

ABELIAN VARIETIES OVER FINITE FIELDS: PROBLEM SET 6

SANTIAGO ARANGO-PIÑEROS, SEOKHYUN CHOI, ALICE LIN, YUXIN LIN,
AND MINGJIA ZHANG

Instructions: The goal of this problem set is to understand the proof of Honda–Tate theory and to see some applications. Problems marked (\star) , $(\star\star)$, and $(\star\star\star)$ denote beginner, intermediate, and advanced problems, respectively.

Notation: As customary, p will be a prime, and q will be a power of p .

Let E be an elliptic curve over \mathbb{F}_q . By the Honda–Tate theorem, E corresponds to a q -Weil number α_1 , whose conjugacy class is completely determined by its trace $a = \alpha_1 + \bar{\alpha}_1 \in [-2\sqrt{q}, 2\sqrt{q}] \cap \mathbb{Z}$. In the following problems, we will characterize the possible traces that appear in the image of the Honda–Tate map. Good complementary references are [EVdGM12], [Wat69], [Ser20], [Bao’s notes](#), and [Papikian’s notes](#).

First, we consider the case of ordinary elliptic curves.

Problem 1 $(\star\star)$

Let $q = p^n$. Let E be an elliptic curve over \mathbb{F}_q and let $a = \text{tr}(\phi_q) = \alpha_1 + \bar{\alpha}_1$ be the trace of the q -Frobenius. Show that the following are equivalent.

- (1) E is ordinary,
- (2) $\gcd(a, q) = 1$, and
- (3) $K := \mathbb{Q}(\alpha_1)$ is an imaginary quadratic field over which p splits.

If this is the case, show that $\alpha_1 \mathcal{O}_K = \mathfrak{p}^n$ for a prime ideal \mathfrak{p} .

The following problem makes use of the theory of complex multiplication of elliptic curves. Good complementary references are [Sil94, Chapter II], and Li’s PAWS lecture notes; especially [Lecture 5](#).

Problem 2 $(\star\star)$

Let $a \in \mathbb{Z}$ lie in the interval $|a| \leq 2\sqrt{q}$. Assume that $\gcd(a, q) = 1$. In this problem, we will provide a roadmap to prove^a that there exists an ordinary elliptic curve E defined over \mathbb{F}_q such that the trace of the Frobenius endomorphism $\phi_q: E \rightarrow E$ is equal to a .

- (1) Let $P(t) = T^2 - aT + q = (T - \alpha)(T - \bar{\alpha})$. Denote by K the number field generated by $P(T)$. Show that $K = \mathbb{Q}(\alpha)$ is quadratic imaginary, and that p splits in K .
- (2) Consider the ring of integers \mathcal{O}_K of K as a lattice in \mathbb{C} . Define the complex elliptic curve \mathbb{C}/\mathcal{O}_K , and argue that $\text{End}(\mathbb{C}/\mathcal{O}_K) \cong \mathcal{O}_K$ has complex multiplication.
- (3) From the theory of complex multiplication, we know that there exists a number field H and an elliptic curve \tilde{E} defined over H , such that $\tilde{E}_{\mathbb{C}} \cong \mathbb{C}/\mathcal{O}_K$.

- (4) For any place $w \mid p$ of H , consider \tilde{E} over the local field H_w . The fact that $j(\tilde{E})$ is an algebraic integer implies that \tilde{E} has potentially good reduction at w . Thus, there exists some finite extension H'_w/H_w such that $\tilde{E}_{H'_w}$ has good reduction. Use [Sil09, VII.5.4] to show there exists some intermediate local field $H_w \subset F_w \subset H'_w$ such that H'_w/F_w is unramified, and F_w/H_w is totally ramified, to conclude that \tilde{E}_{F_w} also has good reduction.
- (5) Let E be the reduction of \tilde{E}/F_w modulo the prime. Then E is defined over $k(w)$, which is the residue field of H_w at w . Let v be the restriction of w to K . Let \mathfrak{p} be the prime in K above p corresponding to v . Let $\text{Cl}(K)$ denote the class group of K and $\text{Frob}_{\mathfrak{p}}$ be the element in $\text{Gal}(H/K)$ corresponding to the prime ideal^b \mathfrak{p} . Use Problem 1 part (3), show that the order of $\text{Frob}_{\mathfrak{p}}$ in $\text{Cl}(K)$ divides n . Conclude that $[k(w) : k(v)] \mid n$ and that $k(w) \subseteq \mathbb{F}_q$. Consequently, E is defined over \mathbb{F}_q .
- (6) Reducing the curve \tilde{E}/K_w at w yields an ordinary elliptic curve E defined over \mathbb{F}_q . The map $\text{End}(\tilde{E}_{K_w}) \rightarrow \text{End}(E)$ is injective and preserves degrees [Sil94, II, Proposition 4.4]. Verify that α maps to the q -Frobenius endomorphism of E .

^aWithout appealing to the Honda–Tate theorem.

^bWe have $\text{Gal}(k(w)/k(v)) \cong \text{Gal}(H_w/K_v) \hookrightarrow \text{Gal}(H/K)$. $\text{Frob}_{\mathfrak{p}}$ is the image of the Frobenius in $\text{Gal}(k(w)/k(v))$. Under the isomorphism $\text{Gal}(H/K) \cong \text{Cl}(K)$, $\text{Frob}_{\mathfrak{p}}$ goes to \mathfrak{p} .

Next, we move on to the supersingular case. We first classify the $a \in \mathbb{Z}$ such that can possibly arises as trace of the Frobenius for a supersingular elliptic curve E/\mathbb{F}_q .

Problem 3 (★★)

Let $q = p^n$. Let E be an elliptic curve over \mathbb{F}_q and let $a = \text{tr}(\phi_q) = \alpha_1 + \bar{\alpha}_1$ be the trace of the q -Frobenius. Suppose E is supersingular, and denote let $K = \mathbb{Q}(\alpha_1)$. Show that there are only three possibilities for a :

- (1) $K = \mathbb{Q}$ and $\alpha_1 = \pm p^{n/2}$ where n is even. In this case, show that $a = 2\sqrt{q}$.
- (2) K is an imaginary quadratic field, p ramifies in K as $p\mathcal{O}_K = \mathfrak{p}^2$, and $\alpha_1\mathcal{O}_K = \mathfrak{p}^n$. In this case, show that:
 - (a) n is odd and $a = 0$,
 - (b) n is even, $p = 2$, and $a = 0$,
 - (c) n is even, $p = 3$, and $a = \pm\sqrt{q}$,
 - (d) n is odd, $p = 2$, and $a = \sqrt{2q}$,
 - (e) n is odd, $p = 3$, and $a = \sqrt{3q}$.
- (3) K is an imaginary quadratic field, p is inert in K , and $\alpha_1\mathcal{O}_K = \mathfrak{p}^{n/2}$ where n is even. In this case, show that:
 - (a) n is even, $p \equiv 3 \pmod{4}$, and $a = 0$,
 - (b) n is even, $p \equiv 2 \pmod{3}$, and $a = \pm\sqrt{q}$.

Next, we construct corresponding supersingular elliptic curve for the a in Problem 3.

Problem 4 (★★)

In this problem, we construct a supersingular elliptic curve defined over \mathbb{F}_q where the characteristic polynomial of ϕ_q is equal to $T^2 - aT + q$, for each a in the list of Problem 3.

- (1) Suppose $a < 2\sqrt{q}$. Let α be a root of $T^2 - aT + q$. Let $K := \mathbb{Q}(\alpha)$. Since $a < 2\sqrt{q}$, we know that K is a quadratic imaginary extension over \mathbb{Q} . Furthermore, p either ramifies or is inert in K . Let v be the valuation on K corresponding to the unique prime \mathfrak{p} in K above p . Let H be the Hilbert class field of K and let w be a place of H above v .
 - (a) Follow the construction in part (1) \rightarrow (5) in Problem 2, obtain an elliptic curve \tilde{E}/F_w , where F_w is some totally ramified extension of H_w , and \tilde{E}/F_w has good reduction at w .
 - (b) Let E be the reduction of \tilde{E}/F_w modulo the prime. Follow the same argument as in part (5) of Problem 2, use the results in Problem 3 part (2) and (3), show that the order of $\text{Frob}_{\mathfrak{p}}$ in $\text{Cl}(K)$ divides n . Conclude that $[k(w) : k(v)] \mid n$ and that $k(w) \subseteq \mathbb{F}_q$. Consequently, E is defined over \mathbb{F}_q .
 - (c) Let ϕ_q be the Frobenius endomorphism of E/\mathbb{F}_q . Show that $\mathbb{Q}(\phi_q) \subseteq K$. Use PSET2, Problem 9, show that if $\mathbb{Q}(\phi_q) = \mathbb{Q}$, then E/\mathbb{F}_q must be supersingular.
 - (d) Now suppose $\mathbb{Q}(\phi_q) = K$. Then we know that p is ramified or inert in $\mathbb{Q}(\phi_q)$. Deduce that in this case E/\mathbb{F}_q is supersingular as well.
 - (e) Show that in both cases, we have $(\phi_q) = (\alpha)$ or $(\bar{\alpha})$ as ideal in K . From the fact that K is a quadratic imaginary field, conclude that $\zeta\phi_q = \alpha$ or $\zeta\bar{\alpha}$, where ζ is a root of unity of order 1, 2, 3, 4, 6.
 - (f) Suppose $\zeta\phi_q = \alpha$. We want to find E'/\mathbb{F}_q supersingular such that $\pi_{E'} = \alpha$ or $\bar{\alpha}$. Let E_{ζ}/\mathbb{F}_q be the twist of E by ζ^a . It has the property that if for the ℓ -adic Galois representation of E , $\rho : \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \rightarrow V_{\ell}(E)$, $\rho(\text{Frob}_q)$ has eigenvalues $\alpha, \bar{\alpha}$, then the ℓ -adic Galois representation of E_{ζ} , $\rho : \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \rightarrow V_{\ell}(E_{\zeta})$ has eigenvalues $\zeta\alpha, \zeta^{-1}\bar{\alpha}$. Show that for this E_{ζ} , $\pi_{E_{\zeta}} = \alpha$ or $\bar{\alpha}$, and hence E_{ζ} is supersingular. This finishes the construction of a supersingular elliptic curve E/\mathbb{F}_q whose trace is equal to the a that we started with.
- (2) Now suppose $a = 2\sqrt{q}$, in which case n is even, and $\pi = \pm q^{\frac{n}{2}}$.
 - (a) Apply the above construction to $a = 0$ and $q = p$, obtain a supersingular elliptic curve E/\mathbb{F}_p such that $\phi_q = \pm i\sqrt{p}$.
 - (b) Let E/\mathbb{F}_q be the base extension of E to \mathbb{F}_q . Show that $\phi_q = \pm i^{\frac{n}{2}} p^{\frac{n}{2}}$. Then choose a twist E_{ζ} such that $\pi_{E_{\zeta}} = p^{\frac{n}{2}}$.

^aFor the existence of this twist, see [Bao, page 4-5].

Now we can characterize the q -Weil numbers that appear as the image of isogeny classes of elliptic curves under the Honda-Tate map. We say that a q -Weil number α is **elliptic** if $\mathbb{Q}(\alpha) = \mathbb{Q}$ or $\mathbb{Q}(\alpha)$ is an imaginary quadratic field and there is only one finite place where α has a positive valuation.

Problem 5 (★)

Let α be a q -Weil number. Conclude from the problems above that α is elliptic if and only if α is an image of an isogeny class of elliptic curves under the Honda-Tate map.

The next problem is an application of Honda-Tate theory to a conjecture of Manin about Newton polygons.

Problem 6 (★)

Fix a prime p . In [Man63, Conj. 2, p.76], Manin conjectured that for any admissible^a Newton polygon \mathcal{N} , there exists an abelian variety A defined over a field of characteristic p such that $\mathcal{N}(A) = \mathcal{N}$.

We can prove this conjecture using Honda-Tate theory.

- (1) Any Newton polygon of total length h can be written as the sum of h line segments, each written in the form (c, d) where $\gcd(c, d) = 1$, indicating a slope of $c/(c + d)$. So an admissible Newton polygon can be written as

$$\mathcal{N} = t \cdot ((1, 0) + (0, 1)) + s \cdot (1, 1) + \sum_i ((d_i, c_i) + (c_i, d_i))$$

for $t, s \in \mathbb{Z}_{\geq 0}$. Verify that it suffices to show that there exist abelian varieties A, A' such that $\mathcal{N}(A) = (1, 0) + (0, 1)$ and $\mathcal{N}(A') = (1, 1)$, and for any (c, d) relatively prime, there exists $A_{c,d}$ such that $\mathcal{N}(A_{c,d}) = (c, d) + (d, c)$.

- (2) Let E be an elliptic curve over the finite field \mathbb{F}_{p^n} . Use the characteristic polynomial of the p^n -Frobenius to determine what the possible Newton polygons are.^b
- (3) Suppose we want to find an abelian variety A whose Newton polygon is of the form $(d, c) + (c, d)$ where c, d are coprime integers with $d > c > 0$. Write down a quadratic polynomial whose roots are p^{c+d} -Weil numbers and have p -adic valuation c and d . By Honda-Tate theory, this Galois-conjugacy class of p^{c+d} -Weil numbers corresponds to a simple abelian variety A over $\mathbb{F}_{p^{c+d}}$.
- (4) Let F denote the splitting field of the quadratic polynomial from part (3). Use F and Theorem 12.9 (main theorem) in the lecture notes to compute the invariants $\text{inv}_v(D)$ of $D := \text{End}_{\mathbb{F}_{p^{c+d}}}^0(A)$.
- (5) For any number field F , the following exact sequence holds.^c

$$0 \rightarrow \text{Br}(F) \rightarrow \bigoplus_{v \in M_F} \text{Br}(F_v) \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$$

where the direct sum is over all finite and infinite places of F . F_v denotes the completion with respect to the place v . The first map is given by extension of scalars, and the second map is given by summing the invariants. Recall that for local fields F_v , $\text{inv}_v : \text{Br}(F_v) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$. Use this exact sequence to check

- that an element $[D] \in \text{Br}(F)$ is uniquely determined by $\text{inv}_v(D)$ for all $v \in M_F$, and
- that the order of an element of $\text{Br}(F)$ is the least common multiple of the denominators in its image in $\bigoplus_{v \in M_F} \text{Br}(F_v) \xrightarrow[\sim]{\oplus_v \text{inv}_v} \bigoplus_{v \in M_F} \mathbb{Q}/\mathbb{Z}$.

- (6) For a central division algebra D over a number field F , the order of $[D]$ in $\text{Br}(F)$ is $\sqrt{[D:F]}$.^d Combine this fact with parts (4) and (5) to compute $[D:F]$ for $D = \text{End}_{\mathbb{F}_{p^{c+d}}}^0(A)$.
- (7) Use Theorem 12.9 from the lecture notes to determine $\dim A$.
- (8) Let $n = c + d$. Let $h_A(T)$ be the minimal polynomial of the p^n -Weil number from part (3) above. Use the fact that $P_A(T) = h_A(T)^e$ for $e = \sqrt{[D:F]}$ to check that the Newton polygon $\mathcal{N}(A)$ is indeed length $2n$ of the form $n((d, c) + (c, d))$.

^aAdmissible Newton polygons are defined in Problem 2 on PSET 5.

^bHint: Consider the ordinary and supersingular cases separately.

^cSee Theorem 3.5 of [these notes](#) for more explanation about Brauer groups over global fields.

^dSee Theorem 3.6 of [these notes](#).

The following exercise, due to Bjorn Poonen [[Poo06](#), Problem 4.10], will apply Honda-Tate theory to understand ordinary abelian varieties. In particular, in the ordinary case we have that the isogeny class of A is in 1-1 correspondence with the Frobenius polynomial $P_A(T)$.

We say that a g -dimensional abelian variety A/\mathbb{F}_q is **ordinary** if half of the zeros of $P_A(T)$ in $\bar{\mathbb{Q}}_p$ are p -adic units, and the other half have q -valuation¹ 1.

Problem 7 (★)

Let A be a simple ordinary abelian variety over \mathbb{F}_q . Write the characteristic polynomial of Frobenius as $P_A(T) = h_A(T)^e$, where $h_A(T) \in \mathbb{Z}[T]$ is the (irreducible) minimal polynomial of the corresponding q -Weil number.

- (1) Show that $h_A(T)$ has no real zeros.^a
- (2) Prove that $e = 1$.^b

^aHint: Use Problem 8 on PSET 4.

^bHint: Use the facts relating order and dimension of division algebras in Brauer groups from Problem 6.

We say that A/\mathbb{F}_q is **supersingular** if all the zeros of $P_A(T)$ in $\bar{\mathbb{Q}}_p$ have q -valuation $1/2$.

Problem 8 (★★)

Let A be a g -dimensional abelian variety defined over \mathbb{F}_q , with Frobenius eigenvalues $\alpha_1, \dots, \alpha_{2g} \in \mathbb{C}$. For $j = 1, \dots, 2g$, let $u_j := \alpha_j / \sqrt{q} \in \mathbf{S}^1 = \{u \in \mathbb{C} : |u| = 1\} \subset \mathbb{C}^\times$ be the corresponding **normalized eigenvalues**. Define the **angle group** of A to be the subgroup $U_A \subset \mathbf{S}^1$ generated by the normalized Frobenius eigenvalues of A , and define the **angle rank** δ_A of A to be the rank of the finitely generated abelian group U_A .

- (1) Show that $\delta_A \in \{0, 1, 2, \dots, g\}$.
- (2) Show that if $g = 1$, A is ordinary if and only if $\delta_A = 1$. Conclude that A is supersingular if and only if u_1 is a root of unity.
- (3) Show that A/\mathbb{F}_q is supersingular if and only if $\delta_A = 0$.

¹See PSET 5, Problem 2 to recall the definition of the q -valuation.

- (4) The angle rank of A/\mathbb{F}_q is invariant under base change: for any integer $r \geq 1$, we have that $\delta_A = \delta_{A_{\mathbb{F}_{q^r}}}$.
- (5) Suppose that A/\mathbb{F}_q is a geometrically simple and ordinary abelian surface. Show that $\delta_A = 2$.
- (6) Does every geometrically simple ordinary abelian variety have maximal angle rank?

In the following problem, we look at an example of an abelian variety defined over local field with dimension ≥ 2 , and we use Shimura-Taniyama formula to see that its reduction is a supersingular abelian variety.

Problem 9 (*)**

Consider the planar curve over \mathbb{Q} with affine equation given by $\tilde{C} : y^7 = x^2(x-1)^3$ and let C denote its normalization. Then C is a smooth projective curve defined over \mathbb{Q} .

- (1) Show that μ_7 acts on \tilde{C} by automorphism $(x, y) \rightarrow (x, \zeta_7 y)$. It extends to an action of μ_7 on C .
- (2) Let A denote the Jacobian of C . Then A is defined over \mathbb{Q} . Show that $\text{End}^0(A_{\overline{\mathbb{Q}}})$ contains the group algebra $\mathbb{Q}[\mu_7]$. Notice that it is a **CM field** with degree 6 over \mathbb{Q} .
- (3) Let $T := \text{Hom}(\mu_7, \mathbb{C})$. Show that $\mathbb{Q}[\mu_7] \otimes_{\mathbb{Q}} \mathbb{C} \cong \prod_{\tau \in T} \mathbb{C}_{\tau}$, where \mathbb{C}_{τ} is a copy of \mathbb{C} indexed by τ , with the action of ζ_7 given as $\zeta_7 \cdot v = \tau(\zeta_7)v$.
- (4) Let V denote the $2g$ -dimensional \mathbb{Q} -vector space $H^1(A, \mathbb{Q})$ where $g = \dim(A)$. Since V admits an action of $\mathbb{Q}[\mu_7]$, $V \otimes_{\mathbb{Q}} \mathbb{C} \cong \bigoplus_{\tau \in T} V_{\tau}$, where V_{τ} is the subspace of $V_{\mathbb{C}}$ such that ζ_7 acts by $\tau(\zeta_7)$. It turns out that $\dim_{\mathbb{C}} V_{\tau} = 1$. Using this fact, show that $A_{\overline{\mathbb{Q}}}$ admits complex multiplication by $K = \mathbb{Q}[\zeta_7]$.
- (5) On the other hand, the **Hodge decomposition** gives $V \otimes_{\mathbb{Q}} \mathbb{C} \cong H^1(A, \mathcal{O}_A) \oplus H^0(A, \Omega_A) \cong \text{Lie}(A_{\mathbb{C}}) \oplus \overline{\text{Lie}(A_{\mathbb{C}})}$, where $\overline{\text{Lie}(A_{\mathbb{C}})} \cong \text{Lie}(A_{\mathbb{C}})$ as an \mathbb{R} vector space, while $\sqrt{-1}$ acts via i on $\text{Lie}(A_{\mathbb{C}})$ and $-i$ on $\overline{\text{Lie}(A_{\mathbb{C}})}$. Let $\Phi := \{\tau \in T : V_{\tau} \subseteq \text{Lie}(A_{\mathbb{C}})\}$. Show that Φ is a CM type, and $A_{\overline{\mathbb{Q}}}$ has CM type (K, Φ) .
- (6) Now fix a prime $p \neq 7$ such that p is inert in K . Show that $\mathbb{Q}_p \otimes_{\mathbb{Q}} K \cong K_{\mathfrak{p}}$, where \mathfrak{p} is the unique prime in K above p and $K_{\mathfrak{p}}$ is the completion of K at \mathfrak{p} .
- (7) Notice that since the endomorphisms in $\mathbb{Q}[\mu_7]$ are defined over K , A_K already has complex multiplication by K . As a consequence of A having complex multiplication by K and $p \nmid 7$, A has a model over $\mathcal{O}_{K_{\mathfrak{p}}}$ which has good reduction at the prime \mathfrak{p} . Let $A_{\mathbb{F}_q}$ denotes the reduction at \mathfrak{p} , we have the injections:

$$K_{\mathfrak{p}} \hookrightarrow \text{End}^0(A_K) \otimes_{\mathbb{Q}} \mathbb{Q}_p \hookrightarrow \text{End}^0(A_{\mathbb{F}_q}) \otimes_{\mathbb{Q}} \mathbb{Q}_p \hookrightarrow \text{End}^0(\mathbb{D}(A_{\mathbb{F}_q}[p^{\infty}]))$$

Using the fact that $A_{\mathbb{F}_q}[p^{\infty}]$ is a p -divisible group of height $2g$, show $\text{End}^0(\mathbb{D}(A_{\mathbb{F}_q}[p^{\infty}])) \cong D_{p, 2g, m} = \mathbb{Q}_{p^{2g}}[F]/(F^{2g} - p^m)$ for some $0 \leq m < 2g$. We say that $A_{\mathbb{F}_q}[p^{\infty}]$ is **isoclinic**.

- (8) Using the **Shimura-Taniyama formula** as stated in Lemma 12.7 in the lecture notes, and the fact that $\pi_{A_{\mathbb{F}_q}}$ goes to F in $\mathbb{D}(A_{\mathbb{F}_q}[p^{\infty}])$, show that $m = g$.^a

^aIn this case, the Newton polygon of $A_{\mathbb{F}_q}$ has only slope $\frac{1}{2}$. Hence $A_{\mathbb{F}_q}$ is supersingular.

In the following problems, we sketch the proof of the following key input (Theorem 12.6 in the lecture notes) to the surjectivity part of Honda-Tate theorem. More details can be found [here](#). Below \mathbb{C} is the complex numbers, but it can be replaced by any algebraically closed field of characteristic zero.

Theorem A. *Let L be a **CM field** with a chosen CM type Φ . Then there exists an abelian scheme of type (L, Φ) defined over the ring of integers of a number field contained in \mathbb{C} .*

Assume $L^\dagger \subset L$ is a totally real subfield of index 2, such that $[L^\dagger : \mathbb{Q}] = g$. We write $\sigma_i : L^\dagger \rightarrow \mathbb{R}$, $i = 1, \dots, g$ for the real places of L^\dagger . Recall that Φ consists of g complex embeddings $\tau_i : L \rightarrow \mathbb{C}$, one above each σ_i . The first step is to construct an abelian variety of type (L, Φ) over the complex numbers.

Problem 10 (★★)

- (1) Show that choosing a CM type Φ for L is equivalent to giving a complex structure on the real algebra $\mathbb{R} \otimes_{\mathbb{Q}} L$, i.e., a map of \mathbb{R} -algebras $\mathbb{C} \rightarrow \mathbb{R} \otimes_{\mathbb{Q}} L$. We denote $\mathbb{R} \otimes_{\mathbb{Q}} L$ with this complex structure by $(\mathbb{R} \otimes_{\mathbb{Q}} L)_{\Phi}$.
- (2) Denote by \mathcal{O}_L the ring of integers in L . Show that the quotient $T_{\Phi} = (\mathbb{R} \otimes_{\mathbb{Q}} L)_{\Phi} / \mathcal{O}_L$ has the structure of a **complex torus** with an embedding $\mathcal{O}_L \hookrightarrow \text{End}(T_{\Phi})$, where \mathcal{O}_L is considered as a subalgebra of $\mathbb{R} \otimes_{\mathbb{Q}} L$ via the embedding $x \mapsto 1 \otimes x$ and $\text{End}(T_{\Phi})$ is the ring of endomorphisms as a complex manifold.
- (3) To show that this complex torus is the complex analytification of an abelian variety A_{Φ} ^a, we need to find an **ample line bundle** on it. According to the Theorem of Lefschetz [Mum70, Page 29], it suffices^b to find a positive definite Hermitian form H on $(\mathbb{R} \otimes_{\mathbb{Q}} L)_{\Phi}$, whose imaginary part $\text{Im}(H)$ is integral on \mathcal{O}_L . Show that there exists $\alpha \in \mathcal{O}_L$, such that $\alpha^2 \in L^\dagger$ and $\tau_i(\alpha) = \sqrt{-1} \cdot \beta_i$, with $\beta_i \in \mathbb{R}_{>0}$ for all i .
- (4) Now let

$$H(x, y) = 2 \sum_{i=1}^g \beta_i \tau_i(x) \overline{\tau_i(y)}, x, y \in (\mathbb{R} \otimes_{\mathbb{Q}} L)_{\Phi}.$$

Show that this H satisfies the desired properties.

^aNamely $T_{\Phi} = A_{\Phi}(\mathbb{C})$ as an abelian group, but is endowed with the usual complex analytic topology.

^bThe map α in the theorem can be taken to be the trivial map that sends \mathcal{O}_L to 1.

We continue to show that the abelian variety A_{Φ} with CM type (L, Φ) descends to some number field K in \mathbb{C} . Namely, there is a CM abelian variety $(B, \iota_B : L \hookrightarrow \text{End}^0(B))$, with an isomorphism $B \times_K \mathbb{C} \cong A_{\Phi}$, compatible with the L -actions.

Problem 11 (★★★)

- (1) Show that \mathbb{C} can be written as a directed colimit of its subalgebras that are finitely generated over \mathbb{Z} . Conclude that $\text{Spec}(\mathbb{C}) = \varprojlim_i S_i$ is the limit for a directed system of schemes of finite type over \mathbb{Z} .
- (2) Apply **Tag 01ZM** to the abelian variety $A_{\Phi}/\text{Spec } \mathbb{C}$ and conclude that there exists some i and a map of finite presentation $f_i : A_i \rightarrow S_i$, such that $A \cong A_i \times_{S_i} \text{Spec}(\mathbb{C})$.

Apply [Tag 0CNU](#) and [Tag 0CNV](#) to deduce that i can be chosen such that f_i is smooth and proper.

- (3) Since the group structure on A_Φ only involves maps of finite presentation, deduce that i can be chosen such that A_i is an abelian scheme over S_i .
- (4) Choose a basis b_1, \dots, b_{2g} of L over \mathbb{Q} . Upon rescaling by an element in \mathbb{Q} , we may assume without loss of generality assume that each b_i lies in $\text{End}(A_\Phi)$ under $L \hookrightarrow \text{End}^0(A_\Phi)$. Each b_i is of finite presentation and hence also descends to A_i for some i . We can therefore conclude that i can be chosen such that A_i is equipped with complex multiplication $\iota_i : L \hookrightarrow \text{End}^0(A_i)$, and that $(A, L \hookrightarrow \text{End}^0(A)) \cong (A_i, \iota_i) \times_{S_i} \text{Spec}(\mathbb{C})$.
- (5) First use the Hilbert Nullstellensatz to show that the residue field $K(s)$ of any closed point $s \in S_i$ above $\text{Spec}(\mathbb{Q})$ is a number field. Now take the fiber of A_i over any such s and denote it by A_s . Show that $\text{End}^0(A_i) \hookrightarrow \text{End}^0(A_s)$ and hence A_s is equipped with an L -action.

In fact, by increasing i if necessary, we may assume $S_i = \text{Spec}(R_i)$ with R_i containing all Galois conjugates of L . It can also be achieved that the decomposition of the $L \otimes_{\mathbb{Q}} \mathbb{C}$ -module $\Gamma(A_\Phi, \Omega_{A_\Phi/\mathbb{C}}) = \text{Lie}(A_\Phi)^\vee := (\mathbb{R} \otimes_{\mathbb{Q}} L)_\Phi^\vee$ into subspaces on which L acts via τ_i descends to a decomposition

$$\Gamma(A_i, \Omega_{A_i/S_i}) = \prod_i V_i,$$

where L acts on V_i via $\tau_i : L \hookrightarrow R_i$. Combined with the fact that upon localizing R_i at the maximal ideal \mathfrak{m}_s corresponding to s , we may assume $K(s)$ to be a subfield of $R_{i, \mathfrak{m}_s} \hookrightarrow \mathbb{C}$, this decomposition is enough to ensure that the base change $A_s \times_{K(s)} \mathbb{C}$ is isogenous to A_Φ . The kernel of the isogeny descends to some finite extension $K/K(s)$, by quotienting $A_s \times_{K(s)} K$ with the kernel of the isogeny, we find the desired B .

Finally, we show that CM abelian varieties can be defined over the ring of integers of a number field, i.e., they have good reduction everywhere.

Problem 12 (★★)

Suppose that A has CM by a CM field L , and A is defined over a number field K . There exists a finite extension K'/K such that $A \times_K K'$ has good reduction at all finite places v' of K' .^a

We will show this in the following steps.

- (1) Read [Theorem 1](#) of [\[ST68\]](#), which is called the “Néron–Ogg–Shafarevich criterion”.
- (2) Let S be the finite set of finite places v of K where A has bad reduction. Choose such a place v , and fix a prime number ℓ such that $v \nmid \ell$. Convince yourself that by [\[ST68, Theorem 1\]](#), it suffices to show that the image of the inertia group $I(v) \subset \text{Gal}(\overline{\mathbb{Q}}/K)$ is finite in $\text{Aut}(T_\ell A)$.
- (3) Recall from PSET 3, Problem 4(1) that since $L \hookrightarrow \text{End}_K^0(A)$, $V_\ell A = T_\ell A \otimes \mathbb{Q}_\ell$ is a free $L \otimes \mathbb{Q}_\ell$ -module of rank $2g/[L : \mathbb{Q}]$, where $g = \dim A$. Since A has CM by L , $[L : \mathbb{Q}] = 2g$. Check that the action of $\text{Gal}(\overline{\mathbb{Q}}/K)$ on $V_\ell A$ commutes with the action of $L \otimes \mathbb{Q}_\ell$, and therefore the image of $\text{Gal}(\overline{\mathbb{Q}}/K)$ is contained in $\text{GL}_1(L \otimes \mathbb{Q}_\ell)$. Use this to show that the action of $\text{Gal}(\overline{\mathbb{Q}}/K)$ on $V_\ell A$ (and hence on $T_\ell A$) is abelian.

- (4) Deduce from part (3) that the action of $I(v)$ factors through $\text{Gal}(K_v^{\text{ab}}/K_v^{\text{un}})$, where we view $I(v) = \text{Gal}(\overline{K_v}/K_v^{\text{un}}) \subset \text{Gal}(\overline{K_v}/K_v) \subset \text{Gal}(\overline{\mathbb{Q}}/K)$, and K_v^{ab} is the maximal abelian extension of the local field K_v , and K_v^{un} is the maximal unramified extension of K_v .
- (5) Recall from local class field theory that $\text{Gal}(K_v^{\text{ab}}/K_v^{\text{un}}) \cong \mathcal{O}_{K_v}^\times$. Convince yourself that $\mathcal{O}_{K_v}^\times$ is the product of a finite group and a pro- p group, where p is the characteristic of the residue field of K_v .
- (6) Observe that the pro- ℓ group $1 + \ell \text{End}_{\mathbb{Z}_\ell}(T_\ell A)$ is a finite-index subgroup of $\text{Aut}_{\mathbb{Z}_\ell}(T_\ell A)$. Conclude that the image of any map from a pro- p group to a pro- ℓ group must have finite image.

^aSee [Liu, Cor. 4.10] for a proof.

REFERENCES

- [Bao] Chengyang Bao, *Honda-tate theorem for elliptic curves*.
- [EVdGM12] Bas Edixhoven, Gerard Van der Geer, and Ben Moonen, *Abelian varieties*, 2012, Available at <http://van-der-geer.nl/~gerard/AV.pdf>, p. 331.
- [Liu] Tong Liu, *CM abelian varieties*, 2004-05 VIGRE Number Theory Working Group, organized by Brian Conrad and Chris Skinner, <http://math.stanford.edu/~conrad/vigregroup/vigre04.html>.
- [Man63] Yuri I Manin, *The theory of commutative formal groups over fields of finite characteristic*, Russian Mathematical Surveys **18** (1963), no. 6.
- [Mum70] David Mumford, *Abelian varieties*, Oxford University Press, published for the Tata Institute of Fundamental Research, 1970.
- [Poo06] Bjorn Poonen, *Lecture on rational points on curves*, <https://math.mit.edu/~poonen/papers/curves.pdf>, March 2006.
- [Ser20] Jean-Pierre Serre, *Rational points on curves over finite fields*, Documents Mathématiques (Paris) [Mathematical Documents (Paris)], vol. 18, Société Mathématique de France, Paris, [2020] ©2020, With contributions by Everett Howe, Joseph Oesterlé and Christophe Ritzenthaler. MR 4242817
- [Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR 1312368
- [Sil09] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094
- [ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Annals of Mathematics (1968), 492–517.
- [Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR 265369