

Weil Conjecture for Elliptic Curves

Shenghao Sun

Dec. 13, 2005

Abstract

Weil made his conjecture on the number of solutions of polynomials over finite fields in 1949, and he also proved his famous conjecture for curves. Here we show how to prove this conjecture for elliptic curves. The way we will prove is due to Hasse. It makes essential use of the group scheme structure of elliptic curves, which makes it different from the way that Weil used for a general curve.

We use R. Hartshorne's Algebraic Geometry for our main reference. Actually the whole paper comes from some exercises in this book, in section 4.4. We also use some results from J. H. Silverman's The Arithmetic of Elliptic Curves. They'll be indicated in the proof.

1 Weil Conjecture

First we state the Weil conjecture. Let X be a projective scheme of finite type over the finite field $k = \mathbb{F}_q$, with dimension n , and let $\bar{X} = X \times_{\mathbb{F}_q} \bar{\mathbb{F}}_q$ be the projective scheme obtained by base extension to the algebraic closure of \mathbb{F}_q . Let N_r be the number of points on \bar{X} with "coordinates" in the subfield $k_r = \mathbb{F}_{q^r}$, i.e., $N_r = \#X(k_r) = \#\text{hom}_k(\text{Spec}(k_r), X)$. N_r is a finite number. Indeed, X is projective over k , so it can be embedded into some \mathbb{P}_k^n as a closed subscheme. The induced map $\text{hom}_k(\text{Spec}(k_r), X) \rightarrow \text{hom}_k(\text{Spec}(k_r), \mathbb{P}_k^n)$ is injective, and $\#\text{hom}_k(\text{Spec}(k_r), \mathbb{P}_k^n) = \sum_{i \leq n} q^{ri}$ is finite. Note that to give a morphism $\text{Spec}(k_r) \rightarrow X$ is equivalent to giving a point $x \in X$ together with a field extension $k(x) \hookrightarrow k_r$. Suppose $k(x) \cong k_i$ for some $i|r$. Then different embeddings $k_i \hookrightarrow k_r$ are related by automorphisms of k_i , so the number of embeddings is $\#\text{Gal}(k_i/k) = \#\mathbb{Z}/(i) = i$. When we make the base extension $\bar{X} = X \times_k \bar{k}$, the point x splits into i different points, each corresponding to an embedding $k_i \hookrightarrow \bar{k}$. So N_r thus defined is really the number of points in \bar{X} with coordinates in k_r . Let $M_i = \#\{x \in X | k(x) \cong k_i\}$, then $N_r = \sum_{i|r} M_i \cdot i$. We define the zeta function of X/k to be $Z(X, t) = Z(t) = \exp(\sum_{r \geq 1} \frac{N_r t^r}{r}) \in \mathbb{Q}[[t]]$. We will assume in addition that X is smooth, so that \bar{X} is a nonsingular variety over \bar{k} , and we can talk about the tangent sheaf of \bar{X} in the conjecture.

(Weil Conjecture) Let X be a smooth projective scheme of finite type over k of dimension n .

1. Rationality. $Z(t) \in \mathbb{Q}(t)$.
2. Functional equation. Let $E = \deg c_n(\mathcal{T}_{\bar{X}}) \in \mathbb{Z}$ be the degree of the top Chern class of the tangent sheaf of \bar{X} . Then

$$Z\left(\frac{1}{q^n t}\right) = \pm q^{nE/2} t^E Z(t).$$

3. Analog of Riemann Hypothesis. $Z(t) = \frac{P_1(t)P_3(t)\cdots P_{2n-1}(t)}{P_0(t)P_2(t)\cdots P_{2n}(t)}$, where $P_0(t) = 1 - t$, $P_{2n}(t) = 1 - q^n t$, $P_i(t) \in \mathbb{Z}[t]$ for all i . For $1 \leq i \leq 2n - 1$, if we factorize $P_i(t)$ over \mathbb{C} , we have

$$P_i(t) = \prod_j (1 - \alpha_{i,j} t),$$

where each $\alpha_{i,j}$ is an algebraic integer with absolute value $|\alpha_{i,j}| = q^{i/2}$.

4. Betti numbers. Let $B_i(X) = \deg(P_i(t))$, and call them betti numbers for X . Then we have $E = \sum_i (-1)^i B_i$, which is analogous to the Gauss-Bonnet formula for complex manifolds. Furthermore, suppose $K \subset \mathbb{C}$ is a number field, and $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal. Let X be a smooth projective scheme of finite type over \mathcal{O}_K , then we can make base extensions to both $\mathcal{O}_K/\mathfrak{p}$, which is a finite field, and \mathbb{C} . For the scheme $X \times_{\mathcal{O}_K} \mathbb{C}$ we have its associated analytic space $(X \times_{\mathcal{O}_K} \mathbb{C})_h$, for which we can talk about its topological betti numbers b_i , which are defined to be the rank of the i th singular cohomology group $H^i((X \times_{\mathcal{O}_K} \mathbb{C})_h, \mathbb{Z})$. For the scheme $X \times_{\mathcal{O}_K} (\mathcal{O}_K/\mathfrak{p})$ we have its betti numbers B_i in the sense above. Then $B_i = b_i$, for all i .

Maybe a few words on why the third one is called the analogue of Riemann Hypothesis. For a scheme X of finite type over \mathbb{Z} , define the Riemann zeta function of X to be

$$\zeta_X(s) = \prod_{x \in X_{cl}} \frac{1}{1 - N(x)^{-s}},$$

where $N(x) = \#(k(x)) = \#(\mathcal{O}_{x,X}/\mathfrak{m}_x)$ is the cardinality of the residue field at x . Note that $\zeta_{Spec(\mathbb{Z})}(s) = \zeta(s)$, the classical Riemann zeta function. Then it turns out that if X is of finite type over \mathbb{F}_q , which is of finite type over \mathbb{Z} ,

$$\zeta_X(s) = Z(X, q^{-s}).$$

Actually some people call $Z(q^{-s})$ the zeta function. Suppose the third part of the conjecture is true. If s is a zero of $\zeta_X(s)$, then $P_{2i-1}(q^{-s}) = \prod (1 - \alpha_{2i-1,j} q^{-s}) = 0$, so some $1 - \alpha_{2i-1,j} q^{-s} = 0$, so $q^{\Re(s)} = |q^s| = |\alpha_{2i-1,j}| = q^{i-\frac{1}{2}} \Rightarrow \Re(s) = i - \frac{1}{2} = \frac{1}{2}, \frac{3}{2}, \dots, n - \frac{1}{2}$, which is analogous to the Riemann Hypothesis. Similarly if s is a pole of $\zeta_X(s)$, then $\Re(s) = i = 0, 1, \dots, n$.

The first example would be projective spaces. For $X = \mathbb{P}_k^n$, $N_r = \sum_{i=0}^n q^{ri}$. So $Z(\mathbb{P}_k^n, t) = \exp\left(\sum_{r \geq 1} \frac{\sum_{i=0}^n (q^i t)^r}{r}\right) = \prod_{i=0}^n \exp\left(\sum_{r \geq 1} \frac{(q^i t)^r}{r}\right)$.

Lemma 1.1. $\exp\left(\sum_{r \geq 1} \frac{t^r}{r}\right) = \frac{1}{1-t}$.

Proof. Let $f(t) = \exp(\sum_{r \geq 1} \frac{t^r}{r})$. Then $\frac{f'(t)}{f(t)} = \frac{d}{dt} \log f(t) = \sum_{r \geq 1} t^{r-1} = \frac{1}{1-t}$, which is an easy-to-solve ODE. Separating variables and integrating both sides, we get $f(t) = \frac{c}{1-t}$ for some constant c . The initial condition $f(0) = 1$ shows $c = 1$. \square

From the lemma we see that $Z(\mathbb{P}^n, t) = \prod_{i=0}^n \frac{1}{1-q^i t}$. The rationality and the analog for the Riemann hypothesis are obvious.

Proposition 1.2. *On $X = \mathbb{P}_k^n$ we have the Euler exact sequence of locally free sheaves:*

$$0 \rightarrow \mathcal{O}_X \rightarrow \bigoplus_{n+1} \mathcal{O}(1) \rightarrow \mathcal{T}_X \rightarrow 0.$$

Proof. See Hartshorne p.176, theorem 8.13. \square

The Chern polynomial is multiplicative, so

$$c_t(\mathcal{O}_X)c_t(\mathcal{T}_X) = c_t\left(\bigoplus_{n+1} \mathcal{O}(1)\right) = \prod_{n+1} c_t(\mathcal{O}(1)) = (1 + Ht)^{n+1},$$

where H is the class of a hyperplane. $c_t(\mathcal{O}) = 1$, so $c_t(\mathcal{T}_X) = (1 + Ht)^{n+1} = 1 + (n+1)Ht + \dots + (n+1)H^n t^n$. So $c_n(\mathcal{T}_X) = (n+1)H^n$, $E = n+1$. Now the functional equation and formula for betti numbers are also easy to verify. Note that these B_i agree with the topological betti numbers of $\mathbb{C}\mathbb{P}^n$, as expected.

Now we are going to define the Frobenius morphism, which is of crucial importance in both understanding the Weil conjecture and elliptic curves.

Definition 1.3. *Suppose X is a scheme over $k = \mathbb{F}_q$, where q is a prime power, and take the base extension to the algebraic closure $\bar{X} = X \times_{\mathbb{F}_q} \bar{\mathbb{F}}_q$, and call it a scheme over \bar{k} which can be defined over k . Then the q -Frobenius morphism on \bar{X} is defined to be a morphism $F : \bar{X} \rightarrow \bar{X}$ whose underlying continuous map is the identity map, and the map on sheaves $F^\# : \mathcal{O}_{\bar{X}} \rightarrow \mathcal{O}_{\bar{X}}$ is given by $\mathcal{O}(U) \rightarrow \mathcal{O}(U)$ sending $s \mapsto s^q$, for every open set $U \subset \bar{X}$. It's a well-defined ring homomorphism because for each U , $\mathcal{O}(U)$ is an algebra over \mathbb{Z}/p , and q is a power of p . Note that F is not a morphism over \bar{k} . Let F also denote the q -Frobenius morphism on $\text{Spec}(\bar{k})$, and let $\pi : \bar{X} \rightarrow \text{Spec}(\bar{k})$ be the \bar{k} -structure on \bar{X} , then define \bar{X}_q to be exactly the same scheme as \bar{X} but a different \bar{k} -structure $F \circ \pi : \bar{X} \rightarrow \text{Spec}(\bar{k}) \rightarrow \text{Spec}(\bar{k})$. Then we have a \bar{k} -linear Frobenius morphism $F' : \bar{X}_q \rightarrow \bar{X}$.*

As a remark, we will show in the case of an elliptic curve that with an embedding into some projective space, the Frobenius morphism just takes the q th power of each of its coordinates, for any local affine coordinates. In fact, the Frobenius morphism is characterized uniquely by this property. See, for instance, J. Milne's Lectures on Étale Cohomology. So the number of fixed points of F'^r is just N_r we defined above; F' here is not exactly the same F' as above, but the composite of it with an isomorphism $\bar{X}_q \cong \bar{X}$.

2 Preliminaries on Curves

Next we are going to focus on curves. By a curve we mean a projective nonsingular 1-dimensional variety over an algebraically closed field k . $g = h^1(\mathcal{O}_X) = h^0(\omega_X)$ is called the genus of the curve X . By a complete linear system $|D|$ we mean the set of effective divisors linearly equivalent to the given divisor D on X , which has a natural structure of a projective space. Indeed, $|D| = \mathbb{P}(H^0(X, \mathcal{L}(D)))$. Denote $h^0(\mathcal{L}(D))$ by $l(D)$, so that $\dim |D| = l(D) - 1$. Let $K = K_X$ be the canonical divisor on X , the divisor such that $\mathcal{L}(K_X) = \omega_X$.

Theorem 2.1. (Riemann-Roch for curves) *For any divisor D on X , we have*

$$l(D) - l(K_X - D) = \deg(D) + 1 - g.$$

Proof. See Hartshorne p.295, theorem 1. □

Corollary 2.2.

$$\deg(K_X) = 2g - 2.$$

Proof. Apply Riemann-Roch to $D = K$ we have

$$l(K) - 1 = \deg(K) + 1 - g,$$

where $l(K) = g$. □

By a linear system we mean a linear subvariety \mathfrak{d} of a complete linear system $|D| = \mathbb{P}(H^0(X, \mathcal{L}(D)))$. Linear systems are used to define maps from the variety to projective spaces. Suppose \mathfrak{d} corresponds to a linear subspace $V \subset H^0(X, \mathcal{L}(D))$ of dimension $r + 1$, then take a basis f_0, \dots, f_r for V . Since every invertible sheaf can be regarded as a subsheaf of \mathcal{K} , the sheaf of rational functions, and H^0 is left exact, we can regard V as a subspace of rational functions on our curve X . Note that $H^0(X, \mathcal{L}(D))$ consists of rational functions f such that $-v_P(f) \leq \text{order}_P(D)$ for all $P \in X$, where v_P is the valuation on $K(X)$ given by \mathcal{O}_P and $D = \sum_P \text{order}_P(D) \cdot P$. This means the orders of f at poles are bounded from above by positive coefficients in D , and the orders at zeros are bounded from below by absolute values of negative coefficients in D .

Now we want to define a map $X \xrightarrow{f_{\mathfrak{d}}} \mathbb{P}_k^r$ by $P \mapsto [f_0(P), \dots, f_r(P)]$. To ensure that it's well-defined, we have to assume that the sheaf $\mathcal{L}(D)$ can be generated by finitely many global sections (in fact a basis) in V , which is equivalent to say that \mathfrak{d} is base-point-free. A base point of \mathfrak{d} is a point $P \in \cap_{D' \in \mathfrak{d}} \text{Supp}(D')$. Whenever $f_{\mathfrak{d}}$ is well-defined, it's "independent" of the choice of basis for V in the sense that if we use another basis, these two maps only differ by an automorphism of \mathbb{P}_k^r given by $[A] \in \mathbb{PGL}_{r+1}(k)$, where A is just the matrix of base change. If $f_{\mathfrak{d}}$ happens to be a closed immersion, then we say D or $\mathcal{L}(D)$ is very ample. An invertible sheaf \mathcal{L} (resp. a divisor D) is ample if $\mathcal{L}^{\otimes n}$ (resp. nD) is very ample for some $n > 0$.

Proposition 2.3. *Let X be a curve of genus g and D a divisor on X . Then $|D|$ has no base point if $\deg(D) \geq 2g$; $|D|$ is very ample if $\deg(D) \geq 2g + 1$. In particular, D is ample if and only if $\deg(D) > 0$.*

Proof. See Hartshorne p.308, cor. 3.2. □

Next we consider finite maps between curves.

Proposition 2.4. *A morphism between two curves is either constant or a finite morphism.*

Proof. See Hartshorne p.137, proposition 6.8. □

Definition 2.5. *Let $f : X \rightarrow Y$ be a finite map of curves. Then the degree of the corresponding field extension $K(Y) \rightarrow K(X)$ is called the degree of the map f . f is said to be separable (or purely inseparable) if the field extension is separable (or purely inseparable). Suppose $P \in X, f(P) = Q \in Y$. Then we have a local homomorphism $f_P^\# : \mathcal{O}_Q \rightarrow \mathcal{O}_P$. Let t_Q be a generator of the maximal ideal in \mathcal{O}_Q , then define the ramification index e_P of P to be $v_P(f_P^\# t_Q)$, where v_P is the valuation for \mathcal{O}_P . If $e_P > 1$ we say that f is ramified at P ; otherwise we say f is unramified at P . In case that $e_P > 1$, if $\text{char}(k) = 0$ or $\text{char}(k) = p$ but p doesn't divide e_P , we say f is tamely ramified at P ; otherwise it's wildly ramified at P . Define a homomorphism $f^* : Cl(Y) \rightarrow Cl(X)$ by sending $Q \in Y$ to $f^*(Q) = \sum_{P \in f^{-1}(Q)} e_P P$ and extend by linearity. Then it's compatible with the map $f^* : Pic(Y) \rightarrow Pic(X)$ in the sense that $f^* \mathcal{L}(D) \cong \mathcal{L}(f^*(D))$ for any divisor D on Y .*

For instance, the p -Frobenius map of a curve over k with $\text{char}(k) = p$ is purely inseparable of degree p , because it corresponds to the fields extension $K(X) \hookrightarrow K(X)^{1/p}$, the field of p th roots of elements in $K(X)$. Note that fixing an algebraic closure of $K(X)$, each element in $K(X)$ has a unique q th root, so $K(X)$ and $K(X)^{1/q}$ are isomorphic as fields abstractly, but the isomorphism is over \mathbb{F}_q , not over k . Conversely, every purely inseparable map is a composite of p -Frobenius maps.

Lemma 2.6. *Let $f : X \rightarrow Y$ be a finite map of curves, purely inseparable of degree $q = p^d$. Then $X \cong Y_q$, and under this isomorphism, f is the same as the q -Frobenius map $F^1 : Y_q \rightarrow Y$.*

Proof. See Hartshorne p.302, proposition 2.5. □

Proposition 2.7. $\sum_{P \in f^{-1}(Q)} e_P = \deg(f)$ for any point $Q \in Y$.

Proof. See Hartshorne p.138, prop. 6.9. □

Proposition 2.8. *Let $f : X \rightarrow Y$ be a finite separable map of curves. Then the support of the sheaf $\Omega_{X/Y}$ on X is exactly the set of ramification points of f , and the set is finite. Moreover, if f is tamely ramified at P , then $e_P - 1 = \text{length}_{\mathcal{O}_{X,P}}(\Omega_{X/Y})_P$. If f is wildly ramified at P then $e_P - 1 < \text{length}_{\mathcal{O}_{X,P}}(\Omega_{X/Y})_P$.*

Proof. See Hartshorne p.300, prop. 2.2. \square

Definition 2.9. Given $f : X \rightarrow Y$ a finite separable map of curves, define the ramification divisor of f on X to be

$$R = \sum_{P \in X} \text{length}(\Omega_{X/Y})_P \cdot P.$$

Note that it's a finite sum.

Theorem 2.10. (Hurwitz) Given $f : X \rightarrow Y$ a finite separable map of curves, we have

$$K_X \sim f^*K_Y + R.$$

Proof. See Hartshorne p.301, prop. 2.3. \square

Corollary 2.11. If $\deg(f) = n$, then

$$2g_X - 2 = n(2g_Y - 2) + \deg(R).$$

If f is tamely ramified, then $\deg(R) = \sum_{P \in X} (e_P - 1)$.

We give an application of the Hurwitz's theorem just for fun.

Proposition 2.12. Let X be a curve of genus $g \geq 2$ with $G = \text{Aut}_k(X)$ finite (which is any curve of $g \geq 2$, if one admits a theorem), $\text{char}(k) = 0$. Then $|G| \leq 84(g - 1)$.

Proof. This is Hartshorne p.305, ex. 2.5. Let $K = K(X)$ be the function field of X , and $L = K^G$ be the fixed field by G . Then K/L is a Galois extension with $\mathcal{G}al(K/L) = G$, of degree n , say. Then L is also a finitely generated field extension of k with transcendental degree 1, so it gives a curve $Y = C_L$ with function field L . Also we have a finite separable map of curves $f : X \rightarrow Y$ of degree n . Let $P_1, P_2 \in X$ both of which are mapped to $Q \in Y$. We want to show that $e_{P_1} = e_{P_2}$. Points on the curve X correspond to discrete valuation rings of $K(X)/k$, so the picture is, we have two discrete valuation rings \mathcal{O}_{P_1} and \mathcal{O}_{P_2} of K/k , and \mathcal{O}_Q of L/k , such that $\mathcal{O}_{P_1} \cap L = \mathcal{O}_{P_2} \cap L = \mathcal{O}_Q$, and we want to show that $\exists \sigma \in G$ such that $\sigma(\mathcal{O}_{P_1}) = \mathcal{O}_{P_2}$. This follows from the extension being Galois. So $e_{P_1} = e_{P_2}$ if they are in the same fiber. Let r be the number of branch points and $e_i, i = 1, \dots, r$ be the ramification indices in each fiber. In each fiber they add up to n , the degree of the map, so $\frac{n}{e_i}$ is the number of points in that fiber. $\text{char}(k) = 0$, so f is tamely ramified. By Hurwitz's theorem we have

$$2g_X - 2 = n(2g_Y - 2) + \sum_{i=1}^r (e_i - 1) \frac{n}{e_i} = n(2g_Y - 2) + \sum_i (1 - \frac{1}{e_i}).$$

$g_X \geq 2$, so $2g_Y - 2 + \sum_i (1 - \frac{1}{e_i}) > 0$. The result follows from the next lemma. \square

Lemma 2.13. $\min\{2b - 2 + \sum_{i=1}^r (1 - \frac{1}{e_i}) | 2b - 2 + \sum_i (1 - \frac{1}{e_i}) > 0, b \geq 0, r \geq 1, e_i \geq 2, \forall i\} = \frac{1}{42}$.

Proof. Let $A = 2b - 2 + \sum_i (1 - \frac{1}{e_i})$. If $b \geq 1$, then $2b - 2 \geq 0$, so $A \geq 0 + 1 - \frac{1}{2} = \frac{1}{2} > \frac{1}{42}$. We can assume $b = 0$. Then r cannot be 1 or 2, because otherwise $A \leq -2 + 1 - \frac{1}{e_1} + 1 - \frac{1}{e_2} < 0$. If $r \geq 5$, then $A \geq -2 + 5(1 - \frac{1}{2}) = \frac{1}{2} > \frac{1}{42}$. So we focus on $r = 3$ or 4. If $r = 3$, then not all e_i 's are 2, since otherwise $A < 0$. Actually there can be at most one of e_i which is 2. If all of $e_i \geq 3$, then they can't be all 3 because otherwise $A = 0$. So assume $e_1 \geq 3, e_2 \geq 3, e_3 \geq 4$. Then $A \geq -2 + \frac{2}{3} + \frac{2}{3} + \frac{3}{4} = \frac{1}{12} > \frac{1}{42}$. So assume one of e_i , say e_1 , is 2. Then e_2 and e_3 can't both be 3, otherwise $A < 0$. If both e_2 and e_3 are ≥ 4 , then $A \geq -2 + \frac{1}{2} + \frac{3}{4} + \frac{3}{4} = 0$, which means that they can't both be 4. Assume $e_2 \geq 4$ and $e_3 \geq 5$, then $A \geq -2 + \frac{1}{2} + \frac{3}{4} + \frac{4}{5} = \frac{1}{20} > \frac{1}{42}$. So assume one of them, say $e_2 = 3$. Then for $e_3 \leq 6, A \leq 0$. So the minimal possible value for A in the case that $r = 3$ is $\frac{1}{42}$, when $e_3 = 7$. Now assume $r = 4$. Not all e_i 's can be 2, since otherwise $A = 0$. So assume one of them ≥ 3 . Then $A \geq -2 + 3 \times \frac{1}{2} + \frac{2}{3} = \frac{1}{6} > \frac{1}{42}$. \square

3 Elliptic Curves

For simplicity we assume that $\text{char}(k) \neq 2$.

Definition 3.1. A curve X is elliptic if its genus $g = 1$.

The genus is a birational invariant, so an elliptic curve is not rational, and hence two different points P, Q on the curve can't be linearly equivalent (see Hartshorne p.138, 6.10.1; or apply Riemann-Roch to P). Also, $\deg(K) = 0, l(K) = 1$, which means that there's exactly one effective divisor linearly equivalent to K . The only effective divisor of degree 0 is 0, so $K = 0$. A finite separable map between two elliptic curves is unramified, by the Hurwitz's theorem, and hence étale, since it's flat.

For a pointed elliptic curve $X, P_0, |2P_0|$ is base-point-free and $|3P_0|$ is very ample. So $|2P_0|$ defines a branched covering $f : X \rightarrow \mathbb{P}^1$ of degree 2 and $|3P_0|$ defines an embedding $i : X \rightarrow \mathbb{P}^2$. f is separable, because if $\text{char}(k) = 0$, then it's automatically separable; if $\text{char}(k) = p > 2$, then f can't factor through any purely inseparable map, since $2 < p$. So we apply Hurwitz's theorem to f to conclude that $\deg(R) = 4$. By a lemma before, $\sum_{P \in f^{-1}Q} e_P = 2$. So if Q is a branch point, then $e_P = 2$ and $\{P\} = f^{-1}(Q)$. So f is tamely ramified at P . This means that $\sum_{P \in X} (e_P - 1) = 4$, thus there are exactly 4 branch points in \mathbb{P}^1 . Say their cross-ratio is λ , then use some $[A] \in \text{PGL}_2(k)$ to change the coordinate on \mathbb{P}^1 such that these four points are $0, 1, \infty$ and λ .

Definition 3.2. The j -invariant of an elliptic curve X is defined to be

$$j(X) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

Theorem 3.3. *The affine line \mathbb{A}^1 is the coarse moduli space for elliptic curves with $j(X) \in k$ representing the curve X .*

Proof. See Hartshorne p.317, thm. 4.1. □

Elliptic curves are 1-dimensional abelian varieties. They are Jacobian varieties of themselves.

Let X be a curve over k , T a scheme of finite type over k . By $Pic^0(X \times T)$ we mean the subgroup of $Pic(X \times T)$ consisting of isomorphism classes of invertible sheaves \mathcal{L} on $X \times T$ such that the pullback on each fiber $X_t, t \in T$, has degree 0. Certainly $p_2^*Pic(T) \subset Pic^0(X \times T)$. Define $Pic^0(X/T) = Pic^0(X \times T)/p_2^*Pic(T)$. If $T \rightarrow S$ is a k -morphism, then it induces a group homomorphism $Pic^0(X/S) \rightarrow Pic^0(X/T)$, just by taking the pullback of sheaves. So $Pic^0(X/\cdot) : \{\text{Schemes of finite type over } k\}^{op} \rightarrow \mathcal{G}rp$ is a functor. It's a big theorem that this functor is representable, for every curve X .

Definition 3.4. *The representing object of the functor above, which is unique up to unique isomorphism, is called the Jacobian variety of X , denoted $\mathcal{J}ac(X)$.*

Since $\text{hom}_k(\cdot, \mathcal{J}ac(X))$ is a functor that ends up in $\mathcal{G}rp$, $\mathcal{J}ac(X)$ is a group scheme over k , by Yoneda's lemma. In fact $\mathcal{J}ac(X)$ is a complete group variety (abelian variety) of dimension g , the genus of the curve X , with tangent space at the identity element canonically identified with $H^1(X, \mathcal{O}_X)$. See Hartshorne p.324-325.

Theorem 3.5. *Let X be an elliptic curve. Then X together with the isomorphism class of the sheaf $\mathcal{L}(\Delta_X) \otimes \mathcal{L}(-P_0)$ on $X \times X$ is a (the) Jacobian variety of X for any point $P_0 \in X$. In particular, X is an abelian variety, and specifying a base point on it amounts to specifying a group structure on it.*

Proof. See Hartshorne p.325, thm. 4.11. □

In fact we have a more elementary way to describe the group structure on a pointed elliptic curve (X, P_0) .

Lemma 3.6. *Every divisor D of degree 0 on X is linearly equivalent to $P - P_0$ for a unique point $P \in X$.*

Proof. Apply Riemann-Roch to the divisor $D + P_0$. Since X is elliptic, $K = 0$, every effective divisor $E \neq 0$ is nonspecial in the sense that $l(K - E) = 0$. So we have

$$l(D + P_0) = \deg(D + P_0) + 1 - g = 1,$$

so there's exactly one point $P \in X$ such that $P \sim D + P_0$. □

According to the lemma, there's a one-to-one correspondence between (closed) points on X and elements in the subgroup $Pic^0(X)$. For any two point $P, Q \in X$, there's a unique point $R \in X$ such that $P + Q \sim R + P_0$. Define the group structure given by P_0 to be such that $P + Q = R$. It's associative because both $(P + Q) + R$ and $P + (Q + R)$ is the unique point O such that $P + Q + R \sim$

$O + 2P_0$. The inverse of the point P is given by the unique point P' such that $P + P' \sim 2P_0$, and the identity element is P_0 . If we embed our elliptic curve X into \mathbb{P}^2 via the complete linear system $|3P_0|$, which is very ample of dimension 2 and degree 3, we get a cubic curve in \mathbb{P}^2 whose hyperplane section is $|3P_0|$. Then 3 points P, Q , and R are colinear iff $P + Q + R \sim 3P_0$, which is equivalent to saying that $P + Q + R = 0$ under the group law above.

Lemma 3.7. *Let $f : X \rightarrow Y$ be a finite map between elliptic curves. Pick $P_0 \in X$ and $P'_0 = f(P_0) \in Y$. Then $f : (X, P_0) \rightarrow (Y, P'_0)$ is a group homomorphism.*

Proof. See Hartshorne p.322, lemma 4.9. □

Let $n_X(P) \in X$ be the point which is the n -fold sum of $P \in X$ under the group law. Then $n_X : X \rightarrow X$ defines a morphism of abelian varieties. It's additive by the lemma above, and it's a morphism of schemes because it's the composite of the diagonal morphism $\Delta : X \rightarrow \prod_n X$ and the addition map. Later we will figure out the degree of the map.

Definition 3.8. *Let $R = \text{End}(X, P_0)$ be the monoid of endomorphisms of the pointed elliptic curve. Then we can define an addition on R as follows. Given $f, g \in R$, let $f + g$ be the composite of the diagonal map $\Delta : X \rightarrow X \times X$ and $f \times g : X \times X \rightarrow X \times X$ followed by the addition map $X \times X \rightarrow X$. By the above lemma, the composition law in R is distributive over the addition, so we put a ring structure on R , with 0 the constant map to P_0 and 1 the identity map.*

Lemma 3.9. *The map $\mathbb{Z} \rightarrow \text{End}(X, P_0)$ given by $n \mapsto n_X$ is an injective ring homomorphism.*

Proof. See Hartshorne p.323, prop.4.10. □

If $k = \mathbb{C}$, then it can be proved that $\text{End}(X, P_0) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\}$, where $X \cong \mathbb{C}/\Lambda$, using the comparison of an algebraic variety over \mathbb{C} and its associated complex analytic space. Hence $\text{End}(X, P_0)$ is a subring of \mathbb{C} , so it's a commutative integral domain. Otherwise (when $k \neq \mathbb{C}$) it's an order of a quaternion algebra, which is not commutative. But for any $n \in \mathbb{Z}, f \in \text{End}(X, P_0)$, $nf = fn$, which follows from the fact that f is a group homomorphism.

Finally we define an important invariant for elliptic curves over a field of characteristic p .

Definition 3.10. *Let X be an elliptic curve over a field k of characteristic p , and let $F : X \rightarrow X$ be the p -Frobenius map. Then it induces a map on cohomology groups*

$$F^* : H^1(X, \mathcal{O}_X) \rightarrow H^1(X, \mathcal{O}_X).$$

If the map is 0, we say that the Hasse invariant of X is 0; otherwise the Hasse invariant is 1.

Note that $F^* : H^1(X, \mathcal{O}_X) \rightarrow H^1(X, \mathcal{O}_X)$ is not k -linear, because F is not. But $F^*(\lambda v) = \lambda^p F^*(v)$ for all $\lambda \in k$. If k is perfect, note that $\dim_k H^1(X, \mathcal{O}_X) = g = 1$, so F^* is not 0 if and only if it's bijective.

4 Proof

Proposition 4.1. *Let $f : (X, P_0) \rightarrow (X', P'_0)$ be a finite map of degree n between elliptic curves. Then the homomorphism $f^* : Pic(X') \rightarrow Pic(X)$ induces a morphism $\hat{f} : (X', P'_0) \rightarrow (X, P_0)$. If $g : X' \rightarrow X''$, then $(g \circ \hat{f}) = \hat{f} \circ \hat{g}$. Moreover, if $f(Q) = Q'$, then $\hat{f}(Q') = n_X(Q)$.*

Proof. We already have a homomorphism $f^* : Pic(X') \rightarrow Pic(X)$. Moreover, $\deg(f^*D) = n \deg(D)$ for any divisor D on X' , so the subgroup $Pic^0(X')$ is mapped into $Pic^0(X)$, hence we have a group homomorphism $\hat{f} : (X', P'_0) \rightarrow (X, P_0)$. It's also a morphism of schemes. See Silverman p.84, thm. 6.1. Let's examine the map carefully. For any point $Q' \in X'$, it corresponds to the invertible sheaf $\mathcal{L}(Q' - P'_0) \in Pic^0(X')$, which is mapped to $\mathcal{L}(f^*(Q' - P'_0)) \in Pic^0(X)$. By a lemma above, it is isomorphic to $\mathcal{L}(\hat{f}(Q') - P_0)$ for a unique point $\hat{f}(Q') \in X$ which is defined to be the image of Q' . $(g \circ \hat{f}) = \hat{f} \circ \hat{g}$ is obvious. So we have to show that $f^*(Q' - P'_0) \sim n_X(Q) - P_0$ if $f(Q) = Q'$. We divide it into two cases: f is separable, and f is purely inseparable.

Suppose f is separable. Then we can apply Hurwitz's theorem to conclude that f is étale. Let $f^{-1}(P'_0) = \{P_0, P_1, \dots, P_{n-1}\}$, $f^{-1}(Q') = \{Q_0, Q_1, \dots, Q_{n-1}\}$, where $Q = Q_0$. f is a group epimorphism, so $\ker(f) = f^{-1}(P'_0)$ and $f^{-1}(Q')$ is the coset $Q_0 + f^{-1}(P'_0)$. Assume $Q_i = Q_0 + P_i$ in the group law. Then $\sum_i Q_i - \sum_i P_i = \sum_i (Q_i - P_i) = n_X(Q)$ in the group law, which means that as divisors, $f^*(Q') - f^*(P'_0) \sim n_X(Q) - P_0$.

Suppose f is purely inseparable. Then by a lemma above, f is isomorphic to some q -Frobenius map. In particular, $n = q$ is a power of p . Frobenius maps are identity on the underlying spaces. On stalks, F' is the q th power map, so it sends the generator t_Q of the maximal ideal to t_Q^q , so $e_Q = q$, hence $f^*(Q) = qQ$, $f^*(P_0) = qP_0$, so $f^*(Q) - f^*(P_0) = q(Q - P_0) = q_X(Q) - P_0$.

Every finite field extension can be factorized as a separable extension followed by a purely inseparable extension, so every finite map between curves can be factorized as a composite of separable map and a purely inseparable map. The degree also factors as the product of the two degrees. Use $(g \circ \hat{f}) = \hat{f} \circ \hat{g}$ and $n_X \circ m_X = (nm)_X$ to complete the proof. \square

Proposition 4.2. *For any $f, g : X \rightarrow X'$, $(f + g) = \hat{f} + \hat{g}$.*

Proof. It suffices to show that $(f + g)^*\mathcal{L} \cong f^*\mathcal{L} \otimes g^*\mathcal{L}$ for all $\mathcal{L} \in Pic^0(X')$. Let $\Gamma_f : X \rightarrow X \times X'$ be the graph of f . Let $\sigma : X \rightarrow X \times X'$ be the section that sends x to (x, P'_0) . Define $Pic^0_\sigma = \{\mathcal{L} \in Pic(X \times X') \mid \deg(\mathcal{L}|_{X'_x}) = 0, \forall x \in X, \sigma^*\mathcal{L} \cong \mathcal{O}_X\}$. It's a general fact that for any morphism f , f^* preserves the tensor product of locally free sheaves. So Pic^0_σ is a subgroup of $Pic^0(X \times X')$, used in the definition of the Jacobian variety. We will see in a minute that the embedding of this subgroup composed with the quotient map to $Pic^0(X \times X')/p_1^*Pic(X) = Pic^0(X'/X)$ is an isomorphism. $Pic^0(X'/X) = \text{hom}_k(X, X')$ by definition of the Jacobian variety, so we have a one-to-one correspondence between maps $X \rightarrow X'$ and sheaves in Pic^0_σ . Denote by $\mathcal{L}_f \in Pic^0_\sigma$ the sheaf corresponding to

the map f . Obviously for any $\mathcal{L} \in \text{Pic}^0(X')$, $p_2^*\mathcal{L} \in \text{Pic}_\sigma^0$. Indeed, the restriction to each fiber $p_1^{-1}(x) = X'_x$ is isomorphic to \mathcal{L} . $\sigma^*p_2^*\mathcal{L} = (p_2 \circ \sigma)^*\mathcal{L} \cong (P'_0)^*\mathcal{L} \cong \mathcal{O}_X$, where $P'_0 : X \rightarrow X'$ is the constant map sending everything to the point P'_0 . We will also prove later that $\Gamma_g^*\mathcal{L}_f \cong \Gamma_f^*\mathcal{L}_g$, for any $f, g : X \rightarrow X'$. Note that $\mathcal{L}_{f+g} \cong \mathcal{L}_f \otimes \mathcal{L}_g$, since $\text{Pic}_\sigma^0 \cong \text{hom}_k(X, X')$ is an isomorphism of groups, so we have that for any $\mathcal{L}' = \mathcal{L}_h \in \text{Pic}_\sigma^0$,

$$\Gamma_{f+g}^*(\mathcal{L}_h) \cong \Gamma_h^*(\mathcal{L}_{f+g}) \cong \Gamma_h^*(\mathcal{L}_f \otimes \mathcal{L}_g) \cong \Gamma_h^*(\mathcal{L}_f) \otimes \Gamma_h^*(\mathcal{L}_g) \cong \Gamma_f^*(\mathcal{L}_h) \otimes \Gamma_g^*(\mathcal{L}_h).$$

Plugging in $\mathcal{L}' = p_2^*\mathcal{L}$ for $\mathcal{L} \in \text{Pic}^0(X')$ we have

$$\Gamma_{f+g}^*p_2^*\mathcal{L} \cong \Gamma_f^*p_2^*\mathcal{L} \otimes \Gamma_g^*p_2^*\mathcal{L}.$$

Note that $\Gamma_f^* \circ p_2^* = (p_2 \circ \Gamma_f)^* = f^*$. So we obtain $(f+g)^*\mathcal{L} \cong f^*\mathcal{L} \otimes g^*\mathcal{L}$ for all $\mathcal{L} \in \text{Pic}^0(X')$, as desired.

Now we prove that

$$\text{Pic}_\sigma^0 \xrightarrow{i} \text{Pic}^0(X \times X') \xrightarrow{\pi} \text{Pic}^0(X \times X')/p_1^*\text{Pic}(X) = \text{Pic}^0(X'/X)$$

composes to give an isomorphism. For injectivity, suppose some $\mathcal{L} \in \text{Pic}_\sigma^0$ maps to 0, which means that $\mathcal{L} \in p_1^*\text{Pic}(X)$, say $\mathcal{L} = p_1^*\mathcal{L}'$ for some $\mathcal{L}' \in \text{Pic}(X)$. $p_1 \circ \sigma = 1_X$, so $\sigma^* \circ p_1^* = 1$. Apply this identity to \mathcal{L}' , we have

$$\mathcal{L}' = \sigma^* \circ p_1^*\mathcal{L}' = \sigma^* \circ \mathcal{L} = \mathcal{O}_X,$$

so $\mathcal{L} = 0$ in Pic_σ^0 .

For surjectivity, given any $\mathcal{L} \in \text{Pic}^0(X \times X')$, $\mathcal{L} \otimes p_1^*\sigma^*\check{\mathcal{L}}$ will be in Pic_σ^0 and it maps to the class of \mathcal{L} in $\text{Pic}^0(X \times X')/p_1^*\text{Pic}(X)$. It's in Pic_σ^0 because

$$\sigma^*(\mathcal{L} \otimes p_1^*\sigma^*\check{\mathcal{L}}) = \sigma^*\mathcal{L} \otimes \sigma^*p_1^*\sigma^*\check{\mathcal{L}} = \sigma^*\mathcal{L} \otimes \sigma^*\check{\mathcal{L}} = 0$$

in $\text{Pic}(X)$. In fact, the assignment above gives the inverse of $\pi \circ i$.

Next we prove $\Gamma_g^*\mathcal{L}_f \cong \Gamma_f^*\mathcal{L}_g$. First let's see what is \mathcal{L}_f . Let $\mathcal{M} = \mathcal{L}(\Delta_{X'}) \otimes p_2^*\mathcal{L}(-P'_0)$ be the universal invertible sheaf on $X' \times X'$, where the first factor is regarded as the Jacobian of itself. Now we have a map $f \times 1_{X'} : X \times X' \rightarrow X' \times X'$, we get a sheaf $(f \times 1_{X'})^*\mathcal{M} \in \text{Pic}^0(X'/X)$. Using the inverse map given above we end up with $\mathcal{L}_f = (f \times 1_{X'})^*\mathcal{M} \otimes p_1^*\sigma^*((f \times 1_{X'})^*\mathcal{M})^\vee \in \text{Pic}_\sigma^0$. $((f \times 1_{X'})^*\mathcal{M})^\vee \cong (f \times 1_{X'})^*\check{\mathcal{M}}$, and $p_1^*\sigma^*(f \times 1_{X'})^* = ((f \times 1_{X'}) \circ \sigma \circ p_1)^* = (f \times 0_{X'})^*$, where $f \times 0_{X'} : X \times X' \rightarrow X' \times X'$ sends (x, x') to $(f(x), P'_0)$. So $\mathcal{L}_f = (f \times 1_{X'})^*\mathcal{M} \otimes (f \times 0_{X'})^*\check{\mathcal{M}}$, and

$$\begin{aligned} \Gamma_g^*\mathcal{L}_f &= \Gamma_g^*(f \times 1_{X'})^*\mathcal{M} \otimes \Gamma_g^*(f \times 0_{X'})^*\check{\mathcal{M}} = ((f \times 1_{X'}) \circ \Gamma_g)^*\mathcal{M} \otimes \\ &((f \times 0_{X'}) \circ \Gamma_g)^*\check{\mathcal{M}} = (f, g)^*\mathcal{M} \otimes (f, P'_0)^*\check{\mathcal{M}} = (f, g)^*\mathcal{L}(\Delta_{X'}) \otimes (f, g)^* \\ &p_2^*\mathcal{L}(-P'_0) \otimes (f, P'_0)^*\mathcal{L}(-\Delta_{X'}) \otimes (f, P'_0)^*p_2^*\mathcal{L}(P'_0) = (f, g)^*\mathcal{L}(\Delta_{X'}) \otimes g^*\mathcal{L}(-P'_0) \\ &\otimes (f, P'_0)^*\mathcal{L}(-\Delta_{X'}) \otimes \mathcal{O}_X = (f, g)^*\mathcal{L}(\Delta_{X'}) \otimes g^*\mathcal{L}(-P'_0) \otimes f^*\mathcal{L}(-P'_0), \end{aligned}$$

where $(f, g) : X \rightarrow X' \times X'$ is the map sending x to $(f(x), g(x))$. We used the fact that $(f, P'_0)^*\mathcal{L}(\Delta_{X'}) = f^*\mathcal{L}(P'_0)$. Let $\tau : X' \times X' \rightarrow X' \times X'$ be the map sending (x, y) to (y, x) , then $\tau^*\Delta_{X'} = \Delta_{X'}$, and $\tau \circ (f, g) = (g, f)$. So it's quite obvious that if we switch f and g , we have that $\Gamma_f^*\mathcal{L}_g$ equals the same thing. \square

Corollary 4.3. For every $n \in \mathbb{Z}$, $\hat{n}_X = n_X$. And it follows that $\deg n_X = n^2$.

Proof. True for $n = 0, 1$, so also true for $n = -1$, because $-1 + 1 = 0$ and use $(f \hat{+} g) = \hat{f} + \hat{g}$. Only need to consider the case when $n > 1$. Then $n_X = 1_X + \cdots + 1_X$, and so $\hat{n}_X = \hat{1}_X + \cdots + \hat{1}_X = 1_X + \cdots + 1_X = n_X$. Let $d = \deg(n_X)$. Then $\hat{n}_X \circ n_X = d_X$. But $\hat{n}_X \circ n_X = n_X \circ n_X = (n^2)_X$, and the ring homomorphism $\mathbb{Z} \rightarrow \text{End}_k(X)$ is injective, so $d = n^2$. \square

Corollary 4.4. For any map $f : X \rightarrow X'$ between elliptic curves, $\deg f = \deg(\hat{f})$.

Proof. Let $\deg(f) = n$. Then $\hat{f} \circ f = n_X$. Taking degree is multiplicative, so $\deg(\hat{f}) \cdot \deg(f) = \deg(n_X) = n^2$, which implies $\deg(\hat{f}) = n$, too. \square

Actually if we are over \mathbb{C} , then $\text{End}_{\mathbb{C}}(\mathbb{C}/\Lambda) = \{\alpha \in \mathbb{C} \mid \alpha \cdot \Lambda \subset \Lambda\}$, and the dual of α is just its complex conjugate $\bar{\alpha}$.

Let $X = \text{Proj}(\mathbb{F}_q[Z_0, Z_1, Z_2]/(h))$ be a smooth scheme over $k = \mathbb{F}_q$, $q = p^r$, such that $X \times_k \bar{k}$ is an elliptic curve over \bar{k} . We say that \bar{X} is an elliptic curve over \bar{k} which can be defined on k . We also assume that there's a point \bar{P}_0 on \bar{X} with coordinates in k , i.e., there's a k -linear map $\text{Spec}(k) \xrightarrow{P_0} X$. First we show that $\bar{X}_q \cong \bar{X}$.

Lemma 4.5. $\bar{X}_q \cong \bar{X}$ naturally, and via this isomorphism, the q -Frobenius map $F' : \bar{X} \rightarrow \bar{X}$ is the map that takes q th power of coordinates of each point, after we embed \bar{X} into \mathbb{P}_k^2 via $|3\bar{P}_0|$.

Proof. We know that

$$\begin{array}{ccc} \bar{X} & \longrightarrow & \text{Spec}(\bar{k}) \\ \downarrow & & \downarrow \\ X & \longrightarrow & \text{Spec}(k) \end{array}$$

is a pullback diagram in the category of schemes; this is how we define \bar{X} . We want to show first that

$$\begin{array}{ccc} \text{Spec}(\bar{k}) & \xrightarrow{F} & \text{Spec}(\bar{k}) \\ \downarrow & & \downarrow \\ \text{Spec}(k) & \xrightarrow{F=id} & \text{Spec}(k) \end{array}$$

is also a pullback. Note that the q th power map restricted on $k = \mathbb{F}_q$ is just the identity map. It's equivalent to showing that

$$\begin{array}{ccc} k & \xrightarrow{F=id} & k \\ \downarrow & & \downarrow \\ \bar{k} & \xrightarrow{F} & \bar{k} \end{array}$$

is a pushout(tensor product) in the category of k -algebras. Certainly it's commutative. Given any k -algebra $g : k \rightarrow A$, and any morphisms $k \rightarrow A$, which has to be the same as the structure map g , and $f : \bar{k} \rightarrow A$ extending g , suppose we have a morphism $H : \bar{k} \rightarrow A$ making the two triangles commute, then $H \circ F(\lambda) = f(\lambda)$, for any $\lambda \in \bar{k}$, which means that $H(\lambda^q) = f(\lambda)$, so $H(\lambda) = f(\lambda)^{\frac{1}{q}}$. This shows that H , if exists, is unique. For the existence, one only needs to check that H thus defined is really a morphism, which follows easily from the "Freshmen's Dream" $f(\lambda + \mu)^{1/q} = f(\lambda)^{1/q} + f(\mu)^{1/q}$.

The composite of two pullbacks is again a pullback. So

$$\begin{array}{ccccc} \bar{X} & \longrightarrow & \text{Spec}(\bar{k}) & \xrightarrow{F} & \text{Spec}(\bar{k}) \\ \downarrow & & \downarrow & & \downarrow \\ X & \longrightarrow & \text{Spec}(k) & \xrightarrow{F=id} & \text{Spec}(k) \end{array}$$

is a pullback, which means that \bar{X}_q serves as a pullback of the wedge $\begin{array}{ccc} & & \text{Spec}(\bar{k}) \\ & & \downarrow \\ X & \longrightarrow & \text{Spec}(k) \end{array}$.

But \bar{X} , by definition, is also the fiber-product of the same wedge, so we have a natural isomorphism $\alpha : \bar{X} \rightarrow \bar{X}_q$ commuting with the two evident morphisms, by the uniqueness of the limit.

Let $P_0 : \text{Spec}(k) \rightarrow X$ be a k -rational point. Without loss of generality we assume P_0 is the intersection of X with the line at infinity $Z_2 = 0$, and $\text{Spec}(A)$ be the open complement $X - P_0$. Let $\bar{P}_0 \in \bar{X}$ be the fiber-product of $P_0 \in X$, and let $B = A \otimes_k \bar{k}$ so that $\bar{X} - \bar{P}_0 = \text{Spec}(B)$. Suppose X is embedded into \mathbb{P}_k^2 via x, y , i.e., $P \mapsto [x(P), y(P), 1]$, where the only pole for either x or y is P_0 . So x and y are regular on $\text{Spec}(A)$, which means $x, y \in A$. To see what $F' : \bar{X} \rightarrow \bar{X}$ is doing in terms of coordinates we have to examine what the isomorphism $\alpha : \bar{X} \rightarrow \bar{X}_q$ is doing. By the universal property of a pushout, the embeddings $\bar{k} \hookrightarrow A \otimes \bar{k}$ and $A \hookrightarrow A \otimes \bar{k}$ induces $H : \bar{k} \rightarrow A \otimes \bar{k}$ such that $1 \otimes \lambda = H \circ F(\lambda) = H(\lambda^q) = H(\lambda)^q$, for any $\lambda \in \bar{k}$, so $H(\lambda) = 1 \otimes \lambda^{1/q}$. Hence $\alpha : B \rightarrow B$ is induced by $i_1 : A \hookrightarrow A \otimes \bar{k}$ and $H : \bar{k} \rightarrow A \otimes \bar{k}$.

Now let's take a look at the Frobenius map $F' : \bar{X}_q \rightarrow \bar{X}$. We claim it's the q th power map $B \rightarrow B$. First, the q th power map is indeed a k -algebra homomorphism from B to B . It induces the identity map on $\text{Spec}(B)$. Indeed, let $\mathfrak{p} \in B$ be a prime ideal. Then the contraction \mathfrak{p}^c consists of q th roots of elements in \mathfrak{p} , which is prime, so by definition $\mathfrak{p}^c = \mathfrak{p}$. Also it induces q th power maps on localizations of B . So the q th power map on B is the Frobenius map on the affine part. Now the composite $\bar{X} \xrightarrow{\alpha} \bar{X}_q \xrightarrow{F'} \bar{X}$ on the affine part is just the composite $B \xrightarrow{q} B \xrightarrow{\alpha} B$ sending $\sum_i a_i \otimes \lambda_i \mapsto \sum_i a_i^q \otimes \lambda_i^q \mapsto \sum_i a_i^q \otimes \lambda_i$.

Now let $x_1 = x \otimes 1, y_1 = y \otimes 1$ in $B = A \otimes \bar{k}$. The embedding of $\bar{X} \hookrightarrow \mathbb{P}_k^2$ is given by x_1, y_1 . For $P \in \bar{X} - \bar{P}_0$, we have $\text{Spec}(\bar{k}) \xrightarrow{P} \text{Spec}(B) \xrightarrow{x_1} \text{Spec}(\bar{k}[T])$, where $\bar{k}[T] \xrightarrow{x_1} B$ sends $T \mapsto x_1$, and the map $B \xrightarrow{P} \bar{k}$ maps $x_1 \mapsto x_1(P)$. Now

consider

$$\bar{k}[T] \xrightarrow{x_1} B \xrightarrow{F'} B \xrightarrow{P} \bar{k},$$

where $B \xrightarrow{F'} B \xrightarrow{P} \bar{k}$ is the "point" $F'(P) \in \bar{X}$. We have

$$T \mapsto x_1 = x \otimes 1 \mapsto x^q \otimes 1 \mapsto P(x^q \otimes 1).$$

But $x_1(F'(P)) = P(x^q \otimes 1) = P(x_1^q) = P(x_1)^q = x_1(P)^q$. Similarly $y_1(F'(P)) = y_1(P)^q$. So the map $[x_1(P), y_1(P), 1] \mapsto [x_1(F'(P)), y_1(F'(P)), 1]$ is the q th power map on coordinates. For the base point $\bar{P}_0 = [0, 1, 0]$ the assertion is trivially true. \square

Theorem 4.6. $1_{\bar{X}} - F' : \bar{X} \rightarrow \bar{X}$ is separable, with kernel the $k = \mathbb{F}_q$ -rational points on \bar{X} .

Proof. $h^0(\bar{X}, \omega_{\bar{X}}) = 1$, and let $\eta \in H^0(\omega_{\bar{X}})$ be a nonzero 1-form. Then $(1_{\bar{X}} - F')^* \eta = 1_{\bar{X}}^* \eta - F'^* \eta = \eta \neq 0$, by Silverman, p.81, thm.5.2, so $1_{\bar{X}} - F'$ is separable. Indeed, if it's not, then it factors as a composite of a separable map with a purely inseparable map, and the pullback-map on differential forms also factors through that of a purely inseparable one, which is 0.

Let $P \in \bar{X}$ be in the kernel of $1_{\bar{X}} - F'$, which means in the group law, $P - F'(P) = \bar{P}_0$, the identity element. So as divisors $P - F'(P) \sim 0$. But \bar{X} is not rational, so $P = F'(P)$, which means that $x_1(P), y_1(P)$ are roots of $t^q = t$, so they are in k . Obviously the converse is true. \square

Theorem 4.7. Let N_1 be the number of points on \bar{X} with coordinates in $k = \mathbb{F}_q$. Then $F' + \hat{F}' = a_{\bar{X}}$, where $a \in \mathbb{Z}$ such that $N_1 = 1 - a + q$.

Proof. $1_{\bar{X}} - F'$ has degree N_1 because it's separable (hence étale) and has N_1 points in the kernel. So $(N_1)_{\bar{X}} = (1 - F')(1 - \hat{F}') = (1 - F')(\hat{1} - \hat{F}') = (1 - F')(1 - \hat{F}') = 1 - (F' + \hat{F}') + F'\hat{F}' = 1 - (F' + \hat{F}') + q_{\bar{X}}$, so $F' + \hat{F}' = a_{\bar{X}}$ where $N_1 = 1 - a + q$. \square

Theorem 4.8. In the theorem above $|a| \leq 2\sqrt{q}$.

Proof. Note that if F' is an integer, then it's $\pm\sqrt{q}$ because its degree is q . So $F' = \hat{F}' = \pm\sqrt{q}$, and then $a = F' + \hat{F}' = \pm 2\sqrt{q}$, whose absolute value is $2\sqrt{q}$.

First we show that $m + nF'$ is a constant map, for $m, n \in \mathbb{Z}$, only when both $m = n = 0$. Suppose F' is not an integer. If one of m, n is 0 but the other is not, then $m + nF'$ is non-constant. If both are nonzero, we can assume they are coprime, because $d(m' + n'F')$ is constant if and only if $m' + n'F'$ is. So let $am + bn = 1$. Then $m + nF' = 0 \Rightarrow am + anF' = 0 \Rightarrow 1 - n(b - aF') = 0 \Rightarrow b - aF' = n = 1$ or $b - aF' = n = -1$. If $n = 1$, then $am + b = 1$, so $-aF' = 1 - b = am$. As before, $a(m + F') = 0 \Leftrightarrow m + F' = 0$, by counting degrees, so this implies $F' = -m$ is an integer, a contradiction. The case when $n = -1$ is similar.

So now $\deg(m + nF') > 0$ for all $m, n \in \mathbb{Z}$, with one of them nonzero. $\deg(m + nF') = (m + nF')(m + \hat{nF}') = (m + nF')(m + n\hat{F}') = m^2 + anm + n^2q$.

This means $t^2 + at + q > 0$ for any rational number t , which implies that $t^2 + at + q \geq 0$ for any real number t , since rationals are dense in the reals. So $a^2 - 4q \leq 0, |a| \leq 2\sqrt{q}$. \square

We will see in the next section that this amounts to say the analogue for Riemann Hypothesis is true for elliptic curves.

5 Conclusion

Theorem 5.1. *The Weil conjecture for elliptic curves is true.*

Proof. Recall that $N_1 = 1 - a + q = 1 - (F' + \hat{F}') + q$, where F' is the \bar{k} -linear q -Frobenius map, and N_1 is the number of points on the curve with coordinates in $k = \mathbb{F}_q$. Note that F' takes q th power of each coordinates, so the q^r -Frobenius map is F'^r . If we replace q by q^r , we have $N_r = 1 - (F'^r + \hat{F}'^r) + q^r$. So the zeta-function is $Z(t) = \exp(\sum_{r \geq 1} \frac{N_r t^r}{r}) = \exp(\sum_r (\frac{t^r}{r}) - \sum_r (\frac{(F't)^r}{r}) - \sum_r (\frac{(\hat{F}'t)^r}{r}) + \sum_r (\frac{(qt)^r}{r})) = \frac{(1-F't)(1-\hat{F}'t)}{(1-t)(1-qt)} = \frac{1-at+qt^2}{(1-t)(1-qt)}$, which proves the rationality.

An elliptic curve has trivial canonical divisor, hence trivial tangent sheaf. So $E = \deg(c_1(\mathcal{T}_{\bar{X}})) = \deg(c_1(\mathcal{O})) = 0$. $Z(\frac{1}{qt}) = \frac{1-\frac{a}{qt}+\frac{q}{(qt)^2}}{(1-\frac{1}{qt})(1-\frac{q}{qt})} = \frac{qt^2-at+1}{(qt-1)(t-1)} = Z(t)$, which proves the functional equation.

If we factorize $1 - at + qt^2$ over \mathbb{C} as $(1 - \alpha t)(1 - \beta t)$, then $\alpha + \beta = a$ and $\alpha\beta = q$, and they are algebraic integers because they satisfy the monic polynomial $x^2 - ax + q = 0$. We show now that $|a| \leq 2\sqrt{q}$ is equivalent to $|\alpha| = \sqrt{q}, |\beta| = \sqrt{q}$. If $|\alpha| = \sqrt{q}, |\beta| = \sqrt{q}$, then $|a| = |\alpha + \beta| \leq |\alpha| + |\beta| = 2\sqrt{q}$. Now suppose $|a| \leq 2\sqrt{q}$. If $|a| = 2\sqrt{q}$, then the equation $x^2 - ax + q = 0$ has a double root $\alpha = \beta = \frac{a}{2}$ with absolute value $|\frac{a}{2}| = \sqrt{q}$. If $|a| < 2\sqrt{q}$, then $x^2 - ax + q = 0$ has two imaginary roots: $\alpha = \frac{a + \sqrt{4q - a^2}\sqrt{-1}}{2}, \beta = \frac{a - \sqrt{4q - a^2}\sqrt{-1}}{2}$.

So $|\alpha| = \sqrt{(\frac{a}{2})^2 + (\frac{\sqrt{4q - a^2}}{2})^2} = \sqrt{q}$, and similarly $|\beta| = \sqrt{q}$. So the result we proved in last section is just the analog of Riemann hypothesis.

$B_0 = 1, B_1 = 2, B_2 = 1$, which are exactly the topological betti numbers of a torus. And $E = 0 = 1 - 2 + 1 = B_0 - B_1 + B_2$. \square

As a corollary, for an elliptic curve, $N_1 = 1 - a + q$ determines a , which determines $Z(t)$, which determines all N_r . It's a more general fact that for a curve of genus g , N_1, \dots, N_g determines all N_r .

References

- [1] Hartshorne, R., *Algebraic Geometry*, GTM 52.
- [2] Silverman, J. H., *The Arithmetic of Elliptic Curves*, GTM 106.
- [3] Milne, J., *Lectures on Étale Cohomology*, available on his homepage.