THE GEOMETRY OF ELLIPTIC CURVES OVER FINITE FIELDS

ARIEH ZIMMERMAN

Abstract. We first provide an overview of the basic results in the geometry of elliptic curves, introducing the Picard Group, Weierstrass Equations, and Isogenies. This is followed by a discussion of the structure of m-torsion points on an elliptic curve, introducing such tools as the Weil pairing and the l-adic Tate module. The paper culminates in a theorem counting the rational points on an elliptic curve over a finite field using the trace of Frobenius.

Contents

1. Preliminaries

We first briefly recount some basic geometric definitions. Throughout, we let K be a perfect field. Additionally, we assume familiarity with fundamental concepts from projective geometry, such as the homogenization of polynomials, how to alternate between affine and projective notation for coordinates (for the former we use parentheses and for the latter we use brackets), and the inductive construction of $\mathbb{P}^n$ as a union of affine points and $\mathbb{P}^{n-1}$. For more on this topic, see [2, A.1-2]

Definition. *A* projective variety V *over* K *is any set of the form*

$$V = \{P \in \mathbb{P}^n(\overline{K}) \mid \forall f \in I,\ f(P) = 0\},$$

where $I \in K[X_0, \ldots, X_n]$ *is a prime ideal generated by homogeneous polynomials with coefficients in* K *(remember that evaluating* f *at* P *makes sense since* f *is homogenous). By* $V(K)$ *we denote the points on* V *with coordinates in* K*.*

Definition. *Let* $I = (f(X_0, \ldots, X_n))$ *be prime with* f *homogeneous, and let* V *be the corresponding variety. Then* V *is* singular *at* $P \in V$ *if*

$$\frac{\partial f}{\partial X_0}(P) = \cdots = \frac{\partial f}{\partial X_n}(P) = 0.$$

If V *is not singular at any point, then we say* V *is* smooth*.*

Date: December 24, 2016.

Example. *Consider a curve associated to a dehomogenized equation of the form*

$$y^2 = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = f(x),$$

referred to as a hyperelliptic curve. *This polynomial is singular at any affine point* (x_0, y_0) *if* $2y_0 = f'(x_0) = 0$. *However, notice that there is also a point on this curve on the line at infinity, namely* $[0, 1, 0]$. *Homogenizing our equation and taking partial derivatives, it is clear that this equation is certainly singular at this point if* $d \geq 4$. *However, for* $d = 2, 3$ *the only singular points must be affine.*

Definition. *The* function field $K(V)$ *of* V *consists of all* $\frac{f}{g} \in K(X_0, \ldots, X_n)$ *such that* f, g *are homogenous of the same degree and* $g \notin I(V)$, *taken modulo the equivalence relation* $\sim$ *defined by* $\frac{f_1}{g_1} \sim \frac{f_2}{g_2} \Leftrightarrow f_1 g_2 - f_2 g_1 \in I(V)$.

The function field can be thought of as quotients of polynomials in I restricted to the variety V.

Definition. *A* curve C *is a projective variety such that* $K(C)$ *has transcendence degree* 1 *over* K.

The motivation for this definition is simple: we would like to have a variety that, as a submanifold, is one-dimensional (a "curved line"). However, given an ideal generated by more polynomials than expected, the corresponding variety may still behave as a curve. This is because there may be redundancies, such f^2 being listed in addition to f. As it happens, generally, these redundancies take the form of algebraic dependencies between roots, which is captured by transcendence degree.

Definition. *With* $P \in C$ *as above, let* $\overline{K}[C]_P$ *be the elements* $\frac{f}{g} \in K(C)$ *such that* $g(P) \neq 0$, *so the rational functions that are defined at* P. *Define* $M_P \subset \overline{K}[C]_P$ *to be the (maximal) ideal* $\left\{ \frac{f}{g} \in \overline{K}[C]_P \mid f(P) = 0 \right\}$.

The previous definition is useful largely because it allows us to define a notion of the degree to which a function vanishes or has a pole at a given point. This information alone is ultimately very valuable.

Definition. *We define a function* $\operatorname{ord}_P : \overline{K}[C]_P \to \mathbb{Z} \cup \{\infty\}$ *by*

$$\operatorname{ord}_P(f) = \sup\{d \in \mathbb{Z} : f \in M_P^d\},$$

letting $M_p^0 = \overline{K}[C]_P$ *by convention. We extend this to* $\overline{K}(C)$ *by letting* $\operatorname{ord}_P\left(\frac{f}{g}\right) = \operatorname{ord}_P(f) - \operatorname{ord}_P(g)$. *We call* $t \in \overline{K}(C)$ *a* uniformizer at P *if* $\operatorname{ord}_P(t) = 1$.

One can easily confirm that ord_P is a discrete valuation on $\overline{K}[C]_P$.

Theorem 1. *If* C *is a curve, than for any* $P \in C(K)$, *there is some uniformizer* t *for* P *in* C.

Proof. Taking any nonconstant homogeneous polynomial in $K[X_0, \ldots, X_n]$ vanishing at P, we get some $f \in M_P$ with $d = \operatorname{ord}_P(f) > 0$. Since $f \in M_P^d$, we have

$$f = a_1 g_{11} \ldots g_{1d} + \cdots + a_n g_{n1} \ldots g_{nd},$$

where $a_1, \ldots, a_n \in K^*$ and $g_{ij} \in M_P \setminus \{0\}$ for all $1 \leq i \leq n$ and $1 \leq j \leq d$. Note that, if all the summands here vanished to order greater than d, then since ord_P is a valuation, we would have $\operatorname{ord}_P(f) > d$. Therefore there is some i such that

$$\operatorname{ord}_P(g_{i1}) + \cdots + \operatorname{ord}_P(g_{id}) = \operatorname{ord}_P(a_i g_{i1} \ldots g_{id}) \leq d.$$

Now every term in this sum is a positive integer, so because there are d of them, each must be 1. This means g_{i1} is a uniformizer. QED

Example. *As a simple example, over* $\mathbb{P}_1$*, we have* $\operatorname{ord}_{[0,1]}\left(\frac{1}{x}\right) = -1$ *and* $\operatorname{ord}_{[1,0]}\left(\frac{1}{x}\right) = 1$*. By the latter,* $\frac{1}{x}$ *is a uniformizer at* ∞*.*

Definition. *Let* C_1, C_2 *be smooth curves. A* morphism $\phi : C_1 \to C_2$ *over* K *is a map given coordinate-wise by elements of* $K(C_1)$ *i.e. there are* $f_1, \ldots, f_i \in K(C_1)$ *such that* $\phi(P) = [f_1(P), \ldots, f_i(P)]$ *for all* $P \in C_1$*. We call* ϕ *an* isomorphism *if there exists a morphism* $\psi : C_2 \to C_1$ *such that* $\phi \circ \psi$ *is the identity on* C_2 *and* $\psi \circ \phi$ *is the identity on* C_1*.*

Example. *Let* $\phi : \mathbb{P}^1(\overline{K}) \to \mathbb{P}^1(\overline{K})$ *be the map* $[X, Y] \mapsto [X^3(X - Y)^2, Y^5]$*. Because we are working over an algebraically closed field, and this map is given by polynomials of degree* 5*, we would expect the preimage of any point in the image to contain* 5 *points. However,* $\phi^{-1}([0, 1])$ *contains only the points* $[0, 1]$ *and* $[1, 1]$*. We will soon return to this issue.*

A morphism $\phi : C_1 \to C_2$ over K naturally induces a map $\phi^* : K(C_2) \to K(C_1)$ defined by $f \to f \circ \phi$. The utility of ϕ^* lies in that it is intimately related to ϕ and yet, as a map of fields, has more algebraic structure. The following definition recognizes this relationship.

Definition. *Let* $\phi : C_1 \to C_2$ *be a nonconstant morphism of smooth curves. The* degree $\deg \phi$ *of* ϕ *is the degree of the extension* $K(C_1)/\phi^*(K(C_2))$*, and we say that* ϕ *is* separable, inseparable, *or* purely inseparable *if this extension has the corresponding property. We also let*

$$\deg_s \phi = [K(C_1) : \phi^*(K(C_2))]_{sep}$$

and

$$\deg_i \phi = \deg \phi / \deg_s \phi.$$

A morphism need not be one-to-one, but based on the previous example, in which ϕ has degree 5, one would expect a morphism ϕ to be "$\deg \phi$-to-one." The next definition measures the extent to which this fails at a given point:

Definition. *Let* $\phi : C_1 \to C_2$ *be as above. The ramification index* $e_\phi(P)$ *of* ϕ *at* $P \in C_1$ *is the value* $\operatorname{ord}_P(\phi^* t)$ *for any uniformizer* $t \in K(C_2)$*.*

We state the following proposition as it illustrates the nature of the ramification index; see [3, II.6.8-9] and [1, II.2.6] for proofs.

Proposition 1. *Let* ϕ *and* P *be as above. Then*

i. For all $Q \in C_2$*,*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi.$$

ii. For all but finitely many $Q \in C_2$*,*

$$|\phi^{-1}(Q)| = \deg_s \phi$$

iii. If $\psi : C_2 \to C_3$ *is another nonconstant morphism, then*

$$e_{\psi \circ \phi}(P) = e_\psi(\phi(P)) e_\phi(P).$$

Example. *If ϕ is given as in our previous example, then ϕ has degree 5. However, $\phi^{-1}([0,1])$ contains only $[0,1]$ and $[1,1]$. To explain this, we notice that $e_\phi([0,1]) = 3$ and $e_\phi([1,1]) = 2$. However, as per Proposition 1, we have*

$$\sum_{P\in\phi^{-1}([0,1])} e_\phi(P) = e_\phi([0,1]) + e_\phi([1,1]) = 3 + 2 = 5.$$

To codify and analyze the information given by ord_P, we place it in a more abstract context:

Definition. *The* divisor group $\mathrm{Div}(C)$ *of a smooth curve C is the free abelian group generated by points of C. If $f \in \overline{K}(C)^*$, we let $\mathrm{div}(f) = \sum_{P\in C} \mathrm{ord}_P(f)(P) \in \mathrm{Div}(C)$. A divisor D is* principal *if $D = \mathrm{div}(f)$ for some $f \in \overline{K}(C)$. Principal divisors form a subgroup of $\mathrm{Div}(C)$, since clearly $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$. The quotient of $\mathrm{Div}(C)$ by its principal divisors is the* Picard Group $\mathrm{Pic}(C)$ *of C.*

Definition. *If $D = \sum_{P\in C} n_p(P)$ is a divisor, then the degree $\deg D$ of D is $\sum_{P\in C} n_P$. By $\mathrm{Div}^0(C)$ we denote the subgroup of $\mathrm{Div}(C)$ consisting of divisors of degree 0, and $\mathrm{Pic}^0(C)$ denotes its image in the Picard Group.*

Any morphism $\phi : C_1 \to C_2$ of smooth curves gives maps

$$\begin{aligned} \phi_* : \mathrm{Div}(C_1) &\to \mathrm{Div}(C_2) & \qquad \phi^* : \mathrm{Div}(C_2) &\to \mathrm{Div}(C_1) \\ (P) &\mapsto (\phi P) & (Q) &\mapsto \sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P) \end{aligned}$$

Lemma. *With the previous notation, $\phi^*\mathrm{div}(f) = \mathrm{div}(\phi^* f)$ for all $f \in \overline{K}(C_2)^*$.*

Proof. Let $P \in C_1$, let t be a uniformizer at $\phi(P)$, and let $n = \mathrm{ord}_{\phi(P)}(f)$. Then, by definition, f has the same order as t^n at $\phi(P)$. Hence it is clear from the definitions that $f \circ \phi$ and $t^n \circ \phi$ have the same order at P, so that

$$\mathrm{ord}_P(\phi^* f) = \mathrm{ord}_P(f \circ \phi) = \mathrm{ord}_P(t^n \circ \phi) = n \cdot \mathrm{ord}_P(t \circ \phi) = e_\phi(P)\mathrm{ord}_{\phi(P)}(f).$$

Summing over all points with nonzero coefficients in $\mathrm{div}(f)$ then gives the lemma. QED

Theorem 2. *If the map ϕ^* is given as above, it induces a corresponding homomorphism $\phi^* : Pic^0(C_2) \to Pic^0(C_1)$.*

Proof. It is clear from the definition and *Proposition 1* that $\deg \phi^* D = (\deg \phi)(\deg D)$. Therefore divisors of degree 0 are taken to divisors of degree 0. Furthermore, by the lemma, principal divisors are taken to principal divisors. Hence, taking quotients, the map is well-defined, and the fact that it is a homomorphism is immediate. QED

Corollary. *If C is a smooth curve with $f \in \overline{K}(C)$, then $\deg \mathrm{div} f = 0$ i.e. principal divisors have degree 0.*

Proof. Consider f as a map from $C \to \mathbb{P}^1$, and let $f^* : \mathrm{Div}(\mathbb{P}^1) \to \mathrm{Div}(C)$ be the corresponding map given by the theorem. It is clear from the definitions that $\mathrm{div}(f) = f^*((0) - (\infty))$. Hence, again using Proposition 1,

$$\deg \mathrm{div}(f) = \deg f^*((0) - (\infty)) = \deg f - \deg f = 0.$$

QED

Definition. *Let D be a divisor. Then $\mathcal{L}(D)$ over $\overline{K}$ is the vector space consisting of all $f \in \overline{K}(C)^*$ such that $div(f) + D$ has nonnegative coefficients, together with the function 0.*

For our next proposition, we will apply a powerful result known as the Riemann-Roch Theroem. While it is well beyond the scope of this paper, we suggest [3, IV] for a rigorous discussion. It utilizes a geometric invariant known as *genus*, but we will need to know nothing about genus except for the definition which begins the next section in conjunction with the following:

Proposition 2. *If C is a curve of genus 1 and $D \in \mathrm{Div}(C)$ has positive degree, then $\mathcal{L}(D)$ has dimension $\deg D$. Additionally, $\mathcal{L}(0) = \overline{K}$.*

2. Elliptic Curves and the Group Law

Definition. *An* elliptic curve *over K is a smooth curve E over K of genus 1, together with a distinguished point $O \in E$.*

Theorem 3. *Any elliptic curve (E, O) is isomorphic to a smooth curve in $\mathbb{P}^2$ given by an equation of the form*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5,$$

where O is sent to $[0, 1, 0]$.

Proof. By *Proposition 2*, the vector space $\mathcal{L}(2(O))$ has dimension 2, and it clearly contains the constant functions. Hence it has a basis consisting of 1 and one other element in $K(E)$ - call it x. By the same proposition, $\mathcal{L}(3(O))$ has dimension 3, and clearly it contains $\mathcal{L}(2(O))$. Hence it has a basis of the form $\{1, x, y\}$, where $y \in \mathcal{L}(2(O)) \setminus \mathcal{L}(3(O))$. Now consider the seven elements $1, x, y, x^2, xy, y^2, x^3 \in \mathcal{L}(6(O))$. Since *Proposition 2* tells us that this vector space has dimension 6, there must be some linear dependence among these functions:

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0.$$

Making the substitutions

$$x \mapsto -A_6A_7x \qquad y \mapsto A_6A_7^2y$$

and dividing by $A_6^3A_7^4$ gives an equation of the desired form. Hence $\phi = [x, y, 1]$ is the morphism we require, sending (E, O) to the curve generated by our equation. To show it has an inverse, we first show it has degree 1. Consider the map $[x, 1] : E \to \mathbb{P}^1$. By construction, $\mathrm{ord}_O([x, 1]) = -2$, and the map has no other poles. Therefore, if t is the identity function over $\mathbb{P}^1(K)$ sending $[v, w] \mapsto \frac{v}{w}$, using the uniformizer $\frac{1}{t}$ at $[1, 0]$, we see using *Proposition 1* that

$$\begin{aligned}[K(E) : K(x)] = \deg[x, 1] &= \sum_{[x,1](P)=[1,0]} e_{[x,1]}(P) \\ &= e_{[x,1]}(O) = \mathrm{ord}_O\left([x, 1]^*\frac{1}{t}\right) = \mathrm{ord}_O\left(\frac{1}{x}\right) = 2.\end{aligned}$$

A similar calculation for y shows that $[K(E) : K(y)] = 3$. Hence $[K(E) : K(x, y)]$ divides both 2 and 3, and therefore must be 1, implying $K(E) \cong K(x, y)$. Let

$\iota : K(E) \to K(x,y)$ be this isomorphism, and let $X_0, \dots, x_n$ be the coordinate functions on $K(E)$. Then one can verify that

$$\left[\iota(1), \iota\left(\frac{X_1}{X_0}\right), \dots, \iota\left(\frac{X_n}{X_0}\right)\right] : \mathrm{Im}(\phi) \to E$$

provides an inverse morphism to ϕ, and we are done. QED

From here on, we assume that any Elliptic curve takes this form.

Examining the proof of the previous theorem, we see that if we could specify $A_1, \dots, A_7 \in K$, we could produce $a_1, \dots, a_5 \in K$. Therefore, [1, II.5.8], which tells us that $\mathcal{L}(6(O))$ has a basis of elements in $K(E)$, begets our next proposition.

Proposition 3. *If E is defined over K, then we may let $a_1, \dots, a_5 \in K$ and $O \in E(K)$.*

There is another critical source of algebraic structure on elliptic curves. Remarkably, via intuitive geometric constructions, it forms an abelian group with O as the identity. Namely, if $P, P' \in E$, let L be the unique line going through these points (or, if $P = P'$, let L be the tangent line at P). Then (Bèzout's Theorem) L will intersect E at precisely one other point P''. Let L' be the vertical line going through P'', and once again L' will intersect E at precisely one other point. This is the point we call $P + P'$. To be explicit, we give the algebraic definition of the group law:

Group Law. *Let (E, O) be an elliptic curve. Then the points of E form an abelian group with identity O, given by the following group law:*

$$(x_1, y_1) + (x_2, y_2) =$$
$$\begin{cases} (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -x_3(\lambda + a_1) - \nu - a_3), & x_1 \neq x_2 \text{ or } y_1 = y_2 \\ O, & x_1 = x_2 \text{ and } y_1 \neq y_2 \end{cases}$$

where

$$\lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2}, & x_1 \neq x_2 \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & x_1 = x_2 \end{cases}$$

and

$$\nu = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \frac{-x_1^3 + a_4x_1 + 2a_5 - a_3y_1}{2y_1 + a_1x_1 + a_3}, & x_1 = x_2 \end{cases}.$$

It is straightforward, though tedious, to verify that the above laws indeed render E an abelian group, with $-(x, y) = (x, -y - a_1x - a_3)$ (see [1, III.2.2]). To denote the sum of P with itself m times, for $m \in \mathbb{N}$, we will write $[m]P$ throughout the rest of this paper.

We now give an extremely useful characterization of the group law in terms of divisors, finishing with a complete description of principal divisors.

Lemma. *Let E be an elliptic curve with $P, Q \in E$. Then $(P) - (Q)$ is principal if and only if $P = Q$.*

Proof. Choose $f \in \overline{K}(E)$ such that $\mathrm{div}(f) = (P) - (Q)$. Then $f \in \mathcal{L}((Q))$. By *Proposition 2*, we have $\dim \mathcal{L}((Q)) = 1$. However, $\overline{K}^* \subset K(E)$ is in $\mathcal{L}((Q))$, since $\deg(\mathrm{div}(c) + (Q))$ for any $c \in \overline{K}^*$. Therefore this is all of $\mathcal{L}((Q))$, implying $f \in \overline{K}^*$. This then immediately shows that $P = Q$. QED

Theorem 4.

i. If $D \in \mathrm{Div}^0(E)$, then there is a unique point $P \in E$ such that $D - (P) + (O)$ is principal.

ii. Let $\sigma : \mathrm{Div}^0(E) \to E$ be the map sending each degree-0 divisor to the point described in (i). Then σ induces a group isomorphism

$$\sigma : \mathrm{Pic}^0(E) \to E.$$

Proof.

i. By *Proposition 2*, we have $\dim \mathcal{L}(D + (O)) = 1$. Let $\{f\}$ be a basis for this space, with $\mathrm{div}(f) = \sum_{P \in E} n_p(P)$. Observe that $\deg \mathrm{div}(f) = 0$ and that $H := \mathrm{div}(f) + D + (O)$ has nonnegative coefficients. The first statement implies that

$$\deg H = \deg \mathrm{div}(f) + \deg D + \deg((O)) = 0 + 0 + 1 = 1,$$

so the coefficients of H sum to 1, and by the second statement, these coefficients are all nonnegative integers. Since the only sum of this sort must consist of a 1 and a series of 0's, we must have $H = (P)$ for some $P \in E$ i.e. $\mathrm{div}(f) = -D - (O) + (P)$, implying $D - (P) + (O)$ is principal. Now assume that $D - (P') + (O)$ is also principal. Then

$$(P) - (P') = (D - (P') - (O)) - (D - (P) - (O))$$

is the difference of two principal divisors, hence also principal. Then, by the lemma, $P = P'$, showing uniqueness.

ii. Clearly σ is surjective, since $\sigma((P) - (O)) = P$. To show it is well defined, let $\sigma(D_1) = P_1$ and $\sigma(D_2) = P_2$ for some $D_1, D_2 \in \mathrm{Div}^0(E)$. Then, being the difference of two principal divisors, the divisor

$$D_1 - D_2 - (P_1) + (P_2) = (D_1 - (P_1) + (O)) - (D_2 - (P_2) + (O))$$

is principal. Hence, we have $P_1 = P_2$ if and only if $D_1 - D_2$ is principal. Reviewing our definition of the Picard Group then makes it clear that this map is well-defined and injective.

To show that σ is a homomorphism, we instead show that σ^{-1}, which takes $P \in E$ to the class of divisors represented by $(P) - (O)$, is a homomorphism. Let $P, Q \in E$. We need to show that $\sigma^{-1}(P + Q) = \sigma^{-1}(P) + \sigma^{-1}(Q)$, where divisor addition occurs on the right and point addition occurs on the left using our group law. Let $f(X, Y, Z) = 0$ be the equation for the projective line $\overline{PQ}$. If R is the point of intersection of this line with E, then let $g(X, Y, Z) = 0$ be the equation for the projective line $\overline{OR}$. Then we have

$$\begin{aligned}
\mathrm{div}\left(\frac{f}{Z}\right) &= \mathrm{div}(f) - \mathrm{div}(Z) = (P) + (Q) + (R) - 3(O), \\
\mathrm{div}\left(\frac{g}{Z}\right) &= \mathrm{div}(g) - \mathrm{div}(Z) = (O) + (R) + (P + Q) - 3(O) \\
&= (R) + (P + Q) - 2(O),
\end{aligned}$$

(the easiest way to see that $\operatorname{div}(Z) = 3(O)$ is by Bézout's Theorem, since O is the only point on E on the line $Z = 0$). Thus,

$$\begin{aligned}\operatorname{div}\left(\frac{f}{g}\right) &= \operatorname{div}\left(\frac{f}{Z}\right) - \operatorname{div}\left(\frac{g}{Z}\right)\\ &= (P) + (Q) + (R) - 3(O) - ((R) + (P+Q) - 2(O))\\ &= (P) + (Q) - (P+Q) = \sigma^{-1}(P) + \sigma^{-1}(Q) - \sigma^{-1}(P+Q).\end{aligned}$$

Reducing modulo principal divisors then gives $\sigma^{-1}(P+Q) = \sigma^{-1}(P)+\sigma^{-1}(Q)$, as needed.

QED

Corollary. *A divisor $D = \sum_{P\in E} n_P(P) \in \operatorname{Div}(E)$ is principal if and only if $\sum_{P\in E} n_P = 0$ and $\sum_{P\in E}[n_P]P = O$.*

Proof. The corollary to *Theorem 2* shows that every principal divisor has degree 0, so we need only be concerned with elements of $\operatorname{Div}^0(E)$. By the theorem, a degree-0 divisor D is principal if and only if

$$\begin{aligned}O = \sigma(D) = \sigma\left(\sum_{P\in E} n_P(P)\right) &= \sigma\left(\sum_{P\in E} n_P((P) - (O))\right)\\ &= \sum_{P\in E}[n_P]\sigma((P) - (O)) = \sum_{P\in E}[n_P]P\end{aligned}$$

where we have added and subtracted equal numbers of (O)'s as necessary. QED

3. Isogenies

Definition. *Let $(E_1, O_1), (E_2, O_2)$ be elliptic curves. An* isogeny *ϕ is a morphism $E_1 \to E_2$ such that ϕ is also a homomorphism of groups. If $(E_1, O_1) = (E_2, O_2)$, then we call ϕ an* endomorphism *of E_1. The set of all such endomorphisms forms a ring under addition and composition, denoted* $\operatorname{End}(E_1)$.

It turns out that *any* morphism of Elliptic Curves preserving the identity element is immediately a homomorphism, but this fact is superfluous to this paper.

Theorem 5. *Let $\phi : E_1 \to E_2$ be a nonzero isogeny.*

i. For all $Q \in E_2$, we have $|\phi^{-1}(Q)| = \deg_s \phi$, yielding $e_\phi(P) = \deg_i \phi$ for all $P \in E_1$.

ii. Let $\tau_T : E_1 \to E_1$ be the isomorphism $P \mapsto P + T$. The map $T \to \tau_T^*$ then gives an isomorphism $\ker\phi \to \operatorname{Aut}(\overline{K}(E_1)/\phi^*\overline{K}(E_2))$.

Proof.

i. By *Proposition 1*, since $E_2(\overline{K})$ is infinite, there is some $Q \in E_2(\overline{K})$ such that $|\phi^{-1}(Q)| = \deg_s \phi$. Let Q' be another point on E_2, and set $R = Q - Q'$. Then for all $P \in \phi^{-1}(Q)$ and $P \in \phi^{-1}(Q')$, we have

$$\phi(P - R) = \phi(P) - \phi(R) = Q + Q' - Q = Q'$$

and

$$\phi(P' + R) = \phi(P') + \phi(R) = Q' + Q - Q' = Q.$$

The first statement shows that τ_{-R} maps $\phi^{-1}(Q)$ into $\phi^{-1}(Q')$, while the second shows that this restriction is surjective. Then, injectivity follows from the injectivity of τ_{-R}, so we have a bijection of the two sets.

To elucidate how this implies the latter statement, let $P, P' \in \phi^{-1}(Q)$ and $R = P - P'$. Then $\phi(R) = \phi(P) - \phi(P') = Q - Q = O$, so $\phi \circ \tau_R = \phi$, giving

$$e_\phi(P') = e_{\phi\circ\tau_R}(P') = e_\phi(\tau_R(P')) = e_\phi(P' + R) = e_\phi(P),$$

so ϕ has the same ramification index at every point in the preimage of Q. Together with *Proposition 1*, this allows us to calculate

$$(\deg_s \phi)(\deg_i \phi) = \deg \phi = \sum_{P\in\phi^{-1}(Q)} e_\phi(P) = |\phi^{-1}(Q)| e_\phi(P) = \deg_s \phi e_\phi(P),$$

and dividing gives the result.

ii. If $T \in \ker\phi$, then $\tau_T^*\phi^* f = f\circ\phi\circ\tau_T = f\circ\phi = \phi^* f$ for any $f \in \overline{K}(E_2)$, showing that τ_T^* fixes $\phi^*\overline{K}(E_2)$, and this map has the correct image. Of course, since the group law is abelian, $\tau_{S+T} = \tau_{T+S} = \tau_T \circ \tau_S = \tau_S^*\tau_T$, making this a homomorphism.

Consider the extension $\overline{K}(E_1)/\overline{K}(E_2)$. By the theory of separability, the minimal polynomial of this extension may be written

$$|\mathrm{Aut}(\overline{K}(E_1)/\phi^*\overline{K}(E_2)| \leq [\overline{K}(E_1) : \phi^*(\overline{K}(E_2))]_{sep} = \deg_s \phi,$$

so to prove bijectivity it suffices to show injectivity. Assume that $T \in E_1$ is in the kernel of the map. Then, in particular, $\tau_T^* x = x$. However, by construction (*Theorem 3*), x has a pole at O and no others. Therefore $T = O$, and we are done.

QED

Example. *The multiplication-by-m map $[m] : E \to E$ is a group homomorphism, and since the group law is given by rational functions, it is inductively an isogeny.*

It will be useful to have a explicit description of the rational functions that give the multiplication-by-n map. We propose such a description without proof, justified in that the ensuing computational intensity would take up too many pages of this paper (though said intensity can be found in [4, Lecture 6 Notes]):

Proposition 4. *In the notation of* Theorem 3*, let*

$$\begin{aligned} b_1 &= a_1^2 + 4a_2, \\ b_2 &= 2a_4 + a_1a_3 \\ b_3 &= a_3^2 + 4a_5 \\ b_4 &= a_1^2a_5 + 4a_2a_5 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

and let

$$\begin{aligned} \psi_1(x) &= 1 \\ \psi_2(x) &= 2y + a_1x + a_3 \\ \psi_3(x) &= 3x^4 + b_1x^3 + 3b_2x^2 + 3b_3x + b_4 \\ \psi_4(x) &= \psi_2 \cdot (2x^6 + b_1x^5 + 5b_2x^4 + 10b_3x^3 + 10b_4x^2 + (b_1b_4 - b_2b_3)x + (b_2b_4 - b_3^2)). \end{aligned}$$

Then, based on these initial values, inductively define

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$$

for $m \geq 2$ and

$$\psi_2\psi_{2m} = \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2$$

for $m \geq 3$. Then ψ_{2m} is a polynomial for all m. Furthermore, if we define

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$$
$$4y\omega_m = \psi_{m-1}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2.$$

then ω_m is always a polynomial as well, and

i. Treated as polynomials over x,

$$\phi_m(x) = x^{m^2} + \dots$$
$$\psi_m(x)^2 = m^2x^{m^2-1} + \dots$$

where ellipses represent lower order terms.

ii. For any point $P \in E$, we have

$$[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right).$$

Corollary.

i. The multiplication-by-m map has degree m^2.

ii. Over a field of characteristic p, $[m]$ is separable if and only if $p \nmid m$.

iii. $[m] : E \to E$ is surjective.

Proof. i. We first prove, in the notation of the proposition, that ϕ_m and ψ_m^2 are relatively prime. Assume that they have some common zero x, and let $P \in E$ with $P = (x, y)$. Then $\psi_m(P)^2 = 0$, so $[m]P = O$. Furthermore, by the induction formulas,

$$0 = \phi_m(x) = x\psi_m^2(x) - \psi_{m+1}\psi_{m-1} = -\psi_{m+1}\psi_{m-1},$$

meaning that either ψ_{m+1} or ψ_{m-1} has x as a root. This in turn would mean that either $[m+1]P = O$ or $[m-1]P = O$, and in these cases we could add or subtract $[m]P = O$ to show that $P = O$. This contradicts our choice of x, so the polynomials are relatively prime. Now, since $\deg \phi_m = m^2$ by the proposition, and ϕ_m and ψ_m^2 are relatively prime, it is clear from the definition of morphism degree that $\deg[m] = m^2$.

ii. For separability, notice that if $p \nmid m$, then by the proposition the leading term of $\phi_m(x)$ is nonzero, so by considering the degrees of ψ_m^2 and ϕ_m we see that $\left(\frac{\phi_m}{\psi_m^2}\right)'$ is nonzero. Therefore, by the definitions one easily finds that the map is separable. If instead, $p \mid m$, then the leading coefficient of ψ_m^2 is 0, so ψ has degree smaller than $m^2 - 1$. Thus the kernel of ψ_m^2 has order less than $m^2 - 1$, meaning the kernel of $[m]$ is smaller than its degree m^2. By *Theorem 5(i)*, the map is inseparable.

iii. We first show that, for any point $(a, b) \in E$, we there is some $(a', b') \in E$ such that $[m](a', b')$ has a as its x-coordinate. By the proposition, this is the same as finding a solution to the polynomial equation $\phi_m(x) = a\psi_m(x)$ and then ensuring that, plugging in a for x in our standard equation for elliptic curves, we can extract some solution in y, which we will call b'. Moving to an algebraic closure $\overline{K}$ ensures both the former and the latter. Now there are at most two possible y-values for b, since the elliptic curve equation is a second degree polynomial in y. We have shown that at least one of these will have a

point P in its preimage. However, the other point, having the same value for a, will be $-(a,b)$. Therefore $[m]$ will map $-P$ to the other point, and we are done.

QED

Example. *Set $q = p^r$. Then, let E be an elliptic curve given by the equation*

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$$

and let E^q be the elliptic curve given by the equation

$$y^2 + a_1^qxy + a_2^qy = x^3 + a_3^qx^2 + a_4^qx + a_5^q,$$

with $a_1, \ldots, a_5 \in \mathbb{F}_q$. Then we see that if $(x,y) \in E$, then $(x^q, y^q) \in E^q$. Hence the map sending $(x,y) \mapsto (x^q, y^q)$ and $O \mapsto O$ is a morphism of curves. Additionally, since the group law is given by rational functions in x and y, and exponentiation by q distributes over addition and multiplication in $\mathbb{F}_q$, it is clear that it is an isogeny. This validates the following definition:

Definition. *The isogeny described above is known as the q^{th}-power* Frobenius morphism.

Lemma. *Let E be an elliptic curve over K and t be a uniformizer at $P \in E$. Then $K(E)/K(t)$ is a separable extension.*

Proof. The characteristic 0 case is trivial, so assume $\mathrm{char}(K) = p$. For $x \in K(E)$, we must show that x is separable over $K(t)$. Let the minimal polynomial for x over this field be $\sum a_{ij}t^iX^j$, where $a_{ij} \in K$ for all i,j. We need to show that the derivative of this polynomial with respect to X is nonzero i.e. there is some $a_{ij} \neq 0$ with $j \not\equiv p \pmod p$. To produce a contradiction, suppose that this polynomial is of the form $\Phi(t, X^p)$. Then, since K is assumed perfect, we may write $a_{ij} = b_{ij}^p$ for some b_{ij} in K for all i,j. Since we are in characteristic p, letting $i = i'p + k$ then gives

$$\Phi(t, X^p) = \sum_{ij} a_{ij}t^iX^{pj} = \sum_{k=0}^{p-1} \left(\sum_{ij} b_{ij}t^{i'}X \right)^p t^k = \sum_{k=0}^{p-1} \phi_k(t,X)^p t^k,$$

where ϕ_k is defined in the obvious manner. Now

$$\mathrm{ord}_P(\phi_k(t,X)^pt^k) = p \cdot \mathrm{ord}(\phi_k(t,X)) + k \equiv k \pmod p,$$

so each term in this sum vanishes to distinct order at P. Therefore, since the entire sum vanishes at $x = X$, the basic theory of discrete valuation rings implies that $\phi_1(t,x) = \cdots = \phi_{p-1}(t,x) = 0$. Since at least one of these polynomials was assumed nonzero, this contradicts the minimality of Φ. QED

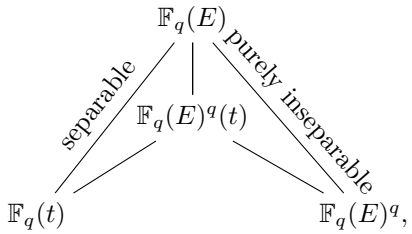
Theorem 6. *If $\phi : E \to E^q$ is the Frobenius morphism, then $\phi^*(\mathbb{F}_q(E^q)) = \mathbb{F}_q(E)^q$, so ϕ is purely inseparable and $\deg \phi = q$.*

Proof. Let $\frac{f}{q} \in \mathbb{F}_q(E)$. Then,

$$\phi^* \left(\frac{f}{g} \right) = \frac{f(x^q, y^q)}{g(x^q, y^q)} = \frac{(f(x,y))^q}{(g(x,y))^q} \in \mathbb{F}_p(E)^q,$$

and since all the elements of $\mathbb{F}_q(E)^q$ can by definition be written as such, the reverse inclusion is shown as well. This gives the first statement, which immediately yields

the pure inseparability of the extension. To prove that $\deg \phi = q$, let $P \in \mathbb{F}_p(E)$ and let t be a uniformizer at P. Using the lemma, we then have



and since intermediate extensions of separable or purely inseparable extensions are, respectively, separable or purely inseparable, we must have $\mathbb{F}_q(E) = \mathbb{F}_q(E)^q(t)$. Therefore the degree of ϕ is $[\mathbb{F}_q(E)^q(t) : \mathbb{F}_q(E)^q]$. Clearly $t^q \in \mathbb{F}_q(E)^q$, so by consideration of minimal polynomials we need only show that nothing dividing t^q is in $\mathbb{F}_q(E)^q$. This amounts to showing that $t^{\frac{q}{p}} \notin \mathbb{F}_q(E)^q$. Assume this were the case. Then $t^{\frac{q}{p}} = f^q$ for some $f \in \mathbb{F}_q(E)$, implying

$$\frac{q}{p} = \mathrm{ord}_P(t^{\frac{q}{p}}) = \mathrm{ord}_P(f^q) = q\mathrm{ord}_P(f).$$

This is a contradiction, since $\mathrm{ord}_P(f)$ must be an integer. QED

To complete this section, we introduce a kind of inverse to isogenies that will prove critical to our later calculations.

Definition. *Let $\phi : E_1 \to E_2$ be an isogeny, let $\phi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)$ be the map ϕ induces by Theorem 2, and let $\sigma_i : \mathrm{Pic}^0(E_i) \to E_i$ be the isomorphisms given by Theorem 4(ii) for $i = 1, 2$. The* dual isogeny *$\hat{\phi}$ of ϕ is the composition $\sigma_1 \circ \phi^* \circ \sigma_2^{-1} : E_2 \to E_1$, illustrated by the following diagram:*

$$\begin{array}{ccc} \mathrm{Pic}^0(E_2) & \xrightarrow{\phi^*} & \mathrm{Pic}^0(E_1) \\ {\scriptstyle\sigma_2}\downarrow & & \downarrow{\scriptstyle\sigma_1} \\ E_2 & \xrightarrow{\hat{\phi}} & E_1 \end{array}.$$

At first there are several strange aspects to this definition. For instance, though it is clear that, as a composition of homomorphisms, $\hat{\phi}$ is a homomorphism, it is not at all clear that it is a morphism. It turns out that this is indeed the case, and that calling it an isogeny is not a misnomer. However, for our purposes, we will not need this fact. One might also wonder why it is "dual" to ϕ. This relationship is elucidated by another theorem:

Theorem 7. *Let $\phi : E_1 \to E_2$ be an isogeny. Then $\hat{\phi} \circ \phi = [\deg \phi]$.*

Proof. The proof is a straightforward calculation. Let $P \in E_1$, and put $Q = \phi(P)$. Then

$$\begin{aligned}\hat{\phi}(Q) &= \sigma_1 \circ \ \phi^* \circ \ \sigma_2^{-1}(Q) = \sigma_1(\phi^*((Q) - (O))) \\ &= \sigma_1 \left(\sum_{P \in \phi^{-1}(Q)} e_\phi(P) - \sum_{Q \in E[m[} e_\phi(T) \right) \\ &= \sum_{P \in \phi^{-1}(Q)} [e_\phi(P)]P - \sum_{X \in \phi^{-1}(O)} [e_\phi(X)]X \\ &= [\deg_i \phi] \left(\sum_{P \in \phi^{-1}(Q)} P - \sum_{X \in \phi^{-1}(O)} X \right),\end{aligned}$$

where the final equality follows by consideration of *Theorem 4(i)* and the corollary to *Theorem 4*. To understand the sum in parentheses, consider *Theorem 5(i)*. There are precisely $\deg_s(\phi)$ elements in both $\phi^{-1}(Q)$ and $\phi^{-1}(O)$, and clearly $P + X$ is unique as P remains constant and X varies within the set $\phi^{-1}(O)$. But every such $P + X$ is also in $\phi^{-1}(Q)$, which has the same size as $\phi^{-1}(X)$. This implies that, given a constant $P \in \phi^{-1}(Q)$, we can match every element of $\phi^{-1}(Q)$ with exactly one element of $\phi^{-1}(O)$ so that, every time, their sum is P. Rearranging the elements in our sum accordingly shows that

$$\hat{\phi} \circ \phi(P) = \hat{\phi}(Q) = [\deg_i \phi][\deg_s \phi]P = [\deg \phi]P.$$

Since P was chosen arbitrarily, we are done. QED

4. The l-adic Weil Pairing

Definition. *By $E[m]$, we denote the set of all $P \in E$ such that $[m]P = O$.*

Theorem 8. *Let E be an elliptic curve over K with $char(K) = p$. Then*

i. If $p = 0$ or $p \nmid m$, then $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
ii. If $p \neq 0$, then for all $e \geq 0$, either $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$ or $E[p^e]$ is trivial.

Proof. Notice first that $E[m]$ is the kernel of $[m]$.

i. By the corollary to *Proposition 4*, the multiplication-by-m map in this case is separable of degree m^2, so by *Theorem 5*, $|E[m]| = m^2$. Of course, the same holds for every divisor d of m. We now proceed by a basic group theoretic argument:

   By the structure theorem for finitely generated abelian groups, we have the decomposition

   $$E[m] \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$$

   for some $n_1, \ldots, n_k \in \mathbb{N}$, where $n_1 \mid \ldots \mid n_k \mid m$. By this decomposition, for every $P \in E[m]$, we have $[n_k]P = O$. This implies that $E[m] = E[n_k]$, and taking orders, we have $n_k^2 = m^2$, which shows that $n_k = m$. Continuing, since $E[n_{k-1}] \subseteq E[m]$, the elements of $E[n_{k-1}]$ are precisely those elements of $E[m]$ that vanish upon being multiplied by n_{k-1}. Note that in $\mathbb{Z}/m\mathbb{Z}$, there are n_{k-1} elements of order dividing n_{k-1}, and of course every element in each of the other cyclic groups in this product vanishes when multiplied by n_{k-1}. Therefore we have

   $$n_{k-1}^2 = |E[n_{k-1}]| = n_1 \cdot \ldots \cdot n_{k-1} \cdot n_{k-1},$$

so, immediately, $n_1 = \cdots = n_{k-2} = 1$. But then $E[m] \cong \mathbb{Z}/n_{k-1}\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Finally, taking orders gives $m^2 = n_{k-1}m$, so $n_{k-1} = m$, completing the proof.

ii. We first consider the case $e = 1$. Because, by the corollary to *Proposition 4*, the multiplication-by-p map is inseparable, *Theorem 5* tells us that

$$E[p] = \ker[p] = \deg_s[p] < \deg[p] = p^2.$$

But the separable degree of the map certainly divides the total degree, so that $E[p] \mid p^2$. This proves that $|E[p]|$ has order either 1 or p. In the former case it is clear that $E[p^e]$ is trivial for all e. In the latter case, let P be a generator for $E[p]$. Since the multiplication-by-p map is surjective by the corollary to *Proposition 4*, let $P' \in E$ such that $[p]P' = P$. Then clearly P' generates the cyclic group $\mathbb{Z}/p^2\mathbb{Z}$. Assume that there is some element Q of $E[p^2]$ such that $Q \neq [n]P$ for any n. Then $[p]Q$ would be in $E[p]$, and would generate additional group elements outside the structure we have observed for $E[p]$, a contradiction. Therefore $E[p^2] = \langle P' \rangle \cong \mathbb{Z}/p^2\mathbb{Z}$. Continuing inductively in this manner gives proves *(ii)*.

QED

The theorem above immediately motivates an analogue to the construction of the p-adic integers:

Definition. *Let p be a prime number and E an elliptic curve. The* p-adic Tate module *over E is the inverse limit*

$$T_p(E) = \varprojlim_n E[p^n]$$

with respect to the maps $E[p^{n+1}] \xrightarrow{[p]} E[p^n]$.

Because $E[p^n]$ is a $\mathbb{Z}/p^n\mathbb{Z}$-module, we see that T_p is a $\mathbb{Z}_p$-module, and *Theorem 8* immediately provides its structure:

Corollary. *Let E be an elliptic curve over a field of characteristic p. As $\mathbb{Z}_m$-modules,*

i. If $p \neq m$, then $T_m(E) \cong \mathbb{Z}_m \times \mathbb{Z}_m$.
ii. If $p \neq 0$, then for all $e \geq 0$, either $T_p(E) \cong \mathbb{Z}_p$ or T_p is trivial.

The Tate module will prove integral to our understanding of isogenies, and, as we will see, to our objective of counting the number of points on E in a given finite field. This is because any isogeny $\phi : E_1 \to E_2$ induces a map $T_p(E_1) \to T_p(E_2)$, since clearly $E_1[p^n]$ maps to $E_2[p^n]$ for all positive integers n, and the algebraic structure of this map can be leveraged to analyze ϕ.

Another important tool in understanding isogenies, and in fact the group structure of an elliptic curve in general, is the Weil pairing. To construct it, let E be an elliptic curve over field of characteristic p, and if $p > 0$, let $m \geq 2$ be an integer such that $p \nmid m$. Consider a function $f \in \overline{K}(E)$ satisfying

$$\operatorname{div}(f) = m(P) - m(O),$$

where $P \in E[m]$. Such a function exists by the corollary to *Theorem 4*. Similarly, if $P' \in E[m^2]$ with $[m]P' = P$, then a function $g \in \overline{K}(E)$ such that

$$\operatorname{div}(g) = \sum_{Q \in E[m]} (P' + Q) - (Q)$$

exists by the same corollary together with *Theorem 8*. Now clearly $f \circ [m]$ has the same divisor as g^m (whose divisor is $m \cdot \operatorname{div}(g)$). Then $\operatorname{div}\left(\frac{f\circ[m]}{g^m}\right) = 0$, and *Proposition 2* then shows that $f \circ [m]$ is equal to g^m up to a scalar. So, redefining f appropriately, we may now assume that $f \circ [m] = g^m$.

Now let $Q \in E[m]$. Then, for all $X \in E$, we have

$$g(X+Q)^m = f([m]X + [m]Q) = f \circ [m](X) = g(X)^m.$$

This shows that, if we keep Q constant, then regardless of our choice of X, the function $\frac{g(X+Q)}{g(X)}$ is an m^{th} root of unity. However, this rational function is continuous, so it either takes on an infinite number of values or is constant. Having eliminated the former, we conclude that it is constant regardless of X, and depends only on Q and our choice of P. This finally gives us the desired definition.

Definition. *The* Weil e_m-pairing *is a map* $e_m : E[m] \times E[m] \to \boldsymbol{\mu}_m$ *defined by*

$$e_m(Q,P) = \frac{g(X+Q)}{g(X)},$$

where g *and* m *are defined as above,* $X \in E$ *is any point such that this quotient is well-defined and nonzero, and* $\boldsymbol{\mu}_m$ *is the group of* m^{th} *roots of unity.*

Theorem 9. *Let* $P, Q \in E[m]$. *The Weil* e_m*-pairing is*

i. bilinear:

$$e_m(Q_1+Q_2,P) = e_m(Q_1,P)e_m(Q_2,P)$$
$$e_m(Q,P_1+P_2) = e_m(Q,P_1)e_m(Q,P_2),$$

ii. alternating:

$$e_m(P,P) = 1 \text{ and } e_m(Q,P) = e_m(P,Q)^{-1},$$

iii. compatible: $e_{mn}(S,P) = e_m([n]S,P)$ *for all* $S \in E[mn]$,

iv. nondegenerate: If $e_m(Q,P) = 1$ *for all* $Q \in E[m]$, *then* $P = O$.

Proof.

i. First, for linearity in the first factor, we quickly see that

$$e_m(Q_1+Q_2,P) = \frac{g(X+Q_1+Q_2)}{g(X)} = \frac{g((X+Q_1)+Q_2)}{g(X+Q_1)} \cdot \frac{g(X+Q_1)}{g(X)} = e_m(Q_2,P)e_m(Q_1,P).$$

For the second factor, let $f_1, f_2, f_3, g_1, g_2, g_3$ be the analogous functions to f and g for the points P_1, P_2, and $P_3 = P_1 + P_2$, respectively. Then, using the corollary to *Theorem 4*, let $h \in \overline{K}(E)$ with $\operatorname{div}(h) = (P_3) - (P_1) - (P_2) + (O)$. Then

$$\operatorname{div}\left(\frac{f_3}{f_1 f_2 h^m}\right) = 0,$$

so *Proposition 2* gives $f_3 = c f_1 f_2 h^m$ for some $c \in \overline{K}^*$. Therefore

$$g_3 = (f_3 \circ [m])^{\frac{1}{m}} = (c f_1 f_2 h^m \circ [m])^{\frac{1}{m}} = (c g_1^m \cdot g_2^m \cdot (h^m \circ [m]))^{\frac{1}{m}} = c^{\frac{1}{m}} g_1 \cdot g_2 \cdot (h \circ [m]).$$

Hence

$$\begin{aligned} e_m(Q, P_1 + P_2) &= \frac{g_3(X+Q)}{g_3(X)} \\ &= \frac{c^{\frac{1}{m}} g_1(X+Q)g_2(X+Q)h([m]X+[m]Q)}{c^{\frac{1}{m}} g_1(X)g_2(X)h([m]X)} \\ &= \frac{g_1(X+Q)g_2(X+Q)h([m]X)}{g_1(X)g_2(X)h([m]X)} \\ &= \frac{g_1(X+Q)g_2(X+Q)}{g_1(X)g_2(X)} = e_m(Q, P_1)e_m(Q, P_2), \end{aligned}$$

where of course we choose X so that $h([m]X)$ is nonzero and well-defined.

ii. We use a symmetry argument to prove the first statement. As in *Theorem 5*, let τ_P be the morphism $X \mapsto X + P$. Then

$$\operatorname{div}\left(\prod_{i=0}^{m-1} f \circ \tau_{[i]P}\right) = \sum_{i=0}^{m-1} \operatorname{div}(f \circ \tau_{[i]P}) = \sum_{i=0}^{m-1} m([1-i]P) - m([-i]T) = 0,$$

so by *Proposition 2*, this product is a constant map - say the constant c. Then, if we choose $P' \in E$ with $[m]P'$, we get

$$\left(\prod_{i=0}^{m-1} g \circ \tau_{[i]P'}\right)^m = \prod_{i=0}^{m-1} f \circ [m] \circ \tau_{[i]P'} = \prod_{i=0}^{m-1} f \circ \tau_{[i]P} \circ [m] = c \circ [m] = c.$$

Therefore, since its m^{th} power is constant, the product in the parentheses is constant as well. In particular, for any $X \in E$, the product has the same value at X and $X + P'$, so

$$\prod_{i=0}^{m-1} g(X + [i]P') = \prod_{i=0}^{m-1} g(X + [i+1]P'),$$

and dividing finally yields $g(X) = g(X + [m]P') = g(X + P)$. Thus

$$e_m(P, P) = \frac{g(X+P)}{g(P)} = 1.$$

This results in the second fact by the calculation

$$\begin{aligned} 1 &= e_m(Q+P, Q+P) \\ &= e_m(Q, Q)e_m(Q, P)e_m(P, Q)e_m(P, P) \\ &= e_m(Q, P)e_m(P, Q). \end{aligned}$$

iii. Notice that

$$\operatorname{div}(f^n) = n \cdot \operatorname{div}(f) = mn(P) - mn(O)$$

and

$$(g \circ [n])^{mn} = (g^m \circ [n])^n = (f \circ [m] \circ [n])^n = f^n \circ [mn].$$

Therefore the functions f^n and $g \circ [n]$ have the requisite properties to define the Weil e_{mn}-pairing when the second entry is P. Thus

$$e_{mn} = \frac{g \circ [n](X+S)}{g \circ [n](X)} = \frac{g([n]X + [n]S)}{g([n]X)} = e_m([n]S, P).$$

iv. To say that $e_m(Q,P)=1$ means that $g(X+Q)=g(X)$ i.e. g is invariant under τ_Q^*. If this is true for all $Q\in E[m]$, then the isomorphism given in *Theorem 5(ii)* shows that g is contained in $[m]^*\overline{K}(E)$, so we may write $g=h\circ[m]$ for some $h\in\overline{K}(E)$. Hence

$$(h\circ[m])^m=g^m=f\circ[m],$$

and taking right inverses (which can be done since $[m]$ is surjective by the corollary to *Proposition 4*) gives $f=h^m$. We now compute

$$m\mathrm{div}(h)=\mathrm{div}(h^m)=\mathrm{div}(f)=m(P)-m(O).$$

This shows that $\mathrm{div}(h)=(P)-(O)$, and the lemma for *Theorem 4* provides the desired result.

QED

Theorem 10. *Let $\phi:E_1\to E_2$ be an isogeny. Then, if $Q\in E_1[m]$ and $P\in E_2[m]$, we have*

$$e_m(Q,\hat{\phi}(P))=e_m(\phi(Q),P).$$

Proof. Let f,g be the usual functions corresponding to the Weil e_m-pairing over E_2 if P is the second entry. Then, it is clear from the definition of $\hat{\phi}$ that

$$\phi^*((P)-(O))=\phi^*\circ\sigma_2^{-1}(P)=\sigma_1^{-1}\circ\hat{\phi}(P)=(\hat{\phi}(P))-(O)$$

within $\mathrm{Pic}^0(E_1)$. Since we are working modulo principal divisors, this means that the difference between the left side and right side of this equation is a principal divisor. In other words, we really have

$$\phi^*((P)-(O))=(\hat{\phi}(P))-(O)+\mathrm{div}(h)$$

for some $h\in\overline{K}(E_1)$. Then, we observe that

$$\begin{aligned}\mathrm{div}\left(\frac{f\circ\phi}{h^m}\right)&=\mathrm{div}(\phi^*f)-m\cdot\mathrm{div}(h)=\phi^*\mathrm{div}(f)-m\cdot\mathrm{div}(h)\\&=\phi^*(m((P)-(O)))-m\cdot\mathrm{div}(h)=m\cdot\phi^*((P)-(O))-m\cdot\mathrm{div}(h)\\&=m(\hat{\phi}(P))-m(O)+m\cdot\mathrm{div}(h)-m\cdot\mathrm{div}(h)=m(\hat{\phi}(P))-m(O),\end{aligned}$$

where the second equality follows from the lemma to *Theorem 2*, and that

$$\left(\frac{g\circ\phi}{h\circ[m]}\right)^m=\frac{f\circ[m]\circ\phi}{(h\circ[m])^m}=\left(\frac{f\circ\phi}{h^m}\right)\circ[m].$$

These are the necessary properties which indicate that the functions $\frac{f\circ\phi}{h^m}$ and $\frac{g\circ\phi}{h\circ[m]}$ define the Weil e_m-pairing when the second entry is $\hat{\phi}(P)$. We may now simply evaluate

$$e_m(Q,\hat{\phi}(P))=\frac{\frac{g\circ\phi(X+Q)}{h\circ[m](X+Q)}}{\frac{g\circ\phi(X)}{h\circ[m](X)}}=\frac{g(\phi(X)+\phi(Q))}{g(\phi(X))}\cdot\frac{h([m]X)}{h([m]X+[m]Q)}=e_m(\phi(Q),P),$$

remembering that $Q\in E_1[m]$. QED

The juxtaposition of our introduction to the Weil pairing just after the Tate module is not coincidence. We wish to merge all Weil e_{p^n}-pairings into a pairing $T_p(E)\times T_p(E)\to T_p(\boldsymbol{\mu})$, where $T_p(\boldsymbol{\mu})$ is the inverse limit

$$\lim_{\underset{n}{\leftarrow}}\boldsymbol{\mu}_{p^n}$$

with respect to the maps $\boldsymbol{\mu}^{p^{n+1}} \xrightarrow{\zeta \mapsto \zeta^p} \boldsymbol{\mu}_{p^n}$, with all of the desirable properties of the Weil pairing. To know that the Weil pairing is compatible with this inverse limit, we need to show that the image of each $e_{p^{n+1}}$-pairing upon exponentiation by p is the element of $\boldsymbol{\mu}_{p^n}$ corresponding to pairing after multiplication by p. This is summarized in the equation

$$e_{p^{n+1}}(Q,P)^p = e_{p^{n+1}}(Q,[p]P) = e_{p^n}([p]Q,[p]P),$$

where the first equality follows from the bilinearity of the Weil pairing, and the second follows from its compatibility. We have now justified the desired definition:

Definition. *The* l-adic Weil Pairing *is the map* $e : T_p(E) \times T_p(E) \to T_p(\boldsymbol{\mu})$ *given above.*

It is easily apparent that the l-adic Weil Pairing inherits all of the nice properties of the Weil e_m-pairing proven in *Theorem 9*. As for *Theorem 10*, recall that for any isogeny $\phi : E_1 \to E_2$ there is an associated map $T_p(E_1) \to T_p(E_2)$. Labeling this map ϕ_p, it's plain to see that the property of the Weil pairing exhibited by the theorem carries over through inverse limits i.e. $e(Q, \hat{\phi}_p(P)) = e(\phi_p(Q), P)$, where the first pairing is over E_1 and the second is over E_2.

5. Counting Points on E over $\mathbb{F}_q$

In this section we apply the tools of the previous section to prove a theorem which counts the number of points on an elliptic curve with coordinates in a given finite field.

Lemma 1. *Let* $\phi : E_1 \to E_2$ *be an isogeny, and let* ϕ_p *be the map* $T_p(E_1) \to T_p(E_2)$ *induced by* ϕ *on the* p*-adic Tate module over* E_1*. Then* $\det(\phi_p) = \deg \phi$ *and*

$$tr(\phi_p) = 1 + \deg(\phi) - \deg(1 - \phi).$$

Before providing a proof, we first explain what is meant by $\det(\phi_p)$ and $\mathrm{tr}(\phi_p)$. Because ϕ_p maps $T_p(E_1) \cong \mathbb{Z}_p \times \mathbb{Z}_p$ onto $T_p(E_2) \cong \mathbb{Z}_p \times \mathbb{Z}_p$, we can represent ϕ_p by a matrix $A \in \mathrm{M}_2(\mathbb{Z}_p)$. Then, since both trace and determinant are invariant with respect to a change of basis, we see that $\mathrm{tr}(\phi_p) := \mathrm{tr}A$ and $\det(\phi_p) := \det A$ are well-defined and depend only on the map ϕ.

Proof. Let $\{v_1, v_2\}$ be a $\mathbb{Z}_p$-basis for $T_p(E_1) \cong \mathbb{Z}_p \times \mathbb{Z}_p \cong T_p(E_2)$. We will let the matrix for ϕ_p relative to this basis be

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Now the properties of the p-adic Weil pairing indicate

$$\begin{aligned} e(v_1,v_2)^{\deg\phi} &= e([\deg\phi]v_1, v_2) = e(\hat{\phi}_p\phi_p v_1, v_2) = e(\phi_p v_1, \phi_p v_2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) = e(v_1,v_2)^{ad-bc} = e(v_1,v_2)^{\det(\phi_p)}, \end{aligned}$$

where almost all equalities follow from the properties of the p-adic Weil pairing we've proven, except for the second, which follows from *Theorem 7*. Another way of stating this is that $e(v_1,v_2)^{\deg\phi - \det(\phi_p)} = 1$. Now, since v_2 is nonzero and v_1 was chosen arbitrarily, we may apply the nondegeneracy of the l-adic to conclude

that $\deg\phi - \det(\phi_p) = 0$, so the first statement is established. The trace equation is then a well-known property of 2×2 matrices:

$$\mathrm{tr}A = 1 + \det A - \det(1-A).$$

QED

Lemma 2. *Let E be an elliptic curve over the field $\mathbb{F}_{q^n}$, and let $\phi : E \to E$ be the q^{nth}-power Frobenius morphism. Then $1-\phi$ is separable.*

Proof. We first give an explicit equation for the map $1-\phi$. If $P=(x,y)\in E$, then

$$\begin{aligned}(1-\phi)(P) = (x,y) - (x^{q^n}, y^{q^n}) &= (x,y) + (x^{q^n}, -y^{q^n} - a_1x^{q^n} - a_3)\\ &= \left(\frac{y^{2q^n} - x^{3q^n} + a_1(xy)^{q^n} - x^{2q^n+1} + \dots}{x^{2q^n} - 2x^{q^n+1} + x^2}, y'\right),\end{aligned}$$

where ellipses are a placeholder for terms with a lower order pole at O, and y' represents the function for the y-coordinate. Recall that, by construction, x has a second order pole at O and y has a third order pole there. After inspection one sees that the coefficients in the polynomial in our numerator with the highest order pole at O are y^{2q^n} and x^{3q^n}. However, if we combine these terms we see that

$$\begin{aligned}y^{2q^n} - x^{3q^n} = (y^2 - x^3)^{q^n} &= (a_2x^2 + a_4x + a_5 - a_1xy - a_3y)^{q^n}\\ &= a_2x^{2q^n} + a_4x^{q^n} + a_5 - a_1(xy)^{q^n} - a_3y^{q^n}.\end{aligned}$$

If we combine this with the rest of the polynomial, we also find that the next highest-pole term, $(xy)^{q^n}$, vanishes. This leaves x^{2q^n+1} with the highest order pole. Additionally, clearly in the denominator the monomial with the highest order pole at O is x^{2q^n}. Hence, if we label this coordinate as $x'\in\mathbb{F}_q^n(E)$, we have

$$\mathrm{ord}_O(x') = \mathrm{ord}_O(x^{2q^n+1}) - \mathrm{ord}_O(x^{2q^n}) = -4q^n - 2 - (-4q^n) = -2.$$

As for the y coordinate function y' of this map, by the group law we have

$$\begin{aligned}y' &= -x'(\lambda + a_1) - \nu + a_3\\ &= -x'\left(\left(\frac{y + y^{q^n} + a_1x^{q^n} + a_3}{x - x^{q^n}}\right) + a_1\right) - \frac{yx^{q^n} + xy^{q^n} + a_1x^{q^n+1} + a_3x}{x^{q^n} - x} + a_3\\ &= \frac{2y^{2q^n+1} + \dots}{x^3 - 3x^{q^n+2} + 3x^{2q^n+1} - x^{3q^n}},\end{aligned}$$

where ellipses represent monomials with lower-order poles at O. This means that $2y^{2q^n+1}$ has the pole of highest order, while this title goes to x^{3q^n} in the denominator. Therefore

$$\mathrm{ord}_O(y') = \mathrm{ord}_O(2y^{2q^n+1}) - \mathrm{ord}_O(x^{3q^n}) = -6q^n - 3 - (-6q^n) = -3.$$

Finally, because $\frac{x}{y}$ has divisor $\mathrm{div}(x) - \mathrm{div}(y) = -2(O) - (-3(O)) = (O)$, it is a uniformizer at O. We now use this uniformizer to directly compute

$$e_\phi(O) = \mathrm{ord}_O\left((1-\phi)^*\left(\frac{x}{y}\right)\right) = \mathrm{ord}_O\left(\frac{x'}{y'}\right) = \mathrm{ord}_O(x') - \mathrm{ord}_O(y') = -2 - (-3) = 1.$$

The lemma then follows from *Theorem 5(i).* QED

Theorem 11. *Let E be an elliptic curve over $\mathbb{F}_{q^n}$, and let $\phi : E \to E$ be the q^{nth} power Frobenius Automorphism. If we set*

$$a = q + 1 - |E(\mathbb{F}_q)|$$

and let α, β be the roots of the polynomial $T^2 - aT + q$, then

$$|E(\mathbb{F}_{q^n})| = q^n + 1 - \alpha^n - \beta^n.$$

Furthermore, α, β are conjugate with $|\alpha| = |\beta| = \sqrt{q}$.

Proof. Since, in any field of characteristic p, the elements belonging to $\mathbb{F}_{q^n}$ are precisely those invariant under the q^{nth}-power Frobenius automorphism, we can apply this fact to each coordinate of a point in E to find that $E(\mathbb{F}_{q^n}) = \ker(1-\phi)$. By *Lemma 2*, the map $1 - \phi$ is separable, so *Theorem 5(i)* implies that

$$|E(\mathbb{F}_{q^n})| = |(1-\phi)^{-1}(O)| = \deg(1-\phi).$$

Combining this with *Lemma 1* then gives

$$\operatorname{tr}(\phi_p) = 1 + \deg\phi - \deg(1-\phi) = 1 + q^n - |E(\mathbb{F}_{q^n})| = a.$$

Now, as with any 2×2 matrix, the characteristic polynomial of ϕ_p is

$$\det(T - \phi_p) = T^2 - \operatorname{tr}(\phi_p) + \det(\phi_p) = T^2 - \operatorname{tr}(\phi_p) + \deg\phi = T^2 - aT + q^n,$$

where the first equality follows from *Lemma 1*. In the case $n = 1$, this reveals α, β as eigenvalues of ϕ_p. In the general case, since eigenvalues are raised to powers as their matrix is, the eigenvalues (and thus the roots of the above polynomial) are α^n and β^n. Finally, we again use *Lemma 1* to determine

$$|E(\mathbb{F}_{q^n})| = \deg(1-\phi) = \det(1-\phi_p) = 1 - \alpha^n - \beta^n + q^n,$$

where the last equality comes from the equation for $\det(T - \phi_p)$ given above applied to the case $T = 1$.

For the second statement, which allows us to calculate α and β in practice, we need to show that, for $n = 1$, the characteristic polynomial of ϕ_p cannot have two distinct real roots. Since it's a quadratic, that amounts to showing that the polynomial is nonnegative for any real T. By continuity, it suffices to prove this for rational T. Suppose $T = \frac{m}{n} \in \mathbb{Q}$. Then

$$\det\left(\frac{m}{n} - \phi_p\right) = \frac{\det(m - n\phi_p)}{n^2} = \frac{\deg(m - n\phi)}{n^2} \geq 0,$$

again by *Lemma 1*. Thus α, β are conjugate, and have the same magnitude, and because

$$\alpha\beta = \det(\phi_p) = \deg\phi = q,$$

that magnitude is $\sqrt{q}$. QED

Naturally, the value a is called the trace of Frobenius.

Acknowledgements

I sincerely thank REU director Peter May for his hard work every year to lead undergraduates to follow their passion for mathematics, and being incredibly patient with my work. Moreover, my mentor Karl Schaefer was instrumental in helping learn the material with a caring, forgiving, and enthusiastic approach, for which I'm more appreciative than I can express.

References

[1] Silverman, Joseph H. The Arithmetic of Elliptic Curves. 2nd ed. Graduate Texts in Mathematics. New York: Springer, 1986.

[2] Silverman, Joseph H., and John T. Tate. Rational Points on Elliptic Curves. Undergraduate Texts in Mathematics. New York: Springer-Verlag, 1992.

[3] Hartshorne, Robin. Algebraic Geometry. Graduate Texts in Mathematics. New York, NY: Springer-Verlag, 1977.

[4] Andrew Sutherland, *18.783 Elliptic Curves*, Spring 2015. (Massachusetts Institute of Technology: MIT OpenCouseWare), http://ocw.mit.edu (Accessed December 24, 2016). License: Creative Commons BY-NC-SA