CRD Expository Report 31
An Elementary Introduction to Elliptic Curves

Leonard S. Charlap
David P. Robbins

December 1988

Abstract

In his paper on elliptic curves over finite fields, R. Schoof assumes certain basic material concerning elliptic curves. This material mainly concerns the division polynomials and the "Weil Conjectures for Elliptic Curves". These notes provide elementary self-contained proofs of these results.

Part I – Elliptic Curves over Algebraically Closed Fields

1 Introduction

The goal of these notes is to prove the results used by Schoof in his paper on elliptic curves over finite fields. On the way, we expose most of the basic notions of elliptic curve theory required for further study. It appears to be impossible to find an elementary presentation of this material in the literature. By "elementary", we mean that the exposition requires little beyond undergraduate mathematics. It is still true, however, that our "elementary" proofs may require some mathematical sophistication. Thus you would not have to consult a lot of other books (as in [6]), but you still may have to expend some thought.

We would like to thank our colleagues at IDA for their unrelenting criticism and good advice. In addition, we would like to thank Ann Stehney for her editorial and mathematical suggestions.

Recall that the *characteristic* of a field K is the smallest positive integer p such that $p \cdot 1 = 0$ where by $p \cdot 1$ we mean $1 + 1 + \cdots + 1$, p times. It can be easily seen that if there is such a p, it is always a prime integer (see [4, page 241]). If there is no such positive integer p, we say the characteristic is zero.

Recall that a field K is said to be *algebraically closed* if every polynomial with coefficients in K splits completely into linear factors. Another way of saying this is that every polynomial of degree n (with coefficients in K) has n roots in K, counting multiplicities. The standard example of an algebraically closed field is $\mathbb{C}$, the complex numbers. It is a standard fact (see [2, page 107], for example) that every field has an algebraic closure, *i.e.,* an algebraically closed superfield.

We assume that the **characteristic of our field K is not** 2 and that K **is algebraically closed**.

We will use some standard notation that we record here. $K[X]$ will denote the ring of polynomials in the indeterminate X with coefficients in K while $K(X)$ will denote its field of quotients, namely the field of rational functions in X with coefficients in K. $K[X,Y]$ and $K(X,Y)$ are defined similarly.

2 Elliptic Curves

We give the basic definition.

Definition 2.1 For any $A, B \in K$, we can define an *elliptic curve* E. E is the set of all points $(h,k) \in K \times K$ that satisfy the equation

$$k^2 = h^3 + Ah + B \tag{1}$$

together with an "idealized point" $\mathcal{O}$. For reasons that will become apparent later, $\mathcal{O}$ is called the *identity*. The points of the curve other than the identity are said to be *finite*.

Definition 2.2 If k is a subfield of K, and A and B are in k, we define the *k–rational* points of E to be the points whose coordinates lie in k. We denote the set of these points by $E(k)$.

Definition 2.3 An elliptic curve defined by Equation (1) is called *nonsingular* if the polynomial $X^3 + AX + B$ has (three) distinct roots; otherwise we say it is *singular*.

Exercise 2.4 Define $\Delta(E) = 4A^3 + 27B^2$. $\Delta(E)$ is called the *discriminant* of the equation of the curve. Show that E is nonsingular if and only if $\Delta(E) \neq 0$.

Remarks.

(i) The symbols "x" and "y" will be reserved for the coordinate functions on E defined by $x(a,b) = a$ and $y(a,b) = b$.

(ii) It is sometimes fruitful to think of the identity as being "at infinity." If we use projective coordinates, we can actually make sense of this notion (see [6]). We will abuse the terminology and use the symbol "∞" for both the x and the y coordinates of $\mathcal{O}$.

(iii) Our definition of elliptic curve is slightly different from the usual one which requires elliptic curves to be nonsingular. Since we will have nothing to do with singular curves, we would not worry about this difference.

(iv) In characteristic 2 or 3, an elliptic curve should be defined by a more complicated equation to correspond to the standard definition (see [6, page 325]). In fact, in characteristic 2, our definition of "singular" is not

the right one. Consider a somewhat more general curve defined by an equation $F(X,Y) = 0$ where F is some irreducible polynomial. The usual definition of *singular* is that the curve is singular if there is a point on the curve (*i.e.,* satisfying the above equation) at which both partial derivatives $\partial F/\partial x$ and $\partial F/\partial y$ are zero. In the case of elliptic curves it is easily seen that if the characteristic is not 2, this is equivalent to our definition. This is not the case in characteristic 2, and, in fact, it is easy to see that if we use the definition in terms of partial derivatives, all curves of the form $Y^2 = X^3 + AX + B$ are singular.

In characteristic 3, we will not be considering the most general elliptic curve, but for the class of curves defined by (1) the proofs all work up to Theorem 8.6. We will say no more here about these characteristics.

In these notes, **we will consider only non–singular elliptic curves**.

3 Polynomial and Rational Functions

We would like to think of the elements of $K[X,Y]$ as defining polynomial functions on E, but clearly two elements of $K[X,Y]$ that differ by a multiple of $Y^2 - X^3 - AX - B$ will define the same function on E. If we wanted to be fancy, we could define polynomials on E to be elements of the quotient ring

$$K[X,Y]/(Y^2 - X^3 - AX - B) \quad ,$$

where $(Y^2 - X^3 - AX - B)$ is the ideal generated by $Y^2 - X^3 - AX - B$. Of course, the idea of these notes is *not* to be fancy, so we will adopt a more concrete definition of polynomials on E. The point is that $Y^2 = X^3 + AX + B$ on E, so any time we see a power of Y higher than one, we can use this relation to replace it by an expression in X times a power of Y no greater than one. Notice that if we consider polynomials in the functions x and y, the relation $y^2 = x^3 + Ax + B$ holds automatically. We therefore consider polynomials to be elements of $K[x,y]$, the ring of polynomials in the functions x and y.

Definition 3.1 A *polynomial on* E is an element of $K[x,y]$. We sometimes denote the ring of polynomials on E by $K[E]$.

An important consequence of this definition is that any polynomial f on E can be written $f(x,y) = v(x) + yw(x)$ for two polynomials v and w of one variable. Also note that using this definition, polynomials are automatically functions on E since x and y are.

Definition 3.2 If $f(x,y) = v(x) + yw(x)$ is a polynomial on E, its *conjugate* $\bar{f}$ is the polynomial $\bar{f}(x,y) = v(x) - yw(x)$ and its *norm* is the polynomial $N(f) = f\bar{f}$.

Remark. Without getting too bogged down in foundational considerations, we would like to examine the notion of polynomial a little more carefully. First notice that

$$N(f)(x,y) = v(x)^2 - s(x)w(x)^2 \quad ,$$

where $s(x) = x^3 + Ax + B$, so we can think of $N(f)$ as being a function of only one variable, *i.e.,* a member of $K[x]$. In addition, $N(fg) = N(f)N(g)$. Many of the proofs in this part depend on thinking of $N(f)$ in this way because we know a lot about polynomials of only one variable. For example, we might like to know that the representation of a polynomial as $v(x) + yw(x)$ is unique. Suppose $f(x, y) = v(x) + yw(x)$ were the zero function. Then $N(f)$ would have to be the zero function (since the degree of s is odd, and the degrees of v^2 and w^2 are even, the polynomial w would have to be zero and hence so would the polynomial v). From this we easily see that the representation $v(x) + yw(x)$ is unique. In a similar fashion, we can see that $K[x, y]$ has no zero divisors, and that the usual rules used with polynomials hold here.

Now we would like to define a rational function to be the quotient of two polynomials, but we must exercise some care.

Definition 3.3 A *rational function on* E is an equivalence class of formal quotients of polynomials f/g (with g not identically zero), where we identify f/g with h/k if $fk = gh$ as polynomials on E. It is easily seen that the set of rational functions on E is a field, which we denote by $K(E)$.

The way to see that $fk = gh$ "as polynomials on E" is to write both fk and gh in the canonical form $v(x) + yw(x)$ using the relation $y^2 = x^3 + Ax + B$, and then see if they are equal. While polynomials have values at every finite point of E, rational functions may not have values at all finite points and may have a value at $\mathcal{O}$. Notice that if $r = f/g$ is a rational function, then by multiplying by $\bar{g}/\bar{g}$, we can write $r(x, y) = a(x) + yb(x)$, where now a and b are rational functions of x alone.

Definition 3.4 If r is a rational function on E and P is a finite point in E, we say r is *finite at* P if there exists a representation $r = f/g$ where f and g are polynomials on E and $g(P) \neq 0$. If r is finite at P, we put $r(P) = f(P)/g(P)$, and it is trivial to see that this is well–defined.

Exercise 3.5 Show that the rational functions that are finite at P form a ring (*i.e.,* sums and products of finite polynomials are finite) and, if you know what it is, show this ring is *local.*

It is somewhat more complicated to define the value of a rational function at $\mathcal{O}$, even if it has one there. The usual way (in calculus) to find the value (or limit) of a rational function at infinity is to compare the degrees of the numerator and denominator. In our case the situation is complicated by the existence of two variables, x and y. While it might seem natural to assign degree 1 to x and y, this would not be consistent with our fundamental relation $y^2 = x^3 + Ax + B$. This relation suggests that the degree of y should be $3/2$ the degree of x. Since we do not want to deal with fractional degrees, we will assign degree 3 to y and degree 2 to x. To avoid confusion, we denote the usual degree of a polynomial f in x alone by $\deg_x(f)$.

Definition 3.6 Let $f(x,y) = v(x) + yw(x)$ be a nonzero polynomial on E. Define the *degree of* f by

$$\deg(f) = \max[2 \cdot \deg_x(v), 3 + 2 \cdot \deg_x(w)] \quad . \tag{2}$$

If f happens to be a function of only the variable x then its degree as a function on E is twice its usual degree as a function of x, *i.e.,* with the degree of x equal 1.

Lemma 3.7 *If f is a polynomial on E then*

$$\deg(f) = \deg_x(N(f)) \quad .$$

Proof. If we write $f(x,y) = v(x) + yw(x)$, then $N(f)(x) = v^2(x) - s(x)w^2(x)$, where $s(x) = x^3 + Ax + B$. The lemma then follows from the definition of degree. ∎

In order to see that this is a useful notion of degree, we must check the fundamental property we expect of degrees.

Proposition 3.8 *dg are polynomials on E, then* $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Proof. Using the lemma, we get

$$\begin{aligned} \deg(fg) =& \deg_x(N(fg)) = \deg_x(N(f)N(g)) \\ =& \deg_x(N(f)) + \deg_x(N(g)) = \deg(f) + \deg(g) \quad , \end{aligned}$$

since we certainly know the result for $\deg_x$. ∎

Note that while we cannot talk about the degree of the numerator (or denominator) of a rational function, the difference between the degree of the numerator and the degree of the denominator is well–defined, *i.e.,* if $r = f/g$, r may also equal h/k and $\deg(f)$ may not equal $\deg(h)$. By the above proposition, however, $\deg(f) - \deg(g) = \deg(h) - \deg(k)$ since $fk = gh$. Therefore we can make the following definitions:

Definition 3.9 Suppose $r = f/g$ is a rational function on E. If $\deg(f) < \deg(g)$, we set $r(\mathcal{O}) = 0$. If $\deg(f) > \deg(g)$, we say that r is not finite at $\mathcal{O}$. If $\deg(f) = \deg(g)$, we must distinguish two cases. If $\deg(f)$ is even, then writing f and g in canonical form, they will have as leading terms (terms of highest degree) ax^d and bx^d respectively (for some $a, b \in K$ and integer d). Then we put $r(\mathcal{O}) = a/b$. Similarly if $\deg(f)$ is odd, the leading terms have the form ayx^d and byx^d, and again we put $r(\mathcal{O}) = a/b$.

Remark. It might seem natural to define the *degree* of a rational function $r = f/g$ to be $\deg(f) - \deg(g)$. If we did this, then r would be finite or infinite at $\mathcal{O}$ depending on whether it had negative or positive degree. The disadvantage of this definition is that it disagrees with the usual one used in algebraic geometry. We will avoid this problem by not defining the degree of a rational function at all.

Exercise 3.10 Show that if r and s are rational functions with $r(\mathcal{O})$ and $s(\mathcal{O})$ finite, then $rs(\mathcal{O}) = r(\mathcal{O})s(\mathcal{O})$, and $(r+s)(\mathcal{O}) = r(\mathcal{O}) + s(\mathcal{O})$.

If r is a rational function on E that is not finite at some $P \in E$, we write $r(P) = \infty$ to indicate this.

4 Zeros and Poles

From the material of the last section it is easy to define what a zero or pole of a rational function should be.

Definition 4.1 Let r be a rational function on E. We say that r has a *zero* at $P \in E$ if $r(P) = 0$ and that r has a *pole* at P if $r(P) = \infty$.

What is not so easy to do is to define the multiplicity of a zero or pole.

Example 4.2 Suppose E is given by the equation $Y^2 = X^3 + X$. Then the point $P = (0,0)$ is in E. Since $x = y^2 - x^3$, it appears that the function x ought to have a zero at P whose multiplicity is twice that of the zero of y at P.

Before we prove a theorem that will show us how to define multiplicities, we want to point out three points on our elliptic curve that will cause us no end of difficulty, beginning here. Remember that we have assumed that E was nonsingular, which means that the polynomial $X^3 + AX + B$ has three distinct roots. Let's call them ω_1, ω_2 and ω_3, and use ω to indicate an arbitrary one. Then E contains three points whose y–coordinate is 0, namely $(\omega_1, 0), (\omega_2, 0)$ and $(\omega_3, 0)$. These three points are called the *points of order two* for reasons that will become apparent in Section 6.

Theorem 4.3 *For each point $P \in E$ there is a rational function u, zero at P, with the following property: If r is any rational function not identically zero, then*

$$r = u^d s \tag{3}$$

for some integer d and some rational function s that is finite and nonzero at P. Furthermore, the number d does not depend on the choice of the function u.

Proof. There are three cases. First we do the generic case, *i.e.,* we assume that P is not of order 2 and that P is not $\mathcal{O}$. For $P = (a,b)$, we will show we can take $u(x,y) = x - a$. Suppose r has a zero at P. Then $r = f/g$ with $f(P) = 0$ and $g(P) \neq 0$. If we can decompose $f = u^d s$ as in the above equation, then we can simply divide by g and get the corresponding result for r.

We write $f(x,y) = v(x) + yw(x)$ so $\bar{f}(x,y) = v(x) - yw(x)$. If $\bar{f}(P) = 0$, then since the characteristic is not two and $y(P) = b \neq 0$, we can solve the linear equations

$$\begin{aligned} v(a) + bw(a) &= 0 \\ v(a) - bw(a) &= 0 \quad , \end{aligned}$$

to conclude that $v(a) = w(a) = 0$. Since v and w are polynomials in one variable, we get

$$f(x,y) = (x-a) \cdot s_1(x,y)$$

for some polynomial s_1.

If $\bar{f}(P) \neq 0$, then we can multiply f by $\bar{f}/\bar{f}$ to get

$$f(x,y) = \frac{v^2(x) - s(x)w^2(x)}{\bar{f}(x,y)} \quad ,$$

where $s(x) = x^3 + Ax + B$. Now $f(P) = 0$ and $\bar{f}(P) \neq 0$ implies

$$v^2(x) - s(x) \cdot w^2(x) = 0 \quad \text{for } x = a \quad ,$$

and the polynomial on the left is a polynomial in one variable. Again we conclude that

$$f(x,y) = (x-a) \cdot s_1(x,y) \quad ,$$

where this time s_1 is some rational function that is finite at P. In either case, if $s_1(P) = 0$, we can continue the process. To see that it eventually comes to an end, note that if $f(x,y) = (x-a)^d s_1(x,y)$, then $N(f)(x) = (x-a)^{2d} N(s_1)(x)$. We know that $N(s_1)(x)$ does not have a pole at a so we can see that $2d$ must be less than the degree of $N(f)$ as a function of x alone.

Thus if r has a zero at $P = (a,b)$, we can take $u(x,y) = x - a$. If r has a pole at P, then $1/r$ has a zero at P, and the same u still works (with d negative). If r has neither a zero nor a pole at P, then we can take $d = 0$ and $s = r$, and what u is is immaterial. Thus in the generic case, we can take $u(x,y) = x - a$.

Now we assume that P is a point of order two, say $P = (\omega_1, 0)$. We show that we can take $u(x,y) = y$ in this case. As above, if r has a zero at P, we can assume $r = f/g$ and $f(P) = 0$. Now $f(\omega_1, 0) = 0$ implies $v(\omega_1) = 0$ where $f(x,y) = v(x) + yw(x)$. Hence we can write $v(x) = (x - \omega_1)v_1(x)$ for some polynomial v_1. Since the roots of $s(x)$ are distinct, $(x - \omega_2)$ and $(x - \omega_3)$ do not vanish at P, so we get

$$\begin{aligned} f(x,y) &= (x-\omega_1)v_1(x) + yw(x) \\ &= \frac{(x-\omega_1)(x-\omega_2)(x-\omega_3)v_1(x) + yw_1(x)}{(x-\omega_2)(x-\omega_3)} \\ &= \frac{y^2 v_1(x) + yw_1(x)}{(x-\omega_2)(x-\omega_3)} \\ &= y\left[\frac{yv_1(x) + w_1(x)}{(x-\omega_2)(x-\omega_3)}\right] \quad , \end{aligned}$$

where $w_1(x) = (x-\omega_2)(x-\omega_3)w(x)$. Now if the function in brackets still vanishes at P, we can do the process over again to the polynomial $w_1(x) + yv_1(x)$. This process must also terminate since in every other step we factor $x - \omega_1$ from v, which can contain only finitely many such factors. Hence in the case of points of order two, we can take $u(x,y) = y$.

Finally in the case $P = \mathcal{O}$, we show that $u(x,y) = x/y$ works. Suppose $r = f/g$ and $r(\mathcal{O}) = 0$. This means that $\deg(f) - \deg(g) = d < 0$. Since $\deg(y) - \deg(x) = 1$, $\deg(y^d f) = \deg(x^d g)$, and $(y/x)^d r$ will be finite and nonzero at the identity. Since

$$r = (x/y)^d \left[(y/x)^d r\right] \quad ,$$

we see that we can take $u(x,y) = x/y$ at the identity.

To see that the number d is unique, suppose that u and u' are both rational functions satisfying the conditions of the theorem. This means that we can write $u = (u')^e s$ and $u' = u^f t$, so $u = u^{ef}(t^e s)$. If $ef \neq 1$, then by dividing this equation by u and plugging in P, we get $1 = 0$. We therefore must have $e = f = 1$. Thus if r is any rational function not identically zero that vanishes at P, we can write $r = u^d s = (u')^d t$. ∎

The above theorem allows us to make the following definitions:

Definition 4.4 A function u that satisfies the above theorem is called a *uniformizing variable* or *uniformizer* at P. If r is a rational function and $r = u^d s$, where u is a uniformizing variable at P, we say that the *order* of r at P is d and write

$$\mathrm{ord}_p(r) = d \quad .$$

We define the *multiplicity* of a zero to be the order of the function and the *multiplicity* of a pole to be the negative of the order. If a zero or pole has multiplicity one, two, or three we say it is *simple*, *double*, or *triple*, respectively.

Example 4.5 (i) Let $P \in E$ and suppose $P = (k,l)$ with $k, l \in K$ and $l \neq 0$. Let $u = x - k$. Since u is a uniformizer at P, we see $\mathrm{ord}_p(u) = 1$. Now $P' = (k, -l)$ is also a point of E, and clearly $\mathrm{ord}_{P'}(u) = 1$. It is also clear that u has order zero at every other finite point. We see that u has a pole at $\mathcal{O}$, and since $\deg(u) = 2$, we get that $\mathrm{ord}_{\mathcal{O}}(u) = -2$. Summing up, we see that u has two simple zeros, and a single double pole.

(ii) Now consider the function y. We have seen that y is a uniformizing variable at the three points $(\omega_1, 0), (\omega_2, 0)$, and $(\omega_3, 0)$, so it has a zero of multiplicity one at these three points. Also y has order zero at every other point except $\mathcal{O}$. Since y has degree three, it has a pole of multiplicity three at $\mathcal{O}$.

(iii) Finally take $u = x/y$. We leave it to the "interested reader" to show that u has a zero of multiplicity one at $\mathcal{O}$, zeros also of multiplicity one at the two points $(0, \sqrt{B})$ and $(0, -\sqrt{B})$ and simple poles at the three points of order two (if $B = 0$, there is a simple zero at $\mathcal{O}$, a simple zero of multiplicity one at $(0,0)$), and poles of multiplicity one at the points $(\sqrt{-A}, 0)$ and $(-\sqrt{-A}, 0)$).

These examples suggest the following theorem, which is a sort of baby Riemann–Roch Theorem in that it places restrictions on what kind of zeros and poles a rational function can have:

Theorem 4.6 *Let r be a rational function on E. Then*

$$\sum_{P \in E} \mathrm{ord}_p(r) = 0 \quad .$$

Before we give its proof, we prove a lemma, which is of interest itself.

Lemma 4.7 *Let f be a polynomial on E. The sum of the multiplicities of the zeros of f equals the degree of f.*

Proof. Let $\deg(f) = n$. By Lemma 3.7, $\deg_x(N(f)) = n$, so we can write

$$N(f)(x) = f\bar{f}(x) = (x - a_1)(x - a_2) \cdots (x - a_n) \quad ,$$

where the a_i are elements of K that may not be distinct. If $a_i \neq \omega$, then $(x - a_i)$ has two distinct roots on E. If $a_i = \omega$, then $x - a_i$ has only one root on E, but it has multiplicity two. Thus we can conclude that $f\bar{f}$ has precisely $2n$ roots on E, counting multiplicities. But clearly f and $\bar{f}$ have the same number of roots on E, so the sum of the multiplicities of the zeros of each must be n. ∎

Now we give the proof of Theorem 4.6.

Proof. It suffices to prove the result for a polynomial f. We know that

$$\sum_{P \in E - \mathcal{O}} \mathrm{ord}_p(f)$$

is the sum of the multiplicities of the zeros of f. On the other hand, by definition, $\mathrm{ord}_{\mathcal{O}}(f)$ is the negative of the degree of f, so the theorem follows from the lemma. ∎

We will need the next two lemmas in several places.

Lemma 4.8 *Let f be a nonconstant polynomial on E. Then f must have at least two simple zeros or one double one at finite points of E.*

Proof. If f is nonconstant, then it must involve an x or a y. Since $\deg(x) = 2$ and $\deg(y) = 3$, this result follows from the previous lemma. ∎

The following exercise is in much the same spirit as the above lemma:

Exercise 4.9 Since K is algebraically closed, E must have an infinite number of points. Show that if two rational functions agree on an infinite number of points of E, then they are equal.

Lemma 4.10 *A rational function without finite poles is a polynomial.*

Proof. We write $r = a + yb$ where, a and b are rational functions of x. If r has no finite poles, then clearly $\bar{r} = a - yb$ has no finite poles. Hence $r + \bar{r} = 2a$ has no finite poles. If a had a pole as a function of x, then it would have one as a function on E. Thus a is a polynomial. This implies that $yb = r - a$ has no finite poles. Hence $(yb)^2 = sb^2$ has no finite poles where, $s(x) = x^3 + Ax + B$. If b has a pole, then it can be written $b = f/g$ where $g(x) = 0$ for some $x \in K$.

In this case, $b^2 = f^2/g^2$ and g^2 has a double root at some x. The only way for sb^2 not to have a pole at P is for s to have a double zero at x, and since E is nonsingular, this is not the case. Therefore b has no finite poles. Finally we see that b must also be a polynomial, so r is a polynomial. ∎

There is an extension of the idea of rational function that we will need later.

Definition 4.11 A *rational map* F on E is a pair (r, s) where r and s are rational functions on E such that

$$s^2 = r^3 + Ar + B \quad .$$

If we make the convention that $F(P) = \mathcal{O}$ if r and s are not finite at P, we see that F actually defines a map from E to E by $F(P) = (r(P), s(P))$ since r and s must have poles at the same points.

Remark. There is an amusing way of looking at rational maps that will actually be useful. Given the field K, we form the elliptic curve E using the equation

$$Y^2 = X^3 + AX + B \quad . \tag{4}$$

Now suppose we consider the field of rational functions $K(E)$. Then we can use the same equation to form a new elliptic curve, which we might denote by $E(K(E))$. Now $K(E)$ may not be algebraically closed, and by our convention, the points of $E(K(E))$ have coordinates in the algebraic closure of $K(E)$. The finite points whose coordinates lie in $K(E)$ (*i.e.,* the $K(E)$–rational points) are precisely the rational maps. We can think of the identity of this curve, call it $\mathcal{O}_M$, as the "map" with the constant value $\mathcal{O}$.

5 Divisors and Lines

It is not hard to imagine that it would be convenient to have a device to keep track of the zeros and poles of a rational functional r. One idea is to use lists

$$[(P_1, m_1), (P_2, m_2), \ldots, (P_n, m_n)]$$

where r has order m_i at P_i. It turns out to be better to consider a formal sum

$$m_1\langle P_1\rangle + m_2\langle P_2\rangle + \cdots + m_n\langle P_n\rangle = \sum_{i=1}^{n} m_i\langle P_i\rangle \quad .$$

The right way to do this is to use the notion of a free Abelian group generated by a given set. We recall the definition here.

Definition 5.1 Let S be any set. *The free Abelian group generated by* S is the set of finite formal linear combinations

$$\sum_{s\in S} m(s)s \quad ,$$

where $m(s) \in \mathbb{Z}$, and $m(s) = 0$ except for finitely many $s \in S$. The addition is also formal; simply juxtapose and collect terms. For example,

$$(m_1 s_1 + m_2 s_2) + (n_1 s_1 + n_3 s_3) = (m_1 + n_1)s_1 + m_2 s_2 + n_3 s_3 \quad .$$

Definition 5.2 Let E be an elliptic curve over an algebraically closed field K. The *group of divisors of* E is the free Abelian group generated by the points of E. We denote it by $\mathrm{Div}(E)$. To distinguish the point P from the divisor whose sole nontrivial entry is P with coefficient 1, we denote this divisor by $\langle P \rangle$. If $\Delta = \sum_{P \in E} m(P)\langle P \rangle$ is a divisor, then we define its *degree* by

$$\deg(\Delta) = \sum_{P \in E} m(P) \in \mathbb{Z} \quad .$$

If r is a nonzero rational function on E, we associate a divisor to r by the following equation:

$$\mathrm{div}(r) = \sum_{P \in E} \mathrm{ord}_p(r)\langle P \rangle \quad .$$

Remarks.

(i) We should observe that a rational function has a finite number of zeros and poles. This can be seen from Lemma 4.7.

(ii) If two rational functions have the same divisor, then Lemma 4.10 implies that their quotient is constant. Thus one way to prove that two functions are equal is to show that they have the same divisor, then to show they agree at any one point of E. Usually the only point on E that we can get our hands on is $\mathcal{O}$, and frequently functions have poles at $\mathcal{O}$. In this case, we can compare leading coefficients, defined below.

Definition 5.3 Let r be a rational function and suppose $\mathrm{ord}_{\mathcal{O}}(r) = d$. Then we define the *leading coefficient* of r to be

$$[(x/y)^d \cdot r](\mathcal{O}) \quad .$$

Exercise 5.4 Show that if two rational functions have the same divisor and the same leading coefficient, they are equal.

Example 5.5 (i) Let $P = (a, b) \in E$ with $b \neq 0$, and $r_1 = (x - a)$. Then we have seen that r_1 has simple zeros at P and $P' = (a, -b)$ and a pole of multiplicity two at $\mathcal{O}$. Therefore $\mathrm{div}(r_1) = \langle P \rangle + \langle P' \rangle - 2\langle \mathcal{O} \rangle$ where we have used $-2\langle \mathcal{O} \rangle$ for $+(-2)\langle \mathcal{O} \rangle$.

(ii) Let $r_2 = y$. If we let P_i $(i = 1, 2, 3)$ be the points of order two, then

$$\mathrm{div}(r_2) = \langle P_1 \rangle + \langle P_2 \rangle + \langle P_3 \rangle - 3\langle \mathcal{O} \rangle \quad .$$

(iii) We take $r_3 = x/y$ and $Q = (0, \sqrt{B})$ and $Q' = (0, -\sqrt{B})$, so

$$\mathrm{div}(r_3) = \langle Q \rangle + \langle Q' \rangle - \langle P_1 \rangle - \langle P_2 \rangle - \langle P_3 \rangle + \langle \mathcal{O} \rangle \quad .$$

Definition 5.6 We say a divisor Δ is *principal* if $\Delta = \mathrm{div}(r)$ for some rational function r. If $\Delta_1 - \Delta_2$ is principal, we say Δ_1 and Δ_2 are *linearly equivalent* or *in the same divisor class*, and write $\Delta_1 \sim \Delta_2$.

Proposition 5.7 *If r_1 and r_2 are rational functions on E, then* $\mathrm{div}(r_1 r_2) = \mathrm{div}(r_1) + \mathrm{div}(r_2)$.

Proof. It is easy to see that $\mathrm{ord}_p(r_1 r_2) = \mathrm{ord}_p(r_1) + \mathrm{ord}_p(r_2)$, and the proposition follows from this. ∎

Definition 5.8 By the above proposition, the set of principal divisors forms a subgroup of $\mathrm{Div}(E)$, which we denote by $\mathrm{Prin}(E)$. We also define $\mathrm{Div}^0(E)$ to be the subgroup of divisors of degree 0. (It is trivial to see it is a subgroup.)

One of our goals in this section is to study which divisors are principal, *i.e.,* what zeros and poles a rational function can have. This is equivalent to studying the divisors that are *not* principal. These divisors are represented by the elements of the group

$$\mathrm{Pic}(E) = \mathrm{Div}(E)/\mathrm{Prin}(E) \quad .$$

$\mathrm{Pic}(E)$ is called the *Picard* or *divisor class group of E*. Actually we can study a smaller group to investigate which divisors are principal. Theorem 4.6 implies $\mathrm{Prin}(E) \subseteq \mathrm{Div}^0(E)$, so we may as well look at the divisors of degree zero that are not principal, *i.e.,* the group

$$\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{Prin}(E) \quad .$$

$\mathrm{Pic}^0(E)$ is called the *degree zero part of the Picard* (or *divisor class) group of E*. We are going to show that $\mathrm{Pic}^0(E)$ is in one–to–one correspondence with the points of E. We need some more definitions first.

Definition 5.9 If $\Delta = \sum_{P \in E} m(P)\langle P \rangle$ is a divisor, we define its *norm* by

$$|\Delta| = \sum_{P \in E - \mathcal{O}} |m(P)| \quad .$$

For example, a divisor of norm one looks like $\pm\langle P \rangle + n\langle \mathcal{O} \rangle$ where n is some arbitrary integer. Also if Δ is the divisor of some polynomial f, then $|\Delta|$ is the sum of the multiplicities of the zeros of f, which is the degree of f.

Definition 5.10 A *line* on E is a polynomial of the form

$$\ell(x, y) = \alpha x + \beta y + \gamma \quad ,$$

for some $\alpha, \beta, \gamma \in K$ with not both α and β zero.

If a point P is a zero of the line ℓ, we say ℓ is a line *through* P, and P is *on* ℓ.

The main result on lines is the following:

Lemma 5.11 *If ℓ is a line with divisor Δ, then $|\Delta| = 2$ or 3.*

Proof. ℓ is a polynomial of degree 2 (if $\beta = 0$) or 3 (if $\beta \neq 0$). Hence by Lemma 4.7, the sum of the multiplicities of the zeros of ℓ is 2 or 3, and this sum is precisely $|\Delta|$. ∎

Exercise 5.12 Show that the possible divisors of a line are the following, where P, Q, and R are distinct:

(i) $\operatorname{div}(\ell) = \langle P\rangle + \langle Q\rangle + \langle R\rangle - 3\langle \mathcal{O}\rangle$.

(ii) $\operatorname{div}(\ell) = 2\langle P\rangle + \langle Q\rangle - 3\langle \mathcal{O}\rangle$.

(iii) $\operatorname{div}(\ell) = 3\langle P\rangle - 3\langle \mathcal{O}\rangle$.

(iv) $\operatorname{div}(\ell) = \langle P\rangle + \langle Q\rangle - 2\langle \mathcal{O}\rangle$.

(v) $\operatorname{div}(\ell) = 2\langle P\rangle - 2\langle \mathcal{O}\rangle$.

Show all of these cases actually occur. (**Hint:** In part (iii), P is an inflection point of the curve.)

The next theorem is the main result of this section. It has an amazingly simple proof. If $P = (a, b)$, we use the notation $-P$ for $(a, -b)$. The reason for this will become clear in the next section.

Theorem 5.13 *(Linear Reduction) Let $\Delta \in \operatorname{Div}(E)$. Then there is $\tilde{\Delta} \in \operatorname{Div}(E)$ with $\Delta \sim \tilde{\Delta}$ and $\deg(\tilde{\Delta}) = \deg(\Delta)$ and $|\tilde{\Delta}| \leq 1$.*

Proof. Suppose $\Delta = \sum_{P \in E} n(P)\langle P\rangle$, and Q and R appear in Δ with nonzero coefficients of the same sign. Let ℓ be the line through Q and R. Then depending on the sign of the coefficient of Q (or R), $\Delta + \operatorname{div}(\ell)$ or $\Delta - \operatorname{div}(\ell)$ will have $|n(Q)|$ and $|n(R)|$ reduced by one if ℓ has three distinct zeros. By the lemma, we will have at worst increased the coefficient of one other point by one. If ℓ has only two distinct zeros, then we will have decreased $|n(Q)|$ or $|n(R)|$ by one, and increased no other coefficient at all. So we will have produced a divisor, say Δ_1, with $\Delta_1 \sim \Delta$, $\deg(\Delta_1) = \deg(\Delta)$ and $|\Delta_1| < |\Delta|$.

After doing this linear reduction a finite number of times, we get a divisor Δ' linearly equivalent to Δ, of the same degree as Δ, and

$$\Delta' = n_1\langle P\rangle - n_2\langle Q\rangle + n\langle \mathcal{O}\rangle \quad ,$$

where n_1 and n_2 are nonnegative integers and n is an integer we do not care about.

Suppose $n_1 > 1$. Consider the line

$$\ell(x, y) = m(x - a) - (y - b)$$

with $P = (a, b)$. P is on ℓ if a is a zero of the polynomial

$$f(x) = [m(x - a) + b]^2 - x^3 - Ax - B$$

because P must satisfy both the equation of the line and the basic equation of the elliptic curve. We have used these two equations to eliminate y and obtain the polynomial f. If we compute $f'(a)$, we see that P will have multiplicity two if

$$m = \frac{3a^2 + A}{2b} \quad .$$

(A neater way to do this computation is to use the derivation of Definition 8.1.) So if $b \neq 0$, this line will have divisor $2\langle P\rangle + \langle S\rangle - 3\langle\mathcal{O}\rangle$. By subtracting it, we can reduce n_1 and $|\Delta'|$. If P is of order two, the line $\ell(x,y) = x - \omega$ has divisor $2\langle P\rangle - 2\langle\mathcal{O}\rangle$ and can be subtracted to reduce n_1.

We can similarly reduce n_2. Eventually we are done, or we arrive at

$$\langle P\rangle - \langle Q\rangle + ?\langle\mathcal{O}\rangle \quad .$$

The line $\ell(x,y) = x - a$ has divisor $\langle P\rangle + \langle R\rangle - 2\langle\mathcal{O}\rangle$ or $2\langle P\rangle - 2\langle\mathcal{O}\rangle$. Thus by subtracting it, we are reduced to a previous case. ∎

The next two corollaries and Proposition 6.7 are analogs of the Riemann–Roch Theorem. They give a rather precise description of which divisors are principal.

Corollary 5.14 *For each $\Delta \in Div^0(E)$, there is a unique point $P \in E$ such that*

$$\Delta \sim \langle P\rangle - \langle\mathcal{O}\rangle \quad .$$

Proof. The theorem tells us that Δ is equivalent to a divisor of norm 1, *i.e.,* a divisor $\pm\langle P\rangle + n\langle\mathcal{O}\rangle$. If the sign of $\langle P\rangle$ is not plus, by subtracting the line with divisor $\langle P\rangle + \langle Q\rangle - 2\langle\mathcal{O}\rangle$, we can change the sign. Since we are given that degree of Δ is zero, the coefficient of $\mathcal{O}$ must be -1, so the only thing to check is whether P is unique. Suppose $\Delta \sim \langle Q\rangle - \langle\mathcal{O}\rangle$ also. Then $\langle Q\rangle \sim \Delta + \langle\mathcal{O}\rangle \sim \langle P\rangle$, so there would have to be a rational function r with $\mathrm{div}(r) = \langle P\rangle - \langle Q\rangle$. By the methods of the proof of the theorem, we can see that if this were the case, there would have to be a rational function r whose divisor is $\langle S\rangle - \langle\mathcal{O}\rangle$ for some $S \in E$. Clearly r would have no finite poles so by Lemma 4.10, r would have to be a polynomial. But then r would be a polynomial with a single finite zero, which by Lemma 4.8 is impossible, so we must have $\langle P\rangle = \langle Q\rangle$. ∎

Define a map $\bar{\sigma} : \mathrm{Div}^0(E) \to E$ by $\bar{\sigma}(\Delta) = P$ where P is the unique point with $\Delta \sim \langle P\rangle - \langle\mathcal{O}\rangle$. Since $\mathrm{div}(r) \sim 0$, $\bar{\sigma}(\mathrm{div}(r)) = \mathcal{O}$, and we see that $\bar{\sigma}$ induces a map

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

Corollary 5.15 *σ is a bijection.*

Proof. σ is surjective since $\sigma(\langle P\rangle - \langle\mathcal{O}\rangle) = P$. It is obviously injective. ∎

6 The Group Laws

We are going to give the group addition laws for an elliptic curve in their algebraic formulation. This is in keeping with our policy of being explicit and computational. It does, however, suffer from two disadvantages. One is that it is somewhat unmotivated, and the other is that the "(direct) verification (of the associativity law) is a pain" ([3, page 40]). Another approach is geometric (see [6, page 55]) and is a little more motivated, but associativity is still difficult (although it can be done, see [1, page 125]). We will use this approach to motivate the algebraic equations. In his book, Lang gives a beautiful definition using doubly periodic functions, but this method only works when K is the field of complex numbers. Finally there is a way to define addition using divisors that makes associativity trivial. We are ultimately going to use this approach by showing it is equivalent to the algebraic formulas presented here.

Remark. The basic idea behind addition on an elliptic curve is that a line will intersect the curve no more than three times. We describe roughly how this works; the formal definitions follow. First we make $\mathcal{O}$ act as the zero or identity element of the group. Then we make $(a, -b)$ be the negative of (a, b). Finally, if the points P, Q, and R are on a line, we define the addition so that $P + Q + R = \mathcal{O}$.

First of all, suppose $P \neq Q$ or $-Q$ and let ℓ be the line through P and Q and let R be the third zero of ℓ, which is easily seen to be finite. Write $P = (a, b)$ and $Q = (c, d)$ so ℓ can be written

$$\ell(x, y) = m(x - a) - (y - b) \quad ,$$

where $m = (d - b)/(c - a)$. We have seen that since (a, b) is a zero of ℓ and is on the curve, a is a zero of the polynomial

$$f(x) = [m(x - a) + b]^2 - x^3 - Ax - B \quad . \tag{5}$$

It is trivial to see that a and c are zeros of f, but what is the third zero of f? Let e be this third zero. Writing $f(x) = (x - a)(x - c)(x - e)$, we see that the coefficient of x^2 in f is $a + c + e$. Using Equation (5), we see that m^2 is the coefficient of x^2, so $a + c + e = m^2$ or $e = -a - c + m^2$. To get the y coordinate of R, we just plug this back into the equation of the line; the y coordinate of R is $m(e - a) + b$.

If $P = Q$, then we use the line tangent to P, *i.e.,* the line with a double zero at P. We have seen that this line has the usual equation with $m = (3a^2 + A)/2b$.

Summing up, to add two distinct nonzero points that are not negatives, draw the line through them and then "flip" the third point of intersection about the x axis (*i.e.,* send (a, b) into $(a, -b)$) to get their sum. If the points to be added are the same, use the line tangent to get the point to be flipped.

Now we give the formal definitions. As usual, we let E be a nonsingular elliptic curve over an algebraically closed field K given by the equation $Y^2 = X^3 + AX + B$. We now define the structure of an Abelian group on E.

Definition 6.1 We let the identity $\mathcal{O}$ be the zero of the group (which explains its notation). So for any point $P \in E$,

$$P + \mathcal{O} = \mathcal{O} + P = P \quad .$$

For $P = (k, l) \in E$, we define $-P$ to be $(k, -l) \in E$, so

$$P + (-P) = (-P) + P = \mathcal{O} \quad .$$

Now suppose P_1 and P_2 are not $\mathcal{O}$, and $P_1 \neq -P_2$. Let $P_1 = (k_1, l_1)$ and $P_2 = (k_2, l_2)$. If $k_1 \neq k_2$ (so $P_1 \neq P_2$), define

$$\lambda = \frac{l_2 - l_1}{k_2 - k_1} \quad ,$$

while if $k_1 = k_2$ (so $P_1 = P_2$ since we have assumed $P_1 \neq -P_2$), define

$$\lambda = \frac{3{k_1}^2 + A}{2l_1} \quad .$$

Define $P_1 + P_2 = (k_3, l_3)$ by

$$k_3 = -k_1 - k_2 + \lambda^2$$

and

$$l_3 = -l_1 - \lambda(k_3 - k_1) \quad .$$

We will call the addition formula in the case $P_1 \neq P_2, -P_2, \mathcal{O}$ (*i.e.*, $\lambda = (l_2 - l_1)/(k_2 - k_1)$) the *generic* addition formula since it is the one to use for practically all pairs of points.

Remarks.

(i) In some real sense, the generic formula works all of the time. We can, for example, use it in the case $P_1 = P_2$, not a point of order two, if we believe the following computation:

$$\begin{aligned} \lambda &= \frac{l_2 - l_1}{k_2 - k_1} \cdot \frac{l_2 + l_1}{l_2 + l_1} \\ &= \frac{[{k_2}^3 - {k_1}^3] + A(k_2 - k_1)}{(k_2 - k_1)(l_2 + l_1)} \\ &= \frac{{k_2}^2 + k_1 k_2 + {k_2}^2 + A}{l_1 + l_2} \quad , \end{aligned} \tag{6}$$

and if $k_2 = k_1 = k$ and $l_2 = l_1 = l \neq 0$, this becomes $\frac{3(k)^2 + A}{2l}$. Geometrically, what this means is that the slope of the line through P_1 and P_2 (namely $\frac{l_2 - l_1}{k_2 - k_1}$) becomes the slope of the line tangent to P_1 (namely

$\frac{3(k)^2+A}{2l}$) as P_1 goes to P_2. There are a number of other cases (*e.g.*, $P = \mathcal{O}$, or $P_1 = -P_2$), and it is not too difficult to work them all out. But what do they mean?

We are really showing here the important fact that addition is a rational function. But a rational function on what? Unfortunately, addition is defined on $E \times E$, which is not an elliptic curve but a product of elliptic curves. It would be very convenient for us to know that addition is rational, but that would involve a more general definition of rational function on a more general algebraic geometric object. All this would lead us too far afield, so we have decided on a different approach.

It might appear that addition is rational simply because it is given by rational formulas. The difficulty is that it is given by *different* rational formulas for different cases. If it is to be obvious that a function is rational, it must be given by the same rational expression at every point it is defined or at least by expressions that are "rationally related", *i.e.,* if $r = f/g$, r may also equal h/k if $fk = gh$.

(ii) One might prefer to use the last expression in Equation (6) to define λ in the case $P_1 = P_2$. This would have the advantage of working not only when $P_1 = P_2$, but whenever $l_1 \neq -l_2$. It might almost appear that this expression for λ would work whenever $P_1 \neq \mathcal{O}$ or $-P_2$. However, there are two other points on E besides $-P_2$ whose y coordinate is $-l_2$, so we would still have the same number of special cases.

(iii) Notice that the three points of order two, $(\omega_1, 0), (\omega_2, 0)$ and $(\omega_3, 0)$, satisfy $2 \cdot P = \mathcal{O}$, and these are the only points (except for $\mathcal{O}$) which do so. This follows since the definition of $-P$ tells us that any point with $P = -P$ must have second coordinate 0, and the three points of order two are the only points that do.

(iv) If P and Q are any points not both $\mathcal{O}$, then we can find a line ℓ whose divisor is

$$\langle P \rangle + \langle Q \rangle + \langle R \rangle - 3\langle \mathcal{O} \rangle \quad ,$$

and then R is $-P - Q$. This is true even if $Q = \pm P$ or $\mathcal{O}$.

(v) Recall the elliptic curve $E(K(E))$ of rational maps of E. Since the field $K(E)$ may not be algebraically closed, it is not immediately clear that the sum of two rational maps is again a rational map; it may be something whose coordinates lie in the algebraic closure of $K(E)$. However, an examination of the algebraic formulas defining addition quickly shows that this is not the case, *i.e.,* the sum of two rational maps *is* again a rational map.

Now we state the basic theorem about addition.

Theorem 6.2 *The elliptic curve with the addition defined above forms an Abelian group.*

All of the group axioms are trivial to check except associativity, which will follow from the next proposition. Recall the bijection

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

defined in the previous section. Let $\kappa = \sigma^{-1}$, so $\kappa(P)$ is the linear equivalence class of the divisor $\langle P\rangle - \langle \mathcal{O}\rangle$. Clearly $\kappa(\mathcal{O})$ is the zero linear equivalence class.

Proposition 6.3 $\kappa(P+Q) = \kappa(P) + \kappa(Q)$.

Proof. The result is trivial if $P = Q = \mathcal{O}$, so we suppose that P and Q are not both $\mathcal{O}$. Let ℓ be the line through P and Q. As we remarked above (iv), we can write the divisor of ℓ as

$$\mathrm{div}(\ell) = \langle P\rangle + \langle Q\rangle + \langle R\rangle - 3\langle \mathcal{O}\rangle \quad .$$

Let ℓ' be the line through R and $-R$, so

$$\mathrm{div}(\ell') = \langle R\rangle + \langle -R\rangle - 2\langle \mathcal{O}\rangle \quad .$$

We have seen that $R = -P - Q$ so $-R = P + Q$ and

$$\mathrm{div}(\ell'/\ell) = \langle P+Q\rangle - \langle P\rangle - \langle Q\rangle + \langle \mathcal{O}\rangle \sim 0$$

since ℓ'/ℓ is a rational function. Rewriting this slightly yields

$$(\langle P+Q\rangle - \langle \mathcal{O}\rangle) - (\langle P\rangle - \langle \mathcal{O}\rangle) - (\langle Q\rangle - \langle \mathcal{O}\rangle) \sim 0 \quad ,$$

which translates to $\kappa(P+Q) - \kappa(P) - \kappa(Q) = 0$ as desired. ∎

Corollary 6.4 *Addition on an elliptic curve is associative.*

This follows because the addition in $\mathrm{Pic}^0(E)$ is certainly associative.

We have proved that κ is a homomorphism, so clearly σ is a homomorphism. Since $\bar{\sigma}$ is the composition of σ and projection from Div^0 to $\mathrm{Pic}^0 = \mathrm{Div}^0/\mathrm{Prin}$, it too is a homomorphism. There is a simpler way of looking at $\bar{\sigma}$.

Definition 6.5 Define a map *sum* from $\mathrm{Div}(E)$ to E by

$$\mathrm{sum}\left(\sum n(P)\langle P\rangle\right) = \sum n(P)P \quad .$$

Exercise 6.6 Show that $\bar{\sigma}$ is merely sum restricted to Div^0.

We can use all this to prove an extremely useful result.

Proposition 6.7 *Let $\Delta = \sum_{P\in E} n(P)\langle P\rangle$ be a divisor. Then Δ is principal if and only if $\deg(\Delta) = \sum_{P\in E} n(P) = 0$ and $\mathrm{sum}(\Delta) = \sum_{P\in E} n(P)P = \mathcal{O}$.*

Proof. We have already proved the part about the degree, so we can assume that $\deg(\Delta) = 0$. Recall that $\bar{\sigma}(\Delta) = P$ where P is the unique point with $\Delta \sim \langle P\rangle - \langle \mathcal{O}\rangle$. Hence $\Delta \sim 0 \Leftrightarrow \bar{\sigma}(\Delta) = \mathcal{O} \Leftrightarrow \mathrm{sum}(\Delta) = \mathcal{O}$, which is what we wanted to prove. ∎

7 Multiplication by n

What we really are interested in is the function $[n] : P \mapsto n \cdot P$, the point P added to itself n times. More precisely, we are interested in the two functions $g_n(P) = x(n \cdot P)$ and $h_n(P) = y(n \cdot P)$, *i.e.*, $n \cdot P = (g_n(P), h_n(P))$.

The next theorem is our version of the fact that addition is rational. Recall that the rational maps on E form an elliptic curve themselves. When we write the sum of two rational maps, we mean the sum on this elliptic curve. Suppose we make the convention that the constant map $\mathcal{O}_M$ whose value is $\mathcal{O}$ everywhere is a rational map. Then the following theorem says that the pointwise sum of rational maps is a rational map.

Theorem 7.1 *Let F and G be rational maps on E. If $K = F+G$, then $K(P) = F(P) + G(P)$.*

Proof. The point of the theorem is that even if F is not $G, -G$, or $\mathcal{O}_M$, $F(P)$ may equal $G(P), -G(P)$, or $\mathcal{O}$, so there are some things to be checked.

If any of F, G, or $F + G$ is $\mathcal{O}_M$, the result is trivial, so we will exclude these trivial cases.

Suppose $F = (r, s)$ and $G = (t, v)$. There are two main cases, namely $r \neq t$, and $r = t$. Let $K = (w, z)$ so

$$w = -(t + r) + \lambda^2 \tag{7}$$

and

$$z = -v - \lambda(w - t) \quad , \tag{8}$$

where in the first case, we put

$$\lambda = \frac{s - v}{r - t} \quad , \tag{9}$$

while in the second case, we put

$$\lambda = \frac{3r^2 + A}{2s} \quad . \tag{10}$$

(I) Let us assume that we are in the first case so λ is given by Equation (9).

(A) If $r(P)$ and $t(P)$ are finite and not equal, then $K(P) = F(P)+G(P)$ is simply the generic addition formula.

(B) If $r(P)$ and $t(P)$ are finite and equal, then we must have $s(P) = -v(P)$, or $s(P) = v(P)$.

(1) If $s(P) = -v(P) \neq \mathcal{O}$, then we have $F(P) = -G(P)$. We see that λ will have a pole at P, which is again just what we want since $F(P) + G(P) = F(P) + (-F(P)) = \mathcal{O}$.

(2) If $r(P)$ and $t(P)$ are finite and $s(P) = v(P)$, the formulas for $F(P) + G(P)$ and $K(P)$ only differ in the definition of λ. Since $v \neq -s$, we get

$$\begin{aligned}\lambda &= \frac{v-s}{t-r} \cdot \frac{v+s}{v+s} \\ &= \frac{[t^3 - r^3] + A(t-r)}{(t-r)(v+s)} \\ &= \frac{t^2 + rt + r^2 + A}{s+v} \quad .\end{aligned}$$

In the case $r(P) = t(P)$ and $s(P) = v(P) \neq 0$, this becomes

$$\lambda(P) = \frac{3r(P)^2 + A}{2s(P)} \quad ,$$

as required by Equation (10).

If $s(P) = v(P) = 0$, then we are at a point $F(P)$ of order two. We see from the above expression that λ has a pole for this P and hence the components of $K(P)$ must also have poles since everything else besides λ in the addition formula is finite. Fortunately this is just what we want because if $F(P) = G(P)$ has order two, then $F(P) + G(P) = \mathcal{O}$.

(3) Next we do the case where exactly one of $F(P)$ or $G(P)$, say $F(P)$, is $\mathcal{O}$. In this case, r and s have poles at P so we can write $r = r_1/u^d$ and $s = s_1/u^e$ where u is a uniformizing variable at P, d and e are positive integers, and r_1 and s_1 are rational functions that are finite and nonzero at P. Then since $s^2 = r^3 + Ar + B$, we must have $2e = 3d$ and ${s_1}^2(P) = {r_1}^3(P)$. The last statement follows from

$$\frac{{s_1}^2}{{r_1}^3} = 1 + \frac{Au^{2e}r_1 + Bu^{3e}}{r_1} \quad .$$

Using Equations (7), (8), and (9), we compute w.

$$\begin{aligned}w &= -(t+r) + \left(\frac{s-v}{r-t}\right)^2 \\ &= \frac{-(r^3 - t^2r - tr^2 + t^3) + (s^2 - 2vs + v^2)}{(r-t)^2} \\ &= \frac{-r^3 + t^2r + tr^2 - t^3 + (r^3 + Ar + B) - 2vs + v^2}{(r-t)^2} \\ &= \frac{tr^2 + (t^2 + A)r + (v^2 - t^3 + B - 2vs)}{r^2 - 2tr + t^2} \\ &= \frac{t{r_1}^2u^{-2d} + (t^2 + A)r_1u^{-d} + (v^2 - t^3 + B - 2vs_1u^{-e})}{{r_1}^2u^{-2d} - 3tr_1u^{-d} + t^2} \\ &= \frac{t{r_1}^2 + u^dR_1 - 2vu^{2d-e}s_1}{{r_1}^2 + u^dR_2} \quad ,\end{aligned}$$

where R_1 and R_2 are rational functions that are finite at P. Since $2e = 3d$, $2d - e > 0$, we see that $w(P) = t(P)$. This is what we want since $F(P) + G(P) = G(P)$ when $F(P) = \mathcal{O}$.
Now we could compute the y coordinate in a similar fashion, but we can avoid that by using the associative law on the elliptic curve of rational maps. Since $F + G = K$, we have $G - K = F$. Now the previous computation of the x coordinate shows that $K(P) \neq \mathcal{O}$, so we know that $(G - K)(P) = G(P) - K(P) = F(P) = \mathcal{O}$, which shows that $G(P) = K(P)$ as desired.

(4) The next case to consider is when F and G both have poles at P. Again we can use associativity of addition on the elliptic curve of rational maps to save a lot of work. Since $K = F + G$, $(F + G) - K = \mathcal{O}_M$, and by associativity $F + (G - K) = \mathcal{O}_M$. Suppose $K(P) = Q$. Then since $G(P) = \mathcal{O}$, we can conclude that $G(P) - K(P) = -Q$ by the previous case. Similarly we get that $F(P) + (G - K)(P) = -Q$, which tells us that $Q = \mathcal{O}$ as desired.

(II) Now we suppose $r = t$. If $s = -v$, then $F = -G$, so $K = \mathcal{O}_M$, the map whose constant value is $\mathcal{O}$. But clearly $F(P) = -G(P)$, so $F(P) + G(P) = \mathcal{O}$ for any point $P \in E$. Hence we can assume that $s \neq -v$ in this case. Of course, $s(P)$ may be $-v(P)$ for any *particular* point P. Since $s \neq v$, $F \neq -G$, so we can assume that $F = G$.

If $r(P)$ is finite, then $K(P) = F(P) + G(P)$ because they are identically defined. Otherwise, we observe that the duplication formula yields

$$w = \frac{-4rs + 3r^2 + A}{2s} \quad ,$$

which shows w has a pole at P if r and s do. As above, z must then also have a pole at P.

■

We now make an important definition.

Definition 7.2

$$E[n] = \{P \in E : n \cdot P = \mathcal{O}\} \quad .$$

Notice that $\mathcal{O} \in E[n]$ for all n, and, in fact, $E[n]$ is a subgroup of E. The points of $E[n]$ are called the *n-torsion* points of E.

Recall that g_n and h_n are defined by $n \cdot P = (g_n(P), h_n(P))$.

Theorem 7.3 *g_n and h_n are rational functions on E with poles precisely at the points of $E[n]$, and $E[n]$ has a finite number of points for all n.*

Proof. The proof is by induction on n. The functions $g_1(x, y) = x$ and $h_1(x, y) = y$ are clearly rational, which gets the induction started. We now assume that g_n and h_n are rational for $n < q$ and that $E[n]$ is finite for $n < q$.

The idea of the inductive step is to write

$$q \cdot P = (q-1) \cdot P + P \quad . \tag{11}$$

By induction we can assume that g_{q-1} and h_{q-1}, the components of $(q-1) \cdot P$, are rational functions of P. Our result will then follow from the previous theorem if we knew that $P \mapsto q \cdot P$ is not the rational map $\mathcal{O}_M$, *i.e.,* if we knew that $(q-1) \cdot P \neq -P$ for some P. But $(q-1) \cdot P = -P$ for all P means $E[q] = E$.

Suppose $E[q] = E$ and $k > 1$ divides q, and say $q/k = \ell$. Then $E[k]$ is a subgroup of $E[q]$, and if $P \in E[q]$, $\ell \cdot P \in E[k]$. Since both k and ℓ are less than q, both $E[k]$ and $E[\ell]$ are finite. It is easy to see that if $E[\ell]$ is finite, then there are only finitely many points Q with $\ell \cdot Q = R$ for a fixed R. Therefore if q has a nontrivial divisor, $E[q]$ is finite, so we may as well assume that q is prime.

Observe that $E[2]$ is finite since there are only four points P with $2 \cdot P = \mathcal{O}$, namely $\mathcal{O}$ and the three points of order two. Also $E[q] = E$ implies $E[2] \subset E[q]$, which implies that q is even. Since q is prime, this says $q = 2$, which contradicts the fact that $E[q]$ is infinite. Hence $E[q] \neq E$ and g_q is rational and not $\mathcal{O}_M$, so $E[q]$ is actually finite since it is the set of poles of a rational function not equal to $\mathcal{O}_M$. ∎

Corollary 7.4 *The rational function $g_n - x$ is not identically zero for any $n > 1$.*

Proof. If $g_n - x = 0$, then we would have $n \cdot P = \pm P$ or, equivalently, $(n \pm 1) \cdot P = \mathcal{O}$ for all $P \in E$. Hence either $E[n-1]$ or $E[n+1]$ would have to be infinite, contradicting the theorem. ∎

For the record, we write g_2 and h_2 here. Recalling that $s(x) = x^3 + Ax + B$, we have

$$g_2(P) = x(2 \cdot P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4s(x)} \quad , \tag{12}$$

and

$$h_2(P) = y(2 \cdot P) = y \cdot \frac{x^6 - 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3}{8s(x)^2} \quad . \tag{13}$$

These formulas follow easily from the duplication formula.

In the next section, we will define a derivation of rational functions on E. Before we discovered this derivation, we used the following exercise to reduce to derivatives of functions of one variable. In the present treatment this fact is used very sparingly.

Exercise 7.5 Show that there are functions $\tilde{g}_n$ and $\tilde{h}_n$ of one variable such that $g_n(P) = \tilde{g}_n(x(P))$ and $h_n(P) = y(P)\tilde{h}_n(x(P))$ (**Hint:** Consider the mapping $F(P) = n \cdot P$. Show that $F(-P) = -F(P)$ and that the components of any map with this property must satisfy the exercise. Alternatively, do the exercise by induction.

We need to know some nonhomogeneous information about g_n and h_n, *i.e.,* we would like to know their values at some point. Since the only point we can really get our hands on is $\mathcal{O}$, we examine the pole of g_n and h_n at $\mathcal{O}$. Let p be the characteristic of K.

Proposition 7.6 *If n is prime to p, then*

$$\frac{g_n}{x}(\mathcal{O}) = \frac{1}{n^2}$$

and

$$\frac{h_n}{y}(\mathcal{O}) = \frac{1}{n^3} \quad .$$

Proof. Yet again, the proof is by induction on n. First assume that $n < p$. Our result clearly is true for $n = 2$ by Equations (12) and (13). Using the equation $n \cdot P = (n-1) \cdot P + P$, we get

$$\begin{aligned} \frac{g_n}{x} &= \frac{-g_{n-1}}{x} - 1 + \frac{1}{x}\left[\frac{h_{n-1} - y}{g_{n-1} - x}\right]^2 \\ &= \frac{-g_{n-1}}{x} - 1 + \frac{y^2}{x^3}\left[\frac{\frac{h_{n-1}}{y} - 1}{\frac{g_{n-1}}{x} - 1}\right]^2 \end{aligned}$$

so

$$\begin{aligned} \frac{g_n}{x}(\mathcal{O}) &= -(n-1)^{-2} - 1 + \left[\frac{+(n-1)^{-3} - 1}{(n-1)^{-2} - 1}\right]^2 \\ &= \left[-(1 + (n-1)^{-2}) + \left(\frac{1 - (n-1)^3}{(n-1) - (n-1)^3}\right)^2\right] \\ &= n^{-2} \quad . \end{aligned}$$

We will leave the result about h_n as an exercise for the reader.

It appears that we are stuck when the induction gets to p. Examining the previous computation, we see that

$$(g_{n-1}/x)(\mathcal{O}) - 1 = n\left(\frac{2-n}{n^2 - 2n + 1}\right) \quad .$$

If $n-1 = p-1$, this is extremely unpleasant because it is in the denominator. It turns out, however, that there is an easy way around this problem that "bridges the gap" at the characteristic, but unfortunately gives no information about what happens at the characteristic.

The idea is to use the equation $n \cdot P = (n-2) \cdot P + 2 \cdot P$ to go directly from $p-1$ to $p+1$. The two relevant computations are similar to those above although they are longer. ∎

Corollary 7.7 *If n is prime to p, the leading coefficient of g_n is $1/n^2$ and the leading coefficient of h_n is $1/n^3$.*

Proof. The proposition shows that the order of g_n at $\mathcal{O}$ is two, so to compute the leading coefficient we must look at $(x/y)^2 g_n$. But

$$\left(\frac{x}{y}\right)^2 = \frac{x^2}{x^3 + Ax + B} \quad ,$$

which has the same leading coefficient and order at $\mathcal{O}$ as $1/x$. Hence the first part of the corollary follows directly from the proposition. We leave the result about h_n as an exercise. ∎

Remark. This is a result that really depends on the characteristic. If n and p are *not* coprime, then the leading terms are quite different.

8 The Divisor of $g_m - g_n$

We want to compute the divisor of $g_m - g_n$ and relate it to the points of $E[k]$ for appropriate k. In order to compute the multiplicities of the zeros and poles of $g_m - g_n$, we must study the notion of derivative. It is possible to work with the functions $\tilde{g}_n$ and $\tilde{h}_n$ of one variable, so differentiation is just what we expect. It turns out that this is *not* the natural derivative on an elliptic curve, and the computations are unnecessarily complicated because of this. We want to define the derivative of an arbitrary rational function on E, but we must take care that the derivative of the polynomial $y^2 - x^3 - Ax - B$ is zero. If we formally take a derivative, we get

$$2yDy = (3x^2 + A)Dx \quad ,$$

which leads us to make the following definition:

Definition 8.1 Define a derivation D on the field of rational functions $K(E) = K(x, y)$ by setting

$$Dx = 2y$$

and

$$Dy = 3x^2 + A \quad .$$

Extend D to arbitrary rational functions so that the usual rules of differentiation hold.

The following exercises should help to familiarize you with this notion:

Exercise 8.2 (i) Show D is well–defined.

(ii) Suppose f is a nonzero polynomial and $f \neq g^p$ for any polynomial g. Show that the degree of Df (as a function of x and y) is one larger than the degree of f.

(iii) Let r be a rational function. Show that if r is finite at $P \in E$, then so is Dr. (**Hint:** You should handle the case $P = \mathcal{O}$ separately.)

The basic fact we need to know about this derivative is the following:

Proposition 8.3 *Let r be a rational function. If $\mathrm{ord}_p(r) = d \neq 0$ is prime to p, then $\mathrm{ord}_p(Dr) = d - 1$.*

Proof. Suppose u is a uniformizing variable at P, and $r = u^d r_1$ where $r_1(P)$ is finite and nonzero. Then

$$Dr = du^{d-1} Du \cdot r_1 + u^d Dr_1 \quad .$$

If we can show that Du is finite and nonzero at P, then we will have written $Dr = u^{d-1} r_2$ where r_2 is finite and nonzero at P, since the above exercise tells us that Dr_1 must be finite at P.

There are the usual three cases. If P is not $\mathcal{O}$ or of order two, then we can take $u(x, y) = x - x(P)$, so $Du = 2y$, which is finite and nonzero in this case. If P is a point of order two, we take $u = y$, and $Du = 3x^2 + A$. Since E is nonsingular, we know that the derivative of $f(x) = x^3 + Ax + B$ is nonzero at a zero of f. But $f'(x) = 3x^2 + A$ and if P has order two, $x(P) = \omega$, a zero of f. Hence Du is finite and nonzero at P in this case too.

If $P = \mathcal{O}$, we take $u = x/y$, and

$$Du = D(x/y) = \frac{2y^2 - 3x^3 - Ax}{y^2} = \frac{-y^2 + 2Ax + 3B}{y^2} \quad ,$$

which is minus one at $\mathcal{O}$. ∎

Remark. It follows from Proposition 8.3 that if a rational function u satisfies $u(P) = 0$ and $Du(P) \neq 0$, then u is a uniformizing variable at P.

We need the following proposition to compute the multiplicity of the zeros of $g_m - g_n$ and $h_m - h_n$.

Proposition 8.4 *We have $Dg_n = 2nh_n$ and $Dh_n = n(3g_n^2 + A)$.*

Proof. Again the proof is by induction on n. The case $n = 1$ is the definition of D. The case $n = 2$ follows upon differentiating Equation (12) and comparing it with n times Equation (13). For the inductive step, we have the following equations:

$$g_n = -g_{n-1} - x + \left(\frac{h_{n-1} - y}{g_{n-1} - x}\right)^2 \quad , \tag{14}$$

$$h_n = -y - \left(\frac{h_{n-1} - y}{g_{n-1} - x}\right)(g_n - x) \quad , \tag{15}$$

$$(h_{n-1})^2 = (g_{n-1})^3 + Ag_{n-1} + B \quad , \tag{16}$$

and

$$Dh_{n-1} = (n-1)(3{g_{n-1}}^2 + A) \quad . \tag{17}$$

Equations (14) and (15) come from the generic addition formula applied to the equation $n \cdot P = (n-1) \cdot P + P$. Equation (16) simply expresses the fact that $(n-1) \cdot P = (g_{n-1}, h_{n-1})$ is on the curve E, and Equation (17) is the inductive hypothesis.

Now we assume that $Dg_{n-1} = 2(n-1)h_{n-1}$ and differentiate (14) to get

$$\begin{aligned} Dg_n = & - Dg_{n-1} - 2y \\ & + 2\left(\frac{h_{n-1}-y}{g_{n-1}-x}\right)\left[\frac{(g_{n-1}-x)(Dh_{n-1}-Dy)-(h_{n-1}-y)(Dg_{n-1}-2y)}{(g_{n-1}-x)^2}\right] \quad . \end{aligned}$$

Then we use (17) to write the result in terms of powers of g_{n-1} and h_{n-1}. Next we use (16) to eliminate the powers of h_{n-1} greater than one obtaining

$$\begin{aligned} Dg_n = & \frac{1}{(g_{n-1}-x)^3} \cdot \\ & \{-2y + 2[(g_{n-1}-x)(-3x^3 + (n-1)(3{g_{n-1}}^3 + A) - A) \\ & - (h_{n-1}-y)(2(n-1)h_{n-1} - 2y)]\} \\ & - 2(n-1)h_{n-1} \quad . \end{aligned}$$

If we compare the result with nh_n using (15), we will see we get the same thing. ■

This proposition is somewhat striking; it is not a result that was at all obvious from the equation of the curve or the addition formulas. Before we get to the theorem about the divisor of $g_m - g_n$, we need a lemma about translations. This lemma will enable us to use information about the order of g_n at one point in $E[n]$ to get information about the order of g_n at all points of $E[n]$. A similar situation will arise in Section 13.

Lemma 8.5 *Let $P, Q \in E$, and suppose u is a uniformizing variable at P. Then the function $T_Q(u)$ defined by*

$$[T_Q(u)](R) = u(R+Q)$$

is a uniformizing variable at $P - Q$.

Proof. The point here is that T_Q is an automorphism of the field $K(E)$ so we can use $T_{(-Q)}$ to go back. Suppose $T_Q(u)$ is not a uniformizing variable at $P-Q$. Since it clearly has a zero at P_Q, it must have order $m > 0$. This means that T_Q takes a function of order d at P into a function of order md at $P-Q$. But this implies that $T_{(-Q)}$ takes a function of order d at P_Q into a function of order d/m at P, which is absurd. ■

It now follows that if a rational function r has divisor $\sum n(P)\langle P \rangle$, then the function $T_Q(r)$ has divisor $\sum n(P)\langle P - Q \rangle$.

Recall that

$$E[n] = \{P \in E : n \cdot P = \mathcal{O}\} \quad .$$

We write $\langle E[n] \rangle$ to denote the divisor whose nonzero entries are the points of $E[n]$, each with coefficient one.

At this point we begin to get into difficulty if the characteristic is 3. Hence from this point on we assume that the CHARACTERISTIC OF K IS NOT 3.

Theorem 8.6 *Suppose $m > n > 0$ and that $m, n, m-n$, and $m+n$ are all prime to p. Then*

$$\operatorname{div}(g_m - g_n) = \langle E[m+n] \rangle + \langle E[m-n] \rangle - 2\langle E[m] \rangle - 2\langle E[n] \rangle \quad . \tag{18}$$

Proof. There are, as usual, various cases. First consider the points in both $E[n]$ and $E[m]$. By definition they are also in $E[m+n]$ and $E[m-n]$. Hence we must show that $g_m - g_n$ has order $1+1-2-2 = -2$ there. One of these points is $\mathcal{O}$. Proposition 7.6 tells us that both g_m and g_n have poles of multiplicity two there. Further Corollary 7.7 tells us that these poles cannot cancel out since g_m and g_n have different leading coefficients at $\mathcal{O}$, namely $1/m^2$ and $1/n^2$, and it is easy to see that our hypothesis implies that $m^2 \not\equiv n^2 \pmod{p}$. Hence $g_m - g_n$ has a pole of order two at $\mathcal{O}$.

Notice that if $P \in E[n]$, then $T_P(g_n) = g_n$ since $n \cdot (Q+P) = n \cdot Q$. Hence by Lemma 8.5, the order of g_n is the same at all points of $E[n]$. Thus we see that $g_m - g_n$ has order -2 at every point of $E[m] \cap E[n]$ as desired.

Second we consider the points that are in $E[m]$ but not in $E[n]$. These points are *not* in either $E[m+n]$ or $E[m-n]$. We must therefore show that $g_m - g_n$ has order -2 here also. Now g_n has order greater than zero here, and we have seen in the previous case that g_m has order -2 here so this case follows easily.

The third case is the difficult one. Here we consider the points that are neither in $E[m]$ nor $E[n]$. There are three subcases, P in $E[m-n]$ but not in $E[m+n]$, P in $E[m+n]$ but not in $E[m-n]$, and P in both $E[m+n]$ and $E[m-n]$. In each of these subcases it is easy to see that $g_m - g_n$ has a zero at P; the problem is to determine the multiplicities. We will use the derivative for this. By Proposition 8.4, $D(g_m - g_n) = 2mh_m - 2nh_n$.

If P in $E[m-n]$ but not in $E[m+n]$, we have $m \cdot P = n \cdot P \neq -n \cdot P$, and since $P \notin E[m] \cup E[n]$, $m \cdot P \neq \mathcal{O}$ and $n \cdot P \neq \mathcal{O}$. In this case $h_m(P) = h_n(P)$, so $D(g_m - g_n)(P) = 2(m-n)h_m(P)$. Now $m-n$ is prime to p, and $h_m(P) \neq 0$ because $m \cdot P \neq -m \cdot P$ so $m \cdot P$ cannot be a point of order two. Hence $g_m - g_n$ has a simple zero here, which is what we want. The case P in $E[m+n]$ but not in $E[m-n]$ is symmetric and also works out as desired.

On the other hand, in the third subcase, we have both $m \cdot P = -n \cdot P$ and $m \cdot P = n \cdot P$ (and $m \cdot P \neq \mathcal{O}$ and $n \cdot P \neq \mathcal{O}$), and the situation is quite different. This case is equivalent to assuming that $2m \cdot P = 2n \cdot P = \mathcal{O}$. We see that $D(g_m - g_n)(P) = 0$ here, so the multiplicity is at least two. We must look at $DD(g_m - g_n)$. Proposition 8.4 tells us that

$$Dh_n = n(3{g_n}^2 + A) \quad .$$

Since $2n \cdot P = \mathcal{O}$,we see that $n \cdot P$ is a point of order two. Therefore $g_n(P) = \omega$ and $h_n(P) = 0$. Hence

$$DD(g_m - g_n)(P) = (m^2 - n^2)(3\omega^2 + A) \quad ,$$

which is nonzero since $m-n$ and $m+n$ are prime to p, and E is nonsingular. Thus $g_m - g_n$ has a double zero here as desired. ∎

Corollary 8.7 *If n is prime to p, then $E[n]$ has n^2 points.*

Proof. Let d_n be the number of points in $E[n]$. By taking degrees in Equation (18), we get $d_{m+n} + d_{m-n} - 2d_m - 2d_n = 0$. We know that $d_1 = 1$ and $d_2 = 4$. It is then easy to see that $d_n = n^2$ satisfies this recursion.

To see that this solution is unique, it suffices to take $\bar{d}_1 = 0$ and $\bar{d}_2 = 0$, and show that if $\bar{d}_n$ satisfies the recursion, $\bar{d}_n$ must also be 0 for all n prime to p. Let k be prime to p. If we take $m = k - 1$ and $n = 1$ in the recursion, we get $\bar{d}_k = 2\bar{d}_{k-1} - \bar{d}_{k-2}$, which says that $\bar{d}_k = 0$ for $k-2$ and $k-1$ prime to p. Now take $n = 2$ and $m = k - 2$. We get $\bar{d}_k = 2\bar{d}_{k-2} - \bar{d}_{k-4}$, which tells us that $\bar{d}_k = 0$ if $k-4$ and $k-2$ are prime to p. Finally take $n = 3$ and $m = k - 3$ to get $\bar{d}_k = 0$ if $k-3$ and $k-6$ are prime to p.

Suppose $k-1$ is not prime to p. Then $k-2$ must be prime to p, and if $k-4$ were not prime to p, then we would have $p = 3$, which we have excluded.

Suppose $k-2$ is not prime to p. Then $k-3$ must be prime to p, and if $k-6$ were not prime to p, then 4 would have to be a multiple of p, which is also excluded.

Hence as long as k is prime to p, we can find a case, which tells us that $\bar{d}_k = 0$. ∎

Exercise 8.8 Suppose n is prime to p. Show that $E[n]$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. (**Hint:** Use the fundamental theorem of Abelian groups).

Remark. It is a fact (see the last remark of this part) that $E[p]$ is either $\{\mathcal{O}\}$ or $\mathbb{Z}/p\mathbb{Z}$. This shows that multiplication by the characteristic is quite different than multiplication by an integer prime to the characteristic.

9 The Division Polynomials

We would like to define a polynomial ψ_n that has divisor $\langle E[n]\rangle$. By Proposition 6.7, we can do this provided the sum of the points in $E[n]$ is $\mathcal{O}$ and the degree of $\langle E[n]\rangle$ is 0. If $P \in E[n]$ then $-P \in E[n]$, and if P is not a point of order two, P and $-P$ are distinct. Also if P is a point of order two, then all of the points of order two are in $E[n]$, and they all sum to zero. Hence the sum of the points in $E[n]$ is $\mathcal{O}$, but $\deg(\langle E[n]\rangle) = n^2$. Therefore if we let Δ be the divisor $\langle E[n]\rangle - n^2\langle\mathcal{O}\rangle$, the sum of the points in Δ will still be zero, and $\deg(\Delta)$ will be 0 at least if n is prime to p. We will want to be able to compute the ψ_n's inductively so we will need to define them even if n is not prime to p. The way we are going to do this is to define them at first only in characteristic 0, prove what we want, then give a different definition for positive characteristic, and finally show that the results in characteristic zero imply the results in characteristic $p > 0$. Therefore until we say otherwise we assume that the CHARACTERISTIC OF K IS ZERO.

We now know that we can get a polynomial with the correct divisor, but it will not be unique. By Exercise 5.4, if we specify the leading coefficient we can select a unique one.

Definition 9.1 Let ψ_n be the unique polynomial whose divisor is $\Delta = \langle E[n] \rangle - n^2 \langle \mathcal{O} \rangle$ and whose leading coefficient is n.

Remark. Since the coefficient of $\mathcal{O}$ in the divisor Δ is $1 - n^2$, we see that the degree of ψ_n is $n^2 - 1$.

Exercise 9.2 (i) Show that

$$\psi_n{}^2(P) = n^2 \prod_{P' \in E[n] - \mathcal{O}} [x(P) - x(P')] \quad .$$

(**Hint:** Look at divisors and leading coefficients.)

(ii) Suppose n is odd. Show that ψ_n is a function of x alone and that its degree as a function of x is $(n^2 - 1)/2$.

(iii) Suppose n is even. Show that ψ_n is y times a function of x alone, and that the degree of this function of x is $(n^2 - 4)/2$.

The goal of the rest of this section is to show that g_n and h_n can be computed in terms of the ψ_n's and that the ψ_n's satisfy a recursion that allows them to be computed.

Theorem 9.3 *Suppose $m > n > 0$. Then*

$$g_m - g_n = -\frac{\psi_{m+n}\psi_{m-n}}{\psi_m{}^2 \psi_n{}^2} \quad . \tag{19}$$

Proof. By Theorem 8.6,

$$\operatorname{div}(g_m - g_n) = \langle E[m+n] \rangle + \langle E[m-n] \rangle - 2\langle E[m] \rangle - 2\langle E[n] \rangle \quad .$$

By definition,

$$\operatorname{div}\left(\frac{\psi_{m+n}\psi_{m-n}}{\psi_m{}^2 \psi_n{}^2}\right) = \langle E[m+n] \rangle + \langle E[m-n] \rangle - 2\langle E[m] \rangle - 2\langle E[n] \rangle \quad .$$

The above two equations show that the two sides of Equation (19) have the same divisor.

Now g_n has leading coefficient $1/n^2$, while ψ_n has leading coefficient n. A brief computation shows that the two sides of Equation (19) have the same leading coefficient, which proves the theorem. ∎

Corollary 9.4 *For any $P \in E$*

$$g_n(P) = x(n \cdot P) = x(P) - \frac{\psi_{n+1}(P)\psi_{n-1}(P)}{\psi_n(P)^2} \quad . \tag{20}$$

Since $g_1 = x$, the proof is trivial. The next theorem gives us the basic properties of the division polynomials.

Theorem 9.5 *The polynomials ψ_n satisfy the following:*

(o) $\psi_0 = 0$,

(i) $\psi_1 = 1$,

(ii) $\psi_2(P) = 2y$,

(iii) $\psi_3(P) = 3x^4 + 6Ax^2 + 12Bx - A^2$,

(iv) $\psi_4(P) = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$,

(v) *for $m > n > 0$,*

$$\psi_n{}^2\psi_{m+1}\psi_{m-1} - \psi_m{}^2\psi_{n+1}\psi_{n-1} = \psi_{m+n}\psi_{m-n} \quad . \tag{21}$$

Proof. (o) and (i) follow by definition. For (ii), note that $E[2]$ consists of $\mathcal{O}$ and the three points of order two. Also $\mathrm{div}(y) = \langle\omega_1\rangle + \langle\omega_2\rangle + \langle\omega_3\rangle - 3\langle\mathcal{O}\rangle = \langle E[2]\rangle - 4\langle\mathcal{O}\rangle$. Since the leading coefficient of $2y$ is manifestly 2, this proves (ii).

To do (iii), observe that by Corollary 9.4

$$x(2\cdot P) = x(P) - \frac{\psi_3(P)\psi_1(P)}{\psi_2(P)^2} \quad .$$

We know $x(2\cdot P)$ (it is just $g_2(x)$, which is given by Equation (12)), and we also know the other ψ's, so we can solve for ψ_3.

We can do a similar computation for ψ_4, but there is a better way which avoids computing g_3. Observe that a 4-torsion point P is either of order two or four. If P is of order two, then $y(P) = 0$. If P is of order four, then $2\cdot P$ is of order two, so $h_2(P) = 0$. A glance at Equation (13) yields ψ_4.

We have already done the hard part of (v) in Theorem 9.5. We write $g_m - g_n = (g_m - g_1) - (g_n - g_1)$, and using Equation (19) we get

$$-\frac{\psi_{m+n}\psi_{m-n}}{\psi_m{}^2\psi_n{}^2} = x - \frac{\psi_{m+1}\psi_{m-1}}{\psi_m{}^2} - x + \frac{\psi_{n+1}\psi_{n-1}}{\psi_n{}^2} \quad ,$$

which proves the desired result. ∎

Corollary 9.6 *(i) For $k > 2$,*

$$\psi_{2k} = \frac{\psi_k}{2y}(\psi_{k+2}\psi_{k-1}{}^2 - \psi_{k-2}\psi_{k+1}{}^2) \quad .$$

(ii) For $k \geq 2$,

$$\psi_{2k+1} = \psi_{k+2}\psi_k{}^3 - \psi_{k+1}{}^3\psi_{k-1} \quad .$$

Proof. For (i), take $m = k+1$ and $n = k-1$ in Equation (21). For (ii), take $m = k+1$ and $n = k$. ∎

We are left with one loose end to tie up, which we do in the next proposition.

Proposition 9.7 *If $P \in E$ and $n \geq 2$, then*

$$h_n(P) = y(n \cdot P) = \frac{\psi_{n+2}(P)\psi_{n-1}(P)^2 - \psi_{n-2}(P)\psi_{n+1}(P)^2}{4y\psi_n(P)^3} \quad . \tag{22}$$

Proof. The proof is again by induction. The beginning of the induction is easy. For the inductive step, we use

$$h_n = -y - \left(\frac{h_{n-1} - y}{g_{n-1} - x}\right)(g_n - x) \quad .$$

We know h_{n-1} in terms of the ψ's by induction, and we know g_n and g_{n-1} in terms of the ψ's by Corollary 9.4. After plugging these results in the above equation, simplifying and subtracting what we get from what we want, we will be left with showing

$$-\psi_{n-2}{\psi_{n-1}}^2\psi_{n+2} + \psi_{n-3}{\psi_n}^2\psi_{n+1} + {\psi_2}^2{\psi_{n-1}}^3\psi_{n+1} - {\psi_2}^2\psi_{n-2}{\psi_n}^3 = 0 \quad .$$

This will follow by applying Equation (21) separately to the last two terms. ■

We would now like to extend the results of this section to positive characteristic. Our argument is somewhat similar to the one that appears in [3] around page 39. The main idea is to note that the results we want are really polynomial identities in the ring $\mathbb{Z}[A, B, x, y]$, and hence still hold upon reduction mod p. It takes a bit of work to get this all together. From now on we let the CHARACTERISTIC OF K BE ARBITRARY.

We use Theorem 9.5 now to *define* ψ_n.

Definition 9.8 The polynomials ψ_n are the unique polynomials that satisfy the following conditions:

(o) $\psi_0 = 0$,

(i) $\psi_1 = 1$,

(ii) $\psi_2(P) = 2y$,

(iii) $\psi_3(P) = 3x^4 + 6Ax^2 + 12Bx - A^2$,

(iv) $\psi_4(P) = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$,

(v) for $k > 2$,

$$\psi_{2k} = \frac{\psi_k}{2y}(\psi_{k+2}(\psi_{k-1})^2 - \psi_{k-2}(\psi_{k+1})^2) \quad ,$$

and for $k \geq 2$,

$$\psi_{2k+1} = \psi_{k+2}(\psi_k)^3 - (\psi_{k+1})^3\psi_{k-1} \quad . \tag{23}$$

Note that because of Theorem 9.3 and Corollary 9.6, this definition agrees with the one we have already in characteristic zero.

Now consider the field of rational functions in two indeterminates $\mathcal{A}$ and $\mathcal{B}$ over the field of rational numbers. Let E be the elliptic curve over this field with the defining polynomial

$$Y^2 = X^3 + AX + B \quad . \tag{24}$$

In this case we can identify the rational functions on E with the quotient field of the ring $\mathbb{Z}[\mathcal{A}, \mathcal{B}, X, Y]$ subject to the relation (24). We can easily see that in this case the polynomials ψ_k are actually in the ring $\mathbb{Z}[\mathcal{A}, \mathcal{B}, X, Y]$ $/(F(X,Y))$ where $F(X,Y) = Y^2 - X^3 - AX - B$. Now consider a polynomial identity such as (21), which is an identity in the ψ_k's involving only integer coefficients. We have proved this so far only for fields of characteristic zero. However we may now deduce that this identity will hold for the ψ_k's in an arbitrary elliptic curve as follows.

The ring $\mathbb{Z}[\mathcal{A}, \mathcal{B}, X, Y]$ has the property that there is a unique ring homomorphism from it to an arbitrary ring R where $\mathcal{A}$, $\mathcal{B}$, X, Y are mapped to any elements of R. If we map these indeterminates to A, B, x and y in the function field of an arbitrary elliptic curve over any field, then the homomorphism induces a mapping from $\mathbb{Z}[\mathcal{A}, \mathcal{B}, X, Y]/(F(X,Y))$ into the function field of the curve. This mapping will obviously map the ψ's to the ψ's. It then follows that any identity that holds in characteristic zero and therefore in particular in $\mathbb{Z}[\mathcal{A}, \mathcal{B}, X, Y]/(F(X,Y))$ will also hold in any elliptic curve over any field.

We are now going to prove Corollary 9.4 and Proposition 9.7, *i.e.,* the expressions for g_n and h_n in terms of the ψ_n's, in characteristic p.

Theorem 9.9 (i) *ψ_n is not identically zero for all $n > 0$.*

(ii) *g_n satisfies*

$$g_n = x - \frac{\psi_{n+1}\psi_{n-1}}{{\psi_n}^2} \quad . \tag{25}$$

(iii) h_n satisfies

$$h_n = \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}{\psi_{n+1}}^2}{4y{\psi_n}^3} \quad . \tag{26}$$

Proof. It is easily seen that ψ_n is not identically zero for $n \leq 4$. Now assume (25), (26) for $n < m$, and that ψ_n is not identically zero all for $n < m + 1$.

Now assume we are in characteristic zero for a moment. If we take the expression for g_m given by (25), and note that

$$g_m = -g_{m-1} - x + \left(\frac{h_{m-1} - y}{g_{m-1} - x}\right)^2 \quad ,$$

then we can use Equations (25) and (26) for $n = m-1$, (which we know are true in characteristic zero) to eliminate g_{m-1} and h_{m-1}. We thus get an identity in the ψ's alone.

Similarly starting with (23) and using

$$h_m = -y - \left(\frac{h_{m-1} - y}{g_{m-1} - x}\right)(g_m - x) \quad ,$$

we get another identity in the ψ's alone.

What these identities are is not important; what is important is that they are polynomial identities in $\mathbb{Z}[\mathcal{A}, \mathcal{B}, X, Y]/(F(X,Y))$. Hence the preceding argument shows they hold in characteristic p. We would now like to convert these polynomial identities in characteristic p back into Equations (25) and (26). To do this we must divide by ψ_{m-2}, ψ_{m-1}, and ψ_m. Fortunately these are the ψ's that we have assumed are not identically zero in the inductive hypothesis. Hence (25) and (26) for $n = m$ hold in characteristic p.

Now we know that

$$g_m - x = \frac{\psi_{m+1}\psi_{m-1}}{{\psi_m}^2} \quad . \tag{27}$$

By Corollary 7.4, we know that $g_m - x$ is not identically zero. Hence we get that $\psi_{m+1} \neq 0$, which allows us to continue the induction. ∎

Hence we have established Corollary 9.4 and Proposition 9.7 even in characteristic p.

About the only thing left to prove about the ψ_n's is that their divisor is $\langle E[n]\rangle - n^2\langle\mathcal{O}\rangle$, which only holds for n prime to p. We have proved.

$$g_n - x = -\frac{\psi_{n+1}\psi_{n-1}}{{\psi_n}^2} \quad . \tag{28}$$

Since we know that $g_n - x$ only has poles on $E[n]$, we see that ψ_n has zeros on $E[n]$. Now we have to show that these zeros are simple and that there are no others. If n is prime to p, then we know that $\deg(\psi_n) = n^2 - 1$ because it is $n^2 - 1$ in characteristic zero, and if n is prime to p, the leading coefficient, n, does not reduce to zero. Since ψ_n has a pole at $\mathcal{O}$ and zeros on $E[n]$, it cannot have any other zeros because $E[n]$ has n^2 points (counting $\mathcal{O}$). Since the poles of $g_n - x$ on $E[n]$ have multiplicity two, Equation (25) shows that the zeros of ψ_n must be simple. This proves $\mathrm{div}(\psi_n) = \langle E[n]\rangle - n^2\langle\mathcal{O}\rangle$ provided n is prime to p.

If n is not prime to p, we can still say something. Look at Equation (23) for $k = n$:

$$\psi_{2n+1} = \psi_{n+2}{\psi_n}^3 - {\psi_{n+1}}^3\psi_{n-1} \quad . \tag{29}$$

ψ_n must be prime to ψ_{n+1} because otherwise the above equation would imply that ψ_{2n+1} has a triple zero. Since $2n+1$ must be prime to p, this is impossible by the result of the previous paragraph. Similarly by looking at Equation (23)

with $k = n - 1$, we see that ψ_n must be prime to ψ_{n-1}. Hence Equation (25) implies that ψ_n has all of its zeros on $E[n]$ but we do not know they are simple. Thus we have proved.

Proposition 9.10 *If n is prime to p, $div(\psi_n) = \langle E[n]\rangle - n^2\langle \mathcal{O}\rangle$ even in positive characteristics. Even if n is not necessarily prime to p, ψ_n has all of its zeros on $E[n]$.*

Remark. Our final remark concerns $E[p]$. In characteristic zero the leading coefficient of ψ_n is n. Hence in characteristic p the degree of ψ_p is less than $p^2 - 1$. Since the elements of $E[p]$ are all zeros of ψ_p, this says that $E[p]$ cannot have p^2 elements. Since $E[p]$ is a group all of whose elements are p-torsion, $E[p]$ must either be the trivial group or $\mathbb{Z}/p\mathbb{Z}$. It turns out that both cases occur.

Part II – Elliptic Curves over Finite Fields

10 Objective

We let p be a prime, n some integer, $q = p^n$, and $k = \mathrm{GF}(q)$, the field with q elements. Let K be the algebraic closure of k. In this part we are interested in elliptic curves defined over k, so the points of our curve E lie in $K \times K$ and satisfy the equation

$$Y^2 = X^3 + AX + B \tag{30}$$

for some fixed $A, B \in k$. Recall that $(a, b) \in E$ is k-rational if $a, b \in k$, and $E(k)$ is the set of k-rational points of E. We make the convention that $\mathcal{O}$ is k-rational so $E(k)$ itself has the structure of an elliptic curve itself. A natural question to ask is, how many points lie on $E(k)$? Another way of asking the same question is how many solutions does Equation (30) have in k. We will let E_q denote the number of k-rational points on E.

There is an heuristic argument that suggests that E_q is approximately $q + 1$. Write $k^* = \{g, g^2, \ldots, g^{q-1} = 1\}$, so $(k^*)^2 = \{g^2, g^4, \ldots, g^{q-1} = 1\}$, and $|(k^*)^2| = (q-1)/2$. We might, therefore, expect that for about half of the elements $a \in k$, $a^3 + Aa + B$ will be a square. For each such a, there will are two values, namely b and $-b$, with $b^2 = a^3 + Aa + B$. Therefore we might expect roughly $2 \cdot \frac{1}{2}q = q$ finite solutions of (30), and, since $\mathcal{O}$ is k-rational, $q + 1$ solutions altogether. We should remark here that there is no general formula known for E_q and that the best known algorithm ([5]) is somewhat complicated. The main theorem of this part will concern the difference between $q+1$ and E_q.

An important tool in the study of this problem is a rational mapping φ, called the Frobenius mapping. We need a trivial result before defining φ.

Exercise 10.1 If $(a, b) \in E$, then $(a^q, b^q) \in E$.

Definition 10.2 The Frobenius mapping $\varphi : E \to E$ is defined by $\varphi(a, b) = (a^q, b^q)$.

Exercise 10.3 Show that $(a, b) \in E$ is k-rational if and only if $\varphi(a, b) = (a, b)$. (**Hint:** Look at the zeros of $x^q - x$.)

We state here the Main Theorem to be proved in the course of this part. It was conjectured by E. Artin and proved by H. Hasse. Generalizations of related results are known as the Weil Conjectures.

Main Theorem (Hasse): *Let E be an elliptic curve defined over $k = \mathrm{GF}(q)$, and $t = q + 1 - E_q$. Then*

(i) $\varphi \circ \varphi - [t] \circ \varphi + [q] = \mathcal{O}_M$ *and*

(ii) $|t| \leq 2\sqrt{q}$,

where $[m]$ is the rational mapping $P \mapsto m \cdot P$.

Although the Main Theorem concerns elliptic curves over finite fields, many of the results leading to it are valid over any field. Only the results involving the Frobenius mapping require k to be finite. Therefore in the rest of this part, unless we say otherwise, k will be an arbitrary field of characteristic $\neq 2$ or 3, and K will be its algebraic closure.

11 The Ramification Index

This section is concerned with general rational mappings and contains results that could well have been done in Part I.

Lemma 11.1 *Suppose r is a nonconstant rational function on E. Then r takes on all values (including $\mathcal{O}$).*

Proof. Lemma 4.8 and Theorem 4.6 showed that r must have at least one zero and one pole. The lemma follows if we apply this result to the function $r - a$ for an arbitrary $a \in K$. ∎

Proposition 11.2 *A nonconstant rational mapping $F : E \to E$ is onto.*

Proof. Let $F = (r, s)$ where r and s are rational functions. If r were constant, then s would have only finitely many values, and hence by the lemma, s would be constant. Then F would be constant, which is a contradiction. Similarly we can see that s is not constant.

It follows that both r and s have poles, but these must occur simultaneously since $(r(P), s(P))$ is always on the curve. Thus F takes the value $\mathcal{O}$. To see that F takes the value $P \in E$, apply this result to the function $Q \mapsto F(Q) - P$. ∎

Now we define the ramification index of a nonconstant rational mapping $F : E \to E$ at a point. Let $P \in E$ and u be a uniformizing variable at $F(P)$. If $u \circ F$ were identically zero, then u would be zero on $F(E)$. Since the previous proposition shows $F(E) = E$, this would imply that u would be identically zero itself, which cannot be. Thus $u \circ F$ is zero at P, but not identically zero on E.

Definition 11.3 The *ramification index of F at P* is defined by

$$e_F(P) = \mathrm{ord}_p(u \circ F) \quad ,$$

where u is a uniformizing variable at $F(P)$.

It is easily verified that $e_F(P)$ is independent of the choice of u. Note that $e_F(P) \geq 1$. The principal property of the ramification index is the following:

Proposition 11.4 *Suppose that r is a nonzero rational function on E and F is a nonconstant rational mapping. Let $P \in E$. Then*

$$\mathrm{ord}_p(r \circ F) = [\mathrm{ord}_{F(P)} r] \cdot [e_F(P)] \quad .$$

Exercise 11.5 Prove this proposition. (**Hint:** Take uniformizing variables at P and $F(P)$ and write everything out.)

We now use the ramification index to investigate the effect of a rational mapping on divisors.

Definition 11.6 Suppose that F is a nonconstant rational mapping. We define $F^* : \mathrm{Div}(E) \to \mathrm{Div}(E)$ to be the homomorphism with

$$F^*(\langle Q \rangle) = \sum_{F(P)=Q} e_F(P)\langle P \rangle \quad .$$

Proposition 11.7 *F^* is one-to-one.*

Exercise 11.8 Prove this proposition.

The preceding definition is made so that the following is true:

Proposition 11.9 *Suppose that F is a nonconstant rational mapping and that r is a nonzero rational function. Then*

$$\mathrm{div}(r \circ F) = F^*(\mathrm{div}(r)) \quad .$$

Proof. Like most of the proofs in this part, this one is a straightforward computation.

$$\begin{aligned}
\mathrm{div}(r \circ F) &= \sum_P \mathrm{ord}_p(r \circ F)\langle P \rangle \\
&= \sum_P [\mathrm{ord}_{F(P)} r] \cdot [e_F(P)]\langle P \rangle \\
&= \sum_Q \mathrm{ord}_Q(r) \cdot \sum_{F(P)=Q} e_F(P)\langle P \rangle \\
&= \sum_Q [\mathrm{ord}_Q r] \cdot F^*(\langle Q \rangle) \\
&= F^*(\mathrm{div}(r)) \quad .
\end{aligned}$$

■

We also need

Lemma 11.10 *Suppose that F_1 and F_2 are nonconstant rational mappings. Then $F_1 \circ F_2$ is nonconstant and for $P \in E$,*

$$e_{F_1 \circ F_2}(P) = e_{F_1}(F_2(P)) \cdot e_{F_2}(P) \quad .$$

Proof. Since rational mappings are onto, it follows that $F_1 \circ F_2$ is nonconstant.

Let u be a uniformizer at $F_1(F_2(P))$. Then

$$\begin{aligned}
e_{F_1 \circ F_2}(P) =& \mathrm{ord}_p(u \circ F_1 \circ F_2) \\
=& \left[\mathrm{ord}_{F_2(P)}(u \circ F_1)\right] e_{F_2}(P) \\
=& e_{F_1}(F_2(P)) \cdot e_{F_2}(P) \quad .
\end{aligned}$$

■

The next proposition justifies the use of the upper star.

Proposition 11.11 *Suppose that F_1 and F_2 are nonconstant rational mappings. Then*

$$(F_1 \circ F_2)^* = F_2^* \circ F_1^* \quad .$$

Proof. The proof is again a routine computation.

$$\begin{aligned} F_2^* \circ F_1^*(\langle R \rangle) &= F_2^* \left(\sum_{F_1(Q)=R} e_{F_1}(Q)\langle Q \rangle \right) \\ &= \sum_{F_1(Q)=R} e_{F_1}(Q) \cdot \sum_{F_2(P)=Q} e_{F_2}(P)\langle P \rangle \\ &= \sum_{F_1 \circ F_2(P)=R} e_{F_1}(F_2(P)) \cdot e_{F_2}(P)\langle P \rangle \\ &= \sum_{F_1 \circ F_2(P)=R} e_{F_1 \circ F_2}(P)\langle P \rangle \\ &= (F_1 \circ F_2)^*(\langle R \rangle) \quad . \end{aligned}$$

■

12 Endomorphisms

We now study a special class of rational mappings that contains the Frobenius mapping.

Definition 12.1 A rational mapping from E to E that is also a group homomorphism is called an *endomorphism*. These mappings form a group, which we denote by $\mathrm{End}(E)$.

Remark. We could also study rational mappings between different elliptic curves and, in particular, those which are homomorphisms, but we do not need them for proving the Main Theorem. Many of the ideas presented here can be easily extended to homomorphisms between elliptic curves.

Example 12.2 (i) The mapping $[m]$ defined by $[m](P) = m \cdot P$ is clearly an endomorphism.

(ii) The Frobenius mapping is an endomorphism.

The following is a striking and important result:

Theorem 12.3 *Suppose $\alpha : E \to E$ is a nonzero endomorphism. Then the ramification index $e_\alpha(P)$ is independent of P.*

Proof. For $P \in E$, let $a\mathcal{T}_P$ be the translation sending Q to $Q + P$. Since α is an endomorphism, $\alpha \circ a\mathcal{T}_P = a\mathcal{T}_{\alpha(P)} \circ \alpha$. Applying Lemma 11.10 to both sides of this equation at the point $\mathcal{O}$ yields

$$e_\alpha(P) \cdot e_{a\mathcal{T}_P}(\mathcal{O}) = e_{a\mathcal{T}_{\alpha(P)}}(\alpha(P)) \cdot e_\alpha(\mathcal{O}) \quad .$$

But it is easily seen from Lemma 8.5 that a translation has ramification index one at every point. Hence $e_\alpha(P) = e_\alpha(\mathcal{O})$. ∎

If α is an endomorphism, we denote by e_α the constant value of $e_\alpha(P)$ for $P \in E$. Now we show how to find e_α in the cases of interest.

Lemma 12.4 *Let m be any integer, r any rational function, and D the derivation of Section 8. Then*

$$D(r \circ [m]) = (m \cdot Dr) \circ [m] \quad .$$

Proof. This is obvious for $m = 0$. If $r = x$, then $r \circ [m] = g_m$, and the result follows from Proposition 8.4. Similarly if $r = y$, we are done. One checks immediately that the set of those rational functions for which the lemma holds is closed under field operations $(+, -, \times, \text{div})$. This proves the lemma for $m \geq 0$. The case $m = -1$ is easily verified directly.

Now take $m \geq 0$. We get

$$\begin{aligned} D(f \circ [-m]) &= D(f \circ [m] \circ [-1]) \\ &= -D(f \circ [m]) \circ [-1] \\ &= (-m)Df \circ [-m] \quad . \end{aligned}$$

∎

Proposition 12.5 *Suppose that E is defined over $k = \mathrm{GF}(q)$ and that φ is the Frobenius mapping. Then $e_\varphi = q$.*

Proof. We know that $e_\varphi = e_\varphi(\mathcal{O})$. Since $u = x/y$ is a uniformizing variable at $\mathcal{O}$, $u \circ \varphi = u^q$, and the result follows from the definition of $e_\varphi(\mathcal{O})$. ∎

Definition 12.6 Let $\alpha : E \to E$ be an endomorphism. If $e_\alpha = 1$, we say α is *separable*. If $e_\alpha > 1$, we say α is *inseparable*.

Remark. Let $F : E \to E$ be a rational function. We can define a map $F^* : K(E) \to K(E)$ by $F^*(r) = r \circ F$. Then $F^*(K(E))$ will be some subfield of $K(E)$. If F is a separable (respectively inseparable) endomorphism, then $K(E)$ is a separable (respectively inseparable) extension of $F^*(K(E))$.

The next result that we need is that the set of separable endomorphisms is closed under addition, but it takes a little work to get to it.

Lemma 12.7 *Suppose that r is a rational function of the single variable x and $r' = 0$ where r' is the usual derivative. Then $r(x) = \tilde{r}(x^p)$ for some rational function $\tilde{r}$.*

Proof. This is obvious for polynomials. Write $r = f/g$ with f and g relatively prime polynomials of the single variable x. Then $r' = 0$ implies $f'g = g'f$, but since f and g are relatively prime, we have $f|f'$ and $g|g'$. Hence f' and g' are zero, and f and g are functions of x^p. ∎

Proposition 12.8 *Suppose r is a rational function on E and $Dr = 0$. Then there is a rational function $\tilde{r}$ with $r(x,y) = \tilde{r}(x^p, y^p)$.*

Proof. First note that

$$y^p = y\left(y^2\right)^{\frac{p-1}{2}} = y \cdot s(x)^{\frac{p-1}{2}}$$

where $s(x) = x^3 + Ax + B$. Therefore r has a unique representation as

$$r(x,y) = u(x) + y^p v(x) \quad ,$$

where u and v are rational functions of x alone. If $Dr = 0$, we have

$$[u'(x) + y^p v'(x)] \cdot 2y = 0 \quad .$$

It follows that $u' = v' = 0$, and our result then follows from the previous lemma. ∎

Proposition 12.9 *Suppose α is an endomorphism. Then α is inseparable if and only if $D(r \circ \alpha) = 0$ for all rational functions r.*

Proof. If $D(r \circ \alpha) = 0$ for all rational functions r, then this is true in particular when $r = u$ is a uniformizing variable at $\alpha(P)$ for some $P \in E$. Hence $D(u \circ \alpha) = 0$, and by the previous proposition, $u \circ \alpha$ is a function of x^p and y^p, and therefore must have order > 1 at P. This implies $e_\alpha > 1$.

On the other hand, suppose there is a rational function r and a point $P \in E$ with

$$[D(r \circ \alpha)](P) \neq 0 \quad .$$

Let $w = r - r(\alpha(P))$. Then $w \circ \alpha(P) = 0$ and

$$[D(w \circ \alpha)](P) = [D(r \circ \alpha)](P) \neq 0 \quad ,$$

so $w \circ \alpha$ has a zero of multiplicity one at P. Thus

$$1 = \mathrm{ord}_p(w \circ \alpha) = \left[\mathrm{ord}_{\alpha(P)} q\right] \cdot e_\alpha$$

by Proposition 11.4, and we see that $e_\alpha = 1$. ∎

Corollary 12.10 *An endomorphism α is inseparable if and only if*

$$\alpha(x,y) = (u(x^p, y^p), v(x^p, y^p))$$

for rational functions u and v.

This follows immediately from the two previous propositions.

Corollary 12.11 *If m is any integer prime to p, then $[m]$ is a separable endomorphism.*

Proof. Let $P \in E$ and let u be a uniformizer at $m \cdot P$. Then by Lemma 12.4,

$$\{D(u \circ [m])\}(P) = \{m \cdot Du\}(m \cdot P) \quad .$$

The result then follows from the proposition. ■

Proposition 12.12 *If α and β are inseparable endomorphisms, then so is $\alpha+\beta$.*

This follows immediately from Corollary 12.10.

Proposition 12.13 *Suppose that E is defined over $k = \mathrm{GF}(q)$ and m and n are integers with m prime to p. If φ is the Frobenius endomorphism, then $[m]+[n]\circ\varphi$ is separable.*

Proof. Let $\alpha = [m] + [n] \circ \varphi$. If α is inseparable, then since $[m] = \alpha - [n] \circ \varphi$, [m] would be the sum of two inseparable endomorphisms. The previous proposition then implies that $[m]$ would be inseparable, which contradicts Corollary 12.11. ■

Recall that the kernel of an endomorphism α is $\{P \in E : \alpha(P) = \mathcal{O}\}$.

Definition 12.14 Suppose that α is a nonzero endomorphism. Let $|\ker\ \alpha|$ denote the number of elements in the kernel of α. We define the *degree* of α by

$$\deg\alpha = |\ker\ \alpha| \cdot e_\alpha \quad .$$

Remark. This is not the usual way the degree of a mapping is defined. For a rational mapping $F : E \to E$, we have seen that $F^*(K(E))$ is a subfield of $K(E)$ (see the previous remark). It turns out that $K(E)$ is a finite-dimensional vector space over $F^*(K(E))$, and the dimension of $K(E)$ over $F^*(K(E))$ is the usual definition of the degree of F. This definition agrees with ours in the case of an endomorphism. These matters are discussed in more generality around page 76 in [6], where an endomorphism is called an isogeny. Since we do not need these more general notions, we omit them.

Exercise 12.15 (i) If m is prime to p, $\deg([m]) = m^2$.

(ii) If E is defined over $\mathrm{GF}(q)$, then the degree of the Frobenius endomorphism is q.

(iii) If α and β are nonconstant endomorphisms, then

$$\deg(\alpha \circ \beta) = (\deg\alpha) \cdot (\deg\beta) \quad .$$

(iv) If α is a nonconstant endomorphism and $\Delta \in \mathrm{Div}(E)$, then

$$\deg(\alpha^*(\Delta)) = (\deg\alpha) \cdot (\deg\Delta) \quad .$$

There is another result about α^* that is special to endomorphisms. Recall the map sum:$\mathrm{Div}(E) \to E$, which takes the divisor $\sum n(P)\langle P\rangle$ into the point $\sum n(P) \cdot P$.

Proposition 12.16 *Let α be a nonzero endomorphism. For $P \in E$, pick P_0 with $\alpha(P_0) = P$. Then*

$$\mathrm{sum}\,[\alpha^*(\langle P\rangle) - \alpha^*(\langle\mathcal{O}\rangle)] = (\deg\alpha) \cdot P_0 \quad .$$

Proof. We have

$$\alpha^*(\langle P\rangle) = e_\alpha \sum_{\alpha(Q)=P} \langle Q\rangle = e_\alpha \sum_{\alpha(R)=\mathcal{O}} \langle P_0 + R\rangle \quad .$$

Hence

$$\begin{aligned}
\mathrm{sum}\,[\alpha^*(\langle P\rangle) - \alpha^*(\langle\mathcal{O}\rangle)] =& \mathrm{sum}\left[e_\alpha \sum_{\alpha(R)=\mathcal{O}} (\langle P_0 + R\rangle - \langle R\rangle)\right] \\
=& e_\alpha \sum_{\alpha(R)=\mathcal{O}} P_0 \\
=& e_\alpha |\ker\,\alpha| P_0 \\
=& (\deg\alpha) P_0 \quad .
\end{aligned}$$

■

13 The Weil Pairing

Another important tool in our proof of the main theorem is the Weil pairing, which is a map from $E[m] \times E[m]$ to K. In order to define it, we will make frequent use of the result that a divisor Δ is principal if and only if $\deg(\Delta) = 0$ and $\mathrm{sum}(\Delta) = \mathcal{O}$.

Fix an integer m prime to p.

Lemma 13.1 *For $T \in E[m]$, the divisor $[m]^*(\langle T\rangle - \langle\mathcal{O}\rangle)$ is principal.*

Proof. Since $\deg(\langle T\rangle - \langle\mathcal{O}\rangle) = 0$,

$$\deg([m]^*(\langle T\rangle - \langle\mathcal{O}\rangle)) = \deg[m] \cdot \deg\,(\langle T\rangle - \langle\mathcal{O}\rangle) = 0$$

by (iv) of Exercise 12.15.

Now pick $T_0 \in E$ with $m \cdot T_0 = T$. Then $\mathrm{sum}([m]^*(\langle T\rangle - \langle\mathcal{O}\rangle)) = m^2 \cdot T_0$ by Proposition 12.16, and $m^2 \cdot T_0 = m \cdot T = \mathcal{O}$. ■

Let g_T be a rational function with

$$\mathrm{div}(g_T) = [m]^*(\langle T\rangle - \langle \mathcal{O}\rangle) \quad .$$

Although g_T is not unique, it *is* unique up to a constant multiple.

Let $a\mathcal{T}_P$ be translation by P, *i.e.* $a\mathcal{T}_P(Q) = Q + P$.

Exercise 13.2 Show that $a\mathcal{T}_P^*(\langle Q\rangle) = \langle Q - P\rangle$.

Lemma 13.3 *Suppose that $S, T \in E[m]$. Then*

$$\mathrm{div}(g_T \circ a\mathcal{T}_S) = \mathrm{div}(g_T) \quad .$$

Proof. Since $S \in E[m]$, $[m] \circ a\mathcal{T}_S = [m]$. Hence using Propositions 11.9 and 11.11, we get

$$\begin{aligned}\mathrm{div}(g_T \circ a\mathcal{T}_S) =& a\mathcal{T}_S^* \circ [m]^*(\langle T\rangle - \langle \mathcal{O}\rangle)\\ =&([m] \circ a\mathcal{T}_S)^*(\langle T\rangle - \langle \mathcal{O}\rangle)\\ =&[m]^*(\langle T\rangle - \langle \mathcal{O}\rangle)\\ =&\mathrm{div}(g_T) \quad .\end{aligned}$$

■

The next proposition provides the basis for the definition of the Weil pairing.

Proposition 13.4 *Suppose $S, T \in E[m]$. Then the function $(g_T \circ a\mathcal{T}_S)/g_T$ is constant, and its value is an m^{th} root of unity in K and is independent of the choice of the function g_T.*

Proof. Since g_T is unique up to a constant multiple, it is clear that $(g_T \circ a\mathcal{T}_S)/g_T$ does not depend on the choice of g_T.

By the lemma, there is an element $\zeta \in K$ such that $g_T \circ a\mathcal{T}_S = \zeta g_T$. Composing this equation repeatedly with $a\mathcal{T}_S$, we see that

$$g_T \circ a\mathcal{T}_S{}^i = \zeta^i g_T \quad .$$

Taking $i = m$, we see that $\zeta^m = 1$. ■

Definition 13.5 Let $S, T \in E[m]$, and let μ_m be the group of m^{th} roots of unity in K. Then the mapping from $E[m] \times E[m]$ to μ_m that sends (S, T) into $(g_T \circ a\mathcal{T}_S)/g_T$ is called the *Weil pairing* and is denoted by w, *i.e.,*

$$w(S, T) = \frac{g_T \circ a\mathcal{T}_S}{g_T} \quad .$$

We summarize the properties of the Weil pairing in the following theorem:

Theorem 13.6 *Let $S_1, S_2, S, T_1, T_2, T \in E[m]$. Then the Weil pairing satisfies the following conditions:*

(i) $w(S_1 + S_2, T) = w(S_1, T) \cdot w(S_2, T)$.

(ii) $w(S, T_1 + T_2) = w(S, T_1) \cdot w(S, T_2)$.

(iii) $w(T, T) = 1$.

(iv) *If* $w(S, T) = 1$ *for all* $S \in E[m]$, *then* $T = \mathcal{O}$.

(v) *If* α *is any endomorphism, then*

$$w(\alpha(S), \alpha(T)) = w(S, T)^{\deg \alpha} \quad .$$

Proof.

(i) This is a straightforward computation.

$$\begin{aligned} w(S_1 + S_2, T) &= \frac{g_T \circ a\mathcal{T}_{S_1+S_2}}{g_T} \\ &= \frac{g_T \circ a\mathcal{T}_{S_1} \circ a\mathcal{T}_{S_2}}{g_T} \\ &= \left(\frac{g_T \circ a\mathcal{T}_{S_2}}{g_T}\right) \circ a\mathcal{T}_{S_1} \cdot \frac{g_T \circ a\mathcal{T}_{S_1}}{g_T} \\ &= w(S_2, T) \cdot w(S_1, T) \quad . \end{aligned}$$

The last equality follows because $(g_T \circ a\mathcal{T}_{S_2})/g_T$ is constant so it has the same value at $S_1 + P$ as at P.

(ii) First note that

$$\operatorname{div}\left(\frac{g_{T_1+T_2}}{g_{T_1} \cdot g_{T_2}}\right) = [m]^*(\langle T_1 + T_2\rangle - \langle T_1\rangle - \langle T_2\rangle + \langle \mathcal{O}\rangle) \quad .$$

Now $\langle T_1 + T_2\rangle - \langle T_1\rangle - \langle T_2\rangle + \langle \mathcal{O}\rangle$ is clearly principal. Let h be a function with this divisor, so

$$\operatorname{div}\left(\frac{g_{T_1+T_2}}{g_{T_1} \cdot g_{T_2}}\right) = [m]^*(\operatorname{div}(h)) = \operatorname{div}(h \circ [m]) \quad ,$$

and we see that

$$\frac{g_{T_1+T_2}}{g_{T_1} \cdot g_{T_2}} = c \cdot h \circ [m]$$

for some $c \in K$. Hence if $S \in E[m]$,

$$\frac{g_{T_1+T_2}}{g_{T_1} \cdot g_{T_2}} \circ a\mathcal{T}_S(P) = (c \cdot h \circ [m])(P + S) = (c \cdot h \circ [m])(P) \quad ,$$

i.e., $\frac{g_{T_1+T_2}}{g_{T_1}\cdot g_{T_2}}$ is invariant under translation by elements of $E[m]$. Hence

$$\begin{aligned} w(S,T_1+T_2) &= \frac{g_{T_1+T_2}\circ a\mathcal{T}_S}{g_{T_1+T_2}} \\ &= \frac{g_{T_1+T_2}\circ a\mathcal{T}_S}{(g_{T_1}\circ a\mathcal{T}_S)(g_{T_2}\circ a\mathcal{T}_S)}\cdot\frac{(g_{T_1}\circ a\mathcal{T}_S)(g_{T_2}\circ a\mathcal{T}_S)}{g_{T_1+T_2}} \\ &= \frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}}\cdot\frac{(g_{T_1}\circ a\mathcal{T}_S)(g_{T_2}\circ a\mathcal{T}_S)}{g_{T_1+T_2}} \\ &= \frac{g_{T_1}\circ a\mathcal{T}_S}{g_{T_1}}\cdot\frac{g_{T_2}\circ a\mathcal{T}_S}{g_{T_2}} \\ &= w(S,T_1)\cdot w(S,T_2) \end{aligned}$$

as desired.

(iii) Pick T_0 with $m\cdot T_0 = T$. Then using Propositions 11.9 and 11.11 and Exercise 13.2, we get

$$\begin{aligned} \mathrm{div}(g_T\circ a\mathcal{T}_{i\cdot T_0}) &= a\mathcal{T}^*_{i\cdot T_0}(\mathrm{div}g_T) \\ &= a\mathcal{T}^*_{i\cdot T_0}\circ[m]^*(\langle T\rangle-\langle\mathcal{O}\rangle) \\ &= ([m]\circ a\mathcal{T}_{i\cdot T_0})^*(\langle T\rangle-\langle\mathcal{O}\rangle) \\ &= (a\mathcal{T}_{i\cdot T}\circ[m])^*(\langle T\rangle-\langle\mathcal{O}\rangle) \\ &= [m]^*\circ a\mathcal{T}^*_{i\cdot T}(\langle T\rangle-\langle\mathcal{O}\rangle) \\ &= [m]^*(\langle(1-i)\cdot T\rangle-\langle -i\cdot T\rangle) \quad . \end{aligned}$$

It follows that the divisor of

$$G = g_T\cdot(g_T\circ a\mathcal{T}_{T_0})\cdot(g_T\circ a\mathcal{T}_{2\cdot T_0})\cdots(g_T\circ a\mathcal{T}_{(m-1)\cdot T_0})$$

is

$$\begin{aligned} [m]^*[(\langle T\rangle-\langle\mathcal{O}\rangle)+(\langle\mathcal{O}\rangle-\langle -T\rangle)+(\langle -T\rangle-\langle -2\cdot T\rangle) \\ +\cdots+(\langle(2-m)\cdot T\rangle-\langle(1-m)\cdot T\rangle)] \quad , \end{aligned}$$

which is zero since $T\in E[m]$. Therefore G is a constant. Clearly, if we compose with $a\mathcal{T}_{T_0}$ again, we get the same constant. Hence

$$g_T\cdot(g_T\circ a\mathcal{T}_{T_0})\cdots(g_T\circ a\mathcal{T}_{(m-1)\cdot T_0}) = (g_T\circ a\mathcal{T}_{T_0})\cdot(g_T\circ a\mathcal{T}_{2\cdot T_0})\cdots(g_T\circ a\mathcal{T}_{m\cdot T_0}) \quad ,$$

so after cancelling, we get

$$g_T = g_T\circ a\mathcal{T}_{m\cdot T_0} = g_T a\mathcal{T}_T \quad .$$

Thus $w(T,T) = g_T\circ a\mathcal{T}_T/g_T = 1$.

(iv) Suppose that $T\in E[m]$ and $w(S,T)=1$ for all $S\in E[m]$. This means that $g_T\circ a\mathcal{T}_S = g_T$ for all $S\in E[m]$, *i.e.*, g_T is invariant under translation by elements of $E[m]$. We now use the following lemma whose proof will be given later:

Lemma 13.7 *Suppose that r is a rational function on E that is invariant under translation by elements of $E[m]$. Then $r = t \circ [m]$ for some rational function t.*

So now we see that $g_T = h \circ [m]$ for some rational function h. But then

$$[m]^*(\mathrm{div}(h)) = \mathrm{div}(g_T) = [m]^*(\langle T \rangle - \langle \mathcal{O} \rangle) \quad .$$

By Proposition 11.7, we get $\langle T \rangle - \langle \mathcal{O} \rangle = \mathrm{div}(h)$ is a principal divisor. Lemma 4.8 then tells us that T must be $\mathcal{O}$.

(v) We need to show that

$$\left(\frac{g_T \circ a\mathcal{T}_S}{g_T} \right)^{\deg \alpha} = \frac{g_{\alpha(T)} \circ a\mathcal{T}_{\alpha(S)}}{g_{\alpha(T)}} \quad .$$

But $a\mathcal{T}_{\alpha(S)} \circ \alpha = \alpha \circ a\mathcal{T}_S$, so if we compose the right side of the above equation with α leaving its constant value unchanged, we obtain

$$\frac{g_{\alpha(T)} \circ \alpha \circ a\mathcal{T}_S}{g_{\alpha(T)} \circ \alpha} \quad .$$

Rewriting what we want to prove, we get

$$\frac{{g_T}^{\deg \alpha} \circ a\mathcal{T}_S}{{g_T}^{\deg \alpha}} = \frac{g_{\alpha(T)} \circ \alpha \circ a\mathcal{T}_S}{g_{\alpha(T)} \circ \alpha} \quad ,$$

which is equivalent to showing

$$\left(\frac{g_{\alpha(T)} \circ \alpha}{{g_T}^{\deg \alpha}} \right) \circ a\mathcal{T}_S = \frac{g_{\alpha(T)} \circ \alpha}{{g_T}^{\deg \alpha}} \quad ,$$

i.e., we must show that

$$\frac{g_{\alpha(T)} \circ \alpha}{{g_T}^{\deg \alpha}}$$

is invariant under translation by elements of $E[m]$.

Since α is an endomorphism, α commutes with $[m]$, and thus α^* commutes with $[m]^*$, so

$$\begin{aligned} \mathrm{div}\left(\frac{g_{\alpha(T)} \circ \alpha}{{g_T}^{\deg \alpha}} \right) &= \alpha^* \circ [m]^*(\langle \alpha(T) \rangle - \langle \mathcal{O} \rangle) - \deg(\alpha) \cdot [m]^*(\langle T \rangle - \langle \mathcal{O} \rangle) \\ &= [m]^* \left[\alpha^* \left(\langle \alpha(T) \rangle - \langle \mathcal{O} \rangle \right) - \deg(\alpha) \cdot (\langle T \rangle - \langle \mathcal{O} \rangle) \right] . \end{aligned}$$

We show that the divisor in square brackets is principal. Since

$$\deg(\alpha^*(\Delta)) = \deg\alpha \cdot \deg\Delta \quad ,$$

it follows that the degree of the divisor in question is zero. By Proposition 12.16,

$$\mathrm{sum}\left(\alpha^* \left(\langle \alpha(T) \rangle - \langle \mathcal{O} \rangle \right) \right) = \deg(\alpha) \cdot T \quad ,$$

which cancels sum applied to the second term. Thus we have

$$\operatorname{div}\left(\frac{g_{\alpha(T)} \circ \alpha}{{g_T}^{\deg\alpha}}\right) = [m]^*(\operatorname{div}(h)) = \operatorname{div}(h \circ [m])$$

for some rational function h. It follows that

$$\frac{g_{\alpha(T)} \circ \alpha}{{g_T}^{\deg\alpha}}$$

is invariant under translation by elements of $E[m]$ as desired. ∎

Now we give the proof of Lemma 13.7, which turns out to be surprisingly nontrivial.

Proof. Let H be the field of all rational functions on E that are invariant under translation by elements of $E[m]$. Let

$$J = \{g \circ [m] : g \in K(E)\} \quad .$$

Then we certainly have

$$J \subset H \subset K(E) \quad .$$

We can consider each of these fields as a vector space over its subfield. Since H is the fixed field of a group of m^2 automorphisms ($E[m]$), Galois theory tells us the dimension of $K(E)$ over H is precisely m^2. We will show that $K(E)$ has dimension $\leq m^2$ when regarded as a vector space over J. This will show that $J = H$, and the lemma will follow.

Consider $J(x)$, the subfield of $K(E)$ generated by J and x. Recall the functions g_m and h_m from Part I. Since $g_m = x \circ [m]$ and $h_m = y \circ [m]$, we have $g_m, h_m \in J$. (In fact, J is generated by g_m and h_m.) By Exercise 7.5, $h_m = y\tilde{h}_m$ where $\tilde{h}_m$ is a function of x alone. Hence $y = h_m/\tilde{h}_m \in J(x)$. Hence $K(E) = J(x)$.

Now if we can show that x satisfies a polynomial in $J[X]$ of degree m^2, we will be done. Recall Equation (25),

$$g_m = x - \frac{\psi_{m-1}\psi_{m+1}}{{\psi_m}^2},$$

or

$$x{\psi_m}^2 - \psi_{m-1}\psi_{m+1} - {\psi_m}^2 g_m = 0 \quad .$$

It follows from Exercise 9.2 (ii) and (iii) that ${\psi_m}^2$ and $\psi_{m-1}\psi_{m+1}$ can be written as polynomials in x alone of degree (in x) $m^2 - 1$ and m^2 respectively. Furthermore, since the leading coefficient of ψ_n is n, the coefficient of x^{m^2} in $x{\psi_m}^2 - \psi_{m-1}\psi_{m+1}$ is $m^2 - (m+1)(m-1) = 1$. Hence x satisfies the polynomial of degree m^2

$$X{\psi_m}^2(X) - \psi_{m-1}(X)\psi_{m+1}(X) - g_m{\psi_m}^2(X) = 0$$

in $J[X]$. ∎

We now give some corollaries of the theorem.

Corollary 13.8 *For $S, T \in E[m]$, $w(S,T) = w(T,S)^{-1}$.*

Proof. This follows from

$$w(S+T,S+T)=1, w(S,S)=1, w(T,T)=1 \quad ,$$

and (i) and (ii) of the theorem. ∎

Remark. If m is not prime, then $\mathbb{Z}/m\mathbb{Z}$ is not a field, and $E[m]$ is not a vector space. $E[m]$ is, however, a free module of rank two over $\mathbb{Z}/m\mathbb{Z}$, so we can do linear algebra there.

Corollary 13.9 *Let T_1 and T_2 be a basis for $E[m]$ as a free module over $\mathbb{Z}/m\mathbb{Z}$. Then $w(T_1,T_2)$ is a primitive m^{th} root of unity.*

Proof. Suppose $w(T_1,T_2)^n = 1$. Then $w(nT_1,T_2) = 1$. It then follows that $w(nT_1, c_1T_1 + c_2T_2) = 1$ for all $c_1, c_2 \in \mathbb{Z}$ from which we may conclude that $nT_1 = \mathcal{O}$ and m divides n. ∎

As our first application of the Weil pairing we present the following:

Theorem 13.10 *Suppose that α is a nonzero endomorphism. Then $\alpha(E[m]) \subset E[m]$. Furthermore, the determinant of α on $E[m]$ is $\deg(\alpha)$ (mod m).*

Proof. Let T_1 and T_2 be a basis for $E[m]$ over $\mathbb{Z}/m\mathbb{Z}$. Then for suitable integers (mod m) $a_{i,j}$ $(i,j=1,2)$, we have

$$\alpha(T_i) = \sum_{j=1}^{2} a_{i,j}T_j \quad ,$$

and $\det(\alpha) = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$ as usual.

It is routine to check that this is independent of the choice of basis. Now we have

$$\begin{aligned} w(T_1,T_2)^{\deg\alpha} &= w(\alpha(T_1),\alpha(T_2)) \\ \text{by Theorem 13.6, (v)} \\ &= w(a_{1,1}T_1 + a_{1,2}T_2, a_{2,1}T_1 + a_{1,2}T_2) \\ &= w(T_1,T_1)^{a_{1,1}\cdot a_{2,1}} \cdot w(T_1,T_2)^{a_{1,1}\cdot a_{2,2}} \\ &\quad \cdot w(T_2,T_1)^{a_{1,2}\cdot a_{2,1}} \cdot w(T_2,T_2)^{a_{1,2}\cdot a_{2,2}} \\ &= w(T_1,T_2)^{a_{1,1}\cdot a_{2,2}} \cdot w(T_1,T_2)^{-a_{1,2}\cdot a_{2,1}} \\ &= w(T_1,T_2)^{a_{1,1}a_{2,2}-a_{1,2}a_{2,1}} \\ &= w(T_1,T_2)^{\det\alpha} \quad . \end{aligned}$$

Since $w(T_1,T_2)$ is a primitive m^{th} root of unity, we are done. ∎

Remark. Note that $\det\alpha$ depends on m while $\deg\alpha$ is defined independently of m. The use of the Weil pairing allows us to pass from local information on $E[m]$ to global information on all of E.

Now we show that the degree of an endomorphism is essentially quadratic in the endomorphism. This will be important in proving the estimate of the number of k-rational points of E. First we need a lemma on 2×2 matrices.

Lemma 13.11 *Let A and B be 2×2 matrices with entries in some ring R. Then for $c_1, c_2 \in R$*

(i) $\det(c_1 A + c_2 B) = {c_1}^2 \det A + {c_2}^2 \det B + c_1 c_2[\det(A+B) - \det A - \det B]$.

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

The proof is an easy exercise.

Theorem 13.12 *If α and β are endomorphisms, then*

$$\deg(c_1\alpha + c_2\beta) = {c_1}^2 \deg\alpha + {c_2}^2 \deg\beta + c_1 c_2[\deg(\alpha+\beta) - \deg\alpha - \deg\beta] \quad .$$

Proof. Let m be any integer prime to p. If we restrict α and β to $E[m]$, by Theorem 13.10 and the previous lemma we get

$$\begin{aligned} \deg(c_1\alpha + c_2\beta) \equiv & \det(c_1\alpha + c_2\beta) \\ \equiv & {c_1}^2 \det\alpha + {c_2}^2 \det\beta + c_1 c_2[\det(\alpha+\beta) - \det\alpha - \det\beta] \\ \equiv & {c_1}^2 \deg\alpha + {c_2}^2 \deg\beta + c_1 c_2[\deg(\alpha+\beta) - \deg\alpha - \deg\beta] \\ & \pmod{m} \quad . \end{aligned}$$

The theorem now follows since this congruence holds for all m prime to p. ■

The next theorem is the principal part of (i) of the Main Theorem.

Theorem 13.13 *If α is any endomorphism, then*

$$\beta = \alpha \circ \alpha - [1 + \deg\alpha - \deg(1-\alpha)] \circ \alpha - [\deg\alpha] = \mathcal{O} \quad .$$

Proof. When we restrict to $E[m]$, we see that β becomes

$$\alpha \circ \alpha - [1 + \det\alpha - \det(1-\alpha)] \circ \alpha - [\det\alpha] = \alpha \circ \alpha - [\mathrm{tr}\alpha] \circ \alpha - \det\alpha \quad .$$

But it is easy to see by direct computation that any 2×2 matrix A satisfies the equation

$$A^2 - (\mathrm{tr}A)A + \det A = 0 \quad .$$

(This is also a special case of the Cayley-Hamilton Theorem.) Hence β restricted to $E[m]$ is zero. Since this holds for infinitely many m, β must be the zero endomorphism. ■

Now we can prove the Main Theorem. Let E be defined over $k = \mathrm{GF}(q)$, and let φ be the Frobenius mapping. Let E_q be the number of k-rational points on E.

Theorem 13.14 (Hasse): *Set $t = q + 1 - E_q$. Then*

(i) $\varphi \circ \varphi - [t] \circ \varphi + [q] = \mathcal{O}$ *and*

(ii) $|t| \leq 2\sqrt{q}$.

Proof. First note that $\ker(1-\varphi)$ is the set of $(a,b) \in E$ with $(a,b) = (a^q, b^q)$ together with the point $\mathcal{O}$. Exercise 10.3 tells us that $\ker(1-\varphi)$ is precisely the set of k-rational points of E, so $|\ker(1-\varphi)| = E_q$. Also Proposition 12.13 tells us that $1-\varphi$ is separable, so by our definition of degree, $\deg(1-\varphi) = E_q$. Since $\deg\varphi = q$ by (ii) of Exercise 12.15, (i) follows from Theorem 13.13.

To prove (ii), we note that

$$c_1{}^2 + c_2{}^2 q + c_1 c_2 (E_q - 1 - q) = \deg(c_1[1] - c_2\varphi) \geq 0$$

for all $c_1, c_2 \in \mathbb{Z}$. Hence

$$\left(\frac{c_1}{c_2}\right)^2 + q + \left(\frac{c_1}{c_2}\right)(E_q - 1 - q) = \left(\frac{1}{c_2}\right)^2 \deg(c_1[1] - c_2\varphi) \geq 0$$

for all rational numbers c_1/c_2. Thus we must have

$$v^2 + q + v(E_q - 1 - q) \geq 0$$

for all real numbers v. It follows that the discriminant of the quadratic function on the left must be ≤ 0. This discriminant is $t^2 - 4q$, which yields $|t| \leq 2\sqrt{q}$. ■

References

[1] William Fulton. *Introduction to Intersection Theory in Algebraic Geometry*, number 54 in Regional Conference Series in Mathematics, American Mathematical Society, 1984.

[2] Serge Lang. *Algebra*, Addison-Wesley, 1965.

[3] Serge Lang. *Elliptic Curves: Diophantine Analysis*, Springer-Verlag, 1978.

[4] Chih-Han Sah. *Abstract Algebra*, Academic Press, 1967.

[5] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.*, 44:483–494, 1985.

[6] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, number 106 in Graduate Texts in Mathematics, Springer-Verlag, 1986.

Keywords

`conjecture, curve, division, elliptic, Frobenius, function, pair, polynomial, ramification, rational, Reiemann, Roch, uniformizing, Weil`