

ABELIAN VARIETIES OVER FINITE FIELDS: PROBLEM SET 4

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

Instructions: The goal of this problem set is to assimilate the Weil conjectures for abelian varieties and curves. Problems marked $(\star)$, $(\star\star)$, and $(\star\star\star)$ denote beginner, intermediate, and advanced problems, respectively. For the computational problems () you may use [CoCalc](#) or [MAGMA](#)'s online calculators.

Notation: As customary, 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 .

Problem 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.^a
- (2) Let $\text{Max}(A)$ be the set of maximal ideals in A ; this is called the **maximal spectrum** of A . Show that $\text{Max}(A)$ is countable.

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

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

- (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) $A = R[x, y]$.

^aConsider the structure map $\mathbb{Z} \rightarrow A$ composed with the projection $A \rightarrow A/\mathfrak{m}$. What are the possibilities for the kernel of the composition?

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

Problem 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.^{ab}
- (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 $N(P) := \#\kappa(P)$. Define the **zeta function** of X as the formal Euler product

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

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

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

^bA possibly useful result from commutative algebra is the [Artin–Tate lemma](#).

Problem 3 (★★)

In this problem we are going to show that the zeta function defined in Problem 2 defines a holomorphic function. This is [Ser65, Theorem 1].

Theorem A. *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 $\operatorname{Re}(s) > \dim X$.^a*

To prove this, proceed as follows:

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

^aIn particular, $\zeta_X(s)$ is a Dirichlet series $\sum a_n/n^s$ with integral coefficients.

^bThis generalizes [Har77, Appendix C, Problem 5.3].

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.

Problem 4 (★★)

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

$$\sum_{d|n} dm_d = \#X(\mathbb{F}_{q^n}).$$

- (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

$$\#X(\mathbb{F}_q), \#X(\mathbb{F}_{q^2}), \dots, \#X(\mathbb{F}_{q^g}).$$

- (4) ($\Rightarrow$) 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) ($\Leftarrow$) 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 ,
 and outputs the first N terms of the zeta function of the hyperelliptic curve $X/\mathbb{F}_q$ with affine equation $y^2 = f(x)$.^a

^aCompare the efficiency of your function with the built-in intrinsics!

The following problem is [Poo06, Problem 3.10].

Problem 5 (★)

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.

Problem 6 (★★)

Let $E/\mathbb{F}_p$ be the elliptic curve

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

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

$$(6.a) \quad Z(E, T) = \frac{(1 - \alpha T)(1 - \bar{\alpha} T)}{(1 - T)(1 - pT)}$$

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

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

$$(6.b) \quad \#\{x \in \mathbb{F}_q : x^k = a\} = \sum_{j=1}^k \chi_{k,q}^j(a), \quad k = 2, 4$$

for $a \neq 0$.

- (3) Note that

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

By applying [Equation 6.b](#), 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

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

- (4) Conclude that

$$\#E(\mathbb{F}_q) = q + 1 - \alpha_q - \bar{\alpha}_q$$

where $\alpha_q = -\chi_{2,q}(n)J(\chi_{2,q}, \chi_{4,q})$.

- (5) Let $N : \mathbb{F}_{p^r}^* \rightarrow \mathbb{F}_p^*$ 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 6.a](#).

Problem 7 (★)

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 PSET2, Problem 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 $\alpha, \beta \in \mathbb{C}$ 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 $\sigma: \mathbb{Q}(\alpha) \rightarrow \mathbb{C}$, $|\sigma(\alpha)| = q^{1/2}$. Two q -Weil numbers α, α' are **conjugate** if they are in the same orbit under the action of $\text{Gal}_{\mathbb{Q}}$. In particular, there exists a field isomorphism $\mathbb{Q}(\alpha) \rightarrow \mathbb{Q}(\alpha')$ mapping α to α' , so that α and α' have the same minimal polynomial over $\mathbb{Q}$.

Problem 8 (★)

Let α be a q -Weil number. Show that there are two possibilities:

- (1) $\mathbb{Q}(\alpha)$ has at least one real embedding $\phi: \mathbb{Q}(\alpha) \rightarrow \mathbb{R}$. 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.

Problem 9 (★)

Let D be a finite dimensional division algebra over $\mathbb{Q}$. An involution $\dagger: D \rightarrow D$ 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

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

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

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 $\psi: L \rightarrow \mathbb{C}$, $\dagger$ 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.

Problem 10 (★★)

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

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

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

- (1) Let $\mathcal{L}$ be a 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 $\lambda: A \rightarrow A^\vee$. 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 $\varphi^\vee: A^\vee(\mathbb{F}_q) \rightarrow A^\vee(\mathbb{F}_q)$ 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 $A(\mathbb{F}_q) \rightarrow A^\vee(\mathbb{F}_q)$.

- (4) Combine with the fact that Rosati involution is positive and Problem 9, 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 $\phi_q: A \rightarrow A$ 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].

Problem 11 (★★)

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 $D := \text{End}^0(A)$ 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^a

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

- (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 $\text{inv}_v(D \otimes_L L_v)$.^b
- (4) Recall the definition and notation of $D_{p,h,m}$ in PSET 2, Problem 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

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

^a $h_A(T)$ 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 .

^bHint: Use [CO09][Theorem 10.17]

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.

Problem 12 (★★)

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

$$\mu: C \times E \rightarrow C.$$

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

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

^aIn fact, the equality $\text{Jac}(C) = E$ is true as functors. That is, for any k -algebra R , we have $\text{Jac}(C)(R) = E(R)$.

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

Problem 13 (★)

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 $\text{Jac}(C)(L) = E(L)$ where $L/\mathbb{Q}$ is an algebraic extension of $\mathbb{Q}$.

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](#).

Problem 14 (★★)

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

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

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

- (3) Split the sum into two parts

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

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

Use the Riemann-Roch theorem to show that

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

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

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

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) (★★★) Use the involution $\mathcal{L} \mapsto \omega_C \otimes \mathcal{L}^{-1}$ 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.

Problem 15 (★★★ [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^a 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.

^aIn particular, the form stated in [Har77, Exercise V.1.9].

REFERENCES

- [CO09] Ching-Li Chai and Frans Oort, *Moduli of abelian varieties and p -divisible groups*, Arithmetic geometry **8** (2009), 441–536.
- [Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. No. 52, Springer-Verlag, New York-Heidelberg, 1977. MR 463157
- [Poo06] Bjorn Poonen, *Lecture on rational points on curves*, <https://math.mit.edu/~poonen/papers/curves.pdf>, March 2006.
- [Ser65] Jean-Pierre Serre, *Zeta and L functions*, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 82–92. MR 194396