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?

Introducción a las Curvas Elípticas
2. Funciones regulares, divisores, Riemann-Roch

Entrega: lunes 19 de mayo, 3 ejercicios a elección.

11. Sea C una curva proyectiva plana. Dado $P \in k(C)$ definimos $\nu_P : k(C) \to \mathbb{Z} \cup \infty$ (orden de cero o polo) de modo que $\nu_P(G/H) = I_P(G, C) - I_P(H, C)$. Observar que $\operatorname{div}(\phi) = \sum_P \nu_P(\phi)[P]$.
    (a) $\nu_P(\phi) = \infty$ si y sólo si $\phi = 0$.
    (b) $\nu_P(\phi\psi) = \nu_P(\phi) + \nu_P(\psi)$.
    (c) $\nu_P(\phi + \psi) \geq \min(\nu_P(\phi), \nu_P(\psi))$.
    (d) Si $\nu_P(\phi) < \nu_P(\psi)$ entonces $\nu_P(\phi + \psi) = \nu_P(\phi)$.
12. Sea C una curva proyectiva plana irreducible.
    (a) Si $a \in k$ entonces $a \in k(C)$ es regular en $C(k)$.
    (b) $\phi \neq 0$ es regular en P si y sólo si $\nu_P(\phi) \geq 0$.
    (c) $\phi \neq 0$ es regular en $C(k)$ si y sólo si $\operatorname{div}(\phi) \geq 0$.
    (d) Si ϕ es regular en P y $a \in k$ entonces $\phi - a$ es regular en P.
    (e) Si ϕ es regular en P, y $a = \phi(P)$ entonces $\nu_P(\phi - a) > 0$.
    (f) Si ϕ es regular en $C(k)$ entonces $\phi \in k$.
    (g) Si $\operatorname{div}(\phi) = \operatorname{div}(\psi)$ entonces $\phi = \lambda\psi$ con $\lambda \in k^\times$.
13. (a) $L(D)$ es un espacio vectorial.
    (b) Si $D \leq D'$ entonces $L(D) \subseteq L(D')$ y $\dim_k(L(D')/L(D)) \leq \operatorname{gr}(D' - D)$.
    (c) $L(0) = k$; $L(D) = \{0\}$ si $\operatorname{gr}(D) < 0$.
    (d) $L(D)$ tiene dimensión finita para todo D.
    (e) Si $\operatorname{gr}(D) \geq 0$ entonces $\ell(D) \leq \operatorname{gr}(D) + 1$.
    (f) Si $D \equiv D'$ entonces $\ell(D) = \ell(D')$.
14. Sea $\mathbb{P}^1 : Y = 0$, curva proyectiva en $\mathbb{P}^2$ con coordenadas $(X : Y : Z)$.
    (a) Probar que $k(\mathbb{P}^1) = k(t)$ donde $t = X/Z$.
    (b) Calcular $\operatorname{div}(t)$
    (c) Calcular $\operatorname{div}(f/g)$ donde $f, g \in k[t]$ son coprimos.
    (d) Concluir que $\operatorname{gr}(\operatorname{div}(f/g)) = 0$.
    (e) Sea $P = (0 : 0 : 1)$. Calcular $L(nP)$ y probar que $\ell(nP) = n + 1$ si $n > 0$.
    (f) ¿Qué puede decir sobre el género de $\mathbb{P}^1$?
15. Sea $C : Y^2 Z = X(X - Z)(X - \lambda Z)$ con $\lambda \neq 0, 1$. Sean $x = X/Z$, $y = Y/Z$.
    (a) Calcular $\operatorname{div}(x)$.
    (b) Calcular $\operatorname{div}(y)$.
    (c) Sea $P = (0 : 1 : 0)$. Mostrar que $L(nP) \subseteq k[x, y]$. Probar que $\ell(nP) = n$ si $n \leq 1$.
    (d) ¿Qué puede decir sobre el género de C?

Introducción a las Curvas Elípticas
3. Curvas elípticas, forma canónica, reducción

Entrega: lunes 23 de junio, 4 ejercicios a elección.

16. Sea C una curva proyectiva plana no singular cúbica definida sobre k, y sea $O \in C(k)$. suponiendo que O no sea un punto de inflexión, mostrar que es posible hacer un cambio de variables (no lineal) que transforma C en una curva de la forma $s^2 = G(t)$ con G de grado 3, y O en $(0 : 1 : 0)$. Sugerencia: ver Milne página 48, o Cassels página 34.

17. Transformar las siguientes cúbicas a la forma canónica

    (a) $X^3 + Y^3 + d\,Z^3 = 0$

    (b) $X^3 + Y^3 + Z^3 - 3m\,X\,Y\,Z = 0$

    (c) $X^2\,Y - X\,Y^2 - X\,Z^2 + Y^2\,Z = 0$

18. Sea C la curva singular de ecuación $Y^2 = X^3$. Mostrar que la función $X/Y : C^{ns} \to G_a$ es un isomorfismo de grupos.

19. Sea C la curva singular de ecuación $Y^2 = X^3 + c\,X^2$, con $c \neq 0$. Encontrar un isomorfismo de C^{ns} en $G_m[c]$. Sugerencia: Cassels página 40.

20. (a) Encontrar todos los puntos definidos sobre $\mathbb{F}_5$ en las curvas

$$Y^2 = X^3 + X$$
$$Y^2 = X^3 + 2\,X$$
$$Y^2 = X^3 + 1$$

    Verificar en todos los casos que forman un grupo, determinando su estructura.

    (b) Calcular ejemplos para otros primos. Encontrar un ejemplo donde el grupo no sea cíclico. ¿Puedes encontrar ejemplos en los que el grupo requiera más de dos generadores?

21. Mostrar que la curva elíptica

$$E : Y^2 + Y = X^3 - X^2 - 10\,X - 20$$

    tiene buena reducción en todos los primos excepto en 11.

22. Sea E una curva elíptica sobre $\mathbb{Q}_p$. Consideramos la función de reducción $E(\mathbb{Q}_p) \to E(\mathbb{F}_p)$. El lema de Hensel implica que la imágen incluye todos los puntos no singulares de $E(\mathbb{F}_p)$.

    Encontrar ejemplos de curvas elípticas $E/\mathbb{Q}$ tal que

    (a) $E(\mathbb{F}_p)$ tiene una cúspide S que levanta a un punto en $E(\mathbb{Q}_p)$.

    (b) $E(\mathbb{F}_p)$ tiene un nodo S que levanta a un punto en $E(\mathbb{Q}_p)$.

    (c) $E(\mathbb{F}_p)$ tiene un nodo S que no levanta a un punto en $E(\mathbb{Q}_p)$.

    En el primer ejemplo, decidir si E adquiere reducción buena o nodal al pasar a una extensión finita de $\mathbb{Q}$.