ELLIPTIC CURVES

SUNAY MIDUTHURI

Abstract. In this paper, we examine elliptic curves. We begin with discussing the elliptic integral, which gave rise to the concept of elliptic curves. Then, we look at elliptic curves themselves and examine their properties, along with the addition operation and how they can be turned into a group. After a discussion on projective space, we look at reduction of elliptic curves. We then talk about the L function before looking at methods of cryptography involving elliptic curves.

1. Introduction

We begin by considering an ellipse. The equation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

defines a horizontal ellipse with semi-major axis a and semi-minor axis b (assuming that $a > b$.) It is known that the area of this ellipse is πab.
However, the perimeter of an ellipse is an unsolved problem that gives rise to several interesting areas of mathematics, including elliptic curves. The most common method to find the elliptic perimeter begins by solving for y to get $y = b\sqrt{1 - \frac{x^2}{a^2}}$. Then $f'(x) = \frac{-bx}{a\sqrt{a^2-x^2}}$. Then the arclength is equal to

$$4\int_0^a \sqrt{1 + f'(x)^2}\, dx = 4\int_0^a \sqrt{1 + \frac{b^2x^2}{a^2(a^2 - x^2)}}\, dx.$$

If we substitute $x = at$, the integral becomes

$$4a\int_0^1 \sqrt{\frac{1 - (1 - \frac{b^2}{a^2})t^2}{1 - t^2}}\, dt = 4a\int_0^1 \sqrt{\frac{1 - k^2t^2}{1 - t^2}}\, dt,$$

where $k = \sqrt{1 - \frac{b^2}{a^2}} = \frac{c}{a}$ is the eccentricity of the ellipse; see Fig 1.1 for a more detailed explanation.

While the last integral is unsolved, and the circumference of the ellipse remains an open problem, the integral itself, known as a complete elliptic integral of the second kind, gives rise to the family of curves called elliptic curves. If $u = \sqrt{\frac{1-e^2t^2}{1-t^2}}$, we find that

$$u^2(1 - t^2) = 1 - e^2t^2,$$

which is considered an elliptic curve [Sut17].

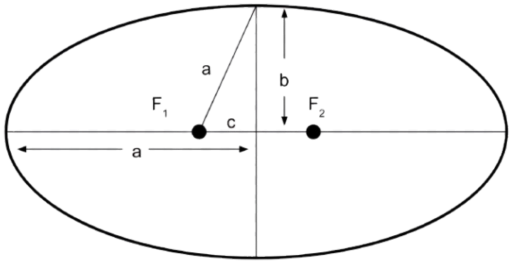

Figure 1. The major lengths of an ellipse. The Pythagorean Theorem gives us $b^2 + c^2 = a^2$.

2. Elliptic Curves

Definition 2.1. An elliptic curve over the real numbers in standard form can be expressed by the equation

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

for some constants A and B.

This is also called Weierstrass Form. Let E be an elliptic curve over $\mathbb{Q}$, and let P be a rational point on E. It is not necessarily true that a line through P with rational slope must intersect E in another rational point. However, this changes when we have two points.

Theorem 2.2. *If E is an elliptic curve over $\mathbb{Q}$, and $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are rational points on E, the line l through P and Q intersects E in a third rational point.*

Proof. The line l between P and Q is given by the equation

$$y = \frac{y_2 - y_1}{x_2 - x_1}x + y_1 - x_1\frac{y_2 - y_1}{x_2 - x_1} = \frac{y_2 - y_1}{x_2 - x_1}x + \frac{y_1x_2 - x_1y_2}{x_2 - x_1}.$$

Intersect this with the curve E with equation $y^2 = x^3 + ax + b$. We then obtain

$$\left(\frac{y_2 - y_1}{x_2 - x_1}x + \frac{y_1x_2 - x_1y_2}{x_2 - x_1}\right)^2 = x^3 + ax + b.$$

Now, substitute

$$\frac{y_2 - y_1}{x_2 - x_1} = m \text{ and } \frac{y_1x_2 - x_1y_2}{x_2 - x_1} = n,$$

so our equation becomes

$$m^2x^2 + 2mnx + n^2 = x^3 + ax + b,$$

or

$$x^3 - m^2x^2 + (a - 2mn)x + (b - n^2) = 0.$$

Since points P and Q are both on the curve and on line l, x_1 and x_2 are roots to this cubic; by Vieta's formula, the third root is equal to $m^2 - x_1 - x_2 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2$. Since we know that x_1, x_2, y_2, and y_1 are all rational, the third root must be rational. If we call the third root x_3, there must exist a third rational point on that cubic, as desired. Note that y_3 must be rational because x_3 is rational and (x_3, y_3) is on a rational line. □

3. Elliptic Curves as a Group

Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$. If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are two points on E, we define the third point $P_3 = P_1 + P_2$ as follows.

Definition 3.1 (Addition)**.** To add points P_1 and P_2, we first draw the line l between them. Let P be the point where that line intersects E, so that P, P_1, and P_2 are collinear. We then reflect point P about the x axis; since an elliptic curve is symmetric about it (as the equation is even in y), we obtain a point $P' = P_3$ that is on E. We define P_3 to be the sum of points P_1 and P_2.

So, how do we explicitly calculate the point P_3? We'll divide it into several cases.
In our first case, assume that $x_1 \neq x_2$ and neither point is the point at infinity. Then the line between P_1 and P_2 has slope $m = \frac{y_2 - y_1}{x_2 - x_1}$. To find the intersections with the cubic, we use the substitution from Theorem 2.2 to obtain

$$x_3' = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2.$$

Reflecting across the y-axis gives us the point

$$\left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \frac{y_1 - y_2}{x_2 - x_1}\left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2\right) - \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1}\right).$$

In our second case, we have $x_1 = x_2$. Then, the line through P_1 and P_2 is vertical, and we say that it intersects the elliptic curve at the "point at infinity".
In the third case, we assume that P_1 and P_2 are very close to each other. In this case, the secant between them approximates the tangent to the elliptic curve, which has slope $m = \frac{dy}{dx}$. In the equation $y^2 = x^3 + ax + b$, implicit differentiation tells us that

$$2y\ dy = 3x^2\ dx + a\ dx,$$

or

$$\frac{dy}{dx} = \frac{3x^2 + a}{2y}.$$

Then the tangent at P_1 has slope $m = \frac{3x_1^2 + a}{2y_1}$. If $y_1 = 0$, the tangent has infinite slope and is therefore infinite, so this is identical to our second case. Otherwise, the line L is given by the equation

$$y = m(x - x_1) + y_1;$$

as before, we obtain the cubic equation

$$x^3 - m^2x^2 + (a - 2mn)x + (b - n^2) = 0,$$

but note that m is now only dependent on P_1, and $n = y_1 - mx_1$. While we only know one root x_1, it is a double root; this means that the other point of intersection has x-coordinate $m^2 - 2x_1$, so we find that our final point is

$$P_2 = P_1 + P_1 = \left(m^2 - 2x_1, m(3x_1 - m^2) - y_1\right),$$

as desired [Nea].

Definition 3.2. A group is a set G and an operation $\star : G \to G$ that satisfies each of the following axioms:

(1) There exists an element $e \in G$ such that for all $g \in G$, $g \star e = e \star g = g$. We call this element e the identity element of G.

(2) For all $g \in G$, there exists $g^{-1} \in G$ such that $g \star g^{-1} = g^{-1} \star g = e$.
(3) The operation $\star$ is associative. i.e. if $g, h, k \in G$, $(g \star h) \star k = g \star (h \star k)$.

Definition 3.3. A group G with the operation $\star$ is abelian if and only if for all $g, h \in G$, $g \star h = h \star g$, i.e. $\star$ is commutative.

Theorem 3.4. *Elliptic curves under the elliptic curve addition operation + are an abelian group if we consider the "point at infinity" to be on the curve.*

Proof. To show the first condition, we claim that the point at infinity is the identity. Let O be the point at infinity. To show that O is the identity, let O' be the identity, and take $P \in G$. If $P + O' = P$, the line through P and O' intersects the elliptic curve at the reflection of P about the y axis P'. Therefore O' is O, and the point at infinity is the identity.

To show the second condition, consider any point P on the elliptic curve. Then $P + P'$ is the intersection of a vertical line with the cubic, which we know from earlier to be the point at infinity, as desired.

The proof of associativity is omitted; however, it can be done simply (albeit tediously) by substituting the equation for addition.

To show commutivity, let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$; then

$$P_1 + P_2 = (m^2 - x_1 - x_2, m(2x_1 + x_2 - m^2) - y_1).$$

Since $m = \frac{y_2 - y_1}{x_2 - x_2}$ is equal to $n = \frac{y_1 - y_2}{x_1 - x_2}$, we know that

$$P_2 + P_1 = (n^2 - x_2 - x_1, n(2x_2 + x_1 - n^2) - y_2) = (m^2 - x_1 - x_2, 2mx_2 + mx_1 - m^3 - y_2).$$

Then our problem is reduced to proving that

$$2mx_2 + mx_1 - m^3 - y_2 = 2mx_1 + mx_2 - m^3 - y_1,$$

or

$$m(x_2 - x_1) = y_2 - y_1,$$

which follows trivially from the definition of slope. □

From now on, we will refer to the point at infinity as 0, as it is the identity.

Theorem 3.5. *Three points on a line add to* 0.

Proof. If these points are P, Q, R, we have that $P + Q$ is the point R' opposite the x-axis from R. But then $R + R' = 0$, as desired. □

Definition 3.6. A group G is finitely generated if and only if there exists a finite $S \subset G$ such that every element in G can be generated using the group operation of G and the members of S.

Theorem 3.7 (Mordell)**.** *The set of rational points on an elliptic curve E, denoted $E(\mathbb{Q})$, is finitely generated.*

We then define the rank as a measure of the size of rational points:

Definition 3.8. The rank of an elliptic curve E is the order of the smallest generating set free from torsion points.

Theorem 3.9 ([BS13])**.** *The average rank of all elliptic curves over* $\mathbb{Q}$ *is less than* 1*.*

We know know it to be over 0.2 and less than 0.9; it is believed to be exactly $\frac{1}{2}$. Manjul Bhargava received the Fields Medal in 2016 for this work.

Theorem 3.10 ([Has36])**.** *The cardinality of* $E(\mathbb{F}_p)$ *satisfies* $\#E(\mathbb{F}_p) = p + 1 - t$*, with* $|t| \leq 2\sqrt{p}$*.*

Definition 3.11. The order of a point P on an elliptic curve E is the smallest integer n such that

$$nP = P + P + \cdots + P \text{ (n P's) } = 0.$$

4. Projective Space and the Discriminant

Definition 4.1. The projective plane $\mathbb{P}^2$ is the set of ordered triples x, y, z under the equivalence relation $\sim$ that satisfies $(x, y, z) \sim (x_1, y_1, z_1)$ if and only if

$$\frac{x_1}{x} = \frac{y_1}{y} = \frac{z_1}{z}.$$

Definition 4.2. The projective point $(x : y : z)$ is the equivalence class of (x, y, z).

Definition 4.3. A polynomial $f(x_1, x_2, \ldots, x_n)$ is homogeneous if an only if all its nonzero coefficients have the same degree.

Definition 4.4. A plane projective curve C_f over a field K is a homogenous polynomial $f(x, y, z)$ whose coefficients belong to K. For any field F such that $K \subseteq F$, the F-rational points of C_f form the set

$$C_f(F) = \{(x : y : z) \in \mathbb{P}^2(F) : f(x, y, z) = 0\}.$$

Definition 4.5. A point P is singular if

$$\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = \frac{\partial f}{\partial z} = 0$$

at P.

We can write an elliptic curve in homogeneous coordinates to get a condition for singularity. Suppose that we can write this elliptic curve E as

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2xz^2 + a_4x^2z + a_6z^3.$$

This equation is called the long Weierstrass Equation. Rearranging terms, we obtain

$$f(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2xz^2 - a_4x^2z - a_6z^3 = 0.$$

If we set the partial derivatives to 0 to get a condition for singularity, we obtain

$$\frac{\partial f}{\partial x} = a_1yz - 3x^2 - a_2z^2 - 2a_4xz = 0$$

$$\frac{\partial f}{\partial y} = 2yz + a_1xz + a_3z^2 = 0$$

$$\frac{\partial f}{\partial z} = y^2 + a_1xy + 2a_3yz - 2a_2xz - a_4x^2 - 3a_6z^3 = 0.$$

While this system is messy, we can (if the coefficients are not of characteristic 2) make a transformation to write the curve in short Weierstrass form:

$$y^2z = x^3 + ax^2z + bxz^2 + cz^3.$$

Here, taking partial derivatives gives us that the condition for singularities to not exist is

$$-4b^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = 0.$$

This turns out to be equal to the discriminant:

Definition 4.6. Let E be an elliptic curve with the equation $y^2 = x^3 + Ax + B$. We define the discriminant $\Delta E = -16(4A^3 + 27B^2)$.

This gives us the following theorem:

Theorem 4.7. *If the discriminant ΔE of an elliptic curve E is not equal to zero, then E has no singularities.*

5. Reduction Modulo a Prime

Definition 5.1. If a prime p satisfies $\Delta E \not\equiv 0 \pmod{p}$ for some elliptic curve E, then E has good reduction at p.

If we reduce A and B mod P, we obtain an elliptic curve

$$E_p \equiv E \pmod{p}$$

defined over the field $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$.

By Theorem 4.7, the condition of good reduction is equivalent to the condition of nonsingularity remaining even in reduction modulo p. But this is not always the case.
For instance, consider the elliptic curve $y^2 = x^3 - 4x^2 + 16$ (note that although there is an x^2 coefficient, it can be removed with a simple shift.) Suppose we reduce this modulo $p = 11$. Since $-4 \equiv 7 \pmod{11}$ and $16 \equiv 5 \pmod{11}$, the curve becomes $y^2 = x^3 + 7x^2 + 5$, which factors as $(x+1)^2(x+5)$. Since the discriminant of this curve is $0 \pmod{11}$, we say that it has bad reduction at 11.

Now suppose that an elliptic curve E has bad reduction at p.

Definition 5.2. We say that E has additive reduction at p if and only if there is a single tangent line at the singularity. The singularity is then called a cusp.

Definition 5.3. We say that E has multiplicative reduction at p if there are two tangent lines at the singularity. The singularity is called a node.

Definition 5.4. If E has multiplicative reduction at p and the slopes of the tangent lines are in the same field as the curve coefficients, we say that E has split multiplicative reduction. Otherwise, it has nonsplit multiplicative reduction.

6. The L function

We define the Hasse-Weil L-function of an elliptic curve as follows:

Definition 6.1 (Prime L-function)**.** If p is prime, we define

$$L_p(s) = \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

if E has good reduction at p,

$$L_p(s) = \frac{1}{1 - p^{-s}}$$

if E has split multiplicative reduction at p, and

$$L_p(s) = \frac{1}{1 + p^{-s}}$$

if E has nonsplit multiplicative reduction at p. Finally, if E has additive reduction at p, we say $L_p(s) = 1$.

Definition 6.2 (Hasse-Weil L-function)**.** We define the Hasse-Weil L-function for a particular elliptic curve E as follows:

$$L_E(s) = \prod_{p \text{ prime}} L_p(s).$$

The Hasse-Weil L-function encodes a lot of number-theoretic information that is important to the elliptic curve.

Theorem 6.3 (Taniyama-Shimura-Weil Conjecture)**.** *The Hasse-Weil function can be expressed as*

$$L_E(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

In addition, the coefficients a_i are the coefficients of the Fourier series of some modular form $f(E, \tau)$, so that

$$f(E, \tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i \tau}.$$

This conjecture, posed by Taniyama and Shimura, was proven in [Wil95], and with it, Fermat's Last Theorem:

Theorem 6.4 (Fermat's Last Theorem)**.** *The equation $x^n + y^n = z^n$ has no integer solutions with $x, y, z \neq 0$ for $n > 2$.*

7. Elliptic Curve Cryptography

To define elliptic curve cryptography, we'll look at the Diffie-Helman algorithm, which offers a method of public-private key encryption for general groups.

Let G be a finite abelian group (with operation $\cdot$), and let $g \in G$ be a known element of order o. If $G_0 = \langle g \rangle$ is the cyclic subgroup of G generated by g, we have an isomorphism $\exp_g : \mathbb{Z}/q\mathbb{Z} \to G_0$ such that $\exp_g(k) = g^k$. The inverse map of $\exp_g$ is called the discrete logarithm: $\log_g : G_0 \to \mathbb{Z}/q\mathbb{Z}$.

The property that is key to group cryptography is the fact that the discrete logarithm is extremely difficult to calculate, and is very computationally complex.

Now, suppose that two parties, Alice and Bob, want to communicate confidentially over an unsecured channel. They then want to send their messages encrypted with a secret key

known only to them. But how do they agree upon a secret key if this information itself must be exchanged over the channel?

This can be done with a public key method invented by Diffie and Helman. First, Alice and Bob agree on a triple (G, g, q) with a group G and an element $g \in G$ with order q. This triplet is a public key.

Now, for every new session, a new private key is established in the following manner:

(1) Alice chooses a random number $\alpha \in \mathbb{Z}/q\mathbb{Z}$ and calculates $a = g^\alpha \in G$, sending this to Bob.

(2) Bob chooses a random number $\beta \in \mathbb{Z}/q\mathbb{Z}$ and calculates $b = g^\beta \in G$, sending this to Alice.

(3) Now, Alice calculates b^α, and Bob calculates a^β. Now, they both have the same number $k = g^{\alpha\beta}$, which can now be used as a private key.

Any adversary who aims to intercept their communication must find g^α and g^β from $g^{\alpha\beta}$; this task, known as the Diffie-Helman problem, has no better solution than to find the discrete logarithm [Hus87].

For elliptic curve cryptography, we do much the same thing.

Definition 7.1 (Elliptic Curve Key Pairs)**.** Given a set of parameters that include a base field prime p, an elliptic curve $E/\mathbb{F}_p$, and a base point G of order n, an elliptic curve key pair consists of a private key d, a randomly selected nonzero integer in $\mathbb{Z}/n\mathbb{Z}$, and a public key $Q = dG$, the result of adding G to itself d times. Then the public key Q is randomly generated from the base point G.

However, as quantum computing advances, elliptic curve cryptography is increasingly threatened by quantum algorithms, which offer faster ways to solve the discrete logarithm problem. [PZ24] discusses the primary quantum algorithm for doing so, which involves using a Quantum Fast Fourier Transform to compute the logarithm using two quantum registers in parallel.

8. Isogeny Cryptography

In preparation for Q-day, or the day in which quantum algorithms finally become able to crack traditional cryptography algorithms, security experts have been analyzing new, even stronger methods of encryption. One such method uses elliptic curve isogeny instead of addition to encrypt messages.

Definition 8.1. Any surjective group morphism between two elliptic curves is called an isogeny.

Definition 8.2. A complex lattice Λ is a discrete subgroup of $\mathbb{C}$ with a basis (w_1, w_2) with $\frac{w_2}{w_1} \notin \mathbb{R}$ such that $\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$.

Definition 8.3. Two lattices Λ_1 and Λ_2 are homothetic if there exists $z \in \mathbb{C}$ such that $\Lambda_1 = z\Lambda_2$.

Definition 8.4. We define the Eisenstein series of weight $2k$ as

$$G_{2k}(\Lambda) = \sum_{w \in \Lambda n\{0\}} w^{-2k}.$$

Definition 8.5. We define $g_2(\Lambda) = g_2 = 60G_4(\Lambda)$ and $g_3(\Lambda) = g_3 = 140G_6(\Lambda)$.

Definition 8.6. The modular j-invariant of a complex lattice Λ is defined by

$$j(\Lambda) = \frac{g_2(\Lambda)^2}{g_2(\Lambda)^2 - 27g_3(\Lambda)^2}.$$

Definition 8.7. Let Λ be a complex lattice. Then the Weierstrass $\wp$ function of Λ is the series

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in \Lambda n\{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

Theorem 8.8. *[Feo17] The Weierstrass $\wp$ function satisfies the following properties:*

(1) *It is an elliptic function on Λ, i.e. $\wp(z) = \wp(z+w)$ whenever $z \in \mathbb{C}$ and $w \in \Lambda$.*

(2) *Its Laurent series around $z = 0$ is*

$$\wp(z) = \frac{1}{z^2} + \sum_{z=1}^{\infty} (2k+1) G_{2k+2} z^{2k}.$$

(3)

$$\left(\frac{d\wp(z)}{dz} \right)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

for all $z \notin \Lambda$.

(4) *The curve E defined by*

$$y^2 = 4x^3 - g_2 x - g_3$$

is an elliptic curve over $\mathbb{C}$.

Theorem 8.9. *[Feo17] Let E_1 and E_2 be elliptic curves over $\mathbb{C}$ with corresponding lattices Λ_1 and Λ_2. Then there exists a bijection between the group of isogenies from E_1 to E_2 and the group of maps ϕ_a for all a such that $\Lambda_1 \subset a\Lambda_2$.*

Theorem 8.10. *[Feo17] Let E be an elliptic curve, and let G be a finite subgroup of E. Then there exists a unique elliptic curve E_1 and a unique isogeny ϕ such that $\ker \phi = G$ and ϕ takes E to E_1.*

Definition 8.11. An isogeny graph is a multi-graph whose nodes are the j-invariants of isogenous curves, and whose edges are the isogenies between said curves.

Now, we define Supersingular Isogeny Diffie-Helman (SIDH) as follows. We choose a large prime p and two small primes p_a and p_b. The large vertex set will be the set of j-invariants under $\mathbb{F}_p^2$. In a similar manner to that of Diffie-Helman, Alice makes a graph of p_a-isogenies, whereas Bob uses p_b-isogenies.

Then Alice and Bob choose cyclic subgroups of their sets. To create a key exchange system, each publishes more information about their isogenies, enabling the other to compute it.

And [Feo17] explains why SIDH is so efficient: to make a 128-qubit secure system, one would need a 768−bit prime of the form $p_a^{e_a} p_b^{e_b} \pm 1$. One such known prime is $2^{387}3^{242} - 1$.

References

[BS13] Manjul Bhargava and Arul Shankar. The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1. *Number Theory*, 2013.
[Feo17] Luca De Feo. Mathematics of isogeny based cryptography. *École mathématique africaine*, 2017.
[Has36] Helmut Hasse. Zur theorie der abstrakten elliptischen funktionenkörper. *Crelle's Journal*, 1936.
[Hus87] Dale Husemoller. *Elliptic Curves*. Springer, 1987.
[Nea] Ashley Neal. Elliptic curves.
[PZ24] John Proos and Christof Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. 2024.
[Sut17] Andrew Sutherland. Elliptic curves. 2017.
[Wil95] Andrew Wiles. Modular ellipic curves and fermat's last theorem. *Annals of Mathematics*, 1995.