Complex multiplication of elliptic curves

Exercises

Andreas Enge

Warwick, 24 to 28 June 2013

1. Let $\wp$ be the Weierstraß function associated to a lattice L. Show that the function $z \mapsto e^{\wp(z)}$ is holomorphic on $\mathbb{C}\backslash L$ and periodic modulo L, but not elliptic.

2. (a) Show that an elliptic function without poles, or an elliptic function without zeroes, is necessarily constant.

   (b) If f is an even elliptic function and $2a \in L$, then f has even order in a. Hint: Use the Taylor expansion of f at a, and look at $f(-z + 2a)$.

   (c) The function $\wp(z) - \wp(a)$ has a simple zero in $\pm a$ if $2a \notin L$ and a double zero otherwise.

   (d) Show that the even elliptic functions are exactly the rational functions in $\wp$, that is, $\mathbb{C}(\wp)$, and that the field of elliptic functions is $\mathbb{C}(\wp.\wp')$.

3. Use the Laurent series of $\wp$ and $\wp'$ to prove the differential equation

$$(\wp')^2 = 4\wp^3 - 60G_2\wp - 140G_3.$$

   A computer algebra system comes in handy for the computations.

4. Let $G_k(L) = \sum'_{\omega \in L} \frac{1}{\omega^{2k}}$ be the Eisenstein series of weight $2k$, with the convention $G_1 = 0$ and $G_0 = -1$.

   (a) Show that for $k \geq 3$,

$$(2k-1)(2k-2)(2k-3)G_k = 6\sum_{j=0}^{k}(2j-1)(2k-2j-1)G_jG_{k-j};$$

   you may use $\wp'' = 6\wp^2 - 30G_2$.

   (b) Show that

$$G_4 = \frac{3}{7}G_2^2, \quad G_5 = \frac{5}{11}G_2G_3, \quad G_6 = \frac{25}{143}G_3^2 + \frac{18}{143}G_2^3,$$

and, more generally, that every Eisenstein series can be computed recursively as a polynomial in G_2 and G_3 via

$$(4k^2-1)(2k-6)G_k = 6\sum_{j=2}^{k-2}(2j-1)(2k-2j-1)G_jG_{k-j}.$$

(Beware of potential subtle errors in the formulæ above.)

5. Show that the following two assertions are equivalent for a lattice $L = \mathbb{Z} + \tau\mathbb{Z}$ and $\alpha \in \mathbb{C}\backslash\mathbb{Z}$:

   (a) $\alpha L \subseteq L$

   (b) $L = \frac{1}{A}\left(A, \frac{-B+\sqrt{D}}{2}\right)_{\mathbb{Z}}$ is a proper fractional ideal of an imaginary quadratic order $\mathcal{O} = \left(1, \frac{D+\sqrt{D}}{2}\right)_{\mathbb{Z}}$ and $\alpha \in \mathcal{O}$.

6. Let $r \in \mathbb{N}$, and consider a primitive matrix R of determinant r.

   (a) Show that

   $$\Gamma_R = R^{-1}\Gamma R \cap \Gamma \supseteq \Gamma(r) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : a \equiv d \equiv 1, b \equiv c \equiv 0 \pmod{r}\right\}.$$

   (b) Show that

   $$\begin{aligned} \Gamma_{\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}} &= \Gamma^0(r) = \{\ldots : b \equiv 0 \pmod{r}\} \text{ or} \\ \Gamma_{\begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix}} &= \Gamma_0(r) = \{\ldots : c \equiv 0 \pmod{r}\} \end{aligned}$$

7. In your favourite language or computer algebra system, write a programme that takes as input an element $\tau \in \mathbb{H}$ and outputs its representative under $\Gamma = \mathrm{Sl}_2(\mathbb{Z})$ in the standard fundamental domain. What is the representative of $\frac{1+2i}{100}$? Of $\frac{1+2i}{1000}$? How many reduction steps does it take to bring them into the fundamental domain?

8. For a primitive matrix R show that $j_R \in \mathbb{C}_{\Gamma_R}$.

9. Once a class polynomial is computed using the floating point approach, how do you check (probabilistically) that it is correct?

10. Devise an algorithm to compute the class group of an imaginary-quadratic order with as a low a complexity as possible, and prove this complexity.

11. (a) Write a program in your favourite computer algebra system that upon input of a negative discriminant D outputs a list of the reduced binary quadratic forms $[A, B.C]$ of discriminant D.

    What are the class numbers h_D of $D = -(10^n + 8)$ for $n = 2, 3, 4, \ldots$? Does the growth of the class numbers correspond to the theoretical predictions?

    (b) For each of the discriminants D of (a), determine the corresponding fundamental discriminant Δ and its class number. Verify that the result is consistent with Kronecker's class number formula.

    (c) For the same discriminants, compute the required (logarithmic) precisions as $p_D = \pi\sqrt{|D|}\sum \frac{1}{A}$. How does $\frac{p_D}{h_D}$ grow?

12. Programme the floating point algorithm for class polynomials. What is the class polynomial H_{-71} for $D = -71$?

13. Class invariants

    (a) Factor $H_{-71}(Y^3)$, and let g be the factor of lowest degree. What do you deduce from the result? How large is the largest coefficient of g compared to that of H_{-71}?

    (b) Now factor $g\left(\frac{Z^{24}-16}{Z^8}\right)$. What do you observe?

14. Isogenies and non-maximal orders. Let D be an imaginary-quadratic discriminant and ℓ a prime such that the Legendre symbol satisfies $\left(\frac{\ell}{D}\right) = -1$. Let $R_D = \mathbb{Q}[X]/(H_D(X))$ and $R_{\ell^2 D} = \mathbb{Q}[X]/(H_{\ell^2 D}(X))$ be the ring class fields attached to D and $\ell^2 D$, respectively (or, to be precise, their real subfields).

    (a) What is the degree of $R_{\ell^2 D}/R_D$?

    (b) Can you realise $R_{\ell^2 D}/\mathbb{Q}$ as a tower of field extensions without computing $H_{\ell^2 D}$?

    (c) What can you do if $\left(\frac{\ell}{D}\right) \in \{0, -1\}$?

    (d) Give equations for R_{-3479} and R_{-639} as field towers. Derive from these the class polynomials H_{-3479} and H_{-639} (hint: resultants).