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

Problem set 3

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. Consider the following elliptic curves:

$$E : y^2 = x^3 + x$$

$$E_7 : y^2 = x^3 + 49x$$

1. Compute the j-invariant of the elliptic curves. Conclude that the two elliptic curves are isomorphic over $\mathbb{C}$.
2. Use sage or magma to compute the ranks of the elliptic curve. Conclude that they are not isomorphic over $\mathbb{Q}$.
3. Can you find an isomorphism between them over an extension of $\mathbb{Q}$?

Problem 2. Let $p \geq 5$ be a prime. Consider the following elliptic curves over $\mathbb{Q}$:

$$E_1 : y^2 = x^3 + 1$$

$$E_2 : y^2 = x^3 + p^6$$

1. Find an isomorphism $E_2 \to E_1$ over $\mathbb{Q}$.
2. Show that E_1 has good reduction at p while E_2 does not.

Problem 3. Let E be an elliptic curve with CM by an order $\mathcal{O}$ in a quadratic imaginary field. Show that $j(E) \in \mathbb{Z}$ if and only if $\mathcal{O}$ has class number 1.

Problem 4. Let $E/\mathbb{C}$ be an elliptic curve associated to the lattice Λ. Suppose E has CM by an order $\mathcal{O}$ in a quadratic imaginary field K. Let $\alpha \in \mathcal{O}$. Show that the endomorphism ϕ_α has degree $Nm_{K/\mathbb{Q}}\alpha$.

Problem 5. Let E be an elliptic curve over $\mathbb{C}$ with an endomorphism $\phi : E \to E$ of degree 2.

1. Show that E has complex multiplication.
2. Notation as in the previous problem. Show that there are only three possibilities for α:

(a) $\alpha = 1 + \sqrt{-1}$, $\mathcal{O} = \mathbb{Z}[\sqrt{-1}]$;
(b) $\alpha = \sqrt{-2}$, $\mathcal{O} = \mathbb{Z}[\sqrt{-2}]$;
(c) $\alpha = \frac{1+\sqrt{-7}}{2}$, $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$.

3. Find the j-invariants for the three isomorphism classes.

Problem 6. It is a well known result that there is no elliptic curve over $\mathbb{Q}$ with everywhere good reduction. But there do are elliptic curves over quadratic extensions with everywhere good reduction. Show that

$$E : y^2 + xy + \left(\frac{5+\sqrt{29}}{2}\right)^2 y = x^3$$

over $K = \mathbb{Q}(\sqrt{29})$ has everywhere good reduction.

Problem 7 ($e^{\pi\sqrt{163}}$ is an almost integer)**.** Consider the quadratic field $F = \mathbb{Q}(\sqrt{-163})$. We note that this is UFD and hence the class group $cl(\mathcal{O}_F) = 1$. Conclude that the j-invariant of the elliptic curve E corresponding to the lattice $\mathcal{O}_K$ is integral. Moreover, using the the $q(= e^{2\pi i\tau})$ expansion of j given by

$$j(q) = 1/q + 744 + o(q)$$

Conclude that $e^{\pi\sqrt{163}}$ is almost an integer.
Indeed plugging in a calculator shows that

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925.....$$

Intermediate

Problem 8. Consider the curve $E : y^2 = x^3 + x$ over $\mathbb{Q}$. We know that the endomorphism algebra of this curve is given by $\mathbb{Q}(i)$. Show that the field $\mathbb{Q}(i)(E(\overline{\mathbb{Q}})[n])$ is an abelian Galois extension of $\mathbb{Q}(i)$.

Problem 9. Let E/K be an elliptic curve. We denote by S a finite set of primes of O_K and by $O_{K,S}$ the localization of O_K at these primes. Suppose that $\mathcal{E}/O_{K,S}$ is an (integral) elliptic curve with generic fiber E. In the following, we will write $\mathfrak{p}$ for a prime of O_K dividing an integer prime $(p) \subseteq \mathbb{Z}$, and $\mathfrak{p} \notin S$. We will also write $\mathcal{E}_{k(\mathfrak{p})}$ for the reduction of $\mathcal{E}$ modulo $\mathfrak{p}$.

1. Let $\overline{\mathbb{Z}}$ be the ring of algebraic integers. Choose a prime $\overline{\mathfrak{p}}$ in $\overline{\mathbb{Z}}$ that lies above $\mathfrak{p}$. Show that $\overline{\mathbb{Z}}/\mathfrak{p} \simeq \overline{\mathbb{F}}_p$. Check that once fixing $\overline{\mathfrak{p}}$, the reduction map $E(\overline{\mathbb{Q}}) \to \mathcal{E}_{k(\mathfrak{p})}(\overline{\mathbb{F}}_p)$ is well defined.

2. Show that the kernel $\mathcal{E}[n]$ of the n-th power map $\mathcal{E} \xrightarrow{n} \mathcal{E}$ is flat over $O_{K,S}$. If you are not familiar with scheme theory, just take this for granted.

3. Let $\mathfrak{p}|p$ be a prime not in S and let n be coprime to p. Use 2 to show that the reduction map on n-torsion points $E(\overline{\mathbb{Q}})[n] \to \mathcal{E}_{k(\mathfrak{p})}(\overline{\mathbb{F}}_p)[n]$ is bijective. In particular, if $l \neq p$, the reduction induces an isomorphism of the Tate modules $T_l(E) \xrightarrow{\sim} T_l(\mathcal{E}_{k(\mathfrak{p})})$.

4. Show that the $\mathrm{Gal}(k(\mathfrak{p}))$-module $T_l(\mathcal{E}_{k(\mathfrak{p})})$ is obtained from the $\mathrm{Gal}(K)$-module $T_l(E)$ by first restricting to the decomposition group $D_{\overline{\mathfrak{p}}}$ and then quotient by the inertial group $I_{\overline{\mathfrak{p}}}$. In particular, $I_{\overline{\mathfrak{p}}}$ acts trivially on $T_l(E)$.

5. The famous criterion by Néron–Ogg–Shafarevich claims the inverse: if $I_{\bar{\mathfrak{p}}}$ acts trivially on $T_l(E)$, then E has good reduction at $\mathfrak{p}$.

Remark 1. Instead of using scheme theory, 3 can also be proved using formal group laws (cf. Arithmetic of Silverman chapter IV and VII). If you are not familiar with both of them, feel free to take 2 and 3 for granted.

Problem 10 (l-adic monodromy)**.** Let E be an elliptic curve over a field K finitely generated over a number field or a finite field. Recall that for any prime $l \neq \operatorname{char} K$, the Tate module $V_l(E) := T_l(E) \otimes \mathbb{Q}_l$ is a dimension two $\mathbb{Q}_l$-representation of $\mathrm{Gal}(K) := \mathrm{Gal}(\overline{K}/K)$. Therefore, there is a map $\rho : \mathrm{Gal}(K) \to \mathrm{GL}(V_l(E)) \simeq \mathrm{GL}_2(\mathbb{Q}_l)$. The Zariski closure of $\operatorname{im}\rho$ in the $\mathbb{Q}_l$-algebraic group $\mathrm{GL}_{2,\mathbb{Q}_l}$ is a $\mathbb{Q}_l$-algebraic subgroup of $\mathrm{GL}_{2,\mathbb{Q}_l}$ (it is OK that you don't know what an algebraic group is, just view it as a Lie group). This subgroup is called the **l-adic monodromy group of** E, denoted $G_l(E)$.

1. Let E' be the base change of E to a finite extension K'. Show that $G_l(E') \subseteq G_l(E)$. Furthermore, show that $G_l^\circ(E') = G_l^\circ(E)$ (here G_l° denotes the identity component, i.e., the connect component which contains identity, it is itself an algebraic subgroup).

2. Show that $\mathrm{End}_{G_l(E)}(V_l(E)) = \mathrm{End}(E) \otimes \mathbb{Q}_l$ and $\mathrm{End}_{G_l^\circ(E)}(V_l(E)) = \mathrm{End}(E_{\overline{K}}) \otimes \mathbb{Q}_l$ (Hint: a version of Tate conjecture for elliptic curves claims that $\mathrm{End}_{\mathrm{Gal}(K)}(V_l(E)) = \mathrm{End}(E) \otimes \mathbb{Q}_l$. The conjecture was proven by Tate for finite fields, by Zarhin for finite generated fields over finite fields, and by Faltings for finite generated fields over number fields).

3. Using 2, show that base changing E from K to an inseparable extension doesn't change $\mathrm{End}(E) \otimes \mathbb{Q}$.

Advanced

Problem 11 (l-adic monodromy, continued)**.** This is a continuation of Problem 10. All the setups will be the same.

1. Suppose that K is finite. If E is supersingular, show that $G_l^\circ(E)$ is the rank 1 diagonal torus, i.e. the center of GL_2. If E is ordinary, show that $G_l^\circ(E)$ is a rank 2 torus containing the diagonal torus. Can you give an explicit description of this torus? (Hint: look at the characteristic polynomial of the Frobenius endomorphism of E).

2. How does the structure of $G_l^\circ(E)$ in 1 reflects the identities in Problem 10 2?

3. Suppose that K is a number field. Show that $G_l(E)$ contains a rank 2 torus containing the diagonal torus. Deduce that when E is CM, then $G_l^\circ(E)$ is a rank 2 torus containing the diagonal torus. Can you give an explicit description of this torus?

4. Suppose that K is a number field. If E is non-CM, show that $G_l(E) = \mathrm{GL}_2$.

Problem 12 (Families of elliptic curves)**.** Let X be a complex variety. A **relative elliptic curve** over X is a smooth projective variety $\mathcal{E} \xrightarrow{\pi} X$ of relative dimension 1, together with a (commutative) relative group law $m : \mathcal{E} \times_X \mathcal{E} \to \mathcal{E}$, a relative identity section $\mathrm{id} : X \to \mathcal{E}$, and a relative inverse map $\iota : \mathcal{E} \to \mathcal{E}$, such that for every point $x \in X(\mathbb{C})$, the fiber $\mathcal{E}_x$ is an elliptic curve with group law m_x, identity $\mathrm{id}(x)$ and inverse map ι_x. Roughly speaking, $\mathcal{E}$ is an algebraic family of elliptic curve parametrized by X. $\mathcal{E}$ is said to be **isotrivial**, if there is an elliptic curve $E/\mathbb{C}$, such that $E \simeq \mathcal{E}_x$ for all $x \in X(\mathbb{C})$. $\mathcal{E}$ is said to be **trivial**, if there is an elliptic curve $E/\mathbb{C}$ such that $\mathcal{E} \simeq X \times E$.

1. Take the base $X = \mathbb{G}_m := \operatorname{Spec} \mathbb{C}[t, t^{-1}]$. The relative projectivization $\mathcal{E} \subseteq \mathbb{G}_m \times \mathbb{P}^2$ of the affine family
$$\mathcal{E}' := \operatorname{Spec} \left(\frac{\mathbb{C}[t, t^{-1}][x, y]}{y^2 = x^3 + tx} \right) \subseteq \mathbb{G}_m \times \mathbb{A}^2 \to \mathbb{G}_m$$
is a relative elliptic curve over $\mathbb{G}_m$. Show that it is an isotrivial family. Find a finite étale cover of $\mathbb{G}_m$ over which $\mathcal{E}$ is trivial (cf. Problem 1).

2. More generally, if $\mathcal{E}$ is isotrivial, then it is trivial up to an étale cover, i.e., there is a finite étale cover $X' \to X$ such that the pullback family $\mathcal{E} \times_X X' \to X'$ is trivial (Hint: in PSET 2, we defined the modular curve of level 1 as $Y(1) := \mathbb{H}/\operatorname{SL}_2(\mathbb{Z})$, which is a fine moduli space of elliptic curves. First, show that $\mathcal{E}$ induces a morphism $X \to Y(1)$. Then, use that fact that for $N \geq 3$, $Y(N) := \mathbb{H}/\Gamma(N)$ is an algebraic curve, which is also a finite étale cover of $Y(1)$).

3. If X is projective, then $\mathcal{E}$ is isotrivial. In particular, if $X = \mathbb{P}^1$, then $\mathcal{E}$ is trivial (Hint: show that $Y(N)$ is affine).

4. If every fiber is CM, then $\mathcal{E}$ is isotrivial. In particular, if $X = \mathbb{A}^1$, then $\mathcal{E}$ is trivial.

Problem 13 (A p-adic proof of integral j-invariant)**.** In this problem, we give a p-adic proof of the fact that the j-invariant of a CM elliptic curve over a number field K is an algebraic integer. Refer to Advanced topics in Silverman for this proof. Let K be a p-adic field such that E/K satisfies $|j(E)| > 1$. We take for granted the Tate uniformisation for elliptic curves which gives a parmetrisation of the $\overline{K}$ points of E: We have an isomorphism
$$\varphi : E(\overline{K}) \to \overline{K}^*/q^{\mathbb{Z}}$$
for some unique $q \in K^*$ such that $|q| < 1$ and $-ord_v(q) = ord_v(j(E))$. Further the map φ commutes with the Galois action on both sides. In particular, $E(L) = L^*/q^{\mathbb{Z}}$ for any finite extension L of K.

1. Let l be a prime not dividing $ord_v(j)$ where v is the valuation on K. Find a basis for $E[l]$ and an element $\sigma \in \operatorname{Gal}(\overline{K}/K)$, in the inertia subgroup, such that
$$\sigma \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mod l$$
HINT: First convince yourself that it is OK to base change and possibly work with a finite extension of K. So assume that K contains ζ, a primitive l^{th} root of unity.

2. Conclude from 1, that if E is an elliptic over a number field F. Then for almost all but finitely many primes the image of $\operatorname{Gal}(\overline{F}/F) \to T_l(E)$ contains an element satisfying the condition in 1.

3. Let $F/\mathbb{Q}$ be a number field. Further, suppose that E/F does not have j-invariant in $\mathcal{O}_F$. We will show that $\psi \in \mathbb{Z}$. Let $\psi \in \operatorname{End}(\psi)$. We know that ψ acts on $T_l(E)$ via, say, $\psi_l \in M_2(\mathbb{Z}_l)$. Show that
$$\psi \equiv \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mod l$$

4. Let $m = \deg(1 + \psi) - \deg(\psi) - 1$. Using the part 1, show that $m \equiv 2a \mod l$.

5. Next, show that $\deg(m - 2\psi) \equiv 0 \mod l$ for all but finitely many l.

6. Conclude that $\psi \in \mathbb{Z}$. This completes the proof that $\operatorname{End}(E) = \mathbb{Z}$ and hence E is not CM.