18.783 Elliptic Curves **Spring 2013**
Problem Set #8 **Due: 04/18/2013**

Description

These problems are related to the material covered in Lectures 16-17. As usual, the first person to spot each non-trivial typo/error will receive one point of extra credit.

Instructions: Solve 3 of the first 4 problems and then complete Problem 5, which is a survey. If you choose to do problem 2, you will also want to do problem 1. **Late problem sets will lose half a point for each hour they are late**.

Problem 1. From lattices to elliptic curves

In this problem you will explicitly construct an elliptic curve corresponding to a given lattice $L = [1, \tau]$ by computing the j-invariant

$$j(L) = 1728\frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2},$$

where

$$g_2(L) = 60\sum_{m,n\in\mathbb{Z}}{}' \frac{1}{(m+n\tau)^4}, \qquad \text{and} \qquad g_3(L) = 140\sum_{m,n\in\mathbb{Z}}{}' \frac{1}{(m+n\tau)^6}. \tag{1}$$

As usual, the prime on the sums indicates that the term with $m = n = 0$ is excluded.

1. Let $L = [1, (1+\sqrt{-7})/2]$ be the ring of integers of $\mathbb{Q}(\sqrt{-7})$. Use Sage to approximate $j(L)$ by computing the sums for $g_2(L)$ and $g_2(L)$ over lattice points with $|m|, |n| < r$ for increasing values of $r = 10, 20, 30, \ldots$, until you are convinced you can correctly approximate $j(L)$ one decimal place (be sure to do this computation over the complex numbers; use `tau=CC((1+sqrt(-7))/2))`. Assuming that $j(L)$ is a rational integer, round the real part of your approximation to the nearest integer.

2. Use the j-invariant $j = j(L)$ you computed in part 1 to construct an elliptic curve $E\colon y^2 = x^3 + Ax + B$ over $\mathbb{Q}$ using $A = 3j(1728 - j)$ and $B = 2j(1728 - j)^2$. Heuristically verify that E has CM[1] by $\mathbb{Q}(\sqrt{-7})$ by checking that E has supersingular reduction modulo all good primes $p < 1000$ for which $\left(\frac{-7}{p}\right) = -1$.

Using (1) to approximate $g_2(L)$ and $g_3(L)$ does not work very well because these sums converge very slowly. A much better approach is to instead use their q-series expansions. Let $q = \exp(2\pi i\tau)$. Then

$$g_2([1,\tau]) = \frac{4\pi^4}{3}\left(1 + 240\sum_{k=1}^{\infty}\frac{k^3q^k}{1-q^k}\right) \quad \text{and} \quad g_3([1,\tau]) \;=\; \frac{8\pi^6}{27}\left(1 - 504\sum_{k=1}^{\infty}\frac{k^5q^k}{1-q^k}\right).$$

[1] When we say that an elliptic curve E "has CM by F" where F is an imaginary quadratic field, we mean that $\mathrm{End}^0(E) = F$. If $\mathcal{O}$ is an order in F we may also say that E "has CM $\mathcal{O}$" if $\mathrm{End}(E) = \mathcal{O}$.

3. Repeat part 1 using the q-expansion formulas for $g_2(L)$ and $g_3(L)$, truncating the sums after 10,000 terms. Extend the precision of your computations be defining `CC=ComplexField(1000)`, and use `q=CC(exp(2*pi*sqrt(-1)*tau))` to compute q. **Important**: compute τ symbolically using `tau=(1+sqrt(-7))/2` (coercing it to $\mathbb{C}$ result in a loss of precision). Compare the resulting approximation to $j(L)$ to the one you computed in part 1 by listing the first 8 decimal places of the real and imaginary parts of both approximations.

4. Use your improved algorithm to compute the j-invariant of the lattice $L = [1, \sqrt{-7}]$. Assuming it is a rational integer, construct the corresponding elliptic curve and heuristically verify that it also has CM by $\mathbb{Q}(\sqrt{-7})$ (but note that in this case L is not the full ring of integers).

5. Now let $L = [1, (1+\sqrt{-23})/2]$ be the ring of integers of $\mathbb{Q}(\sqrt{-23})$. After approximating $j(L)$ you will find that it does not appear to be a rational integer. But it is an algebraic integer. Use Sage to find its minimal polynomial using the `algdep` method with a degree bound of 4 (you should get a monic polynomial of degree 3; if not, you have made a mistake or are not using enough precision).

6. Let $H(x)$ be the minimal polynomial you computed in part 5 and let $D = -23$. Find a prime p for which $\left(\frac{D}{p}\right) = 1$ and $H(x)$ splits completely into linear factors in $\mathbb{F}_p[x]$, and let r be one of its roots. Construct an elliptic curve $E/\mathbb{F}_p$ with j-invariant r and compute its trace of Frobenius t. Verify that $4p = t^2 - v^2 D$ for some integer v. Repeat this for every prime $p < 1000$ for which $\left(\frac{D}{p}\right) = 1$ and $H(x)$ splits completely in $\mathbb{F}_p[x]$. Now use this method to construct an elliptic curve with CM by $\mathbb{Q}(\sqrt{D})$ over a 256-bit finite field.

Problem 2. From elliptic curves to lattices

We now consider the problem of determining the lattice L corresponding to an elliptic curve $E\colon y^2 = x^3 + Ax + B$. This is known as "computing the periods" of E, and involves computing approximate solutions to certain elliptic integrals associated to E, as explained in [2, §9.4]. To simplify matters, we will focus on the case where A and B lie in $\mathbb{R}$.

Given two positive real numbers a and b, we define sequences $\{a_n\}$ and $\{b_n\}$ as follows:

$$a_0 = a, \qquad b_0 = b, \qquad a_n = \frac{a_{n-1} + b_{n-1}}{2}, \qquad b_n = \sqrt{a_{n-1}b_{n-1}}. \tag{2}$$

As proven in [2, Prop. 9.23], these sequences both converge to a common limit $M(a,b)$, which is defined as the *arithmetic-geometric mean* of a and b. As with Newton iteration, the rate of convergence is doubly exponential, which makes the arithmetic-geometric mean a powerful tool for numerical algorithms.

When the cubic $f(x) = x^3 + Ax + B$ has three real roots $e_1 < e_2 < e_3$, we can compute a lattice $L = [\omega_1, \omega_2]$ for E via the formulas

$$\omega_1 = \frac{\pi}{M(\sqrt{e_3 - e_1}, \sqrt{e_3 - e_2})},$$
$$\omega_2 = \frac{\pi i}{M(\sqrt{e_3 - e_1}, \sqrt{e_2 - e_1})},$$

as proven in [2, Thm. 9.26]. When $f(x) = x^3 + Ax + B$ has just one real root e_1, we let $e_2 = \sqrt{3e_1^2 + A}$ and use the formulas

$$\omega_1 = \frac{2\pi}{M(2\sqrt{e_2}, \sqrt{2e_2 + 3e_1})},$$
$$\omega_2 = -\frac{\omega_1}{2} + \frac{\pi i}{M(2\sqrt{e_2}, \sqrt{2e_2 - 3e_1})}.$$

The resulting lattice $L = [\omega_1, \omega_2]$ then satisfies $g_2(L) = -4A$ and $g_3(L) = -4B$, so that the elliptic curve $y^2 = 4x^3 - g_2(L)x - g_3(L)$ corresponding to the torus $\mathbb{C}/L$ is isomorphic to our original curve E.

1. Implement an algorithm in Sage to approximate $M(a, b)$ using (2). Using your algorithm, compute the RHS of the identity[2]

$$\int_0^1 \frac{dz}{\sqrt{1 - z^4}} = \frac{\pi}{2M(1, \sqrt{2})},$$

and then use Sage to compute the LHS. Verify that these values agree to, say, 100 decimal places. You will need to extend the precision of the real field to do this: use `RR=RealField(1000)` to get 1000 bits of precision, and then be sure to coerce the arguments to $M(a, b)$ into `RR` using `M(RR(a),RR(b))`.

2. Using the formulas above, approximate the periods ω_1 and ω_2 associated to the elliptic curve $E\colon y^2 = x^3 - 35x - 98$. Compute the ratio $\tau = \omega_2/\omega_1$, so that L is homothetic to $[1, \tau]$, and then compute the j-invariant $j(L)$ and compare it to $j(E)$. Attempt to identify τ as an algebraic number in a quadratic field using the `algdep` method in Sage, with the degree bound set to 2. In your answers, just list your values for ω_1, ω_2, τ, and $j(L)$ out to 16 decimal places, even though you may need to use higher precision in your computations, and list the polynomial computed by `algdep`.

3. Do the same thing for the elliptic curves

$$E_1\colon y^2 = x^3 - 7x + 6,$$
$$E_2\colon y^2 = x^3 - 608x + 5776,$$
$$E_3\colon y^2 = x^3 - 34790720x + 78984748304.$$

In cases where you are able to provisionally identify τ as an algebraic number in a quadratic field $K = \mathbb{Q}(\sqrt{D})$, heuristically test whether E_i has CM by K by checking if it has supersingular reduction modulo good primes $p < 1000$ for which $\left(\frac{D}{p}\right) = -1$. For the E_i where this test is successful, it may be that τ is an algebraic number but not an algebraic integer. Show that in each such case τ is equivalent under the action of $\mathrm{SL}_2(\mathbb{Z})$ to an algebraic integer with real part 0 or $-1/2$.

4. Lastly, compute the periods for an elliptic curve that is defined over $\mathbb{R}$ but not over $\mathbb{Q}$ (or any number field). Let N be the last 4 digits of your student ID, and compute the periods for $E\colon y^2 = x^3 + \pi x + N$, where $\pi = 3.1415\ldots$ is transcendental.

[2]This identity was of great interest to Gauss; the quantity $1/M(1, \sqrt{2}) = 0.8346268\ldots$ is known as Gauss's constant. A proof can be found in [1, Ex. VI.6.12-14] (NB: there is a typo in part (f) of Exercise VI.6.14 in [1]: the quantity $M(1, \sqrt{2})$ should appear in the denominator, as above).

Problem 3. Elliptic curves over $\mathbb{R}$

Let $L = [1, \tau]$ be a lattice with $0 \le \operatorname{re}\tau < 1$, let $E/\mathbb{C}$ be the corresponding elliptic curve

$$y^2 = 4x^3 - g_2(L)x - g_3(L),$$

and let $\Phi(z) = (\wp(z), \wp'(z))$ be the isomorphism from $\mathbb{C}/L$ to $E(\mathbb{C})$.

1. Prove that E is defined over $\mathbb{R}$ (meaning $g_2(L), g_3(L) \in \mathbb{R}$) if and only if L is stable under complex conjugation.

2. Characterize the lattices $L[1, \tau]$ that are stable under complex conjugation by giving necessary and sufficient conditions on τ.

We now assume that E is defined over $\mathbb{R}$ (so $g_2(L), g_3(L) \in \mathbb{R}$), but still view E as an elliptic curve over $\mathbb{C}$, using $E(\mathbb{R})$ to denote the subgroup of real points in $E(\mathbb{C})$.

3. Prove that if $z \in \mathbb{R}$ then $\Phi(z) \in E(\mathbb{R})$.

4. Prove that if $z = \frac{1}{2} + it$ with $t \in \mathbb{R}$ then $\wp(z) \in \mathbb{R}$ but $\wp'(z) \notin \mathbb{R}$, unless $\wp'(z) = 0$. Conclude that there is at most one $z_0 \notin \mathbb{R}$ in the fundamental region $\mathcal{F}_0$ with real part 1/2 for which $\Phi(z_0) \in E(\mathbb{R})$. Show that such a z_0 exists if and only if the cubic $f(x) = 4x^3 - g_2(L)x - g_3(L)$ has three real roots.

5. Prove that the pre-image $\Phi^{-1}(E(\mathbb{R}))$ is given by

$$\mathcal{R}_0 = \begin{cases} \{z \in \mathcal{F}_0 : \operatorname{im} z = 0\} & \text{if } f(x) \text{ has one real root,} \\ \{z \in \mathcal{F}_0 : \operatorname{im} z = 0 \text{ or } \operatorname{im} z = \frac{1}{2}\operatorname{im}\tau\} & \text{if } f(x) \text{ has three real roots.} \end{cases}$$

Prove that L is rectangular ($\operatorname{re}\tau = 0$) if and only if we are in the latter case.

6. Conclude that $E(\mathbb{R})$ has either one or two components, depending on whether its 2-torsion subgroup is trivial or not. Show that $E(\mathbb{R}) \simeq \mathbb{R}/\mathbb{Z}$ in the first case and $E(\mathbb{R}) \simeq \mathbb{R}/\mathbb{Z} \oplus \mathbb{Z}/2$ in the second.

Problem 4. The modular group $\mathbf{SL_2}(\mathbb{Z})$

Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and let $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{im} z > 0\}$ be the upper half plane. For each $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $\tau \in \mathbb{H}$, define

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}.$$

Let $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and let $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

1. Prove that Γ is generated by S and T.

2. Prove that $\gamma\tau \in \mathbb{H}$ for all $\gamma \in \Gamma$ and $\tau \in \mathbb{H}$.

3. Prove that the map from $\Gamma \times \mathbb{H}$ to $\mathbb{H}$ that sends (γ, τ) to $\gamma\tau$ is a group action.

4. Compute the stabilizers of i and $\rho = e^{2\pi i/3}$ under the action of Γ. Express the elements of each stabilizer in terms of S and T.

5. Prove that the stabilizer of every element of $\mathbb{H}$ that is not Γ-equivalent to i or ρ is the subgroup of order 2 consisting of $\pm I$, where I is the 2×2 identity matrix.

The *extended upper half plane* $\mathbb{H}^*$ is defined as $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, where $\mathbb{P}^1(\mathbb{Q})$ is the projective line over $\mathbb{Q}$, consisting of all projective points $(x : y)$ with rational coordinates. One can view $\mathbb{P}^1(\mathbb{Q})$ as $\mathbb{Q} \cup \{\infty\}$, where $\mathbb{Q}$ consists of the points $(x : 1)$ and ∞ is the point $(1 : 0)$. We extend the action of Γ to $\mathbb{H}^*$ by defining

$$\gamma(x : y) = (ax + by : cx + dy)$$

for each $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $(x : y) \in \mathbb{P}^1(\mathbb{Q})$.

6. Prove that the elements of $\mathbb{P}^1(\mathbb{Q})$ are all Γ-equivalent.

7. Compute the stabilizers of $0 = (0 : 1)$ and $\infty = (1 : 0)$.

8. Compute the stabilizer of $(x : y)$ when $xy \neq 0$.

Problem 5. Survey

Complete the following survey by rating each of the problems you attempted on a scale of 1 to 10 according to how interesting you found the problem (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found the problem (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			
Problem 3			
Problem 4			

Also, please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast", 5="just right") and the novelty of the material (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
4/9	Elliptic functions				
4/11	Complex tori, elliptic curves over C				

Please feel free to record any additional comments you have on the problem sets or lectures, in particular, ways in which they might be improved.

References

[1] Joseph H. Silverman, *The arithmetic of elliptic curves*, second edition, Springer, 2009;.

[2] Lawrence. C. Washington, *Elliptic curves: Number theory and cryptography*, second edition, Chapman and Hall/CRC, 2008.