Introducción a las Curvas Elípticas
1. Curvas Planas, curvas cúbicas, números p-ádicos

Entrega: lunes 21 de abril, 5 ejercicios a elección.

1. Sea P un punto en una curva proyectiva plana $C = C_F$. Mostrar que P es singular en la curva plana afín C_i para algún i si y sólo si
$$F(P) = 0 = \left(\frac{\partial F}{\partial X}\right)_P = \left(\frac{\partial F}{\partial Y}\right)_P = \left(\frac{\partial F}{\partial Z}\right)_P .$$
2. Sea C una curva proyectiva plana sobre un cuerpo k. Probar que $\#C(\overline{k}) = \infty$.
3. (a) Mostrar que la curva cúbica
$$Y^2 Z = X^3 + a X Z^2 + b Z^3$$
es no singular si $4a^3 + 27b^2 \neq 0$.
(b) Si $4a^3 + 27b^2 = 0$, encontrar una singularidad y decidir si es una cúspide o un nodo.
4. Dar una condición necesaria y suficiente para que la recta $L: Y = cX + d$ sea tangente con inflexión a la curva afín $C: Y^2 = X^3 + aX + b$, es decir que $I_P(L, C) = 3$. Usar esto para encontrar una fórmula general para las curvas elípticas en forma canónica con un punto racional de orden 3.
5. (a) Sea
$$F(X_1, X_2, X_3) = a_1 X_1^3 + a_2 X_2^3 + a_3 X_3^3 + d X_1 X_2 X_3 ,$$
donde $a_1 a_2 a_3 \neq 0$. Mostrar que C_F es no singular si $27 a_1 a_2 a_3 + d^3 \neq 0$.
(b) Si $a_1 = a_2 = a_3 = 1$, $d = -3$, mostrar que cualquier punto (x_1, x_2, x_3) con $x_1^3 = x_2^3 = x_3^3 = x_1 x_2 x_3 = 1$ es una singularidad.
(c) ¿Por qué no se contradice esto con el resultado visto en clase, que una curva cúbica tiene a lo sumo una singularidad?
6. Para los valores de p, m, r dados, encontrar un $x \in \mathbb{Z}$ tal que $|r - x|_p \leq p^{-m}$, o probar que no existe tal x.
(a) $p = 257$, $r = 1/2$, $m = 1$;
(b) $p = 3$, $r = 7/8$, $m = 2$;
(c) $p = 3$, $r = 7/8$, $m = 7$;
(d) $p = 3$, $r = 5/6$, $m = 9$;
(e) $p = 5$, $r = 1/4$, $m = 4$;
(f) $p = 5$, $r = 1/20$, $m = 4$.
7. Para los valores de p, m, r dados, encontrar un $x \in \mathbb{Z}$ tal que $\left|r - x^2\right|_p \leq p^{-m}$, o probar que no existe tal x.
(a) $p = 5$, $r = -1$, $m = 4$;
(b) $p = 5$, $r = 10$, $m = 3$;
(c) $p = 13$, $r = -4$, $m = 3$;
(d) $p = 2$, $r = -7$, $m = 6$;
(e) $p = 7$, $r = -14$, $m = 4$;
(f) $p = 7$, $r = 6$, $m = 3$.
8. Observar que $3^2 \equiv 2 \pmod 7$. Encontrar $x \in \mathbb{Z}_7$, con $x \equiv 3 \pmod 7$, tal que $x^2 = 2$.
9. Sea
$$F(X, Y, Z) = 5X^2 + 3Y^2 + 8Z^2 + 6(YZ + ZX + XY) .$$
Encontrar $(a, b, c) \in \mathbb{Z}^3$ no todos divisibles entre 13 tal que
$$F(a, b, c) \equiv 0 \pmod{13^2} .$$
10. Consideramos la curva afín $C: Y^2 = X^3 + p$. Probar que el punto $(0, 0)$ en la curva reducida sobre $\mathbb{F}_p$ no levanta a un punto en $\mathbb{Z}_p^2$. ¿Por qué no contradice esto el lema de Hensel?