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

Problem set 6

Below you will find problems for problem set six. 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. A **quaternion algebra** over a field K is a central simple K-algebra of dimension 4 over K. Concretely, when $\mathrm{char}K \neq 2$, an algebra B over K is a quaternion algebra if there exist $i, j \in B$ such that $1, i, j, ij$ is a K-basis for B and

$$i^2 = a, j^2 = b, ji = -ij \tag{1}$$

for some $a, b \in K$ and we denote this quaternion algebra to be $\left(\frac{a,b}{K}\right)$. Below are some facts about quaternion algebras. Feel free to take them for granted.

1. The ring $M_2(K)$ of 2×2 matrices with coefficients in K is a quaternion algebra over K: there is an isomorphism $\left(\frac{1,1}{K}\right) \to M_2(K)$ of K-algebras induced by $i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. More generally, if $K(\sqrt{a})$ is a splitting field over K for the polynomial $x^2 - a$, then there is an injective map $\left(\frac{a,b}{K}\right) \to M_2(K(\sqrt{a}))$ of K-algebras induced by $i \mapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, j \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$.

2. The map which interchanges i and j gives an isomorphism $\left(\frac{a,b}{K}\right) \simeq \left(\frac{b,a}{K}\right)$. Similarly, one has $\left(\frac{a,b}{K}\right) \simeq \left(\frac{a,-ab}{K}\right) \simeq \left(\frac{b,-ab}{K}\right)$ by interchanging basis elements.

3. If $c, d \in K^\times$, then $\left(\frac{a,b}{K}\right) \simeq \left(\frac{ac^2,bd^2}{K}\right)$. In particular, if $K^\times/(K^\times)^2$ is finite, then there are only finitely many isomorphism classes of quaternion algebras over K, and if $K^\times = (K^\times)^2$ then there is only one isomorphism class $\left(\frac{1,1}{K}\right) \simeq M_2(K)$.

4. If $B = \left(\frac{a,b}{\mathbb{R}}\right)$ is a quaternion algebra over $\mathbb{R}$, then $B \simeq M_2(\mathbb{R})$ or $B \simeq \mathbb{H} := \left(\frac{-1,-1}{\mathbb{R}}\right)$, the latter occuring if and only if $a, b < 0$. If B is a division quaternion algebra over $\mathbb{R}$, then $B \simeq \mathbb{H}$.

5. Let L be a separable quadratic K-algebra and $b \in K^\times$. We denote by $\left(\frac{L,b}{K}\right) := L \oplus Lj$ the K-algebra with basis $1, j$ as a left L-vector space and with the multiplication rules $j^2 = b$

and $j\alpha = \bar{\alpha}j$ for $\alpha \in L$, where $^-$ is the nontrivial involution on L. If K is a nonarchimedean local field, then there is a unique (up to K-algebra isomorphism) division quaternion algebra $B \simeq \left(\frac{L,b}{K}\right)$ over K where L is the unique quadratic unramified extension of K.

6. If L is a field extension of K, then there is a canonical isomorphism $\left(\frac{a,b}{K}\right) \otimes_K L \simeq \left(\frac{a,b}{L}\right)$ extending scalars.

7. Given a quaternion algebra B over $\mathbb{Q}$, we say that a place v is ramified in B if the completion B_v is a division ring, and otherwise v is unramified or split. The map $B \mapsto \operatorname{Ram} B$ gives a bijection $\{\text{Quaternion algebras over } \mathbb{Q} \text{ up to isomorphism}\} \leftrightarrow \{\text{Finite subset of places of } \mathbb{Q} \text{ of even cardinality}\}$. This result can be generalized to global fields.

Problem 2. Consider the $j = 0$ elliptic curve $E : y^2 = x^3 + 1$ defined over $\bar{\mathbb{F}}_p$ for some prime $p \geq 5$.

1. The p-power Frobenius map Frob_p defines an endomorphism of E.

2. Let $\omega \in \bar{\mathbb{F}}_p$ be a cube root of unity, then $(x, y) \mapsto (\omega x, y)$ defines an endomorphism $[\omega]$ of E.

3. Suppose $p \equiv -1 \pmod 3$. Show that the field $\mathbb{F}_p$ does not contain cube roots of unity, i.e., the polynomial $x^2 + x + 1$ is irreducible over $\mathbb{F}_p$, then Frob_p and $[\omega]$ do not commute with each other. Conclude that E is supersingular.

Problem 3 (See Problem 6 for a generalisation)**.** Let $\mathbb{F}_q$ be a finite field with with $q = p^r$ elements with $p > 2$. Let E be an elliptic curve with Weierstrass equation

$$y^2 = f(x)$$

where $f(x) = \mathbb{F}_q[x]$ is a cubic polynomial. one can read off from the equation if E is super-singular or ordinary. More precisely, E is supersingular if and only if the coefficient of x^{p-1} (known as the *Hasse invariant*) in $f(x)^{p-1/2}$ is zero. We take this fact for granted.

1. From PSET 1 problem 7, we know that over $\overline{\mathbb{F}_q}$, we can find a λ such that E has the form $y^2 = x(x-1)(x-\lambda)$. Let $m = p = 1/2$. Define the following polynomial

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i$$

   Show that E is supersingular if and only if $H_p(\lambda) = 0$.

2. Prove that for half the primes in $\mathbb{Z}$ (that is, for $p \equiv 3 \mod 4$) the CM elliptic curve $E : y^2 = x^3 + x$ over $\overline{\mathbb{Q}}$ has supersingular reduction.

3. Let E_p denote the reduction of E mod p. Confirm the above fact by showing that that $\text{End}(E_p)$ is not commutative. In particular, show that the Frobenius endomorphism and "multiplication by i" do not commute if $p \equiv 3 \mod 4$.

Problem 4. Let $E/\mathbb{F}_q$ be an elliptic curve over the finite field with q elements. Let φ denote the Frobenius map.

1. Show that $|E(\mathbb{F}_{q^n})| = \deg(1 - \varphi^n)$.

2. Consider the map φ_l on the l-adic Tate module of E. Let α and β denote the roots of the characteristic polynomial (defined over $\mathbb{Z}$) of φ_l over $\mathbb{C}$. Show that $|\alpha| = |\beta| = \sqrt{q}$

3. Further show that $|E(\mathbb{F}_{q^n})| = 1 - \alpha^n - \beta^n + q^n$.

Problem 5 (Canonical lift)**.** Let $\mathbb{F}_q$ be a finite field, and let $\mathbb{Q}_q$ be a unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$. Denote $\mathbb{Z}_q$ the ring of integers in $\mathbb{Q}_q$. Let $E/\mathbb{F}_q$ be an elliptic curve, a **canonical lift** of E is an elliptic curve $\mathcal{E}/\mathbb{Z}_q$ with the property that 1) the reduction of $\mathcal{E}$ is E, and 2) there is an endomorphism of $\mathcal{E}$ whose reduction is the Frobenius of E. It can be shown that the canonical lift of an ordinary elliptic curve always exist, and is unique [1].

1. Show that canonical lift, if exists, must be CM.

2. Give an explicit equation for the canonical lift of $y^2 = x^3 + x$ over $\mathbb{F}_{97}$.

Intermediate

Problem 6. Let E be a CM elliptic curve over a number field K. Let $\mathfrak{p}$ be a prime of K over the prime p in $\mathbb{Q}$. Let $E_\mathfrak{p}$ denote the reduction of E mod $\mathfrak{p}$.

1. Suppose that $E_\mathfrak{p}$ is ordinary. Then show that, p has to split in K.

2. Conversely suppose p splits in K, then the reduction $E_\mathfrak{p}$ is ordinary.

3. Use Chebotarev Density Theorem to prove that if E is a CM elliptic curve over K, then for half of the primes in $\mathbb{Q}$ it has ordinary reduction.

Problem 7 (A followup problem)**.** Now for arbitrary elliptic curve E over a number field K, show that there are infinitely many places modulo which E has orindary reduction (Hint: again, you need to somehow use Chebotarev density theorem).

Problem 8 (Weil Conjectures for elliptic curves over finite fields)**.** Let E be an elliptic curve over $\mathbb{F}_q$. Define the zeta function of E to be the series

$$Z(E/\mathbb{F}_{q^n}; t) = \exp\left(\sum_{n=1}^{\infty}(|E(\mathbb{F}_{q^n})|)\frac{t^n}{n}\right)$$

1. (Rationality and Factorization and the Riemann Hypothesis) Use problem 4 to prove that

$$Z(E/\mathbb{F}_q; t) = \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-qt)} \in \mathbb{Q}(t)$$

with $|\alpha| = |\beta| = \sqrt{q}$.

2. (Functional equation) Do the transformation $t \to 1/qt$ to get a functional equation for the zeta function:

$$Z(E/\mathbb{F}_q; 1/qt) = Z(E/\mathbb{F}_q; t)$$

Problem 9. Let E be a supersingular elliptic curve over a field F with $\mathrm{char}F = p > 0$, then $\mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. Hint: For $l \neq p$, consider $\mathrm{End}(E) \otimes \mathbb{Q}_l \hookrightarrow \mathrm{End}(T_l(E)) \otimes \mathbb{Q}_l \simeq M_2(\mathbb{Q}_l)$.

[1] This can be done using Serre–Tate deformation theory. Though in practice, it is not easy to compute an explicit equation for the canonical lift.

Advanced

Problem 10. Let k, K be fields. A **K-coefficient cohomology theory** for smooth proper k-varieties is a functor from the category of smooth proper k-varieties to graded K-vector spaces. Such a functor is denoted by H. Taking the n-th graded piece of $H(X)$ gives you n-th cohomology of X, denoted $H^n(X)$. For example, when $k = \mathbb{C}$ and $K = \mathbb{Q}$, the $\mathbb{Q}$-coefficient singular cohomology is a cohomology theory. If $K = \mathbb{C}$, then de Rham (Doubault) cohomology is a cohomology theory.

A good cohomology theory (Weil cohomology theory) is a cohomology theory satisfying certain properties, like excision, Kunneth formula, etc. We don't need a precise notion of this. Just note that singular cohomology and de Rham cohomology are all good cohomology theories.

In the follwing, we fix a prime p and a field k of characteristic p. For each $l \neq p$, there is a good $\mathbb{Q}_l$-coefficient cohomology theory H_l for smooth proper k-varieties, namely, the l-adic étale cohomology. For an elliptic curve E, $H^1_l(E)$ is basically the rational Tate module. More precisely, the l-adic rational Tate module $V_l(E)$ of an elliptic curve E, as a Galois representation, is canonically isomorphic to $H^1_l(E)^\vee$.

What happens when $l = p$? Does there exist a good $\mathbb{Q}_p$-coefficient cohomology theory H_p? Such a cohomology theory, if exists, should satisfy

$$\dim_{\mathbb{Q}_p} H^n_p(X) = \dim_{\mathbb{Q}_l} H^n_l(X)$$

for any smooth proper k-variety X and any integer n.

1. It turns out that p-adic étale cohomology is not a good $\mathbb{Q}_p$-coefficient cohomology theory. Justify this by taking an elliptic curve E and consider its p-adic Tate module $V_p(E)$. You may assume the fact that the first p-adic étale cohomology of E is canonically dual to $V_p(E)$.

2. Show that good $\mathbb{Q}_p$-coefficient cohomology theory does not exist. (Hint: suppose it exists, take a supersingular elliptic curve E and study $H^1_p(E)$, use the functorial property of H_p to deduce a countradiction.)

3. Later on, Grothendieck, Barthlott, Illusie and various other people constructed a good K-coefficient cohomology theory for some p-adic field K. It is called the **crystalline cohomology**. However, the coefficient field K usually depends on k, and is some very large field extension of $\mathbb{Q}_p$.