ELLIPTIC CURVES AND CRYPTOGRAPHY

MICHAEL CALDERBANK

Abstract. We begin with the basics of elliptic curves, assuming some knowledge of group theory and number theory. We shall first build up some general theorems of endomorphisms and torsion points, which will be necessary when we provide Hasse's Theorem about the order of a group of points on an elliptic curve. This will allow us to provide an example of how elliptic curves can be used in cryptography.

Contents

1. What is an Elliptic Curve?

An **elliptic curve** E is the graph of an equation of the form:

$$y^2 = x^3 + Ax + B$$

where A and B are constants. This equation is called the **Weierstrass equation** for an elliptic curve. We will need to specify which field A, B, x, and y belong to, for now we will deal with $\mathbb{R}$, since it is easy to visualize, but for our cryptographic applications, it will make sense to deal with finite fields $\mathbb{F}_q$, where q is a prime power. When working over fields of characteristic 2 or 3, it is more useful to deal with the **generalized Weierstrass equation**:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

With a little algebraic manipulation, an equation of this form can be reduced to a Weirstrass equation if the characteristic of the field is not equal to 2 or 3. We want to look at points on the elliptic curve, so if we have an elliptic curve E over a field K, then for any field L such that $L \supseteq K$ we can consider the set:

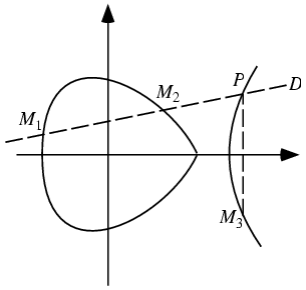
$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L | y^2 = x^3 + Ax + B\}$$

Date: August 21, 2009.

Note that we have added the **point at infinity** to our curve. This concept can be made rigorous using projective space, but it is easiest to regard it as the point (∞, ∞). For computational purposes, it will be a formal symbol satisfying certain rules. At this point, we'll define addition for points. Start with 2 points:

$$M_1 = (x_1, y_1), \quad M_2 = (x_1, y_1)$$

on an elliptic curve E given by the equation $y^2 = x^3 + Ax + B$. We define a new point M_3 as follows: Draw the line D through M_1 and M_2. We'll see below that D intersects E in a third point P. Reflect P across the x-axis to obtain M_3. We define $M_1 + M_2 = M_3$ When E is defined over the reals, then we have the figure below:



For other fields, there is no intuitive picture, so we will need a formal set of rules for addition. Using a bit of basic algebra, we can calculate the coordinates of the

third point given the coordinates of the first two points. Note that if $M_1 = M_2$, then we can use implicit differentiation to find the slope of the line. To summarize:

Definition 1.1. Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E with $P_1, P_2 \neq \infty$. Define $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:

(1) If $x_1 \neq x_2$, then

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{where} \quad m = \frac{y_2 - y_1}{x_2 - x_1}$$

(2) If $x_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = \infty$
(3) If $P_1 = P_2$ and $y_1 \neq 0$, then

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{where} \quad m = \frac{3x_1^2 + A}{2y_1}$$

(4) If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \infty$

Also, define

$$P + \infty = P$$

for all points P on E.

With addition defined, it is only a small step to our first theorem:

Theorem 1.2. *The addition of points on an elliptic curve E form an additive abelian group with ∞ as the identity element.*

Proof. From the formulas, commutativity is obvious, since the line passing through the points is the same, and if we want to find the inverse of P, then if we reflect P across the x-axis to get P', then $P + P' = \infty$. The only tricky part is associativity, and this is a messy calculation involving the formulas above, so we leave it as an exercise.

□

We will want to study the order of specific points and the order of the group in general, but first we have to make rigorous endomorphisms on an elliptic curve

2. Endomorphisms for Elliptic Curves

Definition 2.1. An **endomorphism** of E is a homomorphism $\alpha : E(\overline{K}) \to E(\overline{K})$ that is given by rational functions. So $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$, and there are rational functions $R_1(x, y), R_2(x, y)$ with coefficients in $\overline{K}$ such that

$$\alpha(x, y) = (R_1(x, y), R_2(x, y))$$

for all $(x, y) \in E(\overline{K})$. Naturally, $\alpha(\infty) = \infty$, and we will also assume that any endomorphism is nontrivial, so there exists some (x, y) such that $\alpha(x, y) \neq \infty$.

Using the fact that $y^2 = x^3 + Ax + B$ for all $(x, y) \in E(\overline{K})$, we can show that any endomorphism defined as above can be written as:

$$\alpha(x, y) = (r_1(x), r_2(x)y)$$

with rational functions $r_1(x), r_2(x)$.

Definition 2.2. Let α be as above and write $r_1(x) = \frac{p(x)}{q(x)}$. We define the **degree** of α to be

$$\deg(\alpha) = \text{Max}\{\deg\, p(x), \deg\, q(x)\}$$

Also, we define α to be a **separable** endomorphism if the derivative $r_1'(x)$ is not identically zero. This is equivalent to saying that at least one of $p'(x)$ and $q'(x)$ is not identically zero.

Of particular importance to our study is the **Frobenius map**. Suppose E is defined over the finite field $\mathbb{F}_q$. Let

$$\phi_q(x, y) = (x^q, y^q)$$

.

Lemma 2.3. *Let E be defined over $\mathbb{F}_q$. Then ϕ_q is an endomorphism of E of degree q, and ϕ_q is not separable.*

Proof. Since $\phi_q(x, y) = (x^q, y^q)$ is given by rational functions, it is clear that the degree is q. Also, since $q = 0$ in $\mathbb{F}_q$, the derivative of x^q is indentically zero, so ϕ_q is not separable. The main thing to be proven is that $\phi_q : E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})$ is a homomorphism. Let $(x_1, y_1), (x_2, y_2) \in E(\overline{\mathbb{F}_q})$ with $x_1 \neq x_2$. According to Definition 1.1(1) The sum is (x_3, y_3) with

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{where} \quad m = \frac{y_2 - y_1}{x_2 - x_1}$$

Raise everything to the qth power:

$$x_3^q = m'^2 - x_1^q - x_2^q, \quad y_3^q = m'(x_1^q - x_3^q) - y_1^q, \quad \text{where} \quad m' = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}$$

So if $x_1 \neq x_2$, then we see that

$$\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$$

There is a bit more subtlety when we add a point to itself. According to Definition 1.1(1), we have $2(x_1, y_1) = (x_3, y_3)$, with

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{where} \quad m = \frac{3x_1^2 + A}{2y_1}$$

When we raise everything to the qth power, we will need to use the fact that $2^q = 2, 3^q = 3, A^q = A$, since $2, 3, A \in \mathbb{F}_q$. This is only true if the characteristic of $\mathbb{F}_q$ is not 2 or 3, but if that were the case, then we would have a different addition formula since we would need to use the generalized Weirstrass form. The calculation for that form is essentially the same.

□

We will return to the Frobenius map, but now we need a few general results about endomorphisms.

Proposition 2.4. *Let $\alpha \neq 0$ be a separable endomorphism of an elliptic curve E. Then*

$$deg\ \alpha = \#Ker(\alpha)$$

If $\alpha \neq 0$ is not separable, then

$$deg\ \alpha > \#Ker(\alpha)$$

Proof. Assume first that α is separable. Write $\alpha(x,y) = (r_1(x), r_2(x)y)$ with $r_1(x) = p(x)/q(x)$, as above. Then $r_1' \neq 0$, so $p'q - pq'$ is not the zero polynomial. Let S be the set of $x \in \overline{K}$ such that $(pq' - p'q)(x)q(x) = 0$. Let $(a,b) \in E(\overline{K})$ be such that

(1) $a \neq 0, b \neq 0, (a,b) \neq \infty$,
(2) $\deg(p(x) - aq(x)) = \text{Max}\{\deg(p), \deg(q)\} = \deg(\alpha)$
(3) $a \notin r_1(S)$, and
(4) $(a,b) \in \alpha(E(\overline{K}))$

Since $pq' - p'q$ is not the zero polynomial, S is a finite set, hence its image under α is finite. The function $r_1(x)$ takes on infinitely many distinct values as x runs through $\overline{K}$. Since for each x there is a point $(x,y) \in E(\overline{K})$, we see that $\alpha(E(\overline{K}))$ is an infinite set. Therefore, we know such an (a,b) exists.

We claim that there are exactly $\deg(\alpha)$ points $(x_1, y_1) \in E(\overline{K})$ such that $\alpha(x_1, y_1) = (a,b)$. For such a point, we have

$$\frac{p(x_1)}{q(x_1)} = a, \quad y_1 r_2(x_1) = b.$$

Since $(a,b) \neq \infty$, we must have $q(x_1) \neq 0$. Since $b \neq 0$ and $y_1 r_2(x_1) = b$, we must have $y_1 = b/r_2(x_1)$. Therefore, x_1 determines y_1 in this case, so we only need to count values of x_1.

By assumption (2), $p(x) - aq(x) = 0$ has $\deg(\alpha)$ roots, counting multiplicites. We therefore must show that $p - aq$ has no multiple roots. Suppose that x_0 is a multiple root. Then

$$p(x_0) - aq(x_0) = 0 \quad \text{and} \quad p'(x_0) - aq'(x_0) = 0.$$

Multiplying the equations $p = aq$ and $aq' = p'$ yields

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0).$$

Since $a \neq 0$, this implies that x_0 is a root of $pq' - p'q$, so $x_0 \in S$. Therefore $a = r_1(x_0) \in r_1(S)$, contrary to assumption. Hence it follows that $p - aq$ has no multiple roots, and therefore has $\deg(\alpha)$ distinct roots.

Since there are exactly $\deg(\alpha)$ points (x_1, y_1) with $\alpha(x_1, y_1) = (a,b)$, the kernel of α has $\deg(\alpha)$ elements.

If α is not separable, then the steps of the above proof hold, except that $p' - aq'$ is always the zero polynomial, so $p(x) - aq(x) = 0$ always has multiple roots and therefore has fewer than $\deg(\alpha)$ solutions. □

Theorem 2.5. *Let E be an elliptic curve over a field K. Let $\alpha \neq 0$ be an endomorphism of E. Then $\alpha : E(\overline{K}) \to E(\overline{K})$ is surjective*

Proof. Let $(a,b) \in E(\overline{K})$. Since $\alpha(\infty) = \infty$, we may assume that $(a,b) \neq \infty$. Let $r_1(x) = p(x)/q(x)$ as above. If $p(x) - aq(x)$ is not a constant polynomial, then it has a root x_0. Since p and q have no common roots, $q(x_0) \neq 0$. Choose $y_0 \in \overline{K}$ to be either square root of $x_0^3 + Ax_0 + B$. Then $\alpha(x_0, y_0)$ is defined and equals (a, b') for some b'. Since $b'^2 = a^3 + Aa + B = b^2$, we have $b = \pm b$. If $b' = b$, we're done. If $b' = -b$, then $\alpha(x_0, -y_0) = (a, -b') = (a,b)$.

We now need to consider the case when $p - aq$ is constant. Since $E(\overline{K})$ is infinite and the kernel of α is finite, only finitely many points of $E(\overline{K})$ can map to a point with a given x-coordinate. Therefore, either $p(x)$ or $q(x)$ is not constant. If p and

q are two nonconstant polynomials, then there is at most one constant a such that $p-aq$ is constant (if a' is another such number, then $(a'-a)q = (p-aq)-(p-a'q)$ is constant and $(a'-a)p = a'(p-aq) - a(p-a'q)$ is constant, which implies that p and q are constant). Therefore, there are at most two points, (a,b) and $(a,-b)$ for some b, that are not in the image of α. Let (a_1,b_1) be any other point. Then $\alpha(P_1) = (a_1,b_1)$ for some P_1. We can choose (a_1,b_1) such that $(a_1,b_1)+(a,b) \neq (a,\pm b)$, so there exists P_2 with $\alpha(P_2) = (a_1,b_1)+(a,b)$. Then $\alpha(P_2-P_1) = (a,b)$, and $\alpha(P_1-P_2) = (a,-b)$. Therefore, α is surjective. □

Now, we introduce a few lemmas but we omit the proofs, since they involve lengthy but straightforward calculations using the addition formulas:

Lemma 2.6. *Let E be the elliptic curve $y^2 = x^3 + Ax + B$. Fix a point (u,v) on E. Write*

$$(x,y)+(u,v) = (f(x,y), g(x,y)),$$

where $f(x,y)$ and $g(x,y)$ are rational functions of x, y (the coefficients depend on (u,v)). Then

$$\frac{\frac{d}{dx}f(x,y)}{g(x,y)} = \frac{1}{y}$$

Lemma 2.7. *Let $\alpha_1, \alpha_2, \alpha_3$ be nonzero endomorphisms of an elliptic curve E with $\alpha_1+\alpha_2 = \alpha_3$. Write*

$$\alpha_j(x,y) = (R_{\alpha_j}(x), yS_{\alpha_j}(x)).$$

Suppose there are constants $c_{\alpha_1}, c_{\alpha_2}$ such that

$$\frac{R'_{\alpha_1}(x)}{S_{\alpha_1}(x)} = c_{\alpha_1}, \qquad \frac{R'_{\alpha_2}(x)}{S_{\alpha_2}(x)} = c_{\alpha_2}$$

then

$$\frac{R'_{\alpha_3}(x)}{S_{\alpha_3}(x)} = c_{\alpha_1} + c_{\alpha_2}$$

We can now get back to separable endomorphisms.

Proposition 2.8. *Let E be an elliptic curve defined over a field K, and let n be a nonzero integer. Suppose that multiplication by n on E is given by*

$$n(x,y) = (R_n(x), yS_n(x))$$

for all $(x,y) \in E(\overline{K})$, where R_n and S_n are rational functions. Then

$$\frac{R'_n(x)}{S_n(x)} = n.$$

Therefore, multiplication by n is separable if and only if n is not a multiple of the characteristic p of the field.

Proof. Since $R_{-n} = R_n$ and $S_{-n} = -S_n$, we have $R'_{-n}/S_{-n} = -R'_n/S_n$. Therefore, the result for positive n implies the result for negative n.

Note that the first part of the proposition is trivially true for $n = 1$. If it is true for n, then Lemma 2.7 implies that it is true for $n+1$, which is the sum of n and 1. Therefore, $\frac{R'_n(x)}{S(x)} = n$ for all n.

We have $R'_n(x) \neq 0$ if and only if $n = R'_n(x)/S_n(x) \neq 0$, which is equivalent to p not dividing n. Since the definition of separability is that $R'_n \neq 0$, this proves the second part of the proposition. □

Finally, we get to the main proposition that ties in the Frobenius map and separable endomorphisms. It will be crucial in our quest to find the order of our group of points.

Proposition 2.9. *Let E be an elliptic curve defined over $\mathbb{F}_q$, where q is a power of the prime p. Let r and s be integers, not both 0. The endomorphism $r\phi_q + s$ is separable if and only if $p \nmid s$.*

Proof. Write the multiplication by r endomorphism as

$$r(x, y) = (R_r(x), yS_r(x)).$$

Then

$$(R_{r\phi_q}(x), yS_{r\phi_q}(x) = (r\phi_q)(x, y) = (R_r^q(x), y^q S_r^q(x)) =$$

$$\left(R_r^q(x), y(x^3 + Ax + B)^{(q-1)/2} S_r^q(x)\right).$$

Therefore,

$$c_{r\phi_q} = R'_{r\phi_q}/S_{r\phi_q} = qR_r^{q-1}R'_r/S_{r\phi_q} = 0.$$

Also, $c_s = R'_s/S_s = s$ by Proposition 2.8. By Lemma 2.7,

$$R'_{r\phi_q+s}/S_{r\phi_q+s} = c_{r\phi_q+s} = c_{r\phi_q} + c_s = 0 + s = s.$$

Therefore, $R'_{r\phi_q+s} \neq 0$ if and only if $p \nmid s$. □

3. Torsion Points

Torsion points are those points whose orders are finite. When we study finite fields, every point will be a torsion point, but first we need some general theory.

Definition 3.1. Let E be an elliptic curve defined over a field K. Let n be a positive integer. We say that P is a **torsion point of order n** if P is in the set

$$E[n] = \{P \in E(\overline{K}) | nP = \infty\}$$

As an example, if the characteristic of K is not 2, then E can be put in the form $y^2 =$ cubic, so it is easy to determine $E[2]$. Let

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

with $e_1, e_2, e_3 \in \overline{K}$. A point P satisfies $2P = \infty$ if and only if the tangent line at P is vertical. This means that $y = 0$, so

$$E[2] = \{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\}.$$

As an abstract group, this is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

The situation is a bit more complicated in general, and we will need a proposition before we can prove the general theorem.

Proposition 3.2. *Let E be an elliptic curve. The endomorphism of E given by multiplication by n has degree n^2.*

Unfortunately, the proof of this proposition requires a lengthy discussion of division polynomials, a subject for perhaps another paper. We now state the general theorem:

Theorem 3.3. *Let E be an elliptic curve over a field K and let n be a positive integer. If the characteristic of K does not divide n, or is 0, then*

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$$

If the characteristic of K is $p > 0$ and $p|n$, write $n = p^r n'$ with $p \nmid n'$. Then

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad \text{or} \quad \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$$

Proof. When the characteristic p of the field does not divide n, then by Proposition 2.8, we know that multiplication by n is separable. From Propositions 3.2 and 2.4, $E[n]$, the kernel of multiplication by n, has order n^2. Assuming the structure theorem for finite abelian groups, we have that $E[n]$ is isomorphic to

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k},$$

for some integers $n_1, n_2, \cdots, n_k$ with $n_i | n_{i+1}$ for all i. Let l be a prime dividing n_1. Then $l | n_i$ for all i. This means that $E[l] \subseteq E[n]$ has order l^k. Since we know that $E[l]$ has order l^2, we must have that $k = 2$. Multiplication by n annihilates $E[n] \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, so we must have $n_2 | n$. Since $n^2 = \#E[n] = n_1 n_2$, it follows that $n_1 = n_2 = n$. Therefore,

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$$

when the characteristic p of the field does not divide n.

In the case where $p|n$, we first determine the p-power torsion on E. By Proposition 2.8, multiplication by p is not separable. By Proposition 2.4, the kernel $E[p]$ of multiplication by p has order strictly less than the degree of this endomorphism, which is p^2 by Proposition 3.2. Since every element of $E[p]$ has order 1 or p, the order of $E[p]$ is a power of p, hence must be 1 or p. If $E[p]$ is trivial, then $E[p^k]$ must be trivial for all k. Now suppose $E[p]$ has order p. We claim that $E[p^k] \simeq \mathbb{Z}_{p^k}$ for all k. It is easy to see that $E[p^k]$ is cyclic, but we need to show that the order is p^k, instead of something smaller (it's not clear yet why we can't have $E[p^k] = E[p] \simeq \mathbb{Z}_p$ for all k). Suppose there exists an element P of order p^j. By Theorem 2.5, multiplication by p is surjective, so there exists a point Q with $pQ = P$. Since

$$p^j Q = p^{j-1} P \neq \infty \quad \text{but} \quad p^{j+1} Q = p^j P = \infty,$$

Q has order p^{j+1}. By induction, there are points of order p^k for all k. Therefore, $E[p^k]$ is cyclic of order p^k.

Now, we assemble all the ingredients. Write $n = p^r n'$ with $r \geq 0$ and $p \nmid n'$. Then

$$E[n] \simeq E[n'] \oplus E[p^r].$$

We have $E[n'] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$, since $p \nmid n'$. We have just showed that $E[p^r] \simeq 0$ or $\mathbb{Z}_{p^r}$. Recall that $\mathbb{Z}_{n'} \oplus \mathbb{Z}_{p^r} \simeq \mathbb{Z}_{n'p^r} \simeq \mathbb{Z}_n$. Hence we obtain

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad \text{or} \quad \mathbb{Z}_n \oplus \mathbb{Z}_{n'}.$$

□

Definition 3.4. Let E be an elliptic curve over a field K and let n be an integer not divisible by the characteristic of K. Then $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$. Let

$$\mu_n = \{x \in \overline{K} | x^n = 1\}$$

be the group of nth roots of unity in $\overline{K}$. Since the characteristic of K does not divide n, the equation $x^n = 1$ has no multiple roots, hence has n roots in $\overline{K}$. Therefore

μ_n is a cyclic group of order n. Any generator ζ of μ_n is called a **primitive nth root of unity**. In other words, $\zeta^k = 1$ if and only if n divides k.

Now, we are ready to discuss the Weil pairing on the n-torsion on an elliptic curve, which will also be necessary to determine $\#E(\mathbb{F}_q)$.

Theorem 3.5. *Let E be an elliptic curve defined over a field K and let n be a positive integer. Assume that the characteristic of K does not divide n. Then there is a pairing*

$$e_n : E[n] \times E[n] \to \mu_n,$$

*called the **Weil pairing**, that satisfies the following properties:*

(1) e_n is bilinear in each variable. This means that

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

and

$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

for all $S, S_1, S_2, T, T_1, T_2 \in E[n]$.

(2) e_n is nondegenerate in each variable. This means that if $e_n(S, T) = 1$ for all $T \in E[n]$ then $S = \infty$ and also that if $e_n(S, T) = 1$ for all $S \in E[n]$ then $T = \infty$.

(3) $e_n(T, T) = 1$ for all $T \in E[n]$.

(4) $e_n(T, S) = e_n(S, T)^{-1}$ for all $S, T \in E[n]$.

(5) $e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$ for all endomorphisms σ of $\overline{K}$ such that σ is the identity map on the coefficients of E (if E is in Weirstrass form, this means that $\sigma(A) = A$ and $\sigma(B) = B$).

(6) $e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{deg(\alpha)}$ for all separable endomorphism α of E. If the coefficients of E lie in a finite field $\mathbb{F}_q$, then the statement also holds when α is the Frobenius endomorphism ϕ_q.

The proof that this pairing exists and is well-defined is beyond the scope of this paper, but if we accept that such a pairing exists, then many of the (messy) problems dealing with the degree of an endomorphism can be simplified.

Corollary 3.6. *Let $\{T_1, T_2\}$ be a basis of $E[n]$. Then $e_n(T_1, T_2)$ is a primitive nth root of unity.*

Proof. Suppose $e_n(T_1, T_2) = \zeta$ with $\zeta^d = 1$. Then $e_n(T_1, dT_2) = 1$. Also, $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$ (by (1) and (3)). Let $S \in E[n]$. Then $S = aT_1 + bT_2$ for some integers a, b. Therefore,

$$e_n(S, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1.$$

Since this holds for all S, (2) implies that $dT_2 = \infty$. Since $dT_2 = \infty$ if and only if $n|d$, it follows that ζ is a primitive nth root of unity. □

So, if α is an endomorphism of E, then we obtain a matrix $\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with entries in $\mathbb{Z}_n$, describing the action of α on a basis $\{T_1, T_2\}$ of $E[n]$.

Proposition 3.7. *Let α be an endomorphism of an elliptic curve E defined over a field K. Let n be a positive integer not divisible by the characteristic of K. Then $deg(\alpha_n) \equiv deg(\alpha) (\bmod\ n)$.*

Proof. By Corollary 3.6, $\zeta = e_n(T_1, T_2)$ is a primitive nth root of unity. By part (6) of Theorem 3.5, we have

$$\zeta^{\deg(\alpha)} = e_n(\alpha(T_1), \alpha(T_2)) = e_n(aT_1 + cT_2, bT_1 + dT_2)$$
$$= e_n(T_1, T_1)^{ab} e_n(T_1, T_2)^{ad} e_n(T_2, T_1)^{cb} e_n(T_2, T_2)^{cd} = \zeta^{ad-bc},$$

by the properties of the Weil pairing. Since ζ is a primitive nth root of unity, $\deg(\alpha) \equiv ad - bc (\bmod\ n)$. □

This proposition allows us to reduce quesitions about the degree of endomorphisms to calculations with matrices, which is much easier.

Let α and β be endomorphisms of E and let a, b be integers. The endomorphism $\alpha a + b\beta$ is defined by

$$(a\alpha + b\beta)(P) = a\alpha(P) + b\beta(P).$$

Here $a\alpha(P)$ means multiplication of E of $\alpha(P)$ by the integer a. The result is then added on E to $b\beta(P)$. This process can all be described by rational functions, since this is true for each of the individual steps. Therefore $a\alpha + b\beta$ is an endomorphism. Now, we can put our most recent proposition to good use.

Proposition 3.8.

$$deg(a\alpha + b\beta) = a^2 deg\ \alpha + b^2 deg\ \beta + ab(deg(\alpha + \beta) - deg\ \alpha - deg\ \beta).$$

Proof. Let n be any integer not divisible by the characteristic of K. Represent α and β by matrices α_n and β_n (with respect to some basis of $E[n]$). Then $a\alpha_n + b\beta_n$ gives the action of $a\alpha + b\beta$ on $E[n]$. Using the basic properties of the determinant of a matrix, we get

$$\det(a\alpha_n + b\beta_n) = a^2 \det\ \alpha_n + b^2 \det\ \beta_n + ab(\det(\alpha_n + \beta_n) - \det\ \alpha_n - \det\ \beta_n)$$

for any matrices α_n and β_n. Therefore

$$\deg(a\alpha + b\beta) \equiv a^2 \deg\ \alpha + b^2 \deg\ \beta + ab(\deg(\alpha + \beta) - \deg\ \alpha - \deg\ \beta)(\ \bmod\ n).$$

Since this holds for infinitely many n, it must be an equality. □

4. Elliptic Curves over Finite Fields

We'll start of this section with an example of small characteristic:

Example 4.1. Let E be given by $y^2 + xy = x^3 + 1$ defined over $\mathbb{F}_2$. Checking all the points isn't too hard, and we get:

$$E(\mathbb{F}_2) = \{\infty, (0,1), (1,0), (1,1)\}.$$

This is a cyclic group of order 4, and we can verify using the addition formulas that the points $(1,0), (1,1)$ have order 4 and the point $(0,1)$ has order 2.

Let's look at $E(\mathbb{F}_4)$. We can write it as $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, with the relation $\omega^2 + \omega + 1 = 0$. Checking through all the possibilities for x, we get

$$E(\mathbb{F}_4) = \{\infty, (0,1), (1,0), (1,1), (\omega,0), (\omega,\omega), (\omega^2,0), (\omega^2,\omega^2)\}$$

Since we are in characteristic 2, there is at most one point of order 2 (see Theorem 3.3). In fact, $(0,1)$ has order 2. Hence, we must have that $E(\mathbb{F}_4)$ is cyclic of order 8. Also, any one of the four points containing ω or ω^2 is a generator, since they

do not lie in the order 4 subgroup $E(\mathbb{F}_2)$. Let $\phi_2(x,y) = (x^2, y^2)$ be the Frobenius map. We see that ϕ_2 permutes the elements of $E(\mathbb{F}_4)$, and

$$E(\mathbb{F}_2) = \{(x,y) \in E(\mathbb{F}_4) | \phi_2(x,y) = (x,y)\}.$$

We will generalize this later.

We will prove two main restrictions on the groups $E(\mathbb{F}_q)$. We can tackle one right now using what we know about torsion, but the other will require a few lemmas.

Theorem 4.2. *Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_n \quad \text{or} \quad \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

for some integer $n \geq 1$, or for some integers $n_1, n_2 \geq 1$ with n_1 dividing n_2.

Proof. From group theory, we know that a finite abelian group is isomorphic to a direct sum of cyclic groups

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_i},$$

with $n_i | n_{i+1}$ for $i \geq 1$. Since, for each i, the group $\mathbb{Z}_{n_1}$ has n_1 elements of order dividing n_1, we find that $E(\mathbb{F}_q)$ has n_1^r elements of order dividing n_1. By Theorem 3.3, there are at most n_1^2 such points (even if we allow coordinates in $\overline{\mathbb{F}_q}$). Therefore $r \leq 2$. □

Lemma 4.3. *Let E be defined over $\mathbb{F}_q$, and let $(x,y) \in E(\overline{\mathbb{F}_q})$.*

(1) $\phi_q(x,y) \in E(\overline{\mathbb{F}_q})$
(2) $(x,y) \in E(\mathbb{F}_q)$ if and only if $\phi_q(x,y) = (x,y)$

Proof. This is a straightforward calculation using the Weirstrass equation, along with two basic facts from number theory: $(a+b)^q = a^q + b^q$ when q is a power of the characteristic of the field, and also $a^q = a$ for all $a \in \mathbb{F}_q$. □

Proposition 4.4. *Let E be defined over $\mathbb{F}_q$ and let $n \geq 1$.*

(1) $Ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$.
(2) $\phi_q^n - 1$ is a separable endomorphism, so $\#E(\mathbb{F}_{q^n}) = deg(\phi_{q^n} - 1)$.

Proof. Since ϕ_q^n is the Frobenius map for the field $\mathbb{F}_{q^n}$, part (1) is just a restatement of Lemma 4.3. The fact that $\phi_q^n - 1$ is separable was proved in Proposition 2.9. Therefore (2) follows from Proposition 2.4. □

Lemma 4.5. *Let*

$$a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - deg(\phi_q - 1).$$

Let r, s be integers with $gcd(s,q) = 1$. Then $deg(r\phi_q - s) = r^2 q + s^2 - rsa$.

Proof. Proposition 3.8 implies that

$$\deg(r\phi_q - s) = r^2 \deg(\phi_q) + s^2 \deg(-1) + rs(\deg(\phi_q - 1) - \deg(\phi_q) - \deg(-1)).$$

Since $\deg(\phi_q) = q$ and $\deg(-1) = 1$, the result follows. □

Hasse's Theorem places a bound on $\#E(\mathbb{F}_q)$.

Theorem 4.6. *Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then the order of $E(\mathbb{F}_q)$ satisfies*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$$

Proof. Using the same terminology as Lemma 4.5, since we know $\deg(r\phi_q - s) \geq 0$, the lemma implies that

$$q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0$$

for all r, s with $\gcd(s, q) = 1$. The set of rational numbers r/s such that $\gcd(s, q) = 1$ is dense in $\mathbb{R}$, so therefore

$$qx^2 - ax + 1 \geq 0$$

for all real numbers x. Therefore the discriminant of the polynomial is negative or 0, which means that $a^2 - 4q \leq 0$, hence $|a| \leq 2\sqrt{q}$.

□

This proof is short, but there are several major ingredients coming from previous results. One is that we can identify $E(\mathbb{F}_q)$ as the kernel of $\phi_q - 1$. Another is that $\phi_q - 1$ is separable, so the order of the kernel is the degree of $\phi_q - 1$. A third major ingredient is the Weil pairing, especially part (6) of Theorem 3.5, and its consequence, Propositon 3.8.

Now that we have a bound on the order of the group, we can use a bit of group theory to determine $\#E(\mathbb{F}_q)$. The **order** of P is the smallest positive integer k such that $kP = \infty$. A corollary of Lagrange's theorem requires that the order of a point divides the order of the group $E(\mathbb{F}_q)$. Also, for any integer n, we have $nP = \infty$ if and only if the order of P divides n. Since $\#E(\mathbb{F}_q)$ lies in an interval of length $4\sqrt{q}$, if we can find a point of order greater than $4\sqrt{q}$, there can be only one multiple of this order in the correct interval, and it must be $\#E(\mathbb{F}_q)$. But how do we find the order of a point?

Baby Step, Giant Step: The Order of the Group

Let $\#E(\mathbb{F}_q) = N$. We might not know N yet, but we know that $q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}$. We could try all values of N in this range and see which ones satisfy $NP = \infty$. This takes around $4\sqrt{q}$ steps. However, we can speed this up to around $4q^{1/4}$ steps with the following algorithm:

(1) Compute $Q = (q + 1)P$.

(2) Choose an integer m with $m > q^{1/4}$. Compute and store the points jP for $j = 0, 1, 2, \ldots, m$.

(3) Compute the points

$$Q + k(2mP) \quad \text{for} \quad k = -m, -(m-1), \ldots, m$$

until there is a match $Q + k(2mP) = \pm jP$ with a point (or its negative) on the stored list.

(4) Conclude that $(q + 1 + 2mk \mp j)P = \infty$. Let $M = q + 1 + 2mk \mp j$.

(5) Factor M. Let $p_1, \ldots, p_r$ be the distinct prime factors of M.

(6) Compute $(M/p_i)P$ for $i = 1, \ldots, r$. If $(M/p_i)P = \infty$ for some i, replace M with M/p_i and go back to step (5). If $(M/p_i)P \neq \infty$ for all i then M is the order of the point M.

(7) If we are looking for $\#E(\mathbb{F}_q)$, then repeat steps (1)-(6) with randomly chosen points in $E(\mathbb{F}_q)$ until the greatest common multiple of the orders divides only one integer N with $q+1-2\sqrt{q} \leq N \leq q+1+2\sqrt{q}$. Then $N = \#E(\mathbb{F}_q)$.

There are two points that need to be addressed here. Why is there always a match in step (3)? Why does step (6) yield the order of P?

Lemma 4.7. *Let a be an integer with $|a| \leq 2m^2$. There exist integers a_0 and a_1 with $-m < a_0 \leq m$ and $-m \leq a_1 \leq m$ such that*

$$a = a_0 + 2ma_1$$

Proof. Let $a_0 \equiv a (\bmod 2m)$, with $-m < a_0 \leq m$ and $a_1 = (a - a_0)/2m$. Then

$$|a_1| \leq (2m^2 + m)/2m < m + 1.$$

□

Let $a = a_0 + 2ma_1$ be as in the lemma and let $k = -a_1$. Then

$$Q + k(2mP) = (q + 1 - 2ma_1)P = (q + 1 - a + a_0)P = NP + a_0P = a_0P = \pm jP,$$

where $j = |a_0|$. Therefore, there is a match.

Lemma 4.8. *Let G be an additive group (with identity element 0) and let $g \in G$. Suppose $Mg = 0$ for some positive integer M. Let $p_1, \ldots, p_r$ be the distinct primes dividing M. If $(M/p_i)g \neq 0$ for all i, then M is the order of g.*

Proof. Let k be the order of g. Then $k|M$. Suppose $k \neq M$. Let p_i be a prime dividing M/k. Then $p_ik|M$, so $k|(M/p_i)$. Therefore, $(M/p_i)g = 0$, contrary to assumption. Therefore, $k = M$. □

Remark 4.9. Why is the method called "Baby Step, Giant Step"? The **baby steps** are from a point jP to $(j + 1)P$. The **giant steps** are from a point $k(2mP)$ to $(k + 1)(2mP)$, since we take the "bigger" step $2mP$.

5. Discrete Logarithm Problem

Let p be a prime and let a, b be integers that are nonzero mod p. Suppose we know that there exists an integer k such that $a^k \equiv b (\bmod p)$ The classical **discrete logarithm problem** is to find k. We can generalize this problem so that we are solving it not just for the group $\mathbb{F}_p^\times$, but for $E(\mathbb{F}_q)$. Namely, given two points P, Q on E, we are trying to find an integer k with $kP = Q$.

One way to attack the discrete log problem is with brute force, but that is very impractical when k can be an integer of several hundred digits. Below, we have another algorithm that worked from small steps to big steps:

Baby Step, Giant Step: Discrete Logarithm Problem

This works well for moderately sized N, because it requires about $\sqrt{N}$ storage, where N is the order of the group.

(1) Fix an integer $m \geq \sqrt{N}$ and compute mP.

(2) Make and store a list of iP for $0 \leq i < m$.

(3) Compute the points $Q - jmP$ for $j = 0, 1, \ldots, m-1$ until one matches an element from the stored list.

(4) If $iP = Q - jmP$, we have $Q = kP$ with $k \equiv i + jm (\mathrm{mod}\ N)$.

Why does this work? Since $m^2 > N$, we may assume the answer k satisfies $0 \leq k < m^2$. Write $k = k_0 + mk_1$ with $k_0 = k (\mathrm{mod}\ m)$ and $0 \leq k_0 < m$ and let $k_1 = (k - k_0)/m$. Then $0 \leq k_1 < m$. When $i = k_0$ and $j = k_1$, we have

$$Q - k_1 mP = kP - k_1 mP = k_0 P,$$

so there is a match. The baby step comes from adding P to $(i-1)P$. The point $Q - jmP$ is computed by adding $-mP$ (a giant step) to $Q - (j-1)mP$. Note that we did not need to know the exact order N of G. Therefore, for elliptic curves over $\mathbb{F}_q$, we can use this method with $m^2 \geq q + 1 + 2\sqrt{q}$, by Theorem 4.6.

There are faster attacks for the discrete logarithm problem, but all of them require extra assumptions about q or the group structure of $E(\mathbb{F}_q)$. The discrete logarithm problem curve for elliptic curves E, where $\#E(\mathbb{F}_q) = q$ can be solved using quicker methods that go beyond the scope of this paper. Finally, we explore one cryptographic system based on the fact that solving the discrete logarithm problem is hard.

ElGamal Public Key Encryption

Alice wants to send a message to Bob. First, Bob establishes his public key as follows. He chooses an elliptic curve E over $\mathbb{F}_q$ such that the discrete log problem is hard for $E(\mathbb{F}_q)$. He also chooses a point P on E (usually, it is arranged that the order of P is a large prime). He chooses a *secret* integer s and computes $B = sP$. The elliptic curve E, the finite field $\mathbb{F}_q$, and the points P and B are Bob's public key. Bob's private key is the integer s.

To send a message to Bob, Alice does the following:

(1) Download Bob's public key.

(2) Expresses her message as a point $M \in E(\mathbb{F}_q)$ (this procedure will be explained below)

(3) Chooses a secret random integer k and computes $M_1 = kP$.

(4) Computes $M_2 = M + kB$.

(5) Sends M_1, M_2 to Bob.

How do we represent a message as a point on an Elliptic curve? A method was proposed by Koblitz. Suppose E is an elliptic curve given by $y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$ (The case of an arbitrary finite field $\mathbb{F}_q$ is similar. Let M be the message, expressed as a number $0 \leq M < p/100$. Let $x_j = 100M + j$ for $0 \leq j < 100$. For $j = 0, 1, 2, \ldots, 99$, compute $s_j = x_j^3 + Ax_j + B$. If $s_j^{(p-1)/2} \equiv 1 (\mathrm{mod}\ p)$, then s_j is a square mod p, in which case we do not need to try any more values of j. When $p \equiv 3 (\mathrm{mod}\ 4)$, a square root of s_j is then given by $y_j \equiv s_j^{(p+1)/4} (\mathrm{mod}\ p)$, when $p \equiv 1 (\mathrm{mod}\ 4)$, it takes a bit more algebraic number theory to compute a square

root, but it can be done. We obtain a point (x_j, y_j) on E. To recover M from (x_j, y_j), simply compute $\lfloor x_j/100 \rfloor$. Since s_j is essentially a random element of $\mathbb{F}_p^\times$, which is cyclic of even order, the probability is approximately $1/2$ that s_j is not a square. So the probability of not being able to find a point m after trying 100 values is around 2^{-100}.

Bob decrypts by calculating

$$M = M_2 - sM_1.$$

The decryption works because

$$M_2 - sM_1 = (M + kB) - s(kP) = M + k(sP) - skP = M.$$

Eve knows Bob's public information and the points M_1 and M_2. If she can calculate discrete logs, she can use P and B to find s, which she can then use to decrypt the message as $M_2 - sM_1$. Also, she could use P and M_1 to find k. Then she can calculate $M = M_2 - kB$. If she cannot calculate discrete logs, there does not appear to be a way to find M.

It is important for Alice to use a different random k each times she sends a message to Bob. Suppose Alice uses the same k for both M and M'. Eve recognizes this because then $M_1 = M_1'$. She then computes $M_2' - M_2 = M' - M$. Suppose M is made public after the need for secrecy is gone. Then Eve finds out M, so she calculates $M' = M - M_2 + M_2'$. Therefore, knowledge of one plaintext M allows Eve to deduce another plaintext M' in this case.

6. Conclusion

Naturally, there are a few more cryptosystems that use elliptic curves, and there are several other specific curves that we were not able to discuss. However, we began our study of elliptic curves from scratch, and with a bit of groundwork involving endomorphisms and torsion, we were able to discover the structure of a group of points of an elliptic curve over a finite field. These results allowed us to create a public-key cryptosystem. Like RSA, the ElGamal cryptosystem security hinges on a problem that is computationally hard in general cases, namely the discrete logarithm problem.

Acknowledgments. It is a pleasure to thank my mentor, Evan Jenkins, for guiding me towards the right books and focusing my mathematical energies towards a coherent paper.

References

[1] Lawrence C. Washingtion. Elliptic Curves: Number Theory and Cryptography. Chapman and Hall/CRC Press 2003.

[2] O. N. Vasilenko. Number-Theoretic Algorithms in Cryptography. American Mathematical Society. 2007.