Aritmética de Curvas Elípticas

1er. Cuatrimestre 2014

Guía 3 - Curvas elípticas sobre cuerpos finitos

1. Considerar la curva elíptica
$$y^2 = x^3 + 1$$
   a) Para los primos $5 \leq p < 20$ describir el grupo $E(\mathbb{F}_p)$ (i.e. de puntos de E sobre el cuerpo finito $\mathbb{F}_p$).
   b) Para cada p en el rango anterior, sea $M_p = \#E(\mathbb{F}_p)$. ¿Vé algún patrón para M_p en los primos $p \equiv 2 \pmod 3$?
   c) Probar la fórmula para el número de puntos M_p del item (b) para los primos $p \equiv 2 \pmod 3$.
2. Probar que si E_1 y $E_2/\mathbb{F}_q$ son dos curvas elípticas isógenas, entonces
$$\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q).$$
3. Recordar que si $E/\mathbb{F}_p$ es una curva elíptica, entonces al ser el Frobenius inseparable hace con que
$$E[p] \simeq \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{si } \widehat{\mathrm{Frob}_p} \text{ es separable,} \\ 0 & \text{si } \widehat{\mathrm{Frob}_p} \text{ es inseparable.} \end{cases}$$
   Si $E[p] = 0$, decimos que la curva E es *supersingular* (el término no tiene relación con la noción de singularidad, dado que las curvas elípticas son no-singulares por definición).
   a) Probar que $E/\mathbb{F}_p$ es supersingular si y sólo si $p \mid a_p$.
   (Sugerencia: recordar que el Frobenius como elemento del anillo de endomorfismos satisface la ecuación cuadrática $\mathrm{Frob}_p^2 - a_p \mathrm{Frob}_p + p = 0$).
   b) Probar que si $p \geq 5$ entonces $E/\mathbb{F}_p$ es supersingular si y sólo si $a_p = 0$ (o sea $\#E(\mathbb{F}_p) = p + 1$). En particular, $\widehat{\mathrm{Frob}_p} = -\mathrm{Frob}_p$.
   c) Calcular todas las posibles curvas elípticas $E/\mathbb{F}_p$ para $p = 2$ y $p = 3$ y ver que existen curvas elípticas supersingulares para las cuales $a_p \neq 0$.