Eliptic Curves and Cryptrography systems

Toby Varney

April 2025

1 Introduction

Ever since humans discovered mathematics, we have effectively used graphs and drawings to aid in visualizing the behavior of functions and real world problems. From earlier astronomers like Aristarchus of Samos who calculated the Moon's distance from earth by observing Earth's shadow during a lunar eclipse to Andrew Wile's epic proof of Fermat's Last theorem, simplifying problems using graphs has remained constant throughout time. Though they have also been used for other purposes as time has moved forward, such as their use in Elliptic Curve Cryptography

In this essay, we will discuss one of the most infamous curves of all time, the elliptic curve, and it's interesting properties such as modular forms. We will also investigate their history and how they are used in cryptography.

Some prerequisites...

To begin with, an elliptic curve is a mathematical concept from the field of algebraic geometry and number theory. The history of the elliptic curve dates back to ancient Greece where they were used in studying diophantine equations, which are a type of equation with two or more integer unknown's. The theory behind elliptic curves was first formalized by Carl Jacobi, a German mathematician, in 1834. An elliptic curve is defined by an equation of the form:

$$y^2 = x^3 + ax + b \tag{1}$$

where a and b are constants. The curve must satisfy a condition to be non-singular, which means that it has no sharp points or self-intersections so that every point on the curve has a unique tangent line. The curves are typically studied over the real or complex numbers. (1)
To study the elliptic curve without mentioning Sir Andrew Wile's proof of Fermat's Last Theorem would be like trying to complete a puzzle whilst missing some of the pieces, impossible. Fermat's last theorem is as follows: there exists no three positive integers a, b, and c that satisfy the equation

$$a^n + b^n = c^n \tag{2}$$

for any $n > 2$. This fairly simple looking equation had stumped mathematicians for over 350-years, making the proof even more remarkable. (2)
In order to rigorously prove FLT, Wile's built on the Taniyama-Shimura-Weil conjecture, which states that every elliptic curve is modular, meaning it corresponds to a modular form, something we will be investigating now.

Modular Forms

In number theory, modular forms are functions that specifically work on the set of numbers from the upper half-plane. If you were to imagine the argand diagram, the upper half-plane is the top right-hand quadrant, or the section where the imaginary part of the complex number is positive ($a + bi$ where $b > 0$). What makes modular form's interesting is their symmetry. (3)

The symmetry involves a set of transformations called the modular group, which is a collection of rules for changing an input τ (where τ is a number in the upper half-plane). These transformations are written as:

$$\tau \to \frac{a\tau + b}{c\tau + d} \tag{3}$$

Where a, b, c, d are integers and satisfy a condition: $ad - bc = 1$. We can think of these as transformations to twist or shift the input τ.

How the Symmetry works
The symmetry in the modular group means that the transformations follow the

function below

$$f(\frac{a\tau + b}{c\tau + d}) = (c\tau + d)^k f(\tau) \tag{4}$$

where f(x) is the function for our modular form. As the transformation follows this rule every time, these transformations don't change the function into something completely unrecognizable from before the transformation. The transformation just scales it by a factor which depends on c, d, τ and k, which makes modular forms symmetric in nature. But can't we also just transform graphs by just shifting them right or left, up or down? Whilst this is also a transformation and still applies to elliptic curves, having such a unique symmetry allows the curve to become far more useful than what meets the eye.

Why are transformations important?
It is this symmetry that allows mathematicians to use tools from other areas of maths and connect them to number theory. It also makes elliptic curves useful outside of the abstract world of pure mathematics, such as Elliptic-Curve Cryptography which keeps our bank account's safe (will be discussed later)

2 The connection to eliptic curves

In the 1950s - 1960s a connection between elliptic curves and modular forms was conjectured by the Goro Shimura following on from the work of Yutaka Taniyama. The conjecture states that every rational elliptic curve is modular. Without getting into the specific details of L-functions and fourier series, this connection relates elliptic curves, geometric shapes which may not initially have any obvious rules or predictability (other than the general points on the curve) to modular forms, which are symmetric and have many patterns. This relation is incredibly important as it simplifies finding solutions to equations and, other times, helps formulate a proof. One way in which it is useful is that it allows you to be able to count how many points are on the curve *modulo p*.

Connection for FLT
If Fermat's Last Theorem had a solution, it would give rise to an elliptic curve called the Frey curve when you plot the points (a, b) that satisfy Fermat's equation $a^n + b^n = c^n$. The Modularity Theorem states that every elliptic curve must be associated with a modular form. However, Wiles proved that no mod-

ular form could exist for the Frey curve, as it would contradict the symmetric properties that modular forms must satisfy. Therefore, the Frey curve cannot exist, and neither can the solution to Fermat's equation. (6)

3 Theory aside, what about real life?

The last 3 pages have been fairly abstract and may seem completely inapplicable to real life. However, this could not be further from the truth. As our lives continue to become increasingly digitalized, our need for more advanced personal and large-scale privacy and security also increases. One method for protecting our data is Elliptic Curve Cryptography, or ECC for short.

What is Elliptic Curve Cryptography?

Elliptic-curve cryptography is a public-key cryptography method that is based on the algebraic structure of elliptic curves. ECC was first introduced in 1985 by Victor Miller of IBM and Neil Koblitz of the University of Washington. One interesting property of elliptic curves that is used in ECC is that a line drawn through the curve can only intercept the curve at most three times. In ECC, the curves are defined over a finite field, which is usually a prime field of F_p. However, this language is a bit technical, so I will explain what it all means.

Terminology explanation

Key

The keys used in real life and digitally differ in how they perform their specific task. However, they both serve essentially the same purpose, to "lock" and "unlock" the entry point to something we want to protect. In encryption, a key is a piece of information used to control how data is transformed from an encrypted format to its original form and vice versa. The public key is critical in cryptographic algorithms as it ensures that only authorized parties can access and interpret the encrypted data. The key is usually very long, such as in RSA, however in ECC, the key can be 256 bits long and still offer the same level of security

Public Key Cryptography

In public key cryptography there are two keys: a public key and a private key.

The public key and private key are related using an elliptic curve. The public key is used to encrypt the data, and only its corresponding private key can decrypt it. The private key is kept secret, whilst the public key can be shared openly. Public key cryptography uses something called the trapdoor function. A trapdoor function is a type of function that makes it easy to go from a to b but very difficult to go from b to a. Elliptic curve cryptography is a method of public key cryptography. (8)

Finite Fields

A finite field is a field that contains finitely many elements or objects, where we can imagine a field as a sort of abstract container that holds these elements or objects. A finite prime field, or F_p, is a finite field that takes the integers *modulo* a for some prime p. This means that a can take integers from 0 to p and for integers greater than p, a can be the remainder when that number is divided by p. An example of this in practice would be for instance if we took the finite field F_7 . This means that the points x and y in the point (x,y) can only take integer values between 0 and 6 inclusive. If a calculation goes over 7, we divide by 7 and take the remainder. So, for example if we had the elliptic curve (4)

$$y^2 = x^3 - x + 1 \tag{5}$$

and a point (3,5) for example, we could check to see if it was on the curve by plugging x=3 into the equation, which is equal to $3^3 - 3 + 1 = 25$. We now find the remainder when 25 is divided by 7

$$25 \equiv 4 \pmod 7 \tag{6}$$

Now moving over to the LHS value and we do the same thing, $y = 5$ so $y^2 = 5^2 = 25$ and from earlier we know that

$$25 \equiv 4 \pmod 7 \tag{7}$$

Now, As $x \equiv y \pmod 7$, the point (3,5) is on our elliptic curve. If x and y are not congruent *modulo* 7, then the point (x,y) is not on the curve. These con-

gruent x and y values make up the pairs of point's that are in the prime field F_7.

How ECC works

We said earlier that a line drawn through the elliptic curve intercepts it at most three times. Now imagine a line that intercepts the curve at exactly three distinct points which will call A, B and C. Because of the structure and symmetry of elliptic curves, there exists an operation that we can perform on A and B that produces our third point C. Now, if we were to repeatedly perform this operation, it would result in very large x and y values for our point C. Therefore we have to set a maximum value that x can be on our point, and we will set this equal to n. This maximum value n is the size of our key and therefore as we increase the size of our key, there are more valid values of x that C can take and thus more potential points. Because there are more possible points as the size of the key increases, the length of time it takes to crack the ECC system also increases. The process of repeatedly performing operations on points is called point addition and I will discuss it further in discrete logarithm problem section.

Why use ECC?

The main advantage of ECC is that key sizes that are 256 bits long offer the same security as other cryptography systems, such as RSA, which use keys that are 2056 bits long. This allows ECC certificates, things encrypted using ECC, to be much faster to decrypt and take up less bandwidth when they are being transferred. Furthermore, ECC offers better resilience against quantum computers which will be important in the future.

4 The Discrete Logarithm problem

To understand the discrete logarithm, we need to understand standard logarithms. Logarithms find the exponent required to get from one number, often called the base, to another number. For example:

$$log_2 8 = 3 \tag{8}$$

The discrete logarithm is similar to standard logarithms but instead of working with real number's we use numbers that are part of a finite field, which we

explained earlier. The discrete logarithm asks for what value of x is (5)

$$a^x \equiv c \pmod{b} \tag{9}$$

For example, we will use the finite group of integers modulo 11, which includes the numbers from 0 to 10, and we will take the base of the logarithm as 2. We want to find the discrete logarithm of 9 with respect to base 2 modulo 11. This is equivalent to finding the value of x such that

$$2^x \equiv 9 \pmod{11} \tag{10}$$

Which is asking: What power of 2, when divided by 11, gives a remainder of 9.

Solution
To solve, we try small powers of and continue until we find a power of 2 that has a remainder of 9 when divided by 11

$$\begin{aligned} 2^1 &\equiv 2 \pmod{11} \\ 2^2 &\equiv 4 \pmod{11} \\ 2^3 &\equiv 8 \pmod{11} \\ 2^4 &\equiv 5 \pmod{11} \\ 2^5 &\equiv 10 \pmod{11} \\ 2^6 &\equiv 9 \pmod{11} \end{aligned} \tag{11}$$

As $2^6 \equiv 9 \pmod{11}$ the discrete logarithm of $9 \pmod{11}$ with base 2 is 6.

The challenge of the Discrete Logarithm Problem is that for large numbers it is computationally difficult and (very) time consuming to find x given a, c, and b for very large values. It is this property that the elliptic curve cryptography system relies on and ensures that it is kept secure

ECC and The Discrete Logarithm Problem

Elliptic Curve Cryptography (ECC) uses the discrete logarithm problem but applied to points on the curve instead of numbers modulo a prime.

For example, lets say we have a point P on the elliptic curve. We can add P to itself many times and every new point formed but continually adding P to itself will be on the curve. This process is called point addition and is another

property of elliptic curves. The main goal of the elliptic curve discrete logarithm problem is to find an integer K such that

$$K * P = Q \tag{12}$$

Where P is the original point on the curve and Q is also a point on the curve. The discrete logarithm problem for ECC want's to find the value of K in the equation above

Why do we use the discrete logarithm problem?

It is fair to say that security is relatively important to a cryptography system, so how secure is the discrete logarithm in terms of making ECC safe? The discrete logarithm system make's ECC very secure because of the difficulty of actually solving the problem itself. The discrete logarithm problem for ECC is difficult to solve as the points on an elliptic curve are structured in a way that makes it very difficult to reverse the point addition operation. This is because after being given a point P and a result (another point on the curve) Q, it is infeasible to find the integer K such that $P * K = Q$ due to the computational power and the length of time that the system must run to find a solution as their are no efficient methods that are known currently and as the time it takes to solve grows exponentially as the numbers involved in the equation increase in size.

5 Conclusion

To conclude, we have discussed the general form of an elliptic curve and some of it's interesting properties such as modular forms and how the symmetries behind elliptic curves make them far more interesting than what meets the eye. We then looked into their applications to elliptic curve cryptography and the discrete logarithm problem and how these abstract mathematical concepts are fundamental to the function of some simple, everyday activities. Thank you for taking the time to read my essay.

6 References

(1) `https://en.wikipedia.org/wiki/Elliptic_curve`
(2) `https://en.wikipedia.org/wiki/Fermats_Last_Theorem`

(3) https://en.wikipedia.org/wiki/Modular_form
(4) https://en.wikipedia.org/wiki/Finite_field
(5) https://en.wikipedia.org/wiki/Discrete_logarithm
(6) https://en.wikipedia.org/wiki/Frey_curve
(7) https://en.wikipedia.org/wiki/Public-key_cryptography