AWS 2024 PROBLEM SET ON ARITHMETIC OF ABELIAN VARIETIES

JERRY YU FU

Contents

1. Introduction

The goal of these problems is to familiarize you with the concepts around the arithmetic of abelian varieties, especially these over finite field, and the Diophantine heights on abelian varieties. The problems accompanied Prof. Karemaker and Prof. Silvermans lectures.

In each section, you will find a variety of problems; some of them get you to work with basic concepts with and some are meant to challenge you. Problems marked ($\star$), ($\star\star$), and ($\star\star\star$) denote beginner, intermediate, and advanced problems, respectively. There are some open questions in §3 that may be of interest to you. Please note that the list of problems is long, so I do not expect you to solve every single question during the AWS. Please be kind to yourself and take things at your own pace! You may skip around and find a part of the exercises you are interested in, and start working there.

Many of these questions appeared in the problem sets from the Preliminary Arizona Winter School (PAWS) on abelian varieties over finite fields, many of them (especially these on height theory) are suggested by Joe Silverman's lecture notes, still there are a few problems created by myself that appears useful for you to understand the materials or just beacuse they are interesting to investigate. For the computational problems you may use CoCalc or MAGMA's online calculators.

The problems for PAWS were compiled by Santiago Arango-Pieros, Seokhyun Choi, Alice Lin, Yuxin Lin and Mingjia Zhang.

2. Arithmetic of Abelian varieties

2.1. **General theory of abelian varieties.** A good reference for this section is the book 'Abelian Varieties' by Bas Edixhoven, Gerard van der Geer and Ben Moonen. (As a first (underwhelming) example of a higher-dimensional abelian variety, you can take the product of two elliptic curves!)

Exercise 2.1.1($\star$) Let X_1 and X_2 be varieties over a field k.

(1) If X_1 and X_2 are given the structure of a group variety, show that their product $X_1 \times X_2$ naturally inherits the structure of a group variety.
(2) Suppose $Y := X_1 \times X_2$ carries the structure of an abelian variety. Show that X_1 and X_2 each have a unique structure of an abelian variety such that $Y = X_1 \times X_2$ as abelian varieties.

Morphisms between products of abelian varieties decompose.
Exercise 2.1.2($\star\star$) Let A_1, A_2, B_1, B_2 be abelian varieties over a field k. Show that

$$\mathrm{Hom}(A_1 \times A_2, B_1 \times B_2) \cong \mathrm{Hom}(A_1, B_1) \times \mathrm{Hom}(A_1, B_2) \times \mathrm{Hom}(A_2, B_1) \times \mathrm{Hom}(A_2, B_2).$$

We define group varieties as group objects in the category of k-varieties. What about ring varieties?
Exercise 2.1.3($\star\star$) A ring variety over a field k is a commutative group variety $(X, +, 0)$ over k, together with a ring multiplication morphism $X \times X \to X$ written as $(x, y) \mapsto x \cdot y$, and a k-rational point $1 \in X(k)$, such that the ring multiplication is associative, distributive with respect to addition, and 1 is a 2-sided identity element. Show that the only connected complete ring variety is a point.

The following problems require some background in Algebraic Geometry. By definition, irreducible topological spaces are connected. The converse is true for group varieties.
Exercise 2.1.4($\star\star\star$) Let G be a group variety over a field k.

(1) Show that there exists a unique irreducible component N containing the identity element e.
(2) Show that N is a normal subgroup of finite index in G.
(3) Show that irreducible components of G are exactly connected components of G. Conclude that if G is connected, then G is irreducible.
(4) Show that each open subgroup of G contains N.
(5) Show that each closed subgroup of finite index in G contains N.
(6) Conclude that if G is connected, then G is the only open subgroup and is the only closed subgroup of finite index.

Exercise 2.1.5($\star\star\star$)

Let X be a variety over a field k. Write $k[\epsilon] := k[t]/(t^2)$ for the ring of dual numbers over k, and let $S := \mathrm{Spec}(k[\epsilon])$. Write $\mathrm{Aut}^1(X_S/S)$ for the group of automorphisms of X_S over S which reduce to the identity on the special fiber $X \hookrightarrow X_S$.

(1) Let x be a k-valued point of X. Show that the tangent space $(T_X)_x := (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$ is in natural bijection with the space of $k[\epsilon]$-valued points of X which reduce to x modulo ϵ. (cf. [Har77, Chapter II, Exercise 2.8].)

(2) Suppose $X = \mathrm{Spec}(A)$ is affine. Then we have:

$$H^0(X, \mathcal{T}_{X/k}) \cong \mathrm{Hom}(\Omega^1_{A/k}, A) \cong \mathrm{Der}_k(A, A)$$

Show that $H^0(X, \mathcal{T}_{X/k}) \cong \mathrm{Aut}^1(X_S/S)$. We denote this isomorphism as $h : H^0(X, \mathcal{T}_{X/k}) \to \mathrm{Aut}^1(X_S/S)$. Then for a group variety X that is not affine, we can take an affine cover of X and get the isomorphism $h : H^0(X, \mathcal{T}_{X/k}) \to \mathrm{Aut}^1(X_S/S)$.

(3) Suppose X is a group variety over k. Let $\tau : S \to X$ be a tangent vector at e, the identity section. Let t_τ be the right translation by τ morphism, so it is an element in $\mathrm{Aut}^1(X_S/S)$. Show that the associated global vector field $\zeta := h^{-1}(t_\tau)$ is invariant under the right-translation map. That is, $t_y^*\zeta = \zeta$ for all $y \in X(k)$. Here, $t_y(x) = m(x, y)$ is the right translation by y morphism. [1]

The previous problem might be useful to solve the next two. **Exercise 2.1.6**($\star\star\star$) Show that every morphism from the projective line to an abelian variety is constant.[2]

Exercise 2.1.7($\star\star\star$) Show that 1-dimensional abelian varieties have genus one. In particular, we can define an elliptic curve to be a 1-dimensional abelian variety.

To solve the following question, you may need the knowledge of line bundles and divisors on abelian varieties.

Exercise 2.1.8($\star\star$)
Prove that no abelian variety of dimension g can be embedded into $(\mathbb{P}^1)^{2g-1}$. Analyze when an abelian variety of dimension g can be embedded into $(\mathbb{P}^1)^{2g}$.

2.2. **The Picard variety and dual abelian varieties.** Let X be a scheme and $f : X \to S$ over some basis S, we are led to consider the contravariant functor $P_{X/S} : \left(\mathrm{Sch}_{/S}\right)^0 \to \mathrm{Ab}$ given by

$$P_{X/S} : T \mapsto \mathrm{Pic}\,(X_T) = H^1\left(X \times_S T, \mathbb{G}_m\right)$$

The relative Picard functor $\mathrm{Pic}_{X/S} : \left(\mathrm{Sch}_{/S}\right)^0 \to \mathrm{Ab}$ is defined to be the fppf sheaf (on $(S)_{\mathrm{FPPF}}$) associated to the presheaf $P_{X/S}$. An S-scheme representing $\mathrm{Pic}_{X/S}$ (if such a scheme exists) is called the relative Picard scheme of X over S.

[1] You can check [EVdGM12][Proposition 15, pg. 8] for a more explicit description of the associated vector field ζ. It turns out that the vector field is not preserved under the left translation. Can you see why?

[2] Hint: The canonical bundle of an abelian variety is trivial.

Exercise 2.2.1($\star\star$) Show that the functor $P_{X/S}$ defined in §1 is never representable, at least if we assume X to be a non-empty scheme.

Exercise 2.2.2($\star\star$) Let X and Y be two abelian varieties over a field k.

(i) Write $i_X : X \to X \times Y$ and $i_Y : Y \to X \times Y$ for the maps given by $x \mapsto (x, 0)$ and $y \mapsto (0, y)$, respectively. Show that the map $(i_X^t, i_Y^t) : (X \times Y)^t \to X^t \times Y^t$ that sends a class $[L] \in \mathrm{Pic}^0_{(X\times Y)/k}$ to $\left(\left[L_{|X\times\{0\}}\right], \left[L_{|\{0\}\times Y}\right]\right)$, is an isomorphism. [Note: in general it is certainly not true that the full Picard scheme $\mathrm{Pic}_{X\times Y/k}$ is isomorphic to $\mathrm{Pic}_{X/k} \times \mathrm{Pic}_{Y/k}$.]

(ii) Write

$$p : X \times Y \times X^t \times Y^t \longrightarrow X \times X^t \quad \text{and} \quad q : X \times Y \times X^t \times Y^t \longrightarrow Y \times Y^t$$

for the projection maps. Show that the Poincaré bundle of $X \times Y$ is isomorphic to $p^*\mathscr{P}_X \otimes q^*\mathscr{P}_Y$.

Exercise 2.2.3($\star\star$) Let L be a line bundle on an abelian variety X. Consider the homomorphism $(1, \varphi_L) : X \to X \times X^t$. Show that $(1, \varphi_L)^* \mathscr{P}_X \cong L \otimes (-1)^* L$. **Exercise**

2.2.4($\star\star$) Let $\mathscr{P}$ be the Poincar

Exercise 2.2.5($\star\star$) If τ is a translation on an abelian variety, then what is the induced automorphism τ^t of the dual abelian variety?

2.3. **Polarizations and Weil pairings.** This section is made to assimilate the polarizations and Weil pairings on abelian varieties.

Exercise 2.3.1($\star$) Let $f : X \to Y$ be a homomorphism of abelian varieties with finite kernel. If $\mu : Y \to Y^t$ is a polarization, show that $f^*\mu := f^t \circ \mu \circ f$ is a polarization of X.

Exercise 2.3.2($\star\star$) Let X be an abelian variety over a field k. Suppose there exists a polarization $\lambda : X \to X^t$ with $\deg(\lambda) = m$ odd.

(i) Show that there exist integers a and b with $1 + a^2 + b^2 \equiv 0 \bmod m$. [Hint: Use the Chinese remainder theorem. First find a solution modulo p for any prime p dividing m. Then use the fact that the curve $C \subset \mathbb{A}^2$ given by $1 + x^2 + y^2 = 0$ is smooth over $\mathbb{Z}_p (p \neq 2!)$ to see that the solutions can be lifted to solutions modulo arbitrarily high powers of p.]

(ii) Adapting the proof of Zarhin's trick (see for example Milne chapter I Theorem 13.12), show that $X^2 \times (X^t)^2$ admits a principal polarization.

2.4. **The Tate module and the emdomorphism ring.** The goal of this section is to get comfortable with the Tate module and the endomorphism ring of an abelian variety. Throughout this section, p will be a prime, and q will be a power of p. We use ℓ to denote a prime, usually different from p. For a field K, we will use G_K to denote the absolute Galois group of K.

If this is your first encounter with the p-adics, it is worth to spend some time with Problem 1.

Exercise 2.4.1($\star$)

Let p be a prime, and define the p-adic valuation $v_p\colon \mathbb{Z} \to \mathbb{Z} \cup \{\infty\}$ by the unique factorization property of the integers; that is:

$$a = \prod_p p^{v_p(a)}, \text{ for } a \neq 0.$$

In other words, $v_p(a)$ is the largest power of p dividing a, and put $v_p(0) := \infty$. We extend the p-adic valuation to $\mathbb{Q}$ in the usual way by letting $v_p(a/b) := v_p(a) - v_p(b)$ for integers a, b. In this problem, we will establish some of the main properties of v_p.

(1) Show that $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is a non-archimedean valuation. That is, prove that:
   (a) $v_p(x) = \infty$ if and only if $x = 0$.
   (b) $v_p(xy) = v_p(x) + v_p(y)$ for every $x, y \in \mathbb{Q}$.
   (c) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$ for every $x, y \in \mathbb{Q}$.
   (d) $v_p(x + y) = \min\{v_p(x), v_p(y)\}$ if $v_p(x) \neq v_p(y)$.

(2) Define the p-adic absolute value $|\cdot|_p\colon \mathbb{Q} \to \mathbb{R} \cup \{\infty\}$ by $|x|_p := p^{-v_p(x)}$. Show that $|\cdot|_p$ is a non-archimedean absolute value. That is, prove that:
   (a) $|x|_p = 0$ if and only if $x = 0$.
   (b) $|xy|_p = |x|_p|y|_p$ for every $x, y \in \mathbb{Q}$.
   (c) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$ for every $x, y \in \mathbb{Q}$.

(3) Denote by $|\cdot|_\infty$ the usual absolute value of $\mathbb{Q}$. Prove the product formula:

$$|x|_\infty \cdot \prod_p |x|_p = 1, \text{ for any } x \in \mathbb{Q}^\times.$$

(4) Notice that each for each prime $p \leq \infty$, the p-adic absolute value defines a metric on $\mathbb{Q}$ (for $p = \infty$ this is the usual euclidean distance on the rationals). Intuitively, we say a rational number is p-adically small if it is "very" divisible by p. Show that $(\mathbb{Q}, |\cdot|_p)$ is not a complete metric space. That is, give an example of a Cauchy sequence that does not converge in $\mathbb{Q}$.

(5) Show that for two different primes[3] p and ℓ, the identity is not a homeomorphism between $(\mathbb{Q}, |\cdot|_p)$ and $(\mathbb{Q}, |\cdot|_\ell)$.

(6) Just as how $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value $|\cdot|_\infty$, we define $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the p-adic absolute value. $\mathbb{Z}_p$ is the unit interval of $\mathbb{Q}_p$; that is

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

   Show that $\mathbb{Z}_p$ is compact and an integral domain.

(7) Convince yourself that you understand why $\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

The next problem allows you to get your hands on some 5-adic numbers. You might want to reflect on Hensel's lemma.

Exercise 2.4.2($\star$) Show that -1 is a square in $\mathbb{Q}_5$. Manually calculate one of the square roots to 3 digits of 5-adic precision. Use your favorite computer algebra system to calculate both roots to 100 digits of 5-adic precision.

The following problem introduces key concepts and theorems about semisimple algebras.

[3]Including the prime at infinity!

Exercise 2.4.3($\star\star$) Let K be a field. A K-algebra over K is called semi-simple if any left ideal admits a direct complement. By a central simple algebra over K, we mean a finite-dimensional K-algebra which is simple and for which the center is exactly K. By a central division algebra, we mean a central simple algebra which is also a division algebra.

(1) Show that a matrix algebra over K is a central simple algebra. If a central simple algebra is isomorphic to a matrix algebra, then we say that it is a split central simple algebra.
(2) (Wedderburn's theorem) Show that every central simple algebra is isomorphic to a matrix algebra of some central division algebra.
(3) (Skolem-Noether theorem) Show that every automorphism of a central simple algebra is an inner automorphism.
(4) (Double centralizer theorem) Let A be a semisimple subalgebra of a finite dimensional central simple algebra B over a field K. Then, show that
$$C_B(C_B(A)) = A.$$
Also show the dimension formula
$$[B : K] = [A : K][C_B(A) : K].$$
(5) Assume that A is a semisimple algebra over a field K, with a finite-dimensional faithful representation V over K. Then, show that
$$C_{\mathrm{End}(V)}(C_{\mathrm{End}(V)}(A)) = A.$$
(6) Let A be a central division algebra over K. Use the double centralizer theorem to show that $[A : K]$ is a square. If A is a division algebra over $\mathbb{Q}$, we can define its reduced degree over $\mathbb{Q}$ as $[A : \mathbb{Q}]_{\mathrm{red}} := [A : \mathcal{Z}(A)]^{\frac{1}{2}}[\mathcal{Z}(A) : \mathbb{Q}]$, where $\mathcal{Z}(A) = C_A(A)$ is the center of A.

In the next problem we classify central simple algebras over local fields using the cohomological interpretation of the Brauer group.

Exercise 2.4.4($\star\star\star$) Let K be a field. Recall that a central simple algebra over K is a simple K-algebra with center equal to K. Let $\mathrm{Br}(K)$ be the Brauer group over K, the group[4] of equivalence classes of central simple algebras over K. For any field extension L/K, let $\mathrm{Br}(L/K)$ denote the subgroup of classes of central simple algebras over K that split over L. That is, $[B] \in \mathrm{Br}(K)$ is in $\mathrm{Br}(L/K)$ if and only if $B \otimes_K L \cong M_n(L)$ for some $n \geq 1$. We have a functorial isomorphism
$$\varphi_K : \mathrm{Br}(K) \cong H^2(G_K, (K^{\mathrm{sep}})^\times)$$
inducing an isomorphism
$$\varphi_{L/K} : \mathrm{Br}(L/K) \cong H^2(\mathrm{Gal}(L/K), L^\times),$$
for any finite separable extension L/K. Furthermore, $\varphi_K([A \otimes_K B]) = \varphi_K(A) + \varphi_K(B)$.

(1) Show that $\mathrm{Br}(\mathbb{R}) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, and that the non-trivial element can be represented by $\mathbb{H}$; Hamilton's original quaternion algebra over $\mathbb{R}$. We define the Hasse-invariant of the representatives such that $\mathrm{inv}_\infty([\mathbb{R}]) = 0$ and $\mathrm{inv}_\infty([\mathbb{H}]) = \frac{1}{2}$.

[4]It is not obvious that this set forms a group. Think about what the group operations are!

Now let K_v be a non-archimedean local field. We can describe the composition

$$\mathrm{inv}_v : \mathrm{Br}(K_v) \cong H^2(G_{K_v}, (K_v^{\mathrm{un}})^\times) \cong \mathbb{Q}/\mathbb{Z}$$

as follows. Given a central division algebra D over K_v, let $K_v \subseteq L \subseteq D$ be its maximal subfield. L is an unramified extension of K_v of degree $n := [D : K_v]^{\frac{1}{2}}$.

(2) Let $\sigma \in \mathrm{Gal}(L/K_v)$ be the q-Frobenius automorphism on L, where q is the size of the residue field of K_v. Use the Skolem-Noether theorem to show that there exists $\alpha \in D$, unique up to a multiple in L, such that for every $\beta \in L, \sigma(\beta) = \alpha\beta\alpha^{-1}$.

(3) Let π be a uniformizer of K_v. Show that $\alpha^n = u\pi^r$ for some $u \in \mathcal{O}_L^\times$ and $r \in \mathbb{Z}$. Then we define the Hasse-invariant of D to be $\mathrm{inv}_v(D) := r/n \mod \mathbb{Z}$. Show that $\mathrm{inv}_v(D)$ is well-defined. That is, it does not depend on the choice of α.

(4) Let $\mathbb{Q}_{p^h}$ be the unique unramified extension of $\mathbb{Q}_p$ of degree h. For a pair of integers (m, h) such that $h \geq 1, m \geq 0, \gcd(h, m) = 1$, consider $D_{p,h,m}$. It is the division algebra generated by $\mathbb{Q}_{p^h}$ and an element α, with multiplication defined such that for $\beta \in \mathbb{Q}_{p^h}, \alpha\beta = \beta^\sigma\alpha$, and $\alpha^h = p^m$. Here, $\sigma \in \mathrm{Gal}(\mathbb{Q}_{p^h}/\mathbb{Q}_p)$ is the p-Frobenius automorphism of $\mathbb{Q}_{p^h}$.
   (a) Verify that $D_{p,h,m}$ is a central division algebra over $\mathbb{Q}_p$ and $\mathbb{Q}_{p^h}$ is a maximal subfield. Compute its Hasse-invariant $\mathrm{inv}_p(D_{p,h,m})$ as an element of $\frac{1}{h}\mathbb{Z}/\mathbb{Z}$. Determine the valuation on D that extends the p-adic valuation on $\mathbb{Q}_{p^h}$.
   (b) Notice that inside D, we have an order $\mathcal{O}$ generated by $\mathbb{Z}_{p^h}$ and α, where $\mathbb{Z}_{p^h}$ is the ring of integers in $\mathbb{Q}_{p^h}$. Determine the pairs (m, h) for which $\mathcal{O}$ is a maximal order.[5]

2.4.1. *Endomorphism algebras of Abelian Varieties.* Let's start by calculating some endomorphism rings! You may use the `LMFDB`, or your favorite computer algebra system to verify your answers.

Exercise 2.4.5($\star\star$) Let $\mathbb{Z}_{(3)}$ be the localization of $\mathbb{Z}$ at the prime ideal (3), and E be the elliptic curve over $\mathbb{Z}_{(3)}$ defined by

$$y^2z = x^3 - xz^2.$$

Compute the endomorphism rings $\mathrm{End}(E_{\mathbb{F}_3})$, $\mathrm{End}(E_{\mathbb{Q}(i)})$, $\mathrm{End}(E_{\mathbb{Q}})$, and compare them. Here, i is a root of $T^2 + 1 \in \mathbb{Q}[T]$.[6]

Section §3.2 of the lecture notes from PAWS defines the isogeny category of abelian varieties over a field k and states that it is a semisimple abelian category. Let's unpack this idea.

Exercise 2.4.6($\star\star$) Let k be a field.

(1) Justify why: $A \sim B$ if and only if A is isogenous to B, is an equivalence relation on the set of abelian varieties over k.

(2) Show that for every simple abelian variety A, the endomorphism algebra $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbb{Q}$ is a division algebra over $\mathbb{Q}$.

[5]Hint: notice that $\mathcal{O} \subseteq \mathcal{O}_D := \{x \in D : v(x) \geq 0\}$.

[6]Remark: Recall that the endomorphism ring of an elliptic curve E over a field k is either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra. If $\mathrm{char}(k) = 0$, only the first two are possible. [Sil09, Corollary III.9.4]

(3) Reality check: $\mathrm{End}(A)$ is an order in $\mathrm{End}^0(A)$.
(4) If A is not necessarily simple, conclude that $\mathrm{End}^0(A)$ is a semisimple algebra over $\mathbb{Q}$.

In the next problem, we sketch a proof of Lenstra [Len96] of a fundamental theorem of Deuring [Deu41].

Exercise 2.4.7($\star\star$) Let E be an elliptic curve defined over a field k of characteristic p, and suppose that $\mathrm{rank}_{\mathbb{Z}} \mathrm{End}(E) = 4$. Then $B := \mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$ ramified only at p and ∞. To prove this, denote by $\mathcal{O} := \mathrm{End}\, E \subset B$, and follow the following steps:

(1) Let n be prime to p. Recall that $\mathrm{End}\, E[n] \cong M_2(\mathbb{Z}/n\mathbb{Z})$.
(2) Show that $\mathcal{O}/n\mathcal{O} \to \mathrm{End}\, E[n]$ is injective.
(3) Show that $\#\mathcal{O}/n\mathcal{O} = n^4$ and conclude that $\mathcal{O}/n\mathcal{O} \to \mathrm{End}\, E[n]$ is an isomorphism.
(4) Show that for every prime $\ell \neq p$ we have that $\mathcal{O}_\ell \cong M_2(\mathbb{Z}_\ell)$ as $\mathbb{Z}_\ell$-algebras.
(5) Argue why B is ramified at ∞.
(6) Recall the fundamental exact sequence from class field theory

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_v \mathrm{Br}(\mathbb{Q}_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0 \tag{2.1}$$

where the first map is given by $B \to \bigoplus_v B \otimes_{\mathbb{Q}} \mathbb{Q}_v$ and the second map is given by $(B_v)_v \to \sum_v \mathrm{inv}_v(B_v)$. Use Equation 2.1 to show B is ramified at exactly ∞ and p. [7]
(7) Show that $B \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong D_{p,2,1}$, where $D_{p,2,1}$ is defined as in 4. [8]

Exercise 2.4.8($\star\star$)
Let A be a simple g-dimensional abelian variety defined over $\mathbb{F}_q$. From Problem 2.4.1 we have that $\mathrm{End}^0(A)$ is a division algebra over $\mathbb{Q}$. Recall that for a division algebra D, we defined its reduced degree by $[D : \mathbb{Q}]_{\mathrm{red}} := [D : \mathcal{Z}(D)]^{1/2}[\mathcal{Z}(D) : \mathbb{Q}]$. We say that A has complex multiplication if the reduced degree $[\mathrm{End}^0(A) : \mathbb{Q}]_{\mathrm{red}}$ is equal to $2g$.

Let L be the maximal commutative sub-algebra of $D = \mathrm{End}^0(A)$. Show that A has complex multiplication if and only if $[L : \mathbb{Q}] = 2g$.[9]

Exercise 2.4.9($\star$) Consider an ordinary elliptic curve E over $\mathbb{F}_q$.

(1) Show that $L = \mathbb{Q}(\phi_q)$ has $[L : \mathbb{Q}] = 2$. Conclude that E has complex multiplication.
(2) Show $\mathbb{Q}(\phi_q)$ is a quadratic imaginary extension of $\mathbb{Q}$.[10]
(3) Show that for every element $\alpha \in \mathrm{End}^0(E)$, α commutes with ϕ_q^r for some $r \geq 1$.
(4) Show that for any $m \geq 1$, $\phi_q^m = a\phi_q + b$ for some $a, b \in \mathbb{Z}$ with $a \neq 0$.

[7] See [Voi
, Example 14.2.13] for an explicit description of these quaternion algebras.
[8] Hint: Show that they have the same Hasse-invariant.
[9] Hint: Use the double centralizer theorem.
[10] Hint: See [Sil09][V.1.1] for Hasse bound.

(5) Show that α commutes with ϕ_q and that $\alpha \in \mathbb{Q}(\phi_q)$. Conclude that $\mathrm{End}^0(E)$ is a quadratic imaginary extension of $\mathbb{Q}$.

2.4.2. *The Tate module of an Abelian Variety.* Recall the existence of a Weil pairing on the Tate module of an abelian variety. In the case of elliptic curves, we can use the Weil pairing to deduce useful formulas for the trace and determinant of the map on the Tate module of E induced by an isogeny.

Exercise 2.4.10($\star\star$) Let E be an elliptic curve defined over a field k, and ℓ be a prime different from the characteristic of k. Let $T_\ell E$ be the ℓ-adic Tate module of E. The Weil pairing

$$e : T_\ell E \times T_\ell E \to T_\ell \mu$$

is a bilinear, alternating, non-degenerate, Galois-invariant pairing.[11] Here $T_\ell \mu := \varprojlim \mu_{\ell^n}$, where μ_{ℓ^n} is the group of ℓ^n-th roots of unity in $\bar{k}$. Moreover, for $\phi \in \mathrm{End}(E)$ and $T_\ell(\phi) \in \mathrm{End}(T_\ell E)$, the adjoint of $T_\ell(\phi)$ with respect to e corresponds to the dual isogeny $\hat{\phi}$. That is,

$$e(T_\ell(\phi)(P), Q) = e(P, T_\ell(\hat{\phi})(Q)).$$

Using the existence of e and the fact that $\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [\deg(\phi)]$, show that

- $\det(T_\ell(\phi)) = \deg(\phi)$, and
- $\mathrm{tr}(T_\ell(\phi)) = 1 + \deg(\phi) - \deg(1 - \phi)$.

Exercise 2.4.11($\star\star$) Here are some facts about the q-Frobenius endomorphism ϕ_q of an elliptic curve $E/\mathbb{F}_q$:

(a) ϕ_q is a purely inseparable isogeny of degree q.
(b) Its dual isogeny $\hat{\phi}_q$ is the unique isogeny satisfying $\phi_q \circ \hat{\phi}_q = \hat{\phi}_q \circ \phi_q = [q]$.
(c) The isogeny $[m] + [n]\phi_q$ is separable if and only if $p \nmid m$. In this case, we have that

$$\#\ker([m] + [n]\phi_q) = \deg([m] + [n]\phi_q).$$

Let $\ell \neq p$ be a prime and $T_\ell E$ be the ℓ-adic Tate module of E.

(1) Denote by $P_E(T)$ the characteristic polynomial of $T_\ell(\phi_q)$, the so-called characteristic polynomial of Frobenius. Show that $P_E(T) = T^2 - aT + q$, where $a = q + 1 - \#E(\mathbb{F}_q)$. Let $\alpha, \overline{\alpha} \in \mathbb{C}$ be the roots of $P_E(T)$. Show that

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \overline{\alpha}^n,$$

for every positive integer n.

(2) The zeta function attached to E is the formal power series[12]

$$Z(E/\mathbb{F}_q, T) := \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n}\right).$$

Show that[13] $Z(E/\mathbb{F}_q, T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$.

[11] See [Sil09][III.8].

[12] If we let $T = q^{-s}$, then $\zeta_{E/\mathbb{F}_q}(s) = Z(E/\mathbb{F}_q, q^{-s})$ is a holomorphic function with variable s.

[13] This is the rationality part of the Weil conjectures for $E/\mathbb{F}_q$.

2.5. **The Weil conjectures for abelian varieties and curves.** The goal of this section is to assimilate the Weil conjectures for abelian varieties and curves. Throughout the section, p will be a prime, and q will be a power of p. We use ℓ to denote a prime, different from p. For a field K, we will use G_K to denote the absolute Galois group of K.

Exercise 2.5.1($\star\star$)
Let A be a ring of finite type over $\mathbb{Z}$.

(1) Show that for every maximal ideal $\mathfrak{m}$ in A, the residue field $\kappa(\mathfrak{m}) := A/\mathfrak{m}$ is finite.[14]
(2) Let $\mathrm{Max}(A)$ be the set of maximal ideals in A; this is called the maximal spectrum of A. Show that $\mathrm{Max}(A)$ is countable.

We define the norm of a maximal ideal $\mathfrak{m}$ to be the size of its residue field $\mathrm{N}(\mathfrak{m}) := \#\kappa(\mathfrak{m})$. Define the zeta function of A as the formal Euler product

$$\zeta_A(s) := \prod_{\mathfrak{m}\in \mathrm{Max}(A)} \left(1 - \mathrm{N}(\mathfrak{m})^{-s}\right)^{-1}.$$

(3) Calculate the zeta function of the following rings; for $R = \mathbb{F}_q$ and $\mathbb{Z}$:
   (a) $A = R$.
   (b) $A = R[x]$.
   (c) $A = R[x, y]$.

We can restate (and slightly generalize) the previous problem in the language of schemes as follows.

Exercise 2.5.2($\star\star$)
Let X be a scheme of finite type over $\mathbb{Z}$.

(1) Show that for every closed point $P \in X$ the residue field $\kappa(P) := \mathcal{O}_{X,P}/\mathfrak{m}_P$ is a finite field.[15][16]
(2) Denote by $|X|$ the set of closed points in X. Show that $|X|$ is countable.

We define the norm of a closed point P to be the size of its residue field $\mathrm{N}(P) := \#\kappa(P)$. Define the zeta function of X as the formal Euler product

$$\zeta_X(s) := \prod_{P\in |X|} \left(1 - \mathrm{N}(P)^{-s}\right)^{-1}.$$

(3) Calculate the zeta function of the following schemes; for $R = \mathbb{F}_q$ and $\mathbb{Z}$:
   (a) $X = \operatorname{Spec} R$.
   (b) $X = \mathbb{A}^1_R$.
   (c) $X = \mathbb{P}^1_R$.

Exercise 2.5.3($\star\star\star$)

[14] Consider the structure map $\mathbb{Z} \to A$ composed with the projection $A \to A/\mathfrak{m}$. What are the possibilities for the kernel of the composition?

[15] A closed point P in $\operatorname{Spec} A$ is simply a maximal ideal $\mathfrak{m}$ in A, and its residue field is $\kappa(P) = A/\mathfrak{m}$.

[16] A possibly useful result from commutative algebra is the Artin–Tate lemma.

In this problem we are going to show that the zeta function defined in Problem 2.5 defines a holomorphic function. This is [Ser65, Theorem 1].

Theorem 2.1. *Let X be a scheme of finite type over $\mathbb{Z}$. Then, $\zeta_X(s)$ converges absolutely for a complex variable s in the half-plane* $\mathrm{Re}(s) > \dim X$.[17]

To prove this, proceed as follows:

(1) If X is a finite union of schemes X_i, show that Theorem 2.1 follows if the conclusion is true for each X_i. This reduces the proof to the affine case.
(2) Let $f\colon X \to Y$ be a surjective and finite morphism between schemes of finte type. Show that if the conclusion of Theorem 2.1 is valid for Y, then it is valid for X too.
(3) Reduce to showing that the result holds for $X = \mathbb{A}^n_{\mathbb{F}_p}$.
(4) Let Y be a scheme of finite type over $\mathbb{Z}$. Show that $\zeta_{Y\times\mathbb{A}^1}(s) = \zeta_Y(s-1)$.[18]
(5) Conclude the proof by calculating $\zeta_{\mathbb{A}^n_{\mathbb{F}_p}}(s)$ and showing that it converges absolutely in the half-plane $\mathrm{Re}(s) > n$.

The following problem justifies the definition of the zeta function of a variety over a finite field as the exponential generating series of its point counts.

Exercise 2.5.4($\star\star$) Let X be a variety over $\mathbb{F}_q$. Let m_d denote the number of degree d closed points on X.

(1) Prove that for every $n \geq 1$, we have
$$\sum_{d|n} d m_d = \#X(\mathbb{F}_{q^n}).$$
(2) If we let $T = q^{-s}$, show that
$$\zeta_X(s) = Z(X,T) := \exp\left(\sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{q^n})}{n} T^n\right).$$
(3) Let X be a smooth, projective, and geometrically irreducible curve of genus g defined over $\mathbb{F}_q$. Show that one can recover the zeta function $Z(X,T)$ from the point counts
$$\#X(\mathbb{F}_q), \#X(\mathbb{F}_{q^2}), \ldots, \#X(\mathbb{F}_{q^g}).$$
(4) Use your favorite computer algebra system to write a computer program that receives as input:
   - an irreducible polynomial $f \in \mathbb{F}_q[x]$,

   and outputs the Frobenius polynomial of the Jacobian of the hyperelliptic curve $X/\mathbb{F}_q$ with affine equation $y^2 = f(x)$.
(5) Use your favorite computer algebra system to write a computer program that receives as input:
   - an irreducible polynomial $f \in \mathbb{F}_q[x]$,
   - a positive integer N,

[17] In particular, $\zeta_X(s)$ is a Dirichlet series $\sum a_n/n^s$ with integral coefficients.
[18] This generalizes [Har77, Appendix C, Problem 5.3].

and outputs the first N terms of the zeta function of the hyperelliptic curve $X/\mathbb{F}_q$ with affine equation $y^2 = f(x)$.[19]

The following problem is [Poo06, Problem 3.10].

Exercise 2.5.5($\star$) Let X be the Hermitian curve $x^{q+1} + y^{q+1} + z^{q+1} = 0$ in $\mathbb{P}^2$ over $\mathbb{F}_q$.

(1) Check that X is smooth projective.
(2) Calculate the genus of X.
(3) Calculate $\#X(\mathbb{F}_{q^2})$.
(4) Compute the zeta function of $X_{\mathbb{F}_{q^2}}$.
(5) Calculate $\#X(\mathbb{F}_q)$.
(6) Compute the zeta function of X.

In this problem, we will calculate the zeta functions of some particular elliptic curves, and see that they are indeed of the form predicted by the Weil conjectures.

Exercise 2.5.6($\star\star$) Let $E/\mathbb{F}_p$ be the elliptic curve

$$y^2 = x^3 - n^2 x$$

for some n such that $p \nmid 2n$, and $p \equiv 1 \bmod 4$. We will prove that

$$Z(E,T) = \frac{(1-\alpha T)(1-\overline{\alpha}T)}{(1-T)(1-pT)} \tag{2.2}$$

for some specific $\alpha, \overline{\alpha} \in \mathbb{C}$.

(1) Let q be a power of p. Let $C/\mathbb{F}_q$ be the curve

$$u^2 = v^4 + 4n^2.$$

Show that $\#E(\mathbb{F}_q) = \#C(\mathbb{F}_q) + 1$.

(2) Let $\chi_{k,q} : \mathbb{F}_q^* \to \mathbb{C}^*$ be a character of order k for $k = 2, 4$. Prove

$$\#\{x \in \mathbb{F}_q : x^k = a\} = \sum_{j=1}^{k} \chi_{k,q}^j(a), \quad k = 2, 4 \tag{2.3}$$

for $a \neq 0$.

(3) Note that

$$\begin{aligned}\#C(\mathbb{F}_q) = 1 &+ \#\{u \in \mathbb{F}_q : u^2 = 4n^2\} + \#\{v \in \mathbb{F}_q : v^4 = -4n^2\} \\ &+ \#\{u, v \in \mathbb{F}_q^* : u^2 = v^4 + 4n^2\}.\end{aligned}$$

By applying Equation 2.3, show that

$$\#C(\mathbb{F}_q) = q + 1 + \chi_{2,q}(n)(J(\chi_{2,q}, \chi_{4,q}) + J(\chi_{2,q}, \overline{\chi_{4,q}}))$$

where $J(\chi, \psi)$ is the Jacobi sum

$$J(\chi, \psi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(1-x).$$

[19] Compare the efficiency of your function with the built-in intrinsics!

(4) Conclude that
$$\#E(\mathbb{F}_q) = q + 1 - \alpha_q - \overline{\alpha_q}$$
where $\alpha_q = -\chi_{2,q}(n)J(\chi_{2,q}, \chi_{4,q})$.
(5) Let $N : \mathbb{F}_{p^r}^* \to \mathbb{F}_p^*$ be the norm map. Note that we can take that
$$\chi_{2,p^r} = \chi_{2,p} \circ N, \quad \chi_{4,p^r} = \chi_{4,p} \circ N.$$
By Hasse-Davenport relation, we obtain
$$-J(\chi_{2,p^r}, \chi_{4,p^r}) = -J(\chi_{2,p} \circ N, \chi_{4,p} \circ N) = -J(\chi_{2,p}, \chi_{4,p})^r.$$
Conclude that
$$\alpha_{p^r} = \alpha_p^r.$$
(6) Complete the proof of Equation 2.2.

Exercise 2.5.7($\star$) Let $E/\mathbb{F}_q$ be an elliptic curve. Denote by ϕ_q the q-Frobenius on E and let $P_E(T) = T^2 - aT + q$ be the characteristic polynomial of ϕ_q.
(1) Review 2.4.11 and conclude the rationality of the zeta function $Z(E, T)$.
(2) Verify the functional equation
$$Z(E, (qT)^{-1}) = Z(E, T).$$
(3) Use the fact that $\deg([m] + [n]\phi) > 0$ for all integers m, n to deduce the Hasse bound $|a| \leq 2\sqrt{q}$.
(4) Let α, $\beta \in \mathbb{C}$ be roots of $P_E(T)$. Show that $|\alpha| = |\beta| = \sqrt{q}$.

Recall that a q-Weil number is an algebraic integer α such that for every embedding $\sigma\colon \mathbb{Q}(\alpha) \to \mathbb{C}$, $|\sigma(\alpha)| = q^{1/2}$. Two q-Weil numbers α, α' are conjugate if they are in the same orbit under the action of $\mathrm{Gal}_{\mathbb{Q}}$. In particular, there exists a field isomorphism $\mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha')$ mapping α to α', so that α and α' have the same minimal polynomial over $\mathbb{Q}$.

Exercise 2.5.8($\star$)
Let α be a q-Weil number. Show that there are two possibilities:
(1) $\mathbb{Q}(\alpha)$ has at least one real embedding $\phi : \mathbb{Q}(\alpha) \to \mathbb{R}$. Then either
- $\mathbb{Q}(\alpha) = \mathbb{Q}$, and $\phi(\alpha) = \pm\sqrt{q}$, or
- $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{p})$, and $\phi(\alpha) = \pm\sqrt{q}$.

(2) $\mathbb{Q}(\alpha)$ has no real embeddings. In this case, $\mathbb{Q}(\alpha)$ is a CM field, i.e. an imaginary quadratic extension of a totally real field. In particular, consider the subfield of $\mathbb{Q}(\alpha)$ generated by $\beta := \alpha + q/\alpha$.

Conversely, show that we can characterize all q-Weil numbers by the two above possibilities. In particular, if α is an algebraic integer such that either
- $\alpha = \pm\sqrt{q}$, or
- α is a root of $T^2 - \beta T + q$ where β is a totally real algebraic integer and $|\phi(\beta)| < 2\sqrt{q}$ for every embedding $\phi : \mathbb{Q}(\beta) \hookrightarrow \mathbb{R}$,

then α is a q-Weil number.

The following problem is an exercise in [CO09, Exercise 3.10]. It classifies the center of a division algebra equipped with a positive involution.

Exercise 2.5.9($\star$) Let D be a finite dimensional division algebra over $\mathbb{Q}$. An involution $\dagger\colon D \to D$ is an $\mathbb{Q}$-linear automorphism on D satisfying the following properties:

- For $x, y \in D$, $(xy)^\dagger = y^\dagger x^\dagger$.
- $(x^\dagger)^\dagger = x$

In addition, we say $\dagger$ is a positive involution if for any $x \in D, x \neq 0$, we have

$$\mathrm{tr}_{D/\mathbb{Q}}(xx^\dagger) > 0$$

Here, $\mathrm{tr}_{D/\mathbb{Q}}(x)$ is the trace of x as an element in $\mathrm{End}_{\mathbb{Q}}(D)$.

Now $\dagger$ is a positive involution on D. Let $L = \mathcal{Z}(D)$ be the center of D.

(1) Suppose L is fixed by $\dagger$, then notice that identity is a positive involution on L. Use weak approximation, show that L is totally real.
(2) Suppose L is not fixed by $\dagger$. Let $L^\dagger$ be the fixed subfield. Show that L is totally imaginary extension of $L^\dagger$. Moreover, show that for any embedding $\psi : L \to \mathbb{C}$, $\dagger$ induces complex conjugation on L. That is, for any $x \in L$, we have

$$\overline{\psi(x)} = \psi(x^\dagger)$$

In particular, the endomorphism algebra of a simple abelian variety is equipped with a positive involution induced by polarization.

Exercise 2.5.10($\star\star$) Let $A/\mathbb{F}_q$ be a simple abelian variety. Fix a polarization $\lambda\colon A \to A^\vee$. Then λ induces an involution $\dagger : \mathrm{End}^0(A) \to \mathrm{End}^0(A)$ as follows. Since λ is an isogeny, there exists $\lambda'\colon A^\vee \to A$ such that $\lambda' \circ \lambda = [n]$. So we have the element $\lambda^{-1} := \frac{1}{n}\lambda'$ in $\mathrm{End}^0(A)$. Then, given $\varphi \in \mathrm{End}(A)$, we define

$$\varphi^\dagger := \lambda^{-1} \circ \varphi^\vee \circ \lambda$$

This is the Rosati involution on $\mathrm{End}^0(A)$.

(1) Let $\mathcal{L}$ be an line bundle on A. Show that $\phi_q^*\mathcal{L} = \mathcal{L}^{\otimes q}$.
(2) Now let $\mathcal{L}$ be the line bundle that gives the polarization $\lambda\colon A \to A^\vee$. Show that for any $a \in A(k), n \in \mathbb{Z}_{>0}$, $[n]^*(t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}) \cong (t_a^*\mathcal{L} \otimes \mathcal{L}^{-1})^{\otimes n}$
(3) Recall the $\varphi^\vee\colon A^\vee(\mathbb{F}_q) \to A^\vee(\mathbb{F}_q)$ is given by $\varphi^\vee(\mathcal{L}) = \varphi^*\mathcal{L}$. Deduce the identity:

$$\phi_q^\vee \circ \lambda \circ \phi_q = [q]^\vee \circ \lambda$$

as morphism from $A(\mathbb{F}_q) \to A^\vee(\mathbb{F}_q)$.
(4) Combine with the fact that Rosati involution is positive and Problem item 2.5, show that ϕ_q is a q-Weil number.

Similar to the characteristic polynomial, we define the minimal polynomial $h_A(T)$ of the q-Frobenius endomorphism $\phi_q\colon A \to A$ to be the minimal polynomial of the corresponding endomorphism $T_\ell(\phi_q)$ of the Tate module $T_\ell A$. The following problem is a reformulation of [CO09, Exercise 3.14].

Exercise 2.5.11($\star\star$) Let $A/\mathbb{F}_q$ be a simple abelian variety of dimension g, where $q = p^g$ and $p \neq 2$. Then we know that $D := \mathrm{End}^0(A)$ is a division algebra over $\mathbb{Q}$, with center $L = \mathbb{Q}(\phi_q)$. Moreover, since A is an abelian variety defined over finite fields, it admits complex multiplication.

Let (n, m) be a pair of positive integers such that $g = m + n$ and $\gcd(m, n) = 1$. Suppose ϕ_q has minimal polynomial[20]

$$h_A(T) := T^2 + p^n T + p^g.$$

(1) Show that $h_A(T)$ is irreducible over $\mathbb{Q}$ and that both roots are Weil q-numbers. Compute the p-adic valuation of the roots.
(2) Use the fact that A has complex multiplication, determine $[D : \mathbb{Q}(\phi_q)]$.
(3) For each place v of L, compute the local Hasse invariant $\mathrm{inv}_v(D \otimes_L L_v)$.[21]
(4) Recall the definition and notation of $D_{p,h,m}$ in 2.4.4.
Show that $D \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong D_{p,g,n} \oplus D_{p,g,m}$.
(5) Let $\mathbb{F}_q \subseteq \mathbb{F}_{q^r}$ be a degree r extension and $A_{\mathbb{F}_{q^r}}$ be the base change of A to $\mathbb{F}_{q^r}$. Show that

$$\mathrm{End}^0(A) = \mathrm{End}^0(A_{\mathbb{F}_{q^r}}) \iff \mathbb{Q}(\phi_q) = \mathbb{Q}(\phi_{q^r})$$

Recall that in the lecture note, we see the definition of the Jacobian variety associated to a non-singular curve. The following problem relates elliptic curve and the Jacobian of its homogeneous space.

Exercise 2.5.12($\star\star$) Let K be a perfect field. Let E/K be an elliptic curve with zero marked by O, C/K be a smooth projective curve of genus one with a transitive action

$$\mu \colon C \times E \to C.$$

This means μ is a morphism over K satisfying

(1) $\mu(x, O) = x$ for all $x \in C(\bar{K})$,
(2) $\mu(\mu(x, P), Q) = \mu(x, P + Q)$ for all $x \in C(\bar{K})$, $P, Q \in E(\bar{K})$,
(3) Given $x, y \in C(\bar{K})$, there exists a unique $P \in E(\bar{K})$ satisfying $\mu(x, P) = y$.

We call this pair $(C/K, \mu)$ a homogeneous space for E/K. Recall that

(a) $\mathrm{Pic}^0(C_{\bar{K}}) = \mathrm{Div}^0(C_{\bar{K}})/\bar{K}(C)^\times$
(b) $\mathrm{Pic}^0(C) = \mathrm{Pic}^0(C_{\bar{K}})^{G_K}$

Show that there is an isomorphism $\mathrm{Pic}^0(C) \xrightarrow{\sim} E(K)$. From this, we can deduce $\mathrm{Jac}(C)(L) = E(L)$ for any algebraic field extension L/K. [22]

We can find Jacobian variety for a curve of genus 1 by using above homogeneous space.

Exercise 2.5.13($\star$)
Let $C/\mathbb{Q}$ be the Selmer curve $3x^3 + 4y^3 + 5z^3 = 0$ and let $E/\mathbb{Q}$ be an elliptic curve $x^3 + y^3 + 60z^3 = 0$ with origin $[1 : -1 : 0]$. Show $\mathrm{Jac}(C)(L) = E(L)$ where $L/\mathbb{Q}$ is an algebraic extension of $\mathbb{Q}$.

[20] $h_A(T)$ is Irr_{π_A} in [CO09, Theorem 10.17]. For a simple abelian variety A, it coincides with the minimal polynomial of the algebraic integer ϕ_q.

[21] Hint: Use [CO09][Theorem 10.17]

[22] In fact, the equality $\mathrm{Jac}(C) = E$ is true as functors. That is, for any k-algebra R, we have $\mathrm{Jac}(C)(R) = E(R)$.

In the following two exercises, we prove the Weil conjectures for smooth projective curves. In case you get stuck, a nice reference is available here.

Exercise 2.5.14($\star\star$) Let $C/\mathbb{F}_q$ be a smooth projective curve of genus g. We prove the rationality and functional equation part of the Weil conjectures for C.

(1) Calculate formally that the zeta function

$$Z(C,T) := \prod_{x\in|C|}(1-T^{\deg(x)})^{-1} = \prod_{x\in|C|}\sum_{k=0}^{\infty} T^{k\cdot\deg(x)} = \sum_{D\geq 0} T^{\deg(D)},$$

where the last sum is taken over all effective divisors on C.

(2) Each D corresponds to a pair $(\mathscr{L}, f)$, where $\mathscr{L}$ is a line bundle and $f \in (\Gamma(C,\mathscr{L}) - \{\mathbf{0}\})/\mathbb{F}_q^\times$ is a homogeneous global section. Hence, the above expression further evolves to

$$\sum_{\substack{\mathscr{L}\in\mathrm{Pic}(C)\\ \deg(\mathscr{L})\geq 0}} \#\mathbb{P}(\Gamma(C,\mathscr{L}))\cdot T^{\deg(\mathscr{L})} = \sum_{\substack{\mathscr{L}\in\mathrm{Pic}(C)\\ \deg(\mathscr{L})\geq 0}} \frac{q^{h^0(\mathscr{L})}-1}{q-1}\cdot T^{\deg(\mathscr{L})},$$

where $h^0(\mathscr{L})$ denotes the $\mathbb{F}_q$-dimension of the global sections of $\mathscr{L}$.

(3) Split the sum into two parts

$$g_1(T) = \sum_{0\leq\deg(\mathscr{L})\leq 2g-2} \frac{q^{h^0(\mathscr{L})}-1}{q-1}\cdot T^{\deg(\mathscr{L})}$$

$$g_2(T) = \sum_{\deg(\mathscr{L})>2g-2} \frac{q^{h^0(\mathscr{L})}-1}{q-1}\cdot T^{\deg(\mathscr{L})}.$$

Use the Riemann-Roch theorem to show that

$$g_2(T) = \sum_{\deg(\mathscr{L})>2g-2} \frac{q^{\deg(\mathscr{L})+1-g}-1}{q-1}\cdot T^{\deg(\mathscr{L})}$$

(4) Use the fact that $\mathrm{Pic}^0(C)$ is finite to conclude that $g_1(T)$ is a polynomial of degree $2g-2$, and that

$$g_2(T) = \#\mathrm{Pic}^0(C)\sum_{n>2g-2}\frac{q^{n+1-g}-1}{q-1}\cdot T^n = \frac{h(T)}{(1-T)(1-qT)},$$

for some polynomial $h(T)$ of degree $2g$. Deduce that $Z(C,T)$ is of the form $\frac{P_1(T)}{(1-T)(1-qT)}$, where $P_1(T)$ is a polynomial with degree at most $2g$ and constant term 1.

(5) ($\star\star\star$) Use the involution $\mathscr{L}\mapsto\omega_C\otimes\mathscr{L}^{-1}$ and the Serre duality to verify the functional equation

$$Z(C,(qT)^{-1}) = q^{1-g}T^{2-2g}Z(C,T)$$

and conclude that the polynomial $P_1(T)$ has degree $2g$. Here ω_C is the canonical sheaf, a line bundle of degree $2g-2$.

We continue to prove the Riemann hypothesis part of the Weil conjectures following the proof of Weil. Some intersection theory on surfaces is needed.

Exercise 2.5.15($\star\star\star$) [Har77, Appendix C, 5.7]] Let $C/\mathbb{F}_q$ be a smooth projective curve of genus g as above. Let $t_r := 1+q^r-\#C(\mathbb{F}_{q^r})$ be the trace of the q^r-Frobenius endomorphism. Let $P_1(T)$ be as before, and we write

$$P_1(T) = \prod_{i=1}^{2g}(1-\alpha_i T).$$

(1) Let ϕ_q be the geometric Frobenius on C. Denote by $\Gamma_r \subset C \times C$ the graph of ϕ_q^r and $\Delta \subset C \times C$ the diagonal. Show that the self-intersection $\Gamma_r^2 = q^r(2-2g)$ and $\Gamma_r \cdot \Delta = \#C(\mathbb{F}_{q^r})$.
(2) Apply the Castelnuovo-Severi inequality[23] to $D = a\Gamma_r + b\Delta$ for all a and b to obtain that $|t_r| \leq 2g\sqrt{q^r}$.
(3) Use the definition of the zeta function and taking logs, show that for each r

$$t_r = \sum_{i=1}^{2g} \alpha_i^r.$$

(4) Show that $|t_r| \leq 2g\sqrt{q^r}$ for all r is equivalent to $|\alpha_i| \leq \sqrt{q}$ for all i.
(5) Use the functional equation to show that $|\alpha_i| \leq \sqrt{q}$ for all i implies that $|\alpha_i| = \sqrt{q}$ for all i. Conclude the Riemann hypothesis part of the Weil conjectures from here.

2.6. **Finite flat group schemes, p-divisible groups and the Dieudonné modules.** The goal of this section is to venture into the world of p-divisible groups and Dieudonn modules. Throughout the section p will be a prime, and q will be a power of p.

In the first two problems, we explore the Newton polygon of a polynomial and use it to define the q-Newton polygon of an abelian variety. These problems are inspired by problems from [Poo06], which serves as a good complementary reference.

Exercise 2.6.1($\star$) Let K be a field with a non-archimedean valuation $v\colon K^\times \to \mathbb{R}$. The Newton polygon of a polynomial $P(T) = a_0T^n + a_1T^{n-1} + \cdots + a_{n-1}T + a_n$ is the lower convex hull of the finite set $\{(j, v(a_j)) \in \mathbb{R}^2 : 0 \leq j \leq n \text{ and } a_j \neq 0\}$. We will denote it by $\mathcal{N}(P) = \mathcal{N}(P, v)$. We define the width of a line segment from (a, b) to (c, d) (with $a < c$) to be $c - a$.

Theorem 2.2. *Suppose that (K, v) above is complete, so that there is a unique extension v_L of v to any algebraic field extension $L \supset K$. Let $\bar{K}$ be an algebraic closure of K, and let $\bar{v}$ denote the extension of v to $\bar{K}$. Then,*

$$\#\{\alpha \in \bar{K} : P(\alpha) = 0 \text{ and } \bar{v}(\alpha) = s\} = \text{ width of the segment of slope } s \text{ in } \mathcal{N}(P).$$

(1) Prove Theorem 2.2.[24]

[23] In particular, the form stated in [Har77, Exercise V.1.9].

[24] Hint: By changing $P(T)$ to $P(\lambda T)$ for some suitable $\lambda \in \bar{K}$, reduce to the case of slope $s = 0$. Start with $P(T)$ in factored form, and in terms of the number of zeros with positive and negative valuation, determine the location of the slope-zero part of the Newton polygon.

(2) Let m be a positive integer. How does $\mathcal{N}(P)$ compare to $\mathcal{N}(P^m)$?
(3) How does the Newton polygon of a product of polynomials relate to the Newton polygons of the factors?

In the context of abelian varieties over finite fields, we focus on the case where $K = \mathbb{Q}_p$, and p is the characteristic of our base field $\mathbb{F}_q$.

Exercise 2.6.2($\star$) Let the q-valuation $\bar{v}\colon \overline{\mathbb{Q}}_p^\times \to \mathbb{R}$ to be the p-adic valuation renormalized so that $\bar{v}(q) = 1$. We can define the q-Newton polygon of an abelian variety $A/\mathbb{F}_q$ to be the Newton polygon of the characteristic polynomial of Frobenius $P_A(T)$ with respect to the q-valuation $\bar{v}$. We write $\mathcal{N}(A) := \mathcal{N}(P_A(T), \bar{v})$. Newton polygons of g-dimensional abelian varieties over $\mathbb{F}_q$ satisfy the following properties:[25]

a. The left endpoint is $(0, 0)$ and the right endpoint is $(2g, g)$.
b. The vertices are all integer points with nonnegative second coordinate.
c. The vertices are symmetric: If λ is a slope occuring in multiplicity r, then $(1 - \lambda)$ is a slope occuring in multiplicity r. For example, the polygon with vertices $(0, 0), (g, 0), (2g, g)$ is symmetric, since 0 occurs as a slope for g many times and 1 occurs as a slope for g many times.

We say a Newton polygon is admissible if it satisfies properties a, b, c.

(1) Describe the admissible Newton polygons for $g \leq 3$.
(2) Are all admissible Newton polygons realized by some abelian variety of dimension $g \leq 3$? Find explicit examples in the LMFDB for each one.
(3) How does the Newton polygon of an abelian variety relate to the Newton polygons of its simple factors in the isogeny category?
(4) How does the q-Newton polygon of A compare to the q^r-Newton polygon of $A_{\mathbb{F}_{q^r}}$?
(5) Calculate the Newton polygon of the varieties described in 2.5.11.

The following problem establishes the basics of the ring of Witt vectors attached to a commutative ring. It is taken from [Neu13, Chapter II. Exercise 2-5].

Exercise 2.6.3($\star\star$)

Let $X_0, X_1, \dots$ be an infinite sequence of variables, and p a prime number. For each $n \in \mathbb{Z}_{\geq 1}$, let $W_n(X_0, \dots, X_n) := X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n$.

(1) Show that there exists polynomials $S_0, S_1, \dots; P_0, P_1, \cdots \in \mathbb{Z}[X_0, X_1, \dots; Y_0, Y_1, \dots]$ such that

$$W_n(S_0, S_1, \dots, S_n) = W_n(X_0, X_1, \dots, X_n) + W_n(Y_0, Y_1, \dots, Y_n)$$
$$W_n(P_0, P_1, \dots, P_n) = W_n(X_0, X_1, \dots, X_n) \cdot W_n(Y_0, Y_1, \dots, Y_n)$$

Now, let A be a commutative ring such that $pA = 0$. Let $\underline{a} := (a_0, a_1, \dots)$ be an infinite tuple with $a_i \in A$. We make the set of such tuples into a commutative ring $W(A)$ as follows. For two such tuples $\underline{a} = (a_0, a_1, \dots), \underline{b} = (b_0, b_1, \dots)$, define addition and multiplication

$$\underline{a} + \underline{b} := (S_0(a, b), S_1(a, b), \dots) \text{ and } \underline{a} \cdot \underline{b} := (P_0(a, b), P_1(a, b), \dots).$$

[25] See how many of these you can prove!

$W(A)$ is the ring of (p-typical) Witt vectors attached to A.

(2) Check that $1 := (1, 0, \dots)$ is the multiplicative identity of $W(A)$, and that $p := 1 + 1 + \cdots + 1$ is the element $(0, 1, 0, \dots)$ in $W(A)$.

(3) For every Witt vector $\underline{a} = (a_0, a_1, \dots) \in W(A)$, we define the ghost components $a^{(n)}$ as

$$\underline{a}^{(n)} := W_n(\underline{a}) = a_0^{p^n} + pa_1^{p^{n-1}} + \cdots + p^n a_n.$$

Consider mappings $V, F : W(A) \to W(A)$ defined by

$$V(\underline{a}) := (0, a_0, a_1, \dots) \text{ and } F(\underline{a}) := (a_0^p, a_1^p, \dots).$$

Show that

$$V(\underline{a})^{(n)} = p\underline{a}^{(n-1)} \text{ and } \underline{a}^{(n)} = (F(\underline{a}))^{(n-1)} + p^n a_n.$$

(4) Now let K be a field of characteristic p. Show that V is a homomorphism of $W(K)$ as an additive group, F is a homomorphism of $W(K)$ as a ring, and

$$V \circ F(\underline{a}) = F \circ V(\underline{a}) = p \cdot \underline{a} = (0, a_0^p, a_1^p, \dots)^{26}$$

(5) ($\star\star\star$) If K is a perfect field of characteristic p, then $W(K)$ is a complete discrete valuation ring with residue field K and maximal ideal $pW(K)$.

(6) ($\star\star\star$) Show that $W(\mathbb{F}_{p^n}) \cong \mathbb{Z}_{p^n}$, which is the valuation ring of $\mathbb{Q}_{p^n}$, the unique degree n unramified extension of $\mathbb{Q}_p$.

The next problem is Exercise 7.4.5 in [BC09], which gives a different way to understand the Witt vectors.

Exercise 2.6.4($\star\star$) Let k be an arbitrary field of characteristic $p > 0$.

(1) Use the addition law on the truncated Witt ring W_n defined in Problem 2.6 (applied to all k-algebras), to explain how this gives $\mathbb{A}_k^{n+1}$ the structure of a smooth group variety W_n.

(2) Describe the group variety structure explicitly for $n = 2$ and any k.

(3) Recall the idea of a ring variety. Write down the axioms to define a "commutative ring scheme" and exhibit W_n as such an example.

The following is Lemma/Exercise after Definition 4.28 in [CO09]. It introduces the notion of the Dieudonné ring and the local Cartier ring.

Exercise 2.6.5($\star$) Let K be a perfect field of characteristic p. Let $W(K)$ be the ring of Witt vectors and let $\sigma\colon W(K) \to W(K)$ be the homomorphism $(a_0, a_1, \dots) \mapsto (a_0^p, a_1^p, \dots)$. The Dieudonné ring D_K is defined to the polynomial ring $W(K)[F, V]$ satisfying $FV = VF = p$, $F\underline{a} = \underline{a}^\sigma F$, $V\underline{a}^\sigma = \underline{a}V$.

(1) Show that the Dieudonné ring D_K can be naturally identified with the $\mathbb{Z}$-graded ring $\bigoplus_{i\in\mathbb{Z}} c_i V^i W(K)$ with the relation $\underline{a}V^n = V^n\underline{a}^{\sigma^n}$, where $c_i = p^{-i}$ if $i < 0$ and $c_i = 1$ otherwise. This means $W(k)[F, V]$ is the ring consisting of finite sums $\sum_i a_i V^i$ where $a_i \in W(K)$, $v_K(a_i) \geq \max\{0, -i\}$.

[26] To show that f, g are the same map from $W(A) \to W(A)$, it suffices to show that $W_n \circ f = W_n \circ g$ from $\mathbb{Z}[\underline{X}; \underline{Y}] \to \mathbb{Z}[\underline{X}; \underline{Y}]$. Also, if A has characteristic p, it suffices to show that $f_n \equiv g_n \bmod p$ as an element in $\mathbb{Z}/p\mathbb{Z}[\underline{X}, \underline{Y}]$

(2) Let $W(K)[[V,F\rangle\rangle$ be the ring consisting of formal Laurent series $\sum_i a_i V^i$ where $a_i \in W(K)$, $v_K(a_i) \geq \max\{0,-i\}$, and $v_p(a_i)+i \to \infty$ as $|i| \to \infty$. Again the relation $\underline{a}V^n = V^n \underline{a}^{\sigma^n}$ is given. Let $v\colon W(K)[[V,F\rangle\rangle \to \mathbb{Z}$ be defined by $v(\sum_i a_i V^i) = \min_i\{v_K(a_i)+i\}$. Show that v is a discrete valuation on $W(K)[[V,F\rangle\rangle$. [27]

(3) Show that the inclusion $W(K)[F,V] \hookrightarrow W(K)[[V,F\rangle\rangle$ is a ring homomorphism whose image is dense. [28]

We compute the Cartier duals of some finite flat group schemes.

Exercise 2.6.6($\star\star$) Let k be a field. Compute the Cartier duals of the following commutative k-groups.

(1) $\underline{\mathbb{Z}/n\mathbb{Z}}$. Recall that as a k-scheme, this is given by $\operatorname{Spec} A$ where $A := \prod_{i\in\mathbb{Z}/n\mathbb{Z}} e_i k$. The multiplication on A is defined by $e_i \cdot e_j = \delta_{ij} e_i$, and the co-multiplication is given by $\Delta(e_r) = \sum_{i+j=r} e_i \otimes e_j$.

(2) When k has characteristic p, the group $\alpha_p := \operatorname{Spec} k[x]/(x^p)$, considered as a subgroup of $\mathbb{G}_{a,k}$.

In problem 2.6.7 and 2.6.8, we use Dieudonné modules to classify the commutative finite flat group schemes of order p defined over an algebraically closed field k of characterstic p, and apply this to study the p-torsion group scheme of a supersingular elliptic curve over k. If you get stuck, the solutions can be found here.

Exercise 2.6.7($\star$) Let k be an algebraically closed field of characterstic p. Let $D_k = W(k)[F,V]$ be the Dieudonné ring.

(1) Using [BC09, Theorem 7.2.4], there is an equivalence of categories between commutative order p finite flat group schemes over k and left D_k-modules M whose underlying $W(k)$-module is of length 1. Use (6) from Problem 2.6 to show that such an M must be isomorphic to $W(k)/(p)$ as a $W(k)$-module.

(2) To specify the D_k-module structure on M, it suffices to write down the action of F and V. Let e be a basis element of M as a 1-dimensional k-vector space. Let $\alpha, \beta \in k$ be such that
$$Fe = \alpha e, \quad Ve = \beta e.$$
Show that at least one of α, β is zero.

(3) Conversely, show that upon fixing a basis element e, any choice of (α,β) with at least one of α and β being 0 uniquely determines a Dieudonné module over $W(k)$ of length 1.

(4) Show that upon changing the basis $e' := \lambda e$ for some $\lambda \in k^\times$, then if one of α, β is nonzero, it can be chosen to be 1.

(5) Now we have reduced to the cases (α,β) being $(0,0)$, $(1,0)$, or $(0,1)$. There are three well-known finite flat group schemes of order p over a characteristic p field: μ_p, $\underline{\mathbb{Z}/p\mathbb{Z}}$, and α_p. For each group scheme, find out whether it is connected, étale, or neither.

[27] This ring can be naturally identified with the local Cartier ring $\mathrm{Cart}_p(K)$.

[28] This indicates that the Dieudonné ring can be naturally identified as a dense subring of the local Cartier ring.

(6) Show that the relative Frobenius kills a connected order p group scheme over k, and is an isomorphism on an étale group scheme.[29] Deduce that the $(1,0)$ Dieudonné module must correspond to $\underline{\mathbb{Z}/p\mathbb{Z}}$.
(7) Use the definition of the Verschiebung morphism on a group scheme together with Problem 2.6 to decide which of μ_p, α_p correspond to $(0,1)$, and which to $(0,0)$.

Exercise 2.6.8($\star\star$) Let $E/\overline{\mathbb{F}}_p$ be a supersingular elliptic curve. We will show there is a unique group scheme G over $\overline{\mathbb{F}}_p$ of order p^2 such that $E[p] \cong G$.

(1) Using [BC09, Theorem 7.2.4] again, a group scheme G over k of order p^2 corresponds to a Dieudonné module $M(G)$ of length 2 as a $W(\overline{\mathbb{F}}_p)$-module. Show that if G is p-torsion, then so is $M(G)$. In particular, $M(G)$ must be isomorphic to $W(\overline{\mathbb{F}}_p)/(p) \oplus W(\overline{\mathbb{F}}_p)/(p)$ as a $W(\overline{\mathbb{F}}_p)$-module.
(2) ($\star\star$) Use the connected-étale sequence and the fact that $\#E[p](\overline{\mathbb{F}}_p) = 1$ to show that $E[p]$ is connected.
(3) ($\star\star$) As an extension of Part (6) of Problem 2.6, one can show the relative Frobenius ϕ_G is a finite flat morphism of degree p, and is nilpotent on any connected finite flat group scheme G over a field. Use this to show that the kernel of ϕ_G is an order p flat group scheme, and so the Dieudonné module of $\ker(\phi_G)$ must be isomorphic to $\overline{\mathbb{F}}_p$ as a $W(\overline{\mathbb{F}}_p)$-module.
(4) The induced action of Frobenius on the Dieudonné module $M(E[p])$ is also nilpotent by functoriality, so we can choose an $\overline{\mathbb{F}}_p$-basis e_1, e_2 of $M(E[p])$ so that

$$Fe_1 = e_2, \quad Fe_2 = 0.$$

Show that $Ve_2 = 0$, and $Ve_1 = \alpha e_2$ for some $\alpha \in \overline{\mathbb{F}}_p$. Show that $\alpha \neq 0$.
(5) By scaling e_1 and using that $\overline{\mathbb{F}}_p$ is algebraically closed, show that we can let $\alpha = 1$. In particular, there is a unique Dieudonné module corresponding to the group scheme $E[p]$ for a supersingular elliptic curve.

The case of E ordinary is more straightforward. Use the fact that $\#E[p](\overline{\mathbb{F}}_p) = p$ and the fact that the connected-étale exact sequence splits for group schemes over a perfect field to show that $E[p] \cong \mu_p \times \underline{\mathbb{Z}/p\mathbb{Z}}$.

The following problem is adapted from [CO09, Exercise 4.6]. Here we investigate the endomorphism algebra of simple Dieudonné modules over an algebraically closed base field.

Exercise 2.6.9($\star\star$) Let k be an algebraically closed field containing $\mathbb{F}_p$. Let D_k be the Dieudonné ring as in Problem item 2.6, and $D_k[\frac{1}{p}]$ be the rational Dieudonné ring. Now, let (m,n) be a pair of non-negative integers such that $\gcd(m,n) = 1$. Let $N_{m,n} := D_k[\frac{1}{p}]/D_k[\frac{1}{p}](F^m - V^n)$. $N_{m,n}$ is a simple object in the isogeny category of Dieudonné module over k. We want to compute $\mathrm{End}_{D_k[\frac{1}{p}]}(N_{m,n})$.

(1) Show that $N_{m,n} \cong D_k[\frac{1}{p}]/D_k[\frac{1}{p}](F^{m+n} - p^n)$.

[29] Hint: See these notes by Andrew Snowden.

(2) Let $\varphi \in \mathrm{End}_{D_k[\frac{1}{p}]}(N_{m,n})$. Suppose $\varphi(1) = \sum_{i=0}^{m+n-1} a_i F^i$ with $a_i \in W(k)[\frac{1}{p}]$. Use the fact that $(F^{m+n} - p^n)\varphi(1) \in D_k[\frac{1}{p}](F^{m+n} - p^n)$ to show that all the a_i's lie in $W(\mathbb{F}_{p^{m+n}})[\frac{1}{p}] = \mathbb{Q}_{p^{m+n}}$[30]

(3) Show that the center of $\mathrm{End}_{D_k[\frac{1}{p}]}(N_{m,n})$ is $\mathbb{Q}_p$.

(4) Use the fact that $N_{m,n}$ is a simple left $D_k[\frac{1}{p}]$-module, show that $\mathrm{End}_{D_k[\frac{1}{p}]}(N_{m,n})$ is a central division algebra over $\mathbb{Q}_p$.

(5) Recall the definition and notation of $D_{p,h,n}$ from 2.4.4. It can be written as $\mathbb{Q}_{p^h}[F]/(F^h - p^n)$, where $F\alpha = \alpha^\sigma F$ for $\alpha \in \mathbb{Q}_{p^h}$. Show that $\varphi \mapsto \varphi(1)$ gives an isomorphism $\mathrm{End}_{D_k[\frac{1}{p}]}(N_{m,n}) \cong \mathbb{Q}_{p^{m+n}}[F]/(F^{m+n} - p^n)$.

(6) Conclude that $\mathrm{End}_{D_k[\frac{1}{p}]}(N_{m,n})$ is a central simple algebra over $\mathbb{Q}_p$ with Hasse-invariant $\frac{n}{m+n}$.

The next problem is Exercise 7.4.8 in [BC09]. It displays the role p-divisible groups play compared to ℓ-adic Tate-modules: they are more suitable for encoding information at p!

Exercise 2.6.10($\star\star\star$) Let A and B be abelian varieties over a perfect field k of characteristic $p > 0$. Recall that there is an additive antiequivalence of categories $G \mapsto \mathbb{D}(G)$ between the category of p-divisible groups over k and the category of left $W(k)[F,V]$-modules which are also finite as $W(k)$-modules.

(1) Show that the natural map

$$\mathrm{Hom}_k(A,B) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathrm{Hom}_{W(k)[F,V]}(\mathbb{D}(B[p^\infty]), \mathbb{D}(A[p^\infty]))$$

is injective.

(2) Show, however, that the natural map

$$\mathrm{Hom}_k(A,B) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathrm{Hom}_{\mathbb{Z}_p}(T_pA, T_pB)$$

is never injective[31].

(3) Now require k to be finite. If $f \in \mathrm{End}_k(A)$ is a nonzero endomorphism of A then the common characteristic polynomial $P_f \in \mathbb{Z}[T]$ of all $T_\ell(f) \in \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell A)$ with $\ell \neq \mathrm{char}k$ is also the characteristic polynomial of $\mathbb{D}(f) \in \mathrm{End}_{W(k)}(\mathbb{D}(A[p^\infty]))$.

In Problem item 2.6, we have considered examples of finite flat group schemes of order p. The following problem expands on these examples to give examples of p-divisible groups of height 1.

Exercise 2.6.11($\star\star$) Let k be an algebraically closed field of characteristic p.

(1) Let $\mathbb{G}_m/k$ be the multiplicative group scheme defined over k.

(a) Show that the multiplication $[p^i]$ is given by $x \mapsto x^{p^i}$ on the coordinate ring. Determine the Hopf algebra of the group scheme $\mathbb{G}_m[p^i]$, i.e. the kernel of $[p^i]$.

[30] That is, show that $a_i^{\sigma^{m+n}} = a_i$ for all a_i.

[31] Here $T_p(A) = TA[p^\infty](\overline{k})$ (see Problem 2.6) is the "naive" Tate module

(b) Define $G_i := \mathbb{G}_m[p^i]$. Show that $\mathbb{G}_m[p^\infty] := \{G_i\}_{i\geq 1}$, together with the inclusion $j_i : G_i \to G_{i+1}$, is a p-divisible group of height 1. This p-divisible group is often denoted μ_{p^∞}.

(c) Show that the relative Frobenius $\mathrm{F}_{G_i/k} : G_i \to G_i^{(p)} \cong G_i$, agrees with $[p] : G_i \to G_i$. Conclude that $V_{G_i/k} : G_i \to G_i$ is the identity.

(d) Let $G_{m,n}$ be the p-divisible group whose Dieudonné module is $M_{m,n} := D_k/D_k(F^m - V^n)$. By comparing the action of Frobenius and Verschiebung and using the Dieudonné-Mannin classfication[32], show that μ_{p^∞} is isogenous to $G_{0,1}$. That is, $\mathbb{D}(\mu_{p^\infty}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong M_{0,1} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

(2) Let $H_i = \underline{p^{-i}\mathbb{Z}/\mathbb{Z}}_k$ be the constant group scheme over k attached to the finite group $p^{-i}\mathbb{Z}/\mathbb{Z}$.

(a) Show that $\underline{\mathbb{Q}_p/\mathbb{Z}_p}_k := \{H_i\}_{i\geq 1}$, together with the inclusion $j_i : H_i \to H_{i+1}$, is a p-divisible group of height 1.

(b) Show that $\mathrm{F}_{H_i/k} : H_i \to H_i^{(p)} \cong H_i$ is the identity. Conclude that $V_{H_i/k}$ is $[p]$.

(c) Show that $\underline{\mathbb{Q}_p/\mathbb{Z}_p}_k$ is isogenous to $G_{1,0}$.[33]

The following problem gives the construction of Dieudonné module associated to the Serre dual of a p-divisible group.

Exercise 2.6.12($\star\star$) Let k be an algebraically closed field of characteristic p. Let M be a Dieudonné module[34], i.e. a finite free $W(k)$-module with left D_k action. We construct its dual $M^\vee$ as follows. As a $W(k)$ module, $M^\vee = \mathrm{Hom}_{W(k)}(M, W(k))$, with the action of V and F given as

$$(V \cdot h)(m) = (h(F(m)))^{\sigma^{-1}}, \quad (F \cdot h)(m) = (h(V(m)))^{\sigma}$$

for all $h \in M^\vee$ and $m \in M$.

(1) For a pair of non-negative integers (m, n) such that $\gcd(m, n) = 1$, let $M_{m,n}$ be as in Problem item 2.6. Show that $M_{m,n}^\vee \cong M_{n,m}$.

(2) We have the following facts:

- Let X/k an abelian variety. Let $X[p^\infty]$ denote its p-divisible group, and $X[p^\infty]^{\mathrm{t}}$ the Serre dual of $X[p^\infty]$, then
$$X[p^\infty]^{\mathrm{t}} \cong X^\vee[p^\infty],$$
where $X^\vee$ is the dual abelian variety.
- If G is a p-divisible group over k, and $D(G)$ is its Dieudonné module, then
$$D(G^t) \cong D(G)^\vee$$

Use the above facts, show that the Newton polygon of an abelian variety is symmetric. That is, $X[p^\infty]$ is isogenous to $\bigoplus_i (G_{m_i,n_i} \oplus G_{n_i,m_i})^{r_i}$ for some (m_i, n_i) non-negative and $\gcd(m_i, n_i) = 1$.

[32]Use the statement of [BC09, Theorem 8.1.4]. $M_{m,n} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is $D_{m,m+n}$ in the notation of Theorem 8.1.4, and is $N_{m,n}$ in the notation of Problem item 2.6.

[33]Use the fact that $\mathbb{D}(G^t) = \mathbb{D}(G)^\vee$ and $M_{m,n}^\vee = M_{n,m}$, we see that $\mathbb{G}_m[p^\infty]$ is the Serre dual (see below) of $\underline{\mathbb{Q}_p/\mathbb{Z}_p}_k$.

[34]There is an unfortunate clash of terminology with the Dieudonné module of a finite flat group scheme, which isn't necessarily torsion-free. We hope that the meanings are clear from the context.

The following problem explores examples of p-divisible groups attached to an abelian variety.

Exercise 2.6.13($\star\star$)

(1) Recall that if $f : X \to Y$ is an isogeny between abelian varieties over a field k, then $\deg(f) = \mathrm{rank}(\ker(f))$, i.e. the rank of the finite group scheme $\ker(f)$ over k. Show that the p-divisible group of a g-dimensional abelian variety over k is of height $2g$.

(2) Now let $E/\mathbb{F}_q$ be an elliptic curve.
   (a) Suppose $E/\mathbb{F}_q$ is supersingular. Recall in PSET 3, problem 7, we have shown that $\mathrm{End}^0(E)\otimes_{\mathbb{Q}}\mathbb{Q}_p \cong D_{p,2,1}$, the central division algebra over $\mathbb{Q}_p$ with Hasse-invariant $\frac{1}{2}$. Combine Problem item 2.6 and Problem item 2.6 Part (5) to conclude that $E_{\overline{\mathbb{F}}_q}[p^\infty]$ is isogenous to $G_{1,1}$.
   (b) Suppose $E/\mathbb{F}_q$ is ordinary. Recall in PSET 3, problem 9, we have shown that $L = \mathrm{End}^0(E)$ is an imaginary quadratic extension over $\mathbb{Q}$ generated by ϕ_q. Furthermore, the characteristic polynomial of ϕ_q is $T^2 - aT + q$, where $v_p(a) = 0$. Show that $L \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathbb{Q}_p \times \mathbb{Q}_p$. Use the injection

$$\mathrm{End}^0(E) \otimes_{\mathbb{Q}} \mathbb{Q}_p \to \mathrm{End}^0(E_{\overline{\mathbb{F}}_q}) \otimes_{\mathbb{Q}} \mathbb{Q}_p \to \mathrm{End}(E_{\overline{\mathbb{F}}_p}[p^\infty]) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

   to conclude that $E_{\overline{\mathbb{F}}_q}[p^\infty]$ is isogenous to $G_{1,0} \oplus G_{0,1}$.

(3) Recall that in 2.5.11, for a pair of non-negative integers (m, n) with $n < m$ and $\gcd(m, n) = 1$, we have a simple abelian variety $A/\mathbb{F}_q$ of dimension $g = m + n$, and the Frobenius ϕ_q on A has minimal polynomial $h_A(T) = T^2 - p^n T + p^g$. Moreover, $\mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong D_{p,g,m} \oplus D_{p,g,n}$. Use these to show that $A_{\overline{\mathbb{F}}_q}[p^\infty]$ is isogenous to $G_{n,m} \oplus G_{m,n}$.

As an important notion to study p-divisible groups, we introduce the Tate module of a p-divisible group.

Exercise 2.6.14($\star\star$) Let G be a p-divisible group over an affine perfect scheme S of characteristic p. Consider the inverse limit

$$TG := \varprojlim_{\times p} G[p^n].$$

Show that this limit exists in the category of schemes and TG is an scheme, flat over S. This is called the (schematic) Tate module of the p-divisible group G.[35]

(1) Show that the functor of points of TG identifies with the following functor

$$(T \to S) \mapsto \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, G_T),$$

   where $\mathbb{Q}_p/\mathbb{Z}_p$ is the constant p-divisible group over T, and G_T denotes the base change.

(2) Show that over a quasicompact noetherian test scheme U of characteristic p, the Tate module $T\mu_{p^\infty}(U)$ is trivial.

[35]Depending on conventions, sometimes the Tate module of G refers to the set of $\bar{k}$-points of TG, which is a finite free $\mathbb{Z}_p$-module.

2.7. **Honda-Tate theory and applications.** The goal of this section is to understand the proof of Honda-Tate theory and to see some applications. Throughout the section, p will be a prime, and q will be a power of p.

Exercise 2.7.1($\star\star$) 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 $a = \alpha_1 + \overline{\alpha}_1 \in [-2\sqrt{q}, 2\sqrt{q}] \cap \mathbb{Z}$. 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], [Ser
], Bao's notes, and Papikian's notes.

First, we consider the case of ordinary elliptic curves.

Let $q = p^n$. Let E be an elliptic curve over $\mathbb{F}_q$ and let $a = \mathrm{tr}(\phi_q) = \alpha_1 + \overline{\alpha}_1$ 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.

Exercise 2.7.2($\star\star$) 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[36] that there exists an ordinary elliptic curve E defined over $\mathbb{F}_q$ such that the trace of the Frobenius endomorphism $\phi_q \colon E \to E$ is equal to a.

(1) Let $P(T) = T^2 - aT + q = (T - \alpha)(T - \overline{\alpha})$. 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 $\mathrm{End}(\mathbb{C}/\mathcal{O}_K) \cong \mathcal{O}_K$ has complex multiplication.
(3) From the theory of complex multiplication, we know that there exists a number field H[37] 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 Cl(K) denote the class group

[36] Without appealing to the Honda–Tate theorem.

[37] In fact H can be taken to be the Hilbert class field of K, and we have in particular $\mathrm{Gal}(H/K) \cong \mathrm{Cl}(K)$.

of K and $\mathrm{Frob}_{\mathfrak{p}}$ be the element in $\mathrm{Gal}(H/K)$ corresponding to the prime ideal[38] $\mathfrak{p}$. Use Problem 2.7.1 part (3), show that the order of $\mathrm{Frob}_{\mathfrak{p}}$ in 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 $\mathrm{End}(\tilde{E}_{K_w}) \to \mathrm{End}(E)$ is injective and preserves degrees [Sil94, II, Proposition 4.4]. Verify that α maps to the q-Frobenius endomorphism of E.

Exercise 2.7.3($\star\star$) 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 $E/\mathbb{F}_q$.

Let $q = p^n$. Let E be an elliptic curve over $\mathbb{F}_q$ and let $a = \mathrm{tr}(\phi_q) = \alpha_1 + \overline{\alpha}_1$ 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, $p \equiv 3 \bmod 4$, and $a = 0$,
   (b) n is even, $p \equiv 2 \bmod 3$, and $a = \pm\sqrt{q}$.

Next, we construct corresponding supersingular elliptic curve for the a in Problem 2.7.3.

Exercise 2.7.4($\star\star$)

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 2.7.3.

(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)–(5) in Problem 2.7.2, 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.

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

(b) Let E be the reduction of $\tilde{E}/F_w$ modulo the prime. Follow the same argument as in part (5) of Problem 2.7.2, use the results in Problem 2.7.3 part (2) and (3), show that the order of $\text{Frob}_{\mathfrak{p}}$ in 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 2.4.9, 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 $E_\zeta/\mathbb{F}_q$ be the twist of E by ζ[39]. It has the property that if for the ℓ-adic Galois representation of E, $\rho : \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to V_\ell(E)$, $\rho(\text{Frob}_q)$ has eigenvalues $\alpha, \bar{\alpha}$, then the ℓ-adic Galois representation of $E_\zeta, \rho : \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to V_\ell(E_\zeta)$ 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 $\pi_{E_\zeta} = p^{\frac{n}{2}}$.

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.

Exercise 2.7.5($\star$)

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.

Exercise 2.7.6($\star$)

Fix a prime p. In [Man63, Conj. 2, p.76], Manin conjectured that for any admissible[40] 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

[39] For the existence of this twist, see [Bao, page 4-5].

[40] Admissible Newton polygons are defined in Problem 2 in section 2.6

$c/(c+d)$. 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.[41]

(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 $\mathrm{inv}_v(D)$ of $D := \mathrm{End}^0_{\mathbb{F}_{p^{c+d}}}(A)$.

(5) For any number field F, the following exact sequence holds.[42]

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

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, $\mathrm{inv}_v : \mathrm{Br}(F_v) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$. Use this exact sequence to check

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

(6) For a central division algebra D over a number field F, the order of $[D]$ in $\mathrm{Br}(F)$ is $\sqrt{[D:F]}$.[43] Combine this fact with parts (4) and (5) to compute $[D:F]$ for $D = \mathrm{End}^0_{\mathbb{F}_{p^{c+d}}}(A)$.

(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 $n((d,c)+(c,d))$.

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 $P_A(T)$.

[41] Hint: Consider the ordinary and supersingular cases separately.

[42] See Theorem 3.5 of these notes for more explanation about Brauer groups over global fields.

[43] See Theorem 3.6 of these notes.

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-valuation[44] 1.

Exercise 2.7.7($\star$)
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.[45]
(2) Prove that $e = 1$.[46]

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 $1/2$.

Exercise 2.7.8($\star\star$)
Let A be a g-dimensional abelian variety defined over $\mathbb{F}_q$, with Frobenius eigenvalues $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$. For $j = 1, \ldots, 2g$, 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 $\delta_A \in \{0, 1, 2, \ldots, g\}$.
(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 $\delta_A = 0$.
(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.

Exercise 2.7.9($\star\star\star$)
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 $(x, y) \to (x, \zeta_7 y)$. It extends to an action of μ_7 on C.

[44] See 2.6.2 to recall the definition of the q-valuation.
[45] Hint: Use Problem 2.5.8.
[46] Hint: Use the facts relating order and dimension of division algebras in Brauer groups from Problem 2.7.6.

(2) Let A denote the Jacobian of C. Then A is defined over $\mathbb{Q}$. Show that $\mathrm{End}^0(A_{\overline{\mathbb{Q}}})$ contains the group algebra $\mathbb{Q}[\mu_7]$. Notice that $\mathbb{Q}[\mu_7] \cong \mathbb{Q} \times \mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_7)$ is a CM field with degree 6 over $\mathbb{Q}$.

(3) Let $T := \mathrm{Hom}(\mu_7, \mathbb{C})$. Show that $\mathbb{Q}[\mu_7] \otimes_{\mathbb{Q}} \mathbb{C} \cong \prod_{\tau \in T} \mathbb{C}_\tau$, where $\mathbb{C}_\tau$ 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 $\mathbb{Q}[\mu_7]$, $V \otimes_{\mathbb{Q}} \mathbb{C} \cong \oplus_{\tau \in T} V_\tau$, where V_τ is the subspace of $V_{\mathbb{C}}$ such that ζ_7 acts by $\tau(\zeta_7)$. It turns out that $\dim_{\mathbb{C}} V_\tau = 1$ for all the non-trivial character τ and $\dim_{\mathbb{C}} V_\tau = 0$ for the trivial character. Using this fact, show that $A_{\overline{\mathbb{Q}}}$ admits complex multiplication by $\mathbb{Q}[\zeta_7]$.

(5) On the other hand, the Hodge decomposition gives $V \otimes_{\mathbb{Q}} \mathbb{C} \cong H^0(A, \Omega_A) \oplus H^1(A, \mathcal{O}_A) \cong \mathrm{Lie}(A_{\mathbb{C}})^\vee \oplus \overline{\mathrm{Lie}(A_{\mathbb{C}})}^\vee$. Here, $\mathrm{Lie}(A_{\mathbb{C}})^\vee := \mathrm{Hom}_{\mathbb{C}}(\mathrm{Lie}(A_{\mathbb{C}}), \mathbb{C})$. $\overline{\mathrm{Lie}(A_{\mathbb{C}})} \cong \mathrm{Lie}(A_{\mathbb{C}})$ as an $\mathbb{R}$ vector space, while $\sqrt{1}$ acts via i on $\mathrm{Lie}(A_{\mathbb{C}})$ and $-i$ on $\overline{\mathrm{Lie}(A_{\mathbb{C}})}$. Let $\Phi := \{\tau \in T : V_\tau \subseteq \mathrm{Lie}(A_{\mathbb{C}})^\vee\}$. 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:

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

Using the fact that $A_{\overline{\mathbb{F}}_q}[p^\infty]$ is a p-divisible group of height $2g$, show $\mathbb{D}(A_{\overline{\mathbb{F}}_q}[p^\infty])[\frac{1}{p}] \cong N_{m,n}^r$ for some $(m, n) = 1$ and $r(m+n) = 2g$. Here the $N_{m,n}$ is the $D_k[\frac{1}{p}]$-module as define in 2.6.9. We say that $A_{\overline{\mathbb{F}}_q}[p^\infty]$ is isoclinic of slope $\frac{n}{m+n}$.

(8) Recall that in 2.6.9, we have shown that $\mathrm{End}_{D_k[\frac{1}{p}]}(N_{m,n}) \cong \mathbb{Q}_{p^{m+n}}[F]/(F^{m+n} - p^n)$. Also, by the classification, $N_{m,n}^r \cong N_{mr,nr}$ as $D_k[\frac{1}{p}]$-modules, so $\mathrm{End}_{D_k[\frac{1}{p}]}(N_{m,n}^r) \cong \mathbb{Q}_{p^{r(m+n)}}[F]/(F^{r(m+n)} - p^{rn})$. Using the Shimura-Taniyama formula as stated in Lemma B.5 in the lecture notes, and the fact that $\pi_{A_{\mathbb{F}_q}}$ goes to F^{2g} in $\mathrm{End}^0_{D_k[\frac{1}{p}]}(\mathbb{D}(A_{\overline{\mathbb{F}}_q}[p^\infty])) \cong \mathbb{Q}_{p^{r(m+n)}}[F]/(F^{r(m+n)} - p^{rn})$, show that $m = n = g$. [47]

In the following problems, we sketch the proof of the following key input (Theorem B.4 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 2.3. *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 $\sigma_i : L^\dagger \to \mathbb{R}$, $i = 1, \ldots, g$ for the real places of $L^\dagger$. Recall that Φ consists of g

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

complex embeddings $\tau_i : L \to \mathbb{C}$, one above each σ_i. The first step is to construct an abelian variety of type (L, Φ) over the complex numbers.

Exercise 2.7.10($\star\star$)

(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 $\mathbb{C} \to \mathbb{R} \otimes_{\mathbb{Q}} L$. 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 $\mathcal{O}_L \hookrightarrow \mathrm{End}(T_\Phi)$, 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 $\mathrm{End}(T_\Phi)$ 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[48], we need to find an ample line bundle on it. According to the Theorem of Lefschetz [Mum70, Page 29], it suffices[49] to find a positive definite Hermitian form H on $(\mathbb{R} \otimes_{\mathbb{Q}} L)_\Phi$, whose imaginary part $\mathrm{Im}(H)$ 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

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

Show that this H satisfies the desired properties.

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 $(B, \iota_B : L \hookrightarrow \mathrm{End}^0(B))$, with an isomorphism $B \times_K \mathbb{C} \cong A_\Phi$, compatible with the L-actions.

Exercise 2.7.11($\star\star\star$)

(1) Show that $\mathbb{C}$ can be written as a directed colimit of its subalgebras that are finitely generated over $\mathbb{Q}$. Conclude that $\mathrm{Spec}\,(\mathbb{C}) = \varprojlim_i S_i$ is the limit for a directed system of schemes of finite type over $\mathbb{Q}$.[50]

(2) Apply Tag 01ZM to the abelian variety $A_\Phi / \mathrm{Spec}\,\mathbb{C}$ and conclude that there exists some i and a map of finite presentation $f_i : A_i \to S_i$, such that $A \cong A_i \times_{S_i} \mathrm{Spec}\,(\mathbb{C})$. 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 $b_1, \ldots, b_{2g}$ 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 $\mathrm{End}(A_\Phi)$ under $L \hookrightarrow \mathrm{End}^0(A_\Phi)$. 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 $\iota_i : L \hookrightarrow \mathrm{End}^0(A_i)$, and that $(A, L \hookrightarrow \mathrm{End}^0(A)) \cong (A_i, \iota_i) \times_{S_i} \mathrm{Spec}\,(\mathbb{C})$.

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

[49]The map α in the theorem can be taken to be the trivial map that sends $\mathcal{O}_L$ to 1.

[50]In fact we can replace $\mathbb{Q}$ by $\mathbb{Z}$ in the statement.

(5) First use the Hilbert Nullstellensatz to show that the residue field $K(s)$ of any closed point $s \in S_i$ is a number field. Now take the fiber of A_i over any such s and denote it by A_s. Assume S_i to be connected. Show that $\mathrm{End}^0(A_i) \hookrightarrow \mathrm{End}^0(A_s)$ and hence A_s is equipped with an L-action.

In fact, by increasing i if necessary, we may assume $S_i = \mathrm{Spec}\,(R_i)$ 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 $\Gamma(A_\Phi, \Omega_{A_\Phi/\mathbb{C}}) = \mathrm{Lie}(A_\Phi)^\vee := (\mathbb{R} \otimes_{\mathbb{Q}} L)^\vee_\Phi$ 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.

Exercise 2.7.12($\star\star$)

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'.[51]

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 $I(v) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is finite in $\mathrm{Aut}(T_\ell A)$.
(3) Recall from PSET 3, Problem 4(1) that since $L \hookrightarrow \mathrm{End}^0_K(A)$, $V_\ell A = T_\ell A \otimes \mathbb{Q}_\ell$ 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 $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ on $V_\ell A$ commutes with the action of $L \otimes \mathbb{Q}_\ell$, and therefore the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is contained in $\mathrm{GL}_1(L \otimes \mathbb{Q}_\ell)$. Use this to show that the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ 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 $\mathrm{Gal}(K_v^{\mathrm{ab}}/K_v^{\mathrm{un}})$, where we view $I(v) = \mathrm{Gal}(\overline{K_v}/K_v^{\mathrm{un}}) \subset \mathrm{Gal}(\overline{K_v}/K_v) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, 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 $\mathrm{Gal}(K_v^{\mathrm{ab}}/K_v^{\mathrm{un}}) \cong \mathcal{O}_{K_v}^\times$. 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.

[51] See [Liu, Cor. 4.10] for a proof.

(6) Observe that the pro-ℓ group $1 + \ell\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell A)$ is a finite-index subgroup of $\mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell A)$. Conclude that the image of any map from a pro-p group to a pro-ℓ group must have finite image.

Tate proved that:

Theorem 2.4. *Let A be an abelian variety over a finite field.*

(1) The algebra $\mathrm{End}^0(A)$ is semi-simple. Suppose A is simple; the center of $\mathrm{End}^0(A)$ equals $L := \mathbb{Q}(\pi_A)$.

(2) Suppose A is simple; then

$$2g = [L : \mathbb{Q}] \cdot \sqrt{[D : L]},$$

where g is the dimension of A. Hence: every abelian variety over a finite field admits smCM. Moreover we have

$$f_A = (\mathrm{Irr}_{\pi_A})^{\sqrt{[D:L]}}.$$

Here f_Z is the characteristic polynomial of the Frobenius morphism $\mathrm{Fr}_{A,\mathbb{F}_q} : A \to A$, and Irr_{π_A} is the irreducible polynomial over $\mathbb{Q}$ of the element π_A in the finite extension $L/\mathbb{Q}$.

(3) Suppose A is simple,

$$\mathbb{Q} \quad \subset L := \mathbb{Q}(\pi_A) \quad \subset \quad D = \mathrm{End}^0(A).$$

The central simple algebra D/L
- does not split at every real place of L,
- does split at every finite place not above p,
- and for $v \mid p$ the invariant of D/L is given by

$$\mathrm{inv}_v(D/L) = \frac{v(\pi_A)}{v(q)} \cdot [L_v : \mathbb{Q}_p] \bmod \mathbb{Z},$$

where L_v is the local field obtained from L by completing at v.

Exercise 2.7.13($\star\star$)(Construct abelian varieties with prescribed Newton polygons) Let L be an imaginary quadratic field which is split at p. Let r, s be positive rational numbers such that $\gcd(r, s) = 1$ and $2r < s$. Use Tate's theorem to show that there exists a simple s-dimensional abelian variety A over a finite field $\mathbb{F}_q \supset \mathbb{F}_p$ such that $\mathrm{End}(A)^0 = L$ and the slopes of the Newton polygon of A are $\frac{r}{s}$ and $\frac{s-r}{s}$.

3. Heights on abelian varieties

3.1. **Height functions.** The goal of this section is to get comfortable with height functions on abelian varieties, especially the Weil height and the Weil height machine.
Exercise 3.1.1($\star$) Let $P \in \mathbb{P}^n(\mathbb{Q})$, and write P as

$$P = [a_0, a_1, \ldots, a_n] \text{ with } a_0, \ldots, a_n \in \mathbb{Z} \text{ and } \gcd(a_0, \ldots, a_n) = 1$$

Prove directly from the Definition 4.11 that

$$h(P) = \log \max\{|a_0|, |a_1|, \ldots, |a_n|\}.$$

Exercise 3.1.2($\star$)

(a) Prove the product formula (Proposition 4.3(a), first for $K = \mathbb{Q}$, and then for arbitrary number fields.
(b) Prove the extension formula Proposition 4.3(b).

Exercise 3.1.3($\star$) Let C/K be a smooth projective curve, and let $D_1, D_2 \in \mathrm{Div}(C)$ be divisors with $\deg(D_1) \geq 1$. Prove that

$$\lim_{\substack{t \in C(\bar{K}) \\ h_C(t) \to \infty}} \frac{h_{C,D_2}(t)}{h_{C,D_1}(t)} = \frac{\deg D_2}{\deg D_1}.$$

[Hint: Divisors on a curve C are algebraically equivalent if and only if they have the same degree.]

Exercise 3.1.4($\star$) Let $\beta \in \overline{\mathbb{O}}$ with $\beta \neq 0$, and fix a minimal polynomial

$$F_\beta(X) = a_0 X^d + a_1 X^{d-1} + \cdots + a_d \in \mathbb{Z}[X] \quad \text{with } \gcd(a_0, \ldots, a_d) = 1$$

Factor F_β over $\mathbb{C}$ as

$$F_\beta(X) = a_0 (X - \beta_1)(X - \beta_2) \ldots (X - \beta_d).$$

Prove that

$$h([\beta, 1]) = \frac{1}{d} \left(\log |a_0| + \sum_{i=1}^{d} \max\{|\beta_i|, 1\} \right).$$

Exercise 3.1.5($\star$) Let K be a number field, and let $F(X) \in K[X]$ be a polynomial of degree $d \geq 1$ that factors completely over K, say

$$F(X) = a_0 X^d + a_1 X^{d-1} + \cdots + a_d = (X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_d).$$

Prove that

$$-d \cdot \log(2) \leq h([a_0, \ldots, a_d]) - \sum_{i=1}^{d} h(\alpha_i) \leq (d-1)\log(2).$$

This gives an explicit estimate relating the height of the coefficients of a polynomial to the heights of its roots. [Hint: Prove by induction on d a similar estimate for each $v \in M_K$, and then sum over $v \in M_K$.]

Exercise 3.1.6($\star\star$) Let $m \geq 2$, let $D \in \mathbb{Z}$ be an integer that is m th-power-free, and let

$$P = [1, \alpha_1, \ldots, \alpha_N] \in \mathbb{P}^N(\overline{\mathbb{Q}})$$

be a point whose coordinates generate $\mathbb{Q}\left(D^{1/m}\right)$, i.e.,

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_N) = \mathbb{Q}\left(D^{1/m}\right).$$

Prove that

$$h(P) \geq \frac{1}{2m-2} \left(\frac{1}{m} \log |D| - m \log m \right).$$

[Hint: Try $N = 1$ and/or $m = 2$ first.]

Exercise 3.1.7($\star\star$) Let $K/\mathbb{Q}$ be a number field, and let $\Delta \in K^*$. We define the m-power free height of Δ to be

$$h_K^{(m)}(\Delta) := \min_{\beta \in K^*} h_K\left(\beta^m \cdot \Delta\right).$$

Prove that

$$h_K^{(m)}(\Delta) \asymp \log \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{Disc}\left(K\left(\Delta^{1/m}\right)/K\right)\right) \quad \text{for all } \Delta \in K^*,$$

where the implied constants may depend on K and m.

Exercise 3.1.8($\star\star$) Let h_1 and h_2 be the two height functions on the space of elliptic curves defined by (4.3) and (4.4). Prove that there are positive constants C_{11} and C_{12} so that for all number field E/K and all elliptic curves E/K we have

$$C_{11}h_1(E/K) \le h_2(E/K) \le C_{12}h_1(E/K).$$

Exercise 3.1.9($\star\star$)

(a) Give an example of a dominant rational map

$$\varphi : \mathbb{P}^2 \to \mathbb{P}^2$$

such that functoriality (Theorem 4.8(b)) fails.

(b) Let $\varphi : \mathbb{P}^2 \to \mathbb{P}^2$ be a dominant rational map of degree d. Prove that there are constants $C_{13}(\varphi) > 0$ and $C_{14}(\varphi) \ge 0$ and a non-empty Zariski open set $U_\varphi \subset \mathbb{P}^2$ so that

$$h(\varphi(P)) \ge C_{13}(\varphi) \cdot h(P) - C_{14}(\varphi) \text{ for all } P \in U(\bar{K}).$$

(c) Prove that the constant C_{13} in (b) may be chosen to depend only on the degree of φ.

(d) Generalize (c) to $\mathbb{P}^N$ with a constant $C_{13}(N,d)$ that depends only on the dimension of $\mathbb{P}^N$ and the degree d of the map φ.

(e) The height expansion ratio for degree d maps of $\mathbb{P}^N$ is, roughly speaking, the best possible value for the constant $C_{13}(N,d)$ in (d). More precisely, we define

$$\bar{\mu}_d\left(\mathbb{P}^N\right) = \inf_{\substack{\varphi:\mathbb{P}^N\to\mathbb{P}^N \\ \varphi \text{ dominant} \\ \deg(\varphi)=d}} \sup_{\emptyset\neq U\subset\mathbb{P}^N} \liminf_{\substack{P\in U(\bar{\mathbb{Q}}) \\ h(P)\to\infty}} \frac{h(\varphi(P))}{h(P)}$$

Let $d \ge 2$. Prove that

$$\bar{\mu}_d\left(\mathbb{P}^1\right) = d \quad \text{and} \quad \bar{\mu}_d\left(\mathbb{P}^N\right) \le \frac{1}{d^{N-1}} \quad \text{for } N \ge 2.$$

(f) ($\star\star\star$) Find a formula for $\bar{\mu}_d\left(\mathbb{P}^N\right)$ as a function of N and d. [Hint: For $N \ge 2$, this is an open problem!! See [Sil11].]

3.2. **The canonical heights.** Problems 3.2.1 to 3.2.6 is to get you familiarized with the definition and properties of the canonical (Néron-Tate height) on abelian varieties. Problem 3.2.1 and 3.2.7 contains open problems that may be of interest to you.

Exercise 3.2.1 Let $P, Q \in A(K)$.

(a) ($\star$) Prove that

$$P - Q \in A(K)_{\mathrm{tors}} \quad \Longrightarrow \quad \hat{h}_{A,D}(P) = \hat{h}_{A,D}(Q).$$

(b) ($\star\star\star$) Let $K/\mathbb{Q}$ be a number field. Is the converse to (a) true? I do not know any counterexamples!

Exercise 3.2.2($\star$) Let A/K be an abelian variety, and let $D \in \mathrm{Div}(A)$ be an anti-symmetric divisor, i.e., $[-1]^*D \sim -D$. Prove that the map

$$\hat{h}_{A,D} : A(\bar{K}) \longrightarrow \mathbb{R}$$

is linear, i.e., prove that $\hat{h}_{A,D}(P+Q) = \hat{h}_{A,D}(P) + \hat{h}_{A,D}(Q)$.

Exercise 3.2.3($\star$) Let A/K be an abelian variety, and let $D \in \mathrm{Div}(A)$ be a (not necessarily symmetric or anti-symmetric) divisor on A.

(a) Prove that the Nron-Tate pairing $\langle \cdot, \cdot \rangle_{A,D}$ as given in Definition 5.5 is a symmetric bilinear pairing.

(b) Let $D, D' \in \mathrm{Div}(A)$. Prove that

$$\langle \cdot, \cdot \rangle_{A,D+D'} = \langle \cdot, \cdot \rangle_{A,D} + \langle \cdot, \cdot \rangle_{A,D'}$$

(c) Define the symmetrization of D to be

$$D^\sigma := \frac{1}{2}\left(D + [-1]^*D\right).$$

Prove that D^σ is symmetric, and that

$$\langle \cdot, \cdot \rangle_{A,D^\sigma} = \langle \cdot, \cdot \rangle_{A,D}.$$

(In fancier terminology, this shows that the Nron-Tate pairing for D depends on only the algebraic equivalence class of D, i.e., on the image of D in the Nron-Severi group $\mathrm{NS}(A)$.)

Exercise 3.2.4($\star$) Consider the map

$$q : \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{R}, q(a + b\sqrt{2}) = |a + b\sqrt{2}|^2,$$

where we view $\mathbb{Z}[\sqrt{2}]$ as a free $\mathbb{Z}$-module of rank 2.

(a) Prove that q is a positive definite quadratic form on $\mathbb{Z}[\sqrt{2}]$.

(b) Prove that the extension of q to $\mathbb{Z}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{R}$ is not positive definite.

Exercise 3.2.5($\star\star$) We fix an ample divisor $H \in \mathrm{Div}(A)$, and we use H to define the Rosatti involution

$$\mathrm{End}(A)_{\mathbb{Q}} \longrightarrow \mathrm{End}(A)_{\mathbb{Q}}, \quad \alpha \longmapsto \alpha' := \varphi_H^{-1} \circ \hat{\alpha} \circ \varphi_H,$$

and a map

$$\mathrm{NS}(A)_{\mathbb{Q}} \longrightarrow \mathrm{End}(A)_{\mathbb{Q}}, \quad D \longmapsto \varphi_H^{-1} \circ \varphi_D;$$

see Definition 3.18 in Silverman's lecture notes. Prove that the canonical height pairing satisfies the following two formulas:

(a) $\langle \alpha(P), Q \rangle_{A,D} = \langle P, \alpha'(Q) \rangle_{A,H}$.

(b) $\langle P, Q\rangle_{A,D} = \langle P, \Phi_D(Q)\rangle_{A,H}$. (These formulas are proven in [Ber95, Proposition 3] and [KS16, Propositions 27 & 28], where they are then applied to solve various problems.)

Exercise 3.2.6($\star\star$) Let A/K and B/K be abelian varieties, let $\varphi : B \to A$ an isogeny, and let $D \in \mathrm{Div}(A)$. Prove that

$$\hat{h}_{A,D}(\varphi(P)) = \hat{h}_{B,\varphi^* D}(P) \text{ for all } P \in B(\bar{K}).$$

Exercise 3.2.7($\star\star$ with part (c) an open problem)

(a) Let E be an elliptic curve with CM by the order $\mathbb{Z} + \tau\mathbb{Z}$. Let q be the Néron-Tate height on E. Show that $q(\tau(P)) = N(\tau)q(P)$ for any $P \in A(K)$ where K is a number field and N is the norm map.

(b) Let $f : X \to X'$ be a finite morphism between (quasi-)projective varieties over a number field k, and let h and h' denote height functions on $X(\bar{k})$ and $X'(\bar{k})$, respectively, defined (up to $O(1)$) using embeddings of X and X' in projective spaces. Prove that there exist constants $c_1, c_2 > 0$ such that $h(x) \le c_1 h'(f(x)) + c_2$ for all $x \in X(\bar{k})$.

(c) ($\star\star\star$)(This is a question that came up during my research) Let A be an abelian variety of dimension greater than 1 with CM by the order $\mathbb{Z}+\tau_1\mathbb{Z}+...+\tau_{2g-1}\mathbb{Z}$. Let q be the Neron-Tate height defined with respect to a symmetric ample divisor D. I was wondering if there are similar arguments for the higher dimensional analog. Say if P is a K-point on A, is it true that $q(\tau_i(P)) \le Cq(P)$ where C is an absolute constant that only depends on τ_i and A, D? Or more generally, you can replace τ_i with any isogeny. I guess if this was true then C should be $\mathrm{Tr}_{E^+/\mathbb{Q}}(\tau\bar{\tau})$ up to a constant. Please let me know if you find a proof!

Exercise 3.2.8($\star\star$) Learn how to compute canonical heights on elliptic curves using a computer algebra system such as Magma, Sage, or PARI-GP. Hint: If you ask ChatGPT "How do I compute the canonical height on an elliptic curve using XXX," it will give you some sample code that may or may not actually work. This exercise asks you to compute some canonical heights. Feel free to use a computer algebra system. We consider the elliptic curve

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

and the points

$$\begin{aligned} &P = (-2, 3), \quad Q = (2, 5), \quad R = (-1, 4), \\ &S = (8, 23), \quad T = (52, 375), \quad U = (5234, 378661), \\ &V = \left(\frac{94}{25}, \frac{1047}{125}\right), \quad W = \left(\frac{19}{25}, \frac{522}{125}\right). \end{aligned}$$

Verify that $P, Q, \ldots, W$ are points in $E(\mathbb{Q})$.

(a) Compute the canonical heights of the points $P, Q, \ldots, W$.

(b) Compute the ratios

$$\frac{\hat{h}_E(Q)}{\hat{h}_E(P)}, \frac{\hat{h}_E(R)}{\hat{h}_E(P)}, \frac{\hat{h}_E(S)}{\hat{h}_E(P)}, \frac{\hat{h}_E(W)}{\hat{h}_E(P)}.$$

Draw some conclusions and check that your conclusions are correct.

(c) Compute the 2-by-2 height pairing matrix for P and Q and take its determinant. What can you conclude?

(d) Compute the 3-by-3 height pairing matrix for P, Q, and U and take its determinant. What can you conclude? Verify your conclusion with an explicit algebraic formula.

3.3. **Faltings height and Finiteness theorems for elliptic curves.** One of the important application of the theory of heights is the role it plays in the proof of the Faltings' theorem and one of the key steps in proving Faltings' theorem is to prove the finiteness theorems of abelian varieties. We will take our tour through the proof of the finitness theorems for elliptic curves.

Theorem 3.1. *(Finiteness I, or Conjecture T) Let A be an abelian variety over a number field K. Then there are only finitely many isomorphism classes of abelian varieties over K isogenous to A.*

The proof of Theorem 3.1 consists of two theorems on heights. The first one is about bound on the modular height.

Let (A, λ) be a polarized abelian variety over K of dimension g and degree d. Let $\mathcal{A}_{g,d}$ be the Siegel modular variety with its canonical projective embedding. Then associated with (A, λ) we have a point $j(A, \lambda) \in \mathcal{A}_{g,d}(K)$. We define the modular height of (A, λ) to be $h_M(A, \lambda) = h(j(A, \lambda))$. When $g = d = 1$, the modular height of an elliptic curve is simply the height of its j-invariant.

Theorem 3.2. *(Height I) Let C be a constant. Then there are only finitely many isomorphism classes of polarized abelian varieties (A, λ) over K of dimension g, degree d having semistable reduction everywhere and $h_M(A, \lambda) \leq C$.*

And the second describes how the Faltings' height change inside an isogeny class:

Theorem 3.3. *(Height II) Let A be an abelian variety over K having semistable reduction everywhere. Then h_F is bounded in the isogeny class of A.*

Assuming these two parts, then together with the semistable reduction theorem (every abelian variety has semistable reduction after a finite extension), we can deduce Finiteness I. To combine the Height I result for h_M and Height II result for h_F, we a comparison theorem between h_M and h_F : the boundedness of one of them implies the boundedness of the other.

Theorem 3.4. *(Comparison of heights) There exists constants c_1, c_2, c_3 such that for abelian varieties (A, λ) over K with semistable reduction everywhere,*

$$|h_F(A) - c_1 h_M(A, \lambda)| \leq c_2 \log h_M(A, \lambda) + c_3.$$

Now the road-map for proving Finiteness I is

$$\text{Height I + Height II + Comparison} \Longrightarrow \text{Finiteness I.} \tag{3.1}$$

Let E be an elliptic curve. We prove Theorem 3.1 by two different approaches. The first one is to establish an explicit formula of the Faltings height $h_F(E)$ and prove the comparison theorem of the Faltings height and the modular height for elliptic curves as follows:

Exercise 3.3.1(a)($\star\star\star$) Let K be a number field. Let E/K be an elliptic curve. Suppose $E\left(\overline{K_v}\right) \cong \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau_v$ for $v \in M_K^\infty$. Prove that

$$h_F(E) = \frac{1}{12[K:\mathbb{Q}]}\left(\log\left|\mathbb{N}_{K/\mathbb{Q}}\Delta_{E/K}\right| - \sum_{v\in M_K^\infty} n_v \log\left(\left|\Delta\left(\tau_v\right)\right|\left(\operatorname{Im}\tau_v\right)^6\right)\right),$$

where $\Delta_{E/K}$ is the minimal discriminant and $\Delta(\tau) = (2\pi)^{12} q\prod_n (1-q^n)^{24}$ is the modular discriminant function.

Remark 3.5. When $K = \mathbb{Q}$, we again recover $h_F(E) = -\frac{1}{2}\log(\operatorname{Im}\tau)$ for the minimal Weierstrass equation $y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$.

Exercise 3.3.1(b) Show that there exists some constant C such that for elliptic curves E/K with semistable reduction everywhere,

$$\left|h_F(E) - \frac{1}{12}h_M(E)\right| \le \frac{1}{2}\log\left(1 + h_M(E)\right) + C.$$

Finally, use Siegel's theorem on the integral points of elliptic curves to give a completely different direct proof of Finiteness I for elliptic curves.

Theorem 3.6. *(Siegel) Let E/K be an (affine) elliptic curve, $S \subseteq M_K$ be a finite set containing M_K^∞ and $R_S = \{x \in K : \operatorname{ord}_v x \ge 0, \forall v \notin S\}$ be the ring of S-integers. Then the set of integral points $\{P \in E(K) : x(P) \in R_S\}$ is finite.*

Exercise 3.3.2(a)($\star\star\star$) Use Siegel's theorem to prove the following theorem (original proof is due to Shafarevich).

Theorem 3.7. *Let $S \subseteq M_K$ be a finite set containing M_K^∞. Then there are only finitely many isomorphism classes E/K having good reduction outside S.*

Exercise 3.3.2(b) Use part(a) and show that for a fixed elliptic curve E/K, there are only finitely many elliptic curves K'/K which are isogenous to E.

References

[Bao] Chengyang Bao, *Honda-Tate Theorem for Elliptic Curves.*

[BC09] Olivier Brinon and Brian Conrad, *CMI Summer School notes on p-adic Hodge theory (preliminary version)*, 2009. Available at https://math.stanford.edu/∼conrad/papers/notes.pdf.

[Ber95] D. Bertrand, *Minimal heights and polarizations on group varieties*, Duke Math. J. (1995), 223250.

[CO09] Ching-Li Chai and Frans Oort, *Moduli of abelian varieties and p-divisible groups*, Arithmetic geometry **8** (2009), 441–536.

[Deu41] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272. MR5125

[EVdGM12] Bas Edixhoven, Gerard Van der Geer, and Ben Moonen, *Abelian varieties*, 2012. Available at `http://van-der-geer.nl/~gerard/AV.pdf`.

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. No. 52, Springer-Verlag, New York-Heidelberg, 1977. MR463157

[KS16] S. Kawaguchi and J. H. Silverman, *Dynamical canonical heights for jordan blocks, arithmetic degrees of orbits, and nef canonical heights on abelian varieties*, Trans. Amer. Math. Soc. (2016), 5009–5035.

[Len96] H. W. Lenstra Jr., *Complex multiplication structure of elliptic curves*, J. Number Theory **56** (1996), no. 2, 227–241. MR1373549

[Liu] Tong Liu, *CM abelian varieties*.

[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, *Qabelian varieties*, Oxford University Press, published for the Tata Institute of Fundamental Research, 1970.

[Neu13] Jürgen Neukirch, *Algebraic number theory*, Vol. 322, Springer Science & Business Media, 2013.

[Poo06] Bjorn Poonen, *Lecture on rational points on curves*, 2006.

[Ser] Jean-Pierre Serre, *Rational points on curves over finite fields* (Alp Bassa, Elisa Lorenzo García, Christophe Ritzenthaler, and René Schoof, eds.), 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. MR4242817

[Ser65] ———, *Zeta and L functions*, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), 1965, pp. 82–92. MR194396

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, Second, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094

[Sil11] J. H. Silverman, *Height estimates for equidimensional dominant rational maps*, J. Ramanujan Math. Soc. (2011), 145163.

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Annals of Mathematics (1968), 492–517.

[Voi] John Voight, *Quaternion algebras*, Graduate Texts in Mathematics, vol. 288, Springer, Cham, [2021] ©2021. MR4279905

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR265369