PAWS 2023 – Elliptic Curves with Complex Multiplication

Problem set 1

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. Let (E, O) be an elliptic curve defined over an algebraically closed field K. A Weierstrass equation embeds E in $\mathbb{P}^2$. Let $P, Q \in E(K)$.

(a) Let L be the line connecting P and Q (tangent line to E if $P = Q$), and R the third point of intersection of L with E. Let L' be the line connecting R and O. Explain why the third point of intersection of L' with E is $P + Q$, where $+$ is the group law induced from $E(\bar{K}) \simeq \mathrm{Pic}^0(E)$.

(b) Describe a geometric way to find $-P$.

(c) Suppose E is defined by the Weierstrass equation

$$y^2 = x^3 + 17$$

and $P = (-1, 4), Q = (2, 5)$. Compute $P + Q$.

Problem 2. Prove that isogeny is an equivalence relation. Then prove that given an elliptic curve X, there are countably many curves X' isogenous to it.

Problem 3. Let K be a field of characteristic 0 and let E be the elliptic curve defined by the Weierstrass equation

$$y^2 = x^3 + x.$$

Find an endomorphism $\phi_i \in \mathrm{End}(E_{\bar{K}})$ such that $\phi_i \circ \phi_i$ is the multiplication by -1 map. In particular, conclude that E has complex multiplication.

Problem 4. (Automorphisms of an elliptic curve) For this problem, we require that the char $K \neq 2, 3$. Let E be an elliptic curve over a field K given by the equation

$$y^2 = x^3 + ax + b \tag{1}$$

(a) Let $a = 0$ and $b = 2$. Write down the automorphisms of the elliptic curve over $\overline{K}$

(b) Let $a = 3$ and $b = 0$. Write down the automorphisms of E over $\overline{K}$

(c) What are the automorphisms of an elliptic curve given by the equation (1) in the case $ab \neq 0$.

(d) Conclude that the order of the automorphism group of an elliptic curve as given above divides 24. In particular, it is finite.[1]

Problem 5. Let E be an elliptic curve over a field K of characteristic 0 or p. Let l be a prime (For the latter case, $l \neq p$). Let φ be an endomorphism of E.

(a) Show that φ induces an endomorphism of $E[l^n]$, the l^n torsion of E, for all $n \geq 1$.

(b) Deduce from (a), that $\varphi = (\varphi_n)_{n\geq 1}$ where each φ_n is a 2×2 matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/l^n\mathbb{Z})$$

(c) Further show that if $y_1, y_2, \dots y_n \dots$ such that y_n is an l^n-torsion point for each $n \geq 1$. Further, $y_n \equiv y_{n-1} \mod l^{n-1}$ then any φ preserves the relation of this system. Can you write the relation in terms of φ_n?

(d) Deduce that φ_n can be written as an element of $M_2(\mathbb{Z}_l)$. Moreover, use this to show that φ satisfies a monic polynomial with coefficients in $\mathbb{Z}_l$.

(e) In fact the determinant and the trace of this matrix is given by the degree of φ. See Proposition V.2.3 in Silverman's Arithmetic of elliptic Curves. In particular, this shows that the characteristic polynomial of φ is in fact defined over $\mathbb{Z}$.

Intermediate

Problem 6. Consider the elliptic curve

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

The same proof as in 3 shows that $\mathbb{Z}[i] \subset \mathrm{End}(E)$. In particular $1 + i \in \mathrm{End}(E)$. Show that the map $1 + i$ on $E(\mathbb{Q}(i))$, that is the $\mathbb{Q}(i)$-rational points of E, is not surjective.

HINT: Consider the multiplication by 2 map $[2] = [(1 + i)(1 - i)]$. Show that it is enough to show $[2]$ is not surjective on $\mathbb{Q}(i)$-rational points and then prove that.

Problem 7. Let (E, O) be an elliptic curve over an algebraically closed field K with $\mathrm{char} K \neq 2$.

(a) Use Riemann-Roch to show that the divisor $(2O)$ on E defines a morphism $f : E \to \mathbb{P}^1$ of degree 2.

(b) Show that f is ramified at exactly four points, with O being one of them.

(c) Show that if P_1, P_2, P_3 are three distinct points of $\mathbb{P}^1$, then there exists a unique automorphism φ of $\mathbb{P}^1$ such that $\varphi(P_1) = \infty, \varphi(P_2) = 0, \varphi(P_3) = 1$. Thus, if a, b, c are the three branch points in $\mathbb{P}^1$ besides ∞, then there is a unique automorphism of $\mathbb{P}^1$ leaving ∞ fixed and sending a to 0 and b to 1, and we may assume that f is branched over the points $0, 1, \lambda, \infty$ of $\mathbb{P}^1$.

[1] This is true even in char 2, 3 but requires more effort to prove since we cannot assume the existance of an equation of form given in 1. See Arithmetic of elliptic curves, Apppendix A pg 410 for a proof.

(d) Let the symmetric group Σ_3 act on $K\backslash\{0,1\}$ as follows: given $\lambda \in K\backslash\{0,1\}$, permute the numbers $0, 1, \lambda$ according to $\sigma \in \Sigma_3$, then apply a linear transformation α of $\mathbb{P}^1$ that fixes infinity and sends the first two back to $0, 1$, and let $\alpha(\sigma(\lambda))$ be the image of the third. Show that the possibilities for the orbit of λ, that is $\alpha(\sigma(\lambda))$ consists of $\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}$.

(e) Conclude that there is a correspondence between the set of isomorphism classes of elliptic curves over K, and $K\backslash\{0,1\}$ modulo the action of Σ_3 described above.

Problem 8. (See problem 5 as well) For an elliptic curve E over a field K of characteristic 0 (or p). Define its Tate module to be the inverse limit (for a prime $l \neq p$)

$$E[l^\infty] = \varprojlim_n E[l^n](\overline{K})$$

For two elliptic curves, E_1 and E_2 prove that there exists an injective map of groups

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(E_1[l^\infty], E_2[l^\infty])$$

Problem 9. Let E be an elliptic curve over $\mathbb{C}$ and let $n \geq 1$. We can view E^n as a variety with a group structure respecting the product structure (such a geometric object is an example of an **abelian variety**). Describe the endomorphism ring of E^n. Show that even though E only admits finitely many automorphisms, E^n has infinitely many automorphisms when $n \geq 2$.

Advanced

Problem 10. Show that any étale cover of an elliptic curve is an elliptic curve. Moreover, show that an elliptic curve admits an étale cover of arbitrarily high degree. If you don't remember what étale is, that's OK. Try to use Riemann-Hurwitz Theorem from problem set zero to see what unramified covers of elliptic curves look like.

Definition 1. (Hodge structures)

1. A pure $\mathbb{Z}$-Hodge structure of weight n is a $\mathbb{Z}$-lattice $H_{\mathbb{Z}}$ that admits a Hodge decomposition

$$H_{\mathbb{Z}} \otimes \mathbb{C} = \bigoplus_{p+q=n} H^{p,q}, \tag{2}$$

where each $H^{p,q}$ is a $\mathbb{C}$-vector space satisfying $H^{p,q} = \overline{H^{q,p}}$. A morphism of pure Hodge structures of weight n is a morphism of $\mathbb{Z}$-lattices which respects the Hodge decomposition. Therefore, we have a notion of **the category of pure Hodge structures of weight** n

2. A pure hodge structure of signature $(0,1)+(1,0)$ is a rank two $\mathbb{Z}$-lattice $H_{\mathbb{Z}}$ such that $H_{\mathbb{Z}} \otimes \mathbb{C}$ admits a Hodge decomposition $H_{\mathbb{Z}} \otimes \mathbb{C} = H^{0,1} \oplus H^{1,0}$, where $H^{0,1}, H^{1,0}$ are mutually conjugate $\mathbb{C}$-subspaces. A morphism of two such hodge structure is a morphism of $\mathbb{Z}$-lattices respecting this structure.

The following problem requires some knowledge of parametrization of elliptic curves over $\mathbb{C}$.

Problem 11 (Torelli theorem for elliptic curves)**.** Show that a pure Hodge structure $H_{\mathbb{Z}}$ of signature $(0,1)+(1,0)$ as defined above is equivalent to a complex structure[2] of $H_{\mathbb{Z}} \otimes \mathbb{R}$, which is equivalent to the data of rank 2 full lattices in $\mathbb{C}$. Use this to show that the category of pure Hodge structures of signature $(0,1)+(1,0)$ is equivalent to the category of elliptic curves defined over $\mathbb{C}$. What can you say about the Hodge structures that correspond to CM elliptic curves ?

[2] Recall that a complex structure on a real vector space V is an $\mathbb{R}$-linear map J of V such that $J^2 = -1$

Problem 12 (Reduction of elliptic curves and S-integrality)**.** Let $E : y^2 = x^3 + bx + c$ be an elliptic curve over $\mathbb{Q}$ with $b, c \in \mathbb{Z}$. Define a $\mathbb{Z}$-scheme

$$\mathcal{E}/\operatorname{Spec}(\mathbb{Z}) := \operatorname{Proj}\left(\frac{\mathbb{Z}[x:y:z]}{y^2z - (x^3 + bxz^2 + cz^3)}\right).$$

We call $\mathcal{E}$ an **integral model** of E. The mod p reduction of $\mathcal{E}$ is the $\mathbb{F}_p$-scheme $\mathcal{E} \times_{\operatorname{Spec}(\mathbb{Z})} \operatorname{Spec}(\mathbb{F}_p)$, denoted by $\mathcal{E}_{\mathbb{F}_p}$. We say that $\mathcal{E}$ has **good reduction** at p, if $\mathcal{E}_{\mathbb{F}_p}$ is an elliptic curve.

1. Show that for all but finitely many primes $p \in \mathbb{Z}$, $\mathcal{E}$ has good reduction. Can you find b, c such that $\mathcal{E}$ has good reduction at every prime?

2. Let $K/\mathbb{Q}$ be a finite extension, show that any K point $x \in E(K)$ extends uniquely to an O_K-point of $\mathcal{E}$. Therefore we can talk about the reduction $x_{\mathfrak{p}}$ of x over a prime $\mathfrak{p}$ of O_K. Note that when $\mathfrak{p}|p$, $x_{\mathfrak{p}}$ is an $\mathbb{F}_{\mathfrak{p}}$-point of $\mathcal{E}_{\mathbb{F}_p}$.

3. Let $x, y \in E(K)$. Define $I_K(x, y)$ to be the set of primes $\mathfrak{p}$ in O_K such that $x_{\mathfrak{p}} = y_{\mathfrak{p}}$. Show that if $x \neq y$, then $I_K(x, y) < \infty$. If F/K is a finite extension, then one can naturally view x, y as points in $E(F)$. What is the relation between $I_K(x, y)$ and $I_F(x, y)$?

4. Let $x, y \in E(\overline{\mathbb{Q}})$. For a finite set S of primes $p \in \mathbb{Z}$, we say that x is S-**integral** to y, if there exists a finite extension $K/\mathbb{Q}$ such that $x, y \in E(K)$, and $I_K(x, y)$ consists of primes that only lie above primes in S. Convince yourself that the notion of S-integrality doesn't depend on the choice of K. Show that if x is a point of $E(\overline{\mathbb{Q}})_{\text{tors}}$, i.e., the torsion subgroup of $E(\overline{\mathbb{Q}})$, then there exists a finite set S with the property that infinitely many points in $E(\overline{\mathbb{Q}})_{\text{tors}}$ are S-integral to x.

5. However, if $x \in E(\overline{\mathbb{Q}}) - E(\overline{\mathbb{Q}})_{\text{tors}}$, then for any finite set S, there are only finitely many points in $E(\overline{\mathbb{Q}})_{\text{tors}}$ which are S-integral to x. This is a deep result by Baker–Ih–Ramely (cf. arXiv.0509485).