica con la definición usual.
- Dar un método que envie $\mathcal{C}$ en ecuación de Weierstrass de forma tal que el cambio de coordenadas quede definido sobre K (i.e. dar una forma explícita de la demostración dada en la teórica utilizando Riemann-Roch). Sugerencia: separar los casos en que P sea de inflexión o no.
- Pasar la curva elíptica $x^3 + y^3 - z^3$ con el punto $(1, -1, 0)$ a ecuación de Weierstrass. (al finalizar el curso podremos probar Fermat para $n = 3$)

(3) Sea E/K una curva elíptica, y supongamos que la característica de K no es dos. Probar que E tiene a lo sumo un punto singular y (de tenerlo) dicho punto está en K. ¿Que pasa si la característica de K es 2?

(4) Sea E/K una curva elíptica dada por ecuación de Weierstrass.

(a) Supongamos que E tiene un nodo y que las tangentes en el nodo son $y = \alpha_i x + \beta_i$ con $i = 1, 2$.
- Si $\alpha_1 \in K$ probar que $\alpha_2 \in K$ y $E_{ns}(K) \cong K^\times$.
- Si $\alpha_1 \notin K$ entonces el cuerpo $L = K(\alpha_1, \alpha_2)$ es una extensión cuadrática de K. Como $E_{ns}(K) \subset E_{ns}(L) \cong L^\times$, probar que $E_{ns}(K) = \left\{t \in L^\times \ : \ \mathcal{N}_{L/K}(t) = 1\right\}$.

(Sugerencia: recordar que la función que da el isomorfismo en $\bar{K}$ es $(x, y) \mapsto \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2}$).

(b) Si E tiene una cúspide entonces $E_{ns}(K) \cong K$ (aditivamente).

(5) Sea $F(x, y, z)$ un polinomio en $K[x, y, z]$ homogéneo de grado d. Supongamos que la curva $\mathcal{C}$ dada for $F = 0$ en $\mathbb{P}^2(K)$ es no singular. Definimos el Hessiano H de F en un punto P como la matriz de 3×3 de las derivadas parciales segundas en P.
- Probar que un punto P en $\mathcal{C}$ es de inflexión si y sólo si $\det(H(P)) = 0$. (Sugerencia: para facilitar las cuentas suponer vía un cambio lineal de variables que $P = (0, 1, 0)$ y la recta tangente es $Z = 0$).
- Utilizando el Teorema de Bezout, calcular el número de puntos de inflexión de $\mathcal{C}$ en $\bar{K}$ (para ver que el orden de contacto entre dos curvas es 1, basta con ver que las rectas tangentes en el punto de intersección son distintas).

(6) Sea E/K una curva elíptica en ecuación de Weierstrass. Probar que los puntos de orden dividiendo a 3 (i.e. los puntos $P \in E(\bar{K})$ tales que $3P = \mathcal{O}$) son los puntos de inflexión de E. Deducir el número de puntos de orden exactamente 3. ¿Cuantos hay de orden exáctamente 2?