Aritmética de Curvas Elípticas

1er. Cuatrimestre 2014

Práctica 1

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

1. Sea $\mathcal{C} : ax^2 + bxy + cxz + dy^2 + eyz + fz^2$ una cúbica en $\mathbb{P}^2$ no singular. Sea $P = (x_0, y_0, z_0)$ un punto en $\mathbb{P}^2(K)$. Hallar una parametrización de todos los puntos de $\mathcal{C}(K)$ de manera similar a lo hecho en la teórica con el círculo, o sea mirar la recta tangente a $\mathcal{C}$ por P, desplazarla por algún elemento de $P^2(K)$ y establecer una biyección entre los puntos en K de esta recta y los puntos de $\mathcal{C}(K)\backslash\{P\}$. (Para simplificar las cuentas, se puede suponer que $z_0 \neq 0$, y mirar la curva en K^2 vía reemplazar $z = 1$ en la ecuación que define $\mathcal{C}$ teniendo precaución con los puntos del infinito).
2. Una terna "Pitagórica" es una terna (a, b, c) de números naturales tales que $a^2 + b^2 = c^2$. El nombre proviene de que son los triángulos rectángulos con lados de longitud natural que pueden ser construidos. Una terna Pitagórica se dice *primitiva* si $\gcd(a, b, c) = 1$. Verificar que hay una biyección natural entre ternas Pitagóricas primitivas y puntos racionales del círculo unidad.

   Un problema entre problemas geométricos y problemas diofánticos, es que el encontrar todas las soluciones racionales de una curva no siempre ayuda a resolver el problema geométrico. Por ejemplo: ¿dado un número natural n, como hallar todos los posibles triángulos rectángulos que tengan una arista de longitud n? ¿son finitos?
3. Sea $\mathcal{C} \subset \mathbb{P}^2$ la curva dad por la ecuación $x^2 + y^2 = z^2$. Probar que la función:

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

   es un morfismo definido en todos los puntos.
4. Sea $\mathcal{C}/K$ una cúbica no singular en $\mathbb{P}^2$ (i.e. esta dada por un polinomio homorégeno de grado 3 sin puntos singulares) con un punto $P \in \mathbb{P}^2(K)$. Queremos ver como llevar dicha cúbica a ecuación de Weierstrass (para simplificar la cuenta, se puede suponer que $P = [1 : 0 : 0]$, lo cual impone alguna condición en la ecuación de la cúbica). Sea L_P la recta tangente a $\mathcal{C}$ por el punto P, y tomamos el cambio de variables $Z = L_p$ (con lo cual en las nuevas coordenadas, el eje Z corresponde a la recta tangente). Ahora separamos en dos casos
   - Si P es un punto de inflexión, tomemos como eje X cualquier recta que no pase por P.
   - Si P no es un punto de inlfexión, L_P corta a $\mathcal{C}$ en un segundo punto Q (distinto de P). Tomemos como eje X la recta tangente a $\mathcal{C}$ por Q.

   Por último, tomamos como eje Y a cualquier recta que pase por P y no sea L_P. Probar que:

   a) Con este cambio de variables, la ecuación para $\mathcal{C}$ queda de la forma:

   $$XY^2 + aXYZ + bYZ^2 = cX^2Z + dXZ^2 + eZ^3.$$

   b) Multiplicando la ecuación anterior por X, y haciendo el cambio de variables $y = XY$ obtenemos la ecuación de Weierstrass.
5. 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 $n = 3$)

6. Sea $(E, \mathcal{O})$ una curva elíptica en ecuación de Weierstrass. Dado $P = (x_0, y_0)$ un punto de la curva, escribir explícitamente las coordenadas del punto $2P$.
7. Sea $\mathcal{C}/K \subset \mathbb{P}^2(K)$ una cúbica, y supongamos que la característica de K no es dos. Probar que $\mathcal{C}$ tiene a lo sumo un punto singular y de tenerlo dicho punto esta en K. ¿Que pasa si la característica de K es 2?
8. Sea E/K una curva dada por ecuación de Weierstrass, pero con un punto singular (digamos $P = (0,0)$).
   a) Supongamos que E tiene un nodo (o sea la parte de grado 2 del polinomio de Taylor de la curva en $(0,0)$ se parte como producto de dos de grado 1 distintos) y que las tangentes en el nodo son $\alpha_i x + y = 0$ 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 (o sea la parte de grado 2 del desarrollo de Taylor en el punto es de la forma $(y - \alpha x)^2$) entonces $E_{ns}(K) \cong K$ (aditivamente).
9. Sea $E : y^2 = x^3 - 27c_4 x - 54c_6$ una ecuación de Weierstrass reducida. Probar que:
   - E es singular si y sólo si $\Delta = 0$.
   - E tiene un nodo si y sólo si $\Delta = 0$ y $c_4 \neq 0$.
   - E tiene una cúspide si y sólo si $\Delta = 0$ y $c_4 = 0$.