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 $\mathbb{Q}$.