Aritmética de Curvas Elípticas

1er. Cuatrimestre 2014

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 elijamos L tal que $\overline{L} = L$. 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 $E[2] \subset \mathbb{R}$ (o sea los puntos de orden 2 tienen coordenadas enteras, que es lo mismo que decir que el polinomio cúbico que da la ecuación tiene tres raíces reales). Hint: para la segunda parte considerar el desarrollo de Laurent de $\mathcal{P}_L$.
   c) Probar que los puntos relaes de ua 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. Sean E_1 y E_2 dos curvas elípticas sobre $\mathbb{C}$. Supongamos que E_1 tiene multiplicación compleja. Probar que:

$$E_1 \text{ es isógena con } E_2 \text{ si y sólo si } \operatorname{End}(E_1) \otimes \mathbb{Q} \simeq \operatorname{End}(E_2) \otimes \mathbb{Q}.$$

   Equivalentemente, si suponemos que el retículo de E_i es de la forma $\langle 1, \alpha_i \rangle$, entonces el cuerpo $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$.
5. 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 $\mathcal{P}'_L(z)^2 = 4\mathcal{P}_L(z)^3 - g_2\mathcal{P}_L(z) - g_3$.
6. *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. $G_k \in \mathbb{Q}[G_4, G_6]$.

7. 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.
8. Para $k \in \mathbb{N}$ y $q \in$ con $|q| < 1$, definimos
$$s_k(q) = \sum_{n \geq 1} \sigma_k(n) q^n,$$
donde
$$\sigma_k(n) = \sum_{\substack{d|n \\ d>0}} d^k.$$
Probar que $s_k(q) = \sum_{n \geq 1} \left(\frac{n^k q^n}{1-q^n} \right)$.
9. Sea $\Lambda_\tau = \langle 1, \tau \rangle_{\mathbb{Z}}$ el retículo generado por 1 y por τ, donde τ es un número complejo con $\Im(\tau) > 0$ y $\mathcal{P}(z, \tau) := \mathcal{P}_{\Lambda_\tau}(z)$. Dicha función es holomorfa tanto en la variable z como en la variable τ.
   - Verificar que $\mathcal{P}(z+1, \tau) = \mathcal{P}(z, \tau)$, con lo cual $\mathcal{P}(z, \tau)$ admite desarrollo de Fourier en términos de $u = e^{2\pi i z}$.
   - Verificar que $\mathcal{P}(z, \tau+1) = \mathcal{P}(z, \tau)$, con lo cual $\mathcal{P}(z, \tau)$ admite desarrollo de Fourier en términos de $q = e^{2\pi i \tau}$.
   - Probar que vale:
   $$\frac{1}{(2\pi i)^2} \mathcal{P}(z, \tau) = \sum_{n \in \mathbb{Z}} \frac{q^n u}{(1 - q^n u)^2} + \frac{1}{12} - 2 \sum_{n \geq 1} \frac{q^n}{(1-q^n)^2}.$$
   Para esto verificar:
   a) Que la función del lado derecho converge absoluta y uniformemente en compactos (convencerse).
   b) Que la función de la derecha tiene polos dobles en los puntos de Λ_τ y ningún otro polo.
   c) La expansión de Laurent en $z = 0$ de la función $\sum_{n \in \mathbb{Z}} \frac{q^n u}{(1-q^n u)^2}$ comienza con $\frac{1}{(2\pi i)^2 z^2} - \frac{1}{12} + 2 \sum_{n \geq 1} \frac{q^n}{(1-q^n)^2} +$ potencias de z.