PAWS 2023 – Elliptic Curves with Complex Multiplication. Instructor: Wanlin Li. Problem session leaders: Tejasi Bhatnagar, Fangu Chen, Robin Huang, Ruofan Jiang

Problem set 2

Below you will find problems for problem set one. We divide the problem sets into three parts - beginner, intermediate and advanced.

Feel free to go back and forth between the theory and the problems you like. There is absolutely no pressure to learn all this material at one go. Take your time and keep coming back to it as you move forward in your learning. Please be kind to yourself and your peers while learning and discussing the material. Most importantly, have fun :)

Beginner

Problem 1. Recall an Eisenstein series of weight k is given by:

$$G_{2k}(\Lambda) := G_{2k}(\tau) = \sum_{0\neq\omega\in\Lambda} \frac{1}{\omega^{2k}} = \sum_{(0,0)\neq(m,n)\in\mathbb{Z}} \frac{1}{(m\tau+n)^{2k}}$$

1. Show that $G_{2k}(\alpha\Lambda) = \alpha^{-2k}G_{2k}(\Lambda)$ for all $\alpha \in \mathbb{C}^*$.
2. Consider the lattice $\Lambda = \mathbb{Z}[i]$. Show that $i\Lambda = \Lambda$. Moreover, using (a) convince yourself (and your peers) that $G_6(\Lambda) = 0$.
3. Similarly let $\rho = e^{2\pi i/3}$ be a primitive cube root of unity and let $\Lambda = \mathbb{Z}[\rho]$. Show that $G_4(\Lambda) = 0$.
4. (j-invariant) The j invariant of an elliptic curve $\mathbb{C}/\Lambda$ associated to the lattice Λ is defined by

   $$1728\frac{G_4(\Lambda)^3}{G_4(\Lambda)^3 - G_6(\Lambda)^2}$$

   Write down the Weierstrass equations of the elliptic curves given by the lattices in 2. and 3. and compute their j-invariant.
5. The proposition in [AEC, III 1.4] shows that the field of definition of an elliptic curve over $\mathbb{C}$ (or an algebraically closed field) is $\mathbb{Q}(j)$ where j is as above. As we computed in 4. the j-invariants of these CM elliptic curves are in $\mathbb{Q}$. (In fact note that they lie in $\mathbb{Z}$). Can you find a model for them over $\mathbb{Q}$?

Remark 1. You can use Sage to figure out whether an elliptic curve has CM and find its j-invariant. Here is a link with some functions you can implement. Here is a link: CM for elliptic curves: SAGE. For example here is list of all the j-invariants of CM elliptic curves over $\mathbb{Q}$.

[-262537412640768000, -147197952000, -884736000, -12288000, -884736, -32768, -3375, 0, 1728, 8000, 54000, 287496, 16581375]

In particular, note that all of them lie in $\mathbb{Z}$. This is true in generality. That is if $E/\mathbb{C}$ is an elliptic curve with CM then its j-invariant lies in $\mathbb{Z}$. "Advanced topics in the arithmetic of elliptic curves" gives three proof of this result. Refer to Chapter 2, section 6 (or wait for lecture 3!)

Problem 2. Let $D \in \mathbb{Z}_{>0}$ and $E/\mathbb{C}$ be an elliptic curve associated to the lattice $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ in $\mathbb{C}$. Show that E admits an action of the order $\mathbb{Z}[\sqrt{-D}]$ in the quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$ if and only if τ is a fixed point of a 2×2 matrix $\gamma \in M_2(\mathbb{Z})$ with $\mathrm{Tr}(\gamma) = 0$ and $\det(\gamma) = D$.

Problem 3. Let E_1, E_2 be elliptic curves over $\mathbb{C}$ and assume E_1 has CM by an imaginary quadratic field K. Prove that E_1 and E_2 are isogenous if and only if $\mathrm{End}(E_1) \otimes \mathbb{Q} \simeq \mathrm{End}(E_2) \otimes \mathbb{Q}$, equals K.

Problem 4. For the following problem we recall the definition of a class group: The class group of a number field K, denoted as $\mathrm{Cl}(K)$ is the group of fractional ideals of K, modulo its principle ideals.

1. Suppose Λ_1 and Λ_2 are two lattices. Show that $j(\Lambda_1) = j(\Lambda_2)$ if and only if $\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbb{C}^*$.

2. Let $\mathfrak{a}$ be a fractional ideal of a quadratic number field K. Consider the the elliptic curve $E = \mathbb{C}/\mathfrak{a}$. Show that $j(E) \in \mathbb{R}$ if and only if the the class of $\mathfrak{a}$ lies in $\mathrm{Cl}(K)[2]$, the two torsion of the ideal class group of K.

Problem 5 (Orders in imaginary quadratic fields)**.** Let K be an imaginary quadratic field of discriminant $d_K < 0$ with ring of integers $\mathcal{O}_K$, and let $\mathcal{O}$ be an order of discriminant D in K. Write

$$\alpha = \frac{d_K + \sqrt{d_K}}{2}.$$

1. The index $f = [\mathcal{O}_K : \mathcal{O}]$ is called the conductor of the order. Show that

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = \mathbb{Z}[f\alpha].$$

In particular, the order $\mathcal{O}$ has discriminant

$$D = f^2 d_K.$$

2. Suppose $\tau = \frac{-b+\sqrt{D}}{2a}$ is a root of a quadratic polynomial $ax^2 + bx + c$, $a, b, c \in \mathbb{Z}$ with discriminant $b^2 - 4ac = D$. Show that

$$\mathcal{O} = \mathbb{Z}[a\tau].$$

Moreover, if a, b, c are relatively prime, show that $\mathbb{Z} + \mathbb{Z}\tau$ is a proper fractional ideal for the order $\mathbb{Z}[a\tau]$.

3. We say two integral quadratic polynomials $g(x)$ and $h(x)$ are equivalent if

$$g(x) = (rx + s)^2 h\left(\frac{px + q}{rx + s}\right)$$

for some $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$. Show that the map sending $g(x) = ax^2 + bx + c$ to $\mathbb{Z} + \mathbb{Z}\frac{-b+\sqrt{D}}{2a}$ induces a bijection between the equivalence classes of primitive (i.e., a, b, c are relatively prime) positive definite quadratic polynomials of discriminant D (i.e., $b^2 - 4ac = D < 0$ and $a > 0$) and the ideal class group $C(\mathcal{O})$.

Intermediate

Problem 6. Let $N \geq 1$. An elliptic curve over $\mathbb{C}$ with a **level-N structure** is a pair (E, α) where $\alpha : \frac{\mathbb{Z}}{N} \oplus \frac{\mathbb{Z}}{N} \to E[N]$ is an isomorphism. An automorphism of (E, α) is an automorphism $f : E \to E$ such that $\alpha = f \circ \alpha$. Show that, when $N \geq 3$, an elliptic curve with a level-N structure doesn't admit nontrivial automorphisms. What happens when $N = 1$ or 2?

Problem 7. Let $E = \mathbb{C}/\Lambda$ be an elliptic curve. Suppose that $\overline{\Lambda} = \Lambda$. Show that

1. E is isomorphic to an elliptic curve defined over $\mathbb{R}$.
2. $\Delta(\Lambda) := 60^3 G_4(\Lambda)^3 - 3^3 \cdot 140^2 G_6(\Lambda)^2$ is a real number.
3. $E(\mathbb{R})$ is connected if and only if $\Delta(\Lambda) < 0$.
4. If $E[2] \subseteq E(\mathbb{R})$, then $\Lambda = \mathbb{Z}a + \mathbb{Z}bi$ for some $a, b \in \mathbb{R}$.

Problem 8 (Hecke operators)**.** For $n \geq 0$, define **Hecke operator** T_n to be a linear operator on the free abelian group of rank 2 full lattices $\Lambda \subseteq \mathbb{C}$ by the relation

$$T_n(\Lambda) = \sum_{[\Lambda:\Lambda']=n} \Lambda'.$$

Also define the **homethety operator** R_α by $\Lambda \to \alpha\Lambda$, for all $\alpha \in \mathbb{C}^*$. Show that

1. For all n and α, T_n commutes with R_α.
2. For all $\gcd(m, n) = 1$, $T_{mn} = T_m T_n$.
3. For all primes p and $r \geq 1$, $T_{p^{r+1}} = T_{p^r} T_p - p T_{p^{r-1}} R_p$.
4. For all m, n, T_m commutes with T_n.
5. Let $E = \mathbb{C}/\Lambda$ be a complex elliptic curve and let $n \geq 1$ be an integer. Show that there are $\sum_{d|n} d$ many isomorphism classes of degree n isogenies $E' \to E$ (two isogenies $\varphi' : E' \to E$ and $\varphi'' : E'' \to E$ are called isomorphic, if there exists an isomorphism $f : E' \to E''$ with $\varphi'' \circ f = \varphi'$).

Advanced

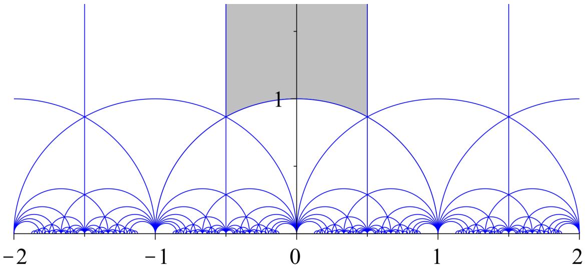
Problem 9 (Étale fundamental groups)**.** Let k be an algebraically closed field. One easy way of defining the étale fundamental group of a smooth algebraic curve C/k is as follows. Define $\pi_1^{\text{ét}}(C) := \varprojlim_{K'} \operatorname{Gal}(K'/K)$, where K is the function field of C and K' runs over all Galois extensions of K such that the corresponding curve C' is a finite étale cover of C.

1. Use the results from earlier worksheets to compute the étale fundamental group of $\mathbb{P}^1$.
2. Use the results from earlier worksheets to compute the étale fundamental group of an elliptic curve E (you might assume that char$k = 0$. In positive characteristic, this is more challenging).
3. (Galois correspondence) Show that the category of finite étale covers of E is equivalent to the category of finite $\pi_1^{\text{ét}}(E)$-sets.

Problem 10 (Modular curves)**.** There is an $\mathrm{SL}_2(\mathbb{Z})$-action on the upper half plane $\mathbb{H}$ given by:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \circ \tau = \frac{a\tau + b}{c\tau + d}, \ \tau \in \mathbb{H}.$$

The action factors through $\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm \mathbf{I}\}$. So we will freely switch between $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{PSL}_2(\mathbb{Z})$ actions. The action admits a **fundamental domain** Σ [1], which is the grey region of the following graph[2]:



More precisely, it is the open set $\{|z| > 1\} \cap \{|\mathrm{Re}\, z| < \frac{1}{2}\}$ together with the boundary on the left plus half the arc on the bottom including the point i. In the following, let $\omega = \frac{-1+\sqrt{3}i}{2}$.

1. Check that Σ is a fundamental domain, i.e., its points are in bijection with $\mathrm{SL}_2(\mathbb{Z})$-orbits.

2. Let $\Sigma' = \Sigma - \{i, \omega\}$. Show that the $\mathrm{PSL}_2(\mathbb{Z})$-stabilizer of any points in Σ' is trivial. Show that for $g, h \in \mathrm{PSL}_2(\mathbb{Z})$, $g \circ \Sigma' = h \circ \Sigma'$ if and only if $g = h$. Compute the stablizers of ω and i, respectively, and use this to give a conceptual reason why there are three arcs [3] passing through ω. What are the angles between the three arcs?

3. Show that the isomorphic classes of elliptic curves over $\mathbb{C}$ are in bijection with Σ (or equivalent, with the quotient set $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$). What is the relation between the stabilizer of a $\tau \in \Sigma$ and the automorphism group of the corresponding elliptic curve ?(Compare Problem 4 of PSET 2).

4. For $N \geq 1$, define the **congruence subgroup of level** N, denoted $\Gamma(N)$, to be the kernel of the natural map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N)$. Show that the isomorphic classes of elliptic curves with a level-N structure is in bijection with $\mathbb{H}/\Gamma(N)$. What can you say about the fundamental domain of the action of $\Gamma(N)$ on $\mathbb{H}$?

5. (Background story) The quotient $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ is not only a set, but a geometric object. In complex geometry, it is usually termed an **orbifold**. With more efforts, it can be shown to be algebraic, and algebraic geometers call it an **algebraic stack**. Indeed, it is the **fine moduli space** of elliptic curves over $\mathbb{C}$, and is called the **modular curve of level 1**, denoted $Y(1)$. If you don't like to work with orbifolds or stacks, you can take a more classical approach: put a natural structure of complex manifold on $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$. As a complex manifold, it is isomorphic to $\mathbb{A}^1_{\mathbb{C}}$ (it is called the ***j*-line**). By doing this, you obtain the **coarse moduli space** of elliptic curves over $\mathbb{C}$. Use your browser, try to understand what these terminologies mean.

[1] Loosely speaking, a fundamental domain is a region in $\mathbb{H}$ that is in bijection with the $\mathrm{SL}_2(\mathbb{Z})$-orbits.

[2] The graph is taken from en.wikipedia.org/wiki/Fundamental_domain.

[3] We also view a line as an arc of infinite radius. In fact, these are **geodesics** of $\mathbb{H}$ as a hyperbolic space.

6. (More background story) Similarly, the quotient $\mathbb{H}/\Gamma(N)$ is not only a set, but a geometric object. It is the fine moduli space of elliptic curves with a level-N structure, and is called the modular curve of level N, denoted $Y(N)$. For $N \geq 3$, $\mathbb{H}/\Gamma(N)$ is even a smooth algebraic curve. The quotient map $Y(N) \to Y(1)$ is an étale cover. $Y(N)$ is an example of **Shimura variety**.

7. (Modular forms) Now let's take for granted that $Y(1) := \mathbb{H}/\operatorname{SL}_2(\mathbb{Z})$ is a dimension 1 smooth orbifold (you don't need to know what this really means). The quotient map $\mathbb{H} \to Y(1)$ can be thought of as a universal cover with deck group $\operatorname{PSL}_2(\mathbb{Z})$. Consider the cotangent bundle $\Omega_{Y(1)}$. The way to think about $\Omega_{Y(1)}$ is to view it as $\Omega_{\mathbb{H}}$ with $\operatorname{PSL}_2(\mathbb{Z})$-action (why?). The global sections of $\Omega_{Y(1)}$ are then global sections of $\Omega_{\mathbb{H}}$ invariant under $\operatorname{PSL}_2(\mathbb{Z})$-action (why?). In other words:

   $$H^0(Y(1), \Omega_{Y(1)}) = H^0(\mathbb{H}, \Omega_{\mathbb{H}})^{\operatorname{PSL}_2(\mathbb{Z})}.$$

   Show that $H^0(Y(1), \Omega_{Y(1)}^{\otimes k})$ is isomorphic to the space of **meromorphic modular forms** of weight $2k$. Here, a meromorphic modular form of weight n is a moromorphic function $f : \mathbb{H} \to \mathbb{C}$ such that $f(g\tau) = (c\tau + d)^n f(\tau)$ for all $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \operatorname{SL}_2(\mathbb{Z})$.

8. A T_n-**Hecke correspondence** $\mathcal{T}_n \subseteq Y(1) \times Y(1)$ is a divisor parametrizing isomorphic classes of a pair of elliptic curves (E_1, E_2) with a degree n isogeny $E_1 \to E_2$. Check that $\mathcal{T}_1$ is nothing other than the diagonal. Pick a point $E \in Y(1)$, which corresponds to an elliptic curve.

   Use your intuition (it is OK to be non-rigorous): how many intersection points (counting multiplicities) are there in $(Y(1) \times E) \cap \mathcal{T}_n$? How many intersection points (counting multiplicities) are there in $(E \times Y(1)) \cap \mathcal{T}_n$? (Compare Problem 8).

9. (Special divisors) A CM point of $Y(1)^n$ is a point corresponding to a product of n CM elliptic curves. A irreducible divisor $D \subsetneq Y(1) \times Y(1)$ is called **special**, if it is either $Y(1) \times E_1$ or $E_2 \times Y(1)$ (where E_1, E_2 are CM), or a component of a Hecke correspondence. Show that a special divisor contains a Zariski dense collection of CM points.

   The converse is also true: if a irreducible divisor $D \subsetneq Y(1) \times Y(1)$ contains a Zariski dense collection of CM points, then it must be special. This is a baby case of the André–Oort conjecture, which is solved recently, see arxiv.org/abs/2109.08788.