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

Problem set 5

Below you will find problems for problem set five. 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 (Review on algebraic number theory)**.** Let E/F be a finite extension of number fields. Let p be a prime of F and $\mathfrak{p}|p$ be a prime of E. Denote $I_{\mathfrak{p}|p} \subseteq G_{\mathfrak{p}|p} \subseteq \mathrm{Gal}(E/F)$ be the inertia and decomposition groups of $\mathfrak{p}$. Let L/F be another finite extension, and let $M = EL$. Write $\mathfrak{P}$ for a prime of M lying over $\mathfrak{p}$ and let $\mathfrak{q}$ be the prime ideal $\mathfrak{P}|_L$.

1. Let $E_{I_{\mathfrak{p}|p}}$ and $E_{G_{\mathfrak{p}|p}}$ be the fixed fields of the respective groups. Show that $E_{I_{\mathfrak{p}|p}}$ (resp. $E_{G_{\mathfrak{p}|p}}$) is the largest among the subfields $K \subseteq E$ such that $\mathfrak{p}|_K$ is unramified (resp. totally split) over p. Show that $E_{I_{\mathfrak{p}|p}}$ (resp. $E_{G_{\mathfrak{p}|p}}$) is the smallest among the subfields $K \subseteq E$ such that $\mathfrak{p}$ is totally ramified (resp. the only prime) over $\mathfrak{p}|_K$.
2. Show that if p is unramified (resp. totally split) in both E and L, then it is unramified (resp. totally split) in M.
3. If E/F is Galois and $\mathfrak{p}|p$ is unramified (resp. totally split), show that $\mathfrak{P}|\mathfrak{q}$ is unramified (resp. totally split).
4. Give an example that E, L are both Galois, and p is totally ramified in both E, L, but not totally ramified in M.
5. Justify the assertion: Galois extensions of F are completely determined by the primes of F that are totally split in the extension (Hint: Use Chebotarev's density theorem).

Problem 2 (Hilbert class field)**.** The Hilbert class field $\mathcal{H}(K)$ of a number field K is the maximal unramified[1] abelian extension of K. It is a consequence of Artin's reciprocity law that $\mathcal{H}(K)$ is a finite extension of K of degree $\#\mathrm{Cl}(K)$ and there is an isomorphism

$$\mathrm{Cl}(K) \xrightarrow{\sim} \mathrm{Gal}(\mathcal{H}(K)/K),\ \mathfrak{p} \to \mathrm{Frob}_{\mathfrak{p}},$$

Here, $\mathrm{Frob}_{\mathfrak{p}}$ is defined as follows: Pick any $\mathfrak{P}$ lying above p, since $\mathcal{H}/K$ is unramified, we have that $D_{\mathfrak{P}|\mathfrak{p}} \simeq \mathrm{Gal}(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}})$, where $\kappa_{\mathfrak{p}}$ stands for the corresponding residue field. Define $\mathrm{Frob}_{\mathfrak{p}}$ to be the Frobenius of $\mathrm{Gal}(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}})$. Since $\mathcal{H}(K)/K$ is abelian, $\mathrm{Frob}_{\mathfrak{p}}$ is independent of the choice of $\mathfrak{P}$. We will take this result for granted.

[1] including being unramified at infinite places. This means, a real embedding extends to a real embedding.

1. Show that $\mathcal{H}(\mathbb{Q}(\sqrt{-163})) = \mathbb{Q}(\sqrt{-163})$, while $\mathcal{H}(\mathbb{Q}(\sqrt{-5})) = \mathbb{Q}(\sqrt{-5}, i)$.

2. Find $\mathcal{H}(\mathbb{Q}(\sqrt{-15}))$.

3. Show that every prime ideal $\mathfrak{p}$ of K decomposes into a product of $\#\mathrm{Cl}(K)/f$ primes in $\mathcal{H}(K)$, where f is the order of $\mathfrak{p}$ in $\mathrm{Cl}(K)$. In particular, if $\mathfrak{p}$ is principal, then it totally splits in $\mathcal{H}(K)$.

Problem 3. Show that the $j(\sqrt{-5}) = a + b\sqrt{5}$, where $a, b \in \frac{1}{2}\mathbb{Z}$. One can then use numerical methods to determine a and b.

Problem 4. As a consequence of PSET 4 Problem 6, we have shown that if K is an imaginary quadratic field whose discriminant is a prime l, then $\mathrm{Cl}(K)[2] = 1$. Give another proof of this fact using Hilbert class field (Hint: show that every quadratic extension of K is ramified at some prime). See Problem 9 for a generalization.

Problem 5. Let E be an elliptic curve over $\mathbb{C}$ (with or without CM). Assume that its j-invariant is not 0 or 1728. Let $w = 27j/j - 1728$. Then show that the Weierstrass equation for E can be written in the form $y^2 = 4x^3 - u^2wx - u^3w$ for a unique $u \in \mathbb{C}^*$. Conclude that E can be defined over $\mathbb{Q}(j)$. As for the two exceptions, we have already seen that elliptic curves corresponding to those j-invariants can be defined over $\mathbb{Q}$.

Problem 6. Show that the map $X(N) \to X(1)$ is ramified at exactly $j = 0, 1728, \infty$ with ramification index $3, 2, N$, respectively. Use Riemann–Hurwitz formula, prove that

$$g(X(N)) = 1 + \frac{N^2(N-6)}{24} \prod_{p|N} (1 - p^{-2}). \tag{1}$$

What are the values of N such that $g(X(N)) = 0$?

Intermediate

Problem 7. Let E be an elliptic curve over $\mathbb{Q}$. Show that $\mathrm{End}_{\mathbb{Q}}(E) = \mathbb{Z}$.

Problem 8. Let K be an imaginary quadratic field of discriminant D and L be its Hilbert class field. Let d be the number of primes dividing D, and let $p_1, \ldots, p_r$ be the odd primes dividing D (so that $d = r$ or $d = r + 1$ according to whether $D \equiv 1$ or $d \equiv 0 \pmod 4$). Set $p_i^* = (-1)^{(p_i-1)/2} p_i$. Let M be the unramified abelian extension of K corresponding to the subgroup $\mathrm{Gal}(L/K)^2 \subset \mathrm{Gal}(L/K)$.

1. Let $G = \mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z})$, where the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ acts on $\mathrm{Gal}(L/K)$ by conjugation of complex conjugation. Note that under the isomorphism $\mathrm{Gal}(L/K) \simeq Cl(K)$, the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ sends an element of $Cl(K)$ to its inverse. Show that M is the maximal unramified extension of K abelian over $\mathbb{Q}$ by proving $\mathrm{Gal}(L/K)^2 = [G, G]$, where $[G, G]$ is the commutator subgroup of G. Hint: For one direction, show that $G/\mathrm{Gal}(L/K)^2 \simeq (Cl(K)/Cl(K)^2) \times (\mathbb{Z}/2\mathbb{Z})$.

2. Let $a \in \mathbb{Z}$ with $a \mid D$ and $a \equiv 1 \pmod 4$. Show that $K \subset K(\sqrt{a})$ is unramified. Hint: Note that $D = ab$, where $K(\sqrt{a}) = K(\sqrt{b})$. Consequently, by Problem 1, $K \subset K(\sqrt{p_1^*}, \ldots, \sqrt{p_r^*})$ is unramified.

3. Show that $M = K(\sqrt{p_1^*}, \ldots, \sqrt{p_r^*})$.

Problem 9 (Continuation of Problem 4 and Problem 8)**.** Use Hilbert class field, prove the following theorem [2]:
• (Gauss) If K is an imaginary quadratic field whose discriminant is D, then $\mathrm{Cl}(K)[2] \simeq (\mathbb{Z}/2)^{d-1}$, where d is the number of prime factors of D.

Use this to deduce a classification result on CM elliptic curves defined over $\mathbb{R}$.

Problem 10. For $N \geq 3$, compute the dimension of the space $\mathcal{M}_{N,2k}$ of weight $2k$ modular forms of level N (Hint: use PSET 4 Problem 10 and Problem 6).

Advanced

Problem 11. For an integer $D > 0$, the **Hurwitz class number** $H(D)$ is defined to be the weighted size of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of positive definite binary quadratic forms

$$ax^2 + bxy + cy^2, \text{ with discriminant } b^2 - 4ac = -D, a, b, c \in \mathbb{Z}.$$

Here the forms equivalent to $a(x^2+y^2)$ and $a(x^2+xy+y^2)$ are counted with multiplicities 1/2 and 1/3 respectively. When m is not a perfect square, show that

1. (Hurwitz's formula)
$$\sum_{dd'=m} \max\{d, d'\} = \sum_{t \in \mathbb{Z}, 4m-t^2>0} H(4m - t^2).$$
(Hint: use PSET 4 Problem 12).

Problem 12 (Explicit local class field theory (Lubin–Tate theory))**.** Let K be a local field with a uniformizer π and residue characteristic p. The main theorem of local class field theory states that there is a unique group homomorphism (called the Artin homomorphism)

$$\theta : K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

such that for every finite abelian extension L/K, the induced morphism $K^*/N(L^*) \xrightarrow{\sim} \mathrm{Gal}(L/K)$. In other words, θ induces an isomorphism $\widehat{\theta} : \widehat{K^*} \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K)$ of topological groups, where $\widehat{K^*}$ is the completion of K^* for the topology generated by $\{\pi^n\}_{n \geq 1}$. Recall that for imaginary quadratic fields, the maximal abelian extension can be generated by the j-invariant and torsion points on a certain elliptic curve. Lubin–Tate theory is its local counterpart: it claims that the maximal abelian extension of K can also be generated by torsion points on a certain "formal group of dimension 1".

1. Show that $\widehat{K^*} = O_K^* \times \widehat{\mathbb{Z}}$ (depending on the choice of π). Show that the fixed field of $\widehat{\theta}(O_K^*)$ is the maximal unramified extension K^{unr}/K. Let K_π be the fixed field of $\widehat{\theta}(\widehat{\mathbb{Z}})$, it is a maximal totally ramified extension of K. We have $K^{\mathrm{ab}} = K^{\mathrm{unr}} K_\pi$.
2. Show that K^{unr}/K can be constructed as $K^{\mathrm{unr}} = \bigcup_{(n,p)=1} K(\zeta_n)$. So it suffices to understand K_π/K. This is achieved by adjoining torsions of the "Lubin–Tate formal group", as we will explain.

[2] It is also possible to prove it by using quadratic lattices, which is Gauss' original proof.

3. For any commutative ring A, a **(commutative) formal group law** over A is a power series $F \in A[[X,Y]]$ such that (commutativity) $F(X,Y) = F(Y,X)$, (identity) $F(X,0) = X$ and (associativity) $F(X, F(Y,Z)) = F(F(X,Y),Z)$. We will write $X +_F Y := F(X,Y)$. Show that inverse exists, i.e., there is a unique element $h(T) \in TA[[T]]$ such that $F(f(T), h(f(T))) = 0$ for all $f(T) \in TA[[T]]$.

   An endomorphism $f : F \to G$ between formal group laws is a power series $f \in TA[[T]]$ such that $f(X +_F Y) = f(X) +_G f(Y)$. So we can talk about the endomorphism ring $\mathrm{End}(F)$. **A formal A-module** is a formal group law F together with a injection $A \hookrightarrow \mathrm{End}(F)$.

4. Let $\mathbb{F}_q$ be the residue field of K. Let $f = \pi T + T^q \in TO_K[[T]]$[3]. Show that there is a unique formal group law F_f over O_K such that $f \in \mathrm{End}(F_f)$. It is called the **Lubin–Tate formal group law** for f. Furthermore, for every $a \in O_K$, show that there is a unique $[a]_f \in TO_K[[T]]$ such that $[a]_f = aX + O(X^2)$ and $[a]_f \circ f = f \circ [a]_f$. Then show that $[a]_f \in \mathrm{End}(F_f)$, hence there is an injection $O_K \hookrightarrow \mathrm{End}(F_f)$, making F_f a formal O_K-module.

5. Let Λ_f be the set $\mathfrak{m}O_{\overline{K}}$ equipped with the group structure $x +_{\Lambda_f} y = F_f(x,y)$. Let $\Lambda_{f,n}$ be the set of n-torsion points of Λ_f under this group structure. Let $K_{f,n} := K(\Lambda_{f,n})$. Show that $\Lambda_{f,n} \simeq O_K/\pi^n$ and $K_{f,n}$ is a totally ramified Galois extension of K of degree $(q-1)q^{n-1}$.

6. Show that the action of O_K on Λ_f induces an isomorphism $(O/\pi^n)^\times \xrightarrow{\sim} \mathrm{Gal}(K_{f,n}/K)$ (so $K_{f,n}/K$ is abelian). Deduce that $K_\pi = \bigcup_n K_{f,n}$.

[3] More generally, one can take f to be any series with $f(T) = \pi T + O(T^2)$ and $f(T) \equiv T^q \mod \pi$. But it turns out that all formal groups arising this way are isomorphic.