Aritmética de Curvas Elípticas

2do. Cuatrimestre 2006

Guía 3 - Curvas elípticas sobre cuerpos finitos y cuerpos globales

(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) Sea $p \in \mathbb{Z}$ un primo, y miremos la curva elíptica

$$E_p : y^2 = x^3 + px$$

Hallar los puntos de torsión de E_p para cualquier valor de p.

(3) Dada la curva elíptica

$$E : y^2 = x^3 + x$$

hallar todos los puntos racionales de E (en términos de generadores).

(4) Probar que si $E/\mathbb{Q}$ es una curva elíptica y $P \in E(\mathbb{Q})$ entonces
   (a) Existe el límite $\hat{h}(P) = \lim_{n\to\infty} \frac{h_x(2^n P)}{4^n}$ (Sug. ver que es de Cauhy).
   (b) Existe una constante κ tal que para todo $P \in E(\mathbb{Q})$ vale que

$$-\kappa \leq \hat{h}(P) - h_x(P) \leq \kappa$$

   (c) $\hat{h}(mP) = m^2\hat{h}(P)$ para todo $m \in \mathbb{N}$.
   (d) $\hat{h}(P) = 0$ si y sólo si P es de torsión.

   A la altura $\hat{h}$ se la llama la altura canónica y define una forma cuadrática en los puntos racionales de E. Además se puede ver que no depende de la altura h_x elegida (i.e. dada cualquier f en el cuerpo de funciones de E, la altura canónica asociada a h_f es siempre la misma).

(5) Consideremos el producto de Euler

$$\prod_p \frac{1}{(1 - a_p p^{-s})}$$

donde el producto es sobre todos los primos y a_p son números complejos tales que $|a_p| \leq p^c$ para alguna constante $c \in \mathbb{R}$. Probar que el producto converge absolutamente para $\Re(s) > 1 + c$. Concluir que si E es una curva elíptica entonces $L(E, s)$ converge absolutamente para $\Re(s) > 3/2$.

(6) Para cada una de las siguientes curvas elípticas calcular el grupo de puntos de torsión:
   (a) $y^2 = x^3 - 2$.
   (b) $y^2 = x^3 + 8$.
   (c) $y^2 = x^3 + 4$.
   (d) $y^2 = x^3 + 4x$.
   (e) $y^2 - y = x^3 - x^2$.
   (f) $y^2 = x^3 + 1$.
   (g) $y^2 = x^3 - 43x + 166$.

(h) $y^2 + 7xy = x^3 + 16x$.
(i) $y^2 + xy + y = x^3 - x^2 - 14x + 29$.
(j) $y^2 + xy = x^3 - 45x + 81$.
(k) $y^2 + 43xy - 210y = x^3 - 210x^2$.
(l) $y^2 = x^3 - 4x$.
(m) $y^2 + xy - 5y = x^3 - 5x^2$.
(n) $y^2 + 5xy - 6y = x^3 - 3x^2$.
(o) $y^2 + 17xy - 120y = x^3 - 60x^2$.