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

Problem set 4

Below you will find problems for problem set four. 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.

1. For $N \geq 1$, find the cardinality of $|SL(\mathbb{Z}/N\mathbb{Z})|$. (Hint: Do this for $N = p^n$ for $n \geq 1$ and then use the Chinese remainder theorem)
2. Show that the map $\Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z}$ given by
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b \mod N$$
has kernel $\Gamma(N)$
3. Show that the map given by $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \mod N$$
has kernel $\Gamma_1(N)$
4. Use previous parts to compute the index of $\Gamma(N)$, $\Gamma_1(N)$, $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$, respectively. In particular note that the index is finite.

Problem 2. Show that the modular curve $Y(1) = \mathbb{H}/SL_2(\mathbb{Z})$ has exactly one cusp. Moreover, show that the modular curves $X(N), X_1(N)$ and $X_0(N)$ have only finitely many cusps.

Problem 3. Suppose that $N > 2$ for this problem. For all modular curves mentioned above convince yourselves that we can define a well defined map $X \to X(1)$ where $X = X(N), X_1(N)$ or $X_0(N)$.

1. Show that the degree the map $X_0(N) \to X(1)$ is $[\Gamma_0(N) : SL_2(\mathbb{Z})]$ which is computed in problem 1.
2. However, the degree of the map in the other two cases is given by $[\Gamma : SL_2(\mathbb{Z})]/2$ where $\Gamma = \Gamma(N)$ or $\Gamma_1(N)$. (HINT: Note that -I acts trivially on $\mathbb{H}$ and this parity is seen based in whether $-I$ is in the congruence subgroup or not.)

Problem 4. As seen in the lecture, the modular curves corresponding to the congruence subgroups we saw above have a "moduli interpretation".

1. We recall that the affine part of $X(1) = \mathbb{H}/SL_2(\mathbb{Z})$ parametrizes elliptic curves over $\mathbb{C}$ up to isomorphism. This space is along with the cusp ∞ is $\mathbb{P}^1$.

2. The affine part of $X_0(N)$ parametrizes isomorphism classes of pairs $[E, C]$ where C is a cyclic subgroup of E of order N.

3. The affine part of $X_1(N)$ parametrizes isomorphism classes of pairs $[E, P]$ where P is a point of E of order N.

4. The affine part of $X(N)$ parametrizes isomorphism classes of pairs $[E, P, Q]$ where P, Q are basis for $E[N]$ such the the Weil pairing on them $e(P, Q) = -1 \in \mathbb{Z}/N\mathbb{Z}$.

A. Similar to problem 3, more generally convince yourselves that we have maps

$$X(N) \to X_1(N) \to X(N) \to X(1).$$

B. Can you find an interpretation of these maps in terms of the points they parametrise?

C. Show that the map $X(N) \to X(1)$ is ramified at most at ∞ (cusp), or the two points corresponding to elliptic curves with extra automorphims ($j = 0$ and 1728).

Problem 5 ($Y(N)$ is a $K(\pi, 1)$[1])**.** Show that for $N \geq 3$, $\Gamma(N)$ acts freely on $\mathbb{H}$. For each $n \geq 1$, compute the homotopy group $\pi_n(Y(N))$, where we view $Y(N)$ as a differentiable manifold.

Problem 6. Let $\mathcal{F} = \{\tau \in \mathbb{H} || \Re(\tau)| \leq \frac{1}{2}, |\tau| \geq 1\}$ be a fundamental domain for $Y(1) = SL_2(\mathbb{Z})\backslash\mathbb{H}$.

1. Describe the points $\tau \in \mathcal{F}$ such that the corresponding elliptic curve E can be defined over $\mathbb{R}$, i.e., find $\{\tau \in \mathcal{F} \,|\, j(\tau) \in \mathbb{R}\}$.

2. Let $l \equiv -1 \pmod 4$ be a prime number. Show that up to isomorphism over $\mathbb{C}$, there is a unique elliptic curve E over $\mathbb{C}$ with CM by $\mathbb{Z}[\frac{1+\sqrt{-l}}{2}]$, such that $j(E) \in \mathbb{R}$, and $j(E) = j(\frac{1+\sqrt{-l}}{2})$.

Problem 7 (Heegner points over $\mathbb{C}$)**.** Let $N \geq 1$ be an integer. Let K be an imaginary quadratic field with discriminant D and $\mathcal{O}_K$ be its ring of integers. Assume $D \equiv 1 \pmod 4$ and $(N, D) = 1$.

1. Show that there is a 1-1 correspondence between pairs $([\mathfrak{a}], \mathfrak{n})$, where $[\mathfrak{a}] \in Cl_K, \mathfrak{n} \subset \mathcal{O}_K$ an integral ideal such that $\mathcal{O}_K/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$, and equivalence classes of pairs of elliptic curves having CM by $\mathcal{O}_K$, together with a cyclic degree N isogeny. The correspondence is given by

$$([\mathfrak{a}], \mathfrak{n}) \leftrightarrow (\mathbb{C}/\mathfrak{a} \xrightarrow{id_{\mathbb{C}}} \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}).$$

2. Let $N = p_1^{r_1} \cdots p_s^{r_s}$ be the prime factorization of N. Show that the existence of integral ideals $\mathfrak{n} \subset \mathcal{O}_K$ satisfying $\mathcal{O}_K/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$ is equivalent to all p_i split in K. In this case, there are exactly 2^s such ideals of norm N.

Problem 8. Here are some old PSET problems which were intermediate or advanced, but are now within beginners' grasp. Recall that $Y(1)$ is the modular curve with level 1, viewed as a curve over $\mathbb{Q}$. 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 $E_1 \to E_2$. Show that:

[1] In algebraic topology, this is called an Eilenberg–MacLane space.

1. $\mathcal{T}_1$ is nothing other than the diagonal.
2. $\mathcal{T}_m \subseteq \mathcal{T}_{mn^2}$. In particular, $\mathcal{T}_n$ may be non-irreducible.
3. $\mathcal{T}_n$ is cut out by the equation $\Phi_n(x, y) = 0$, where x, y are coordinates on two copies of $Y(1)$'s, respectively. Deduce that $\mathcal{T}_n$ is also a curve over $\mathbb{Q}$.
4. $\mathcal{T}_n$ contains a Zariski dense collection of CM points (a CM point of $Y(1)^n$ is a point corresponding to a product of n CM elliptic curves).

Intermediate

Problem 9. This is a continuation of Problem 8:

1. Fix a complex elliptic curve E, show that there are $\sum_{d|n} d$ many equivalent classes of isogeny $E \to E'$ with degree n. Here $E \to E'$ and $E \to E''$ are called equivalent, if there is an isomorphism $E' \to E''$ that commutes with the respective isogenies (Hint: consider matrices in $M_2(\mathbb{Z})$ with determinant n).
2. For two divisors in $C, D \subseteq X(1) \times X(1)$. We write $C \cdot D$ for the number of intersections of C and D (counting multiplicities). Let $\overline{\mathcal{T}}_n$ be the Zariski closure of $\mathcal{T}_n$ in $X(1) \times X(1)$. Fix $e \in X(1)(\mathbb{C})$, compute $\overline{\mathcal{T}}_n \cdot (e \times X(1))$, $\overline{\mathcal{T}}_n \cdot (X(1) \times e)$ and $\overline{\mathcal{T}}_n \cdot \overline{\mathcal{T}}_1$.

   The number $\overline{\mathcal{T}}_n \cdot \overline{\mathcal{T}}_1$ is of particular interest: it almost counts the number of elliptic curves together with a degree n isogeny to itself (though there is over-counting at ∞), see Problem 12.

Problem 10 (Modular forms)**.** Let Γ be one of the groups $\Gamma(N)$, $\Gamma_0(N)$ and $\Gamma_1(N)$. A level Γ modular form of weight k is a holomorphic function $f : \mathbb{H}^* \to \mathbb{C}$ such that $f(g\tau) = (c\tau + d)^{-k} f(\tau)$ for all $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$. Show that the global section of the line bundle $\omega^{\otimes k}$ of the (compactified) modular curve $X(\Gamma)$ is isomorphic to the space of level Γ modular forms of weight $2k$. Here ω is the tangent bundle of $X(\Gamma)$.

Problem 11. Show that for an elliptic curve E over a local field $K = \mathbb{Q}_q$ with good reduction, the identity component of the local l-adic monodromy (i.e, the Zariski closure of the image of $\mathrm{Gal}(K)$ in $\mathrm{GL}(V_l(E))$) is a torus. Use this, deduce that when K is a local field, the analogue of Tate's isogeny theorem "$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_l = \mathrm{Hom}_{\mathrm{Gal}(K)}(T_l(E_1), T_l(E_2))$" is false.

Advanced

Problem 12. This is a continuation of Problem 8 and Problem 9. Show that when n is not a perfect square, the local intersection number of $\overline{\mathcal{T}}_n \cdot \overline{\mathcal{T}}_1$ at (∞, ∞) is $\sum_{dd'=n} \min\{d, d'\}$ (Hint: use Tate curve). Conclude that the number of elliptic curves together with a degree n isogeny to itself is $\sum_{dd'=n} \max\{d, d'\}$. For example, when $n = 2$, there are 4 such elliptic curves with degree 2 isogenies, what are they ? (cf. PSET 3 Problem 5)

Problem 13 (Hodge structures and Mumford–Tate groups)**.** Let A be a subring of $\mathbb{R}$ (ususally taken as $\mathbb{Z}, \mathbb{Q}$ or $\mathbb{R}$). An A-Hodge structure of is a finite free A-module H_A that admits a Hodge decomposition

$$H_A \otimes \mathbb{C} = \bigoplus H^{p,q}, \tag{1}$$

where each $H^{p,q}$ is a $\mathbb{C}$-vector space satisfying $H^{p,q} = \overline{H^{q,p}}$. A morphism of A-Hodge structures is a morphism of A-modules which respects the Hodge decomposition. Therefore, we have a notion of **the category of A-Hodge structures**. An A-Hodge structure is called **pure of weight** n, if $H^{p,q} = 0$ for all $p + q \neq n$. Let $H^n = \bigoplus_{p+q=n} H^{p,q}$, it is an $\mathbb{R}$-vector space. The **weight decomposition** induced by the Hodge decomposition is

$$H_A \otimes \mathbb{R} = \bigoplus_{n \in \mathbb{Z}} H^n. \tag{2}$$

It is a decomposition over $\mathbb{R}$.

1. The **Deligne torus** $\mathbb{S}$ an algebraic group over $\mathbb{R}$, defined as the Weil restriction of $\mathbb{G}_{m,\mathbb{C}}$ from $\mathbb{C}$ to $\mathbb{R}$. This means, $\mathbb{S}$ admits the following funtor of points: $\mathbb{S}(R) = (R \otimes \mathbb{C})^*$ for all $\mathbb{R}$-algebra R. Show that $\mathbb{S}$ is a rank 2 torus over $\mathbb{R}$ with a $\mathrm{Gal}(\mathbb{R})$-invariant isomorphism $\mathbb{S} \otimes \mathbb{C} \simeq \mathbb{G}_{m,\mathbb{C}} \times \mathbb{G}_{m,\mathbb{C}}$, where $\mathrm{Gal}(\mathbb{R})$ acts on the left over the scalar $\mathbb{C}$, and on the right by swapping the two factors. There is a cocharacter $c_0 : \mathbb{G}_{m,\mathbb{R}} \to \mathbb{S}$ defined by the inclusion $\mathbb{R}^* \hookrightarrow \mathbb{C}^*$ (over $\mathbb{R}$-points).

2. Show that the category of $\mathbb{R}$-Hodge structures is equivalent to the category of finite dimensional $\mathbb{S}$-representations: an $\mathbb{R}$-Hodge structure $H_\mathbb{R}$ is the same as a morphism $\mathbb{S} \to \mathrm{GL}(H_\mathbb{R})$ (where we view $H_\mathbb{R}$ as an $\mathbb{R}$-vector space). Show that the cocharacter c_0 induces the weight decomposition. (Hint: consider two characters z *resp.* $\overline{z}$: $\mathbb{S} \otimes \mathbb{C} = \mathbb{G}_{m,\mathbb{C}} \times \mathbb{G}_{m,\mathbb{C}} \to \mathbb{G}_{m,\mathbb{C}}$ sending (w_1, w_2) to w_1 *resp.* w_2. Show that the cocharacter group $X^*(\mathbb{S}) := \mathrm{Hom}_{\mathrm{gp}}(\mathbb{S} \otimes \mathbb{C}, \mathbb{G}_{m,\mathbb{C}})$ is $\mathbb{Z}z \oplus \mathbb{Z}\overline{z}$, with $\mathrm{Gal}(\mathbb{R})$-action swapping z and $\overline{z}$. Then use the fact that a representation of a torus admits splitting indexed by its cocharacter group).

3. For a $\mathbb{Z}$ or $\mathbb{Q}$-Hodge structure H, define its **Mumford–Tate group** $\mathrm{MT}(H)$ as the samllest $\mathbb{Q}$-algebraic subgroup of $\mathrm{GL}(H_\mathbb{Q})$ through which the representation $\mathbb{S} \to \mathrm{GL}(H_\mathbb{R})$ factors. Show that $\mathrm{MT}(H)$ is connected, and contains the central torus $\mathbb{G}_{m,\mathbb{Q}} \subseteq \mathrm{GL}(H_\mathbb{Q})$ if H is pure of nonzero weight.

4. As we have seen in PSET 1 Problem 11, the category of elliptic curves over $\mathbb{C}$ is equivalent to the category of rank 2 pure $\mathbb{Z}$-Hodge structures of type $(1,0) + (0,1)$, the equivalence can be constructed as $E \to H_1(E, \mathbb{Z})$ (or $H^1(E, \mathbb{Z})$). We write $\mathrm{MT}(E) := \mathrm{MT}(H_1(E, \mathbb{Q})) \subseteq \mathrm{GL}(H_1(E, \mathbb{Q})) \simeq \mathrm{GL}_{2,\mathbb{Q}}$ for the Mumford–Tate group of E. Show that $\mathrm{MT}(E) = \mathrm{GL}_{2,\mathbb{Q}}$ if E is non-CM, and is the Weil restriction of $\mathbb{G}_{m,K}$ from K to $\mathbb{Q}$ (in particular it is a rank 2 torus), if E admits CM by an order of K.

5. Let E be an elliptic curve over a number field $K \subseteq \mathbb{C}$. In PSET 3 Problem 10 we defined the l-adic monodromy group $G_l^\circ(E)$ as the Zariski closure of the image of $\mathrm{Gal}(K)$ in $\mathrm{GL}(V_l(E))$. Show that for every l, there is a canonical identification $H_1(E_\mathbb{C}, \mathbb{Z}) \otimes \mathbb{Q}_l = V_l(E)$.

6. Prove the **Mumford–Tate conjecture** for elliptic curves: under the identification in 5, we have $\mathrm{MT}(E_\mathbb{C}) \otimes \mathbb{Q}_l = G_l^\circ(E)$.