Aritmética de Curvas Elípticas
2do. Cuatrimestre 2006
Guía 2 - Curvas elípticas sobre $\mathbb{C}$

(1) (a) Sea $L = \mathbb{Z} + \mathbb{Z}i$ (los enteros de Gauss). Probar que $g_3(L) = 0$ pero $g_2(L)$ es un número real no nulo.
(b) Sea $L = \mathbb{Z} + \mathbb{Z}w$ donde w es una raíz cúbica primitiva de la unidad (en particular $L \subset \mathbb{Q}[\sqrt{-3}]$). Probar que $g_2(L) = 0$ pero $g_3(L)$ es un número real no nulo.
(c) Probar que si $c \in \mathbb{R}^\times$ (i.e. es no nulo) entonces $G_k(cL) = c^{-k}G_k(L)$ (esto explica la indexación de las funciones G_k).
(d) De los puntos anteriores probar que las curvas elípticas $y^2 = 4x^3 - g_2x - g_3$ con $g_2 = 0$ ó $g_3 = 0$ tienen un retículo L asociado tales que $g_i(L) = g_i$.

(2) Dado $L \subset \mathbb{C}$ un retículo definimos

$$\Delta(L) = g_2(L)^3 - 27g_3(L)^2 \qquad j(L) = 1728g_2(L)^3/\Delta(L)$$

(a) Probar que si $\alpha \in \mathbb{C}^\times$ entonces $\Delta(\alpha L) = \alpha^{-12}\Delta(L)$ y que $j(\alpha L) = j(L)$.
(b) Probar que $j(L_1) = j(L_2)$ si y sólo si existe $\alpha \in \mathbb{C}^\times$ tal que $\alpha L_1 = L_2$.
(c) Probar que $j(\mathbb{Z} + \mathbb{Z}i) = 1728$ y $j(\mathbb{Z} + \mathbb{Z}e^{2\pi i/3}) = 0$.

(3) Sea $E/\mathbb{C}$ una curva elíptica que corresponde con un retículo $L \subset \mathbb{C}$.
(a) Probar que E se puede definir sobre $\mathbb{R}$ (i.e. existe un cambio de variables tal que la ecuación de E queda con coeficientes reales o equivalentemente $j(E) \in \mathbb{R}$) si y sólo si existe $\alpha \in \mathbb{C}^\times$ tal que αL queda estable por conjugación (i.e. $\overline{\alpha L} = \alpha L$). (Hint: probar que $\overline{j(L)} = j(\bar{L})$ y utilizar el ejercicio anterior).
(b) Supongamos que E se puede definir sobre $\mathbb{R}$ y elegimos L tal que $\bar{L} = L$. Probar que se puede elegir una base de L tal que $L = \mathbb{Z}\omega + \mathbb{Z}\tau$ donde $\omega \in \mathbb{R}$ y $\Re(\tau) = 0$ ó $\Re(\tau) = \frac{\omega}{2}$. Además probar que $\Re(\tau) = 0$ si y sólo si $E[2] \subset \mathbb{R}$ (i.e. el polinomio cúbico tiene tres raíces reales). Hint: para la segunda parte considerar el desarrollo de Laurent de $\mathcal{P}_L$.
(c) Probar que los puntos reales de una curva elíptica definida sobre $\mathbb{R}$ son isomorfos a $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ó $\mathbb{R}/\mathbb{Z}$ dependiendo si $E[2] \subset \mathbb{R}$ o no (respectivamente).

(4) Dado un retículo L, considerar la función elíptica par $\mathcal{P}''_L(z)$ y escribirla como un polinomio en $\mathcal{P}_L(z)$ de dos maneras:
- Comparando los desarrollos de Laurent.
- Derivando la igualdad $\mathcal{P}'_L(z)^2 = 4\mathcal{P}_L(z)^3 - g_2\mathcal{P}_L(z) - g_3$.

(5) (a) Probar que $G_8 = \frac{3}{7}G_4^2$.
(b) Demostrar por inducción que todos los G_k se pueden escribir como polinomios en G_4 y G_6 con coeficientes racionales, i.e. $G_k \in \mathbb{Q}[G_4, G_6]$.

(6) Sea $\omega_1 = it$ con $t \in \mathbb{R}_{\geq 0}$ y $\omega_2 = \pi$. Si definimos la función zeta de Riemann para $s \in \mathbb{C}$ con $\Re(s) > 1$ como

$$\zeta(s) = \sum_{n \in \mathbb{N}} \frac{1}{n^s}$$

probar que cuando t tiende a infinito $G_k(it, \pi)$ (i.e. G_k evaluado en el retículo $\mathbb{Z}it + \mathbb{Z}\pi$) tiende a $2\pi^{-k}\zeta(k)$. Asumiendo que $\zeta(2) = \frac{\pi^2}{6}$, $\zeta 4 = \frac{\pi^4}{90}$ y $\zeta(6) = \frac{\pi^6}{945}$ calcular $\zeta(8)$. Deducir que $\pi^{-k}\zeta(k) \in \mathbb{Q}$ para todo k positivo y par.