Extended Essay

Topic: Elliptic curve and its application to cryptography

Subject: Mathematics

Research Question: How is an elliptic curve derived from an ellipse, and how can the properties of an elliptic curve be applied to cryptography?

Word Count: 3282

Contents

Introduction

A few years ago, I read a book related to cryptography. It introduced various types of cryptography methods from the history of time, such as Caesar cipher, Enigma, to modern cryptography methods such as AES or RSA. One of the cryptography methods that piqued my interest is elliptic curve cryptography, which is only introduced but not explained in the book. As it is not explained other than briefly mentioned that it exists, it made me very interested in what the elliptic curve cryptography is about. However, at that time, I was not able to find resources on how the elliptic curve works, and I did not have enough knowledge to understand how cryptography works. Now, I am able to understand how the elliptic curve cryptography works from new mathematical concepts I have learned over the years, and I was also able to find out how the elliptic curve originated. The in-depth concepts are difficult to understand as the knowledge required for it is only imparted in graduate programs. Therefore, I tried to understand and explain what the elliptic curve is, and how the elliptic curve cryptography is created, using my limited knowledge.

What an Elliptic Curve is About

An Elliptic curve is a curve that is defined as:

$$y^2 = x^3 + ax + b$$[1]

On a cartesian coordinate system, and a and b being real numbers. Additionally, it also has to satisfy a discriminant not being equal to zero:

$$\Delta = -16(4a^3 + 27b^2)$$

The discriminant comes from calculating the existence of repeated root in cubic equation, in special form $y = x^3 + ax + b$. For repeated root to exist, the root of the original equation should also be the root of the derivative of original equation. This means that $y = x^3 + ax + b$ and $y' = 3x^2 + a$ have the same root. Let the repeated root x, then

$$0 = x^3 + ax + b$$

$$0 = 3x^2 + a$$

Rearranging the second equation gives:

$$x = \sqrt{-\frac{a}{3}}$$

Substituting into first equation gives:

$$-b = \sqrt{-\frac{a}{3}}^3 + a\sqrt{-\frac{a}{3}}$$

$$= \sqrt{-\frac{a}{3}}\left(a - \frac{a}{3}\right)$$

$$= \sqrt{-\frac{a}{3}}\frac{2a}{3}$$

Squaring both sides give:

[1] https://mathworld.wolfram.com/EllipticCurve.html

$$b^2 = -\frac{4a^3}{27}$$

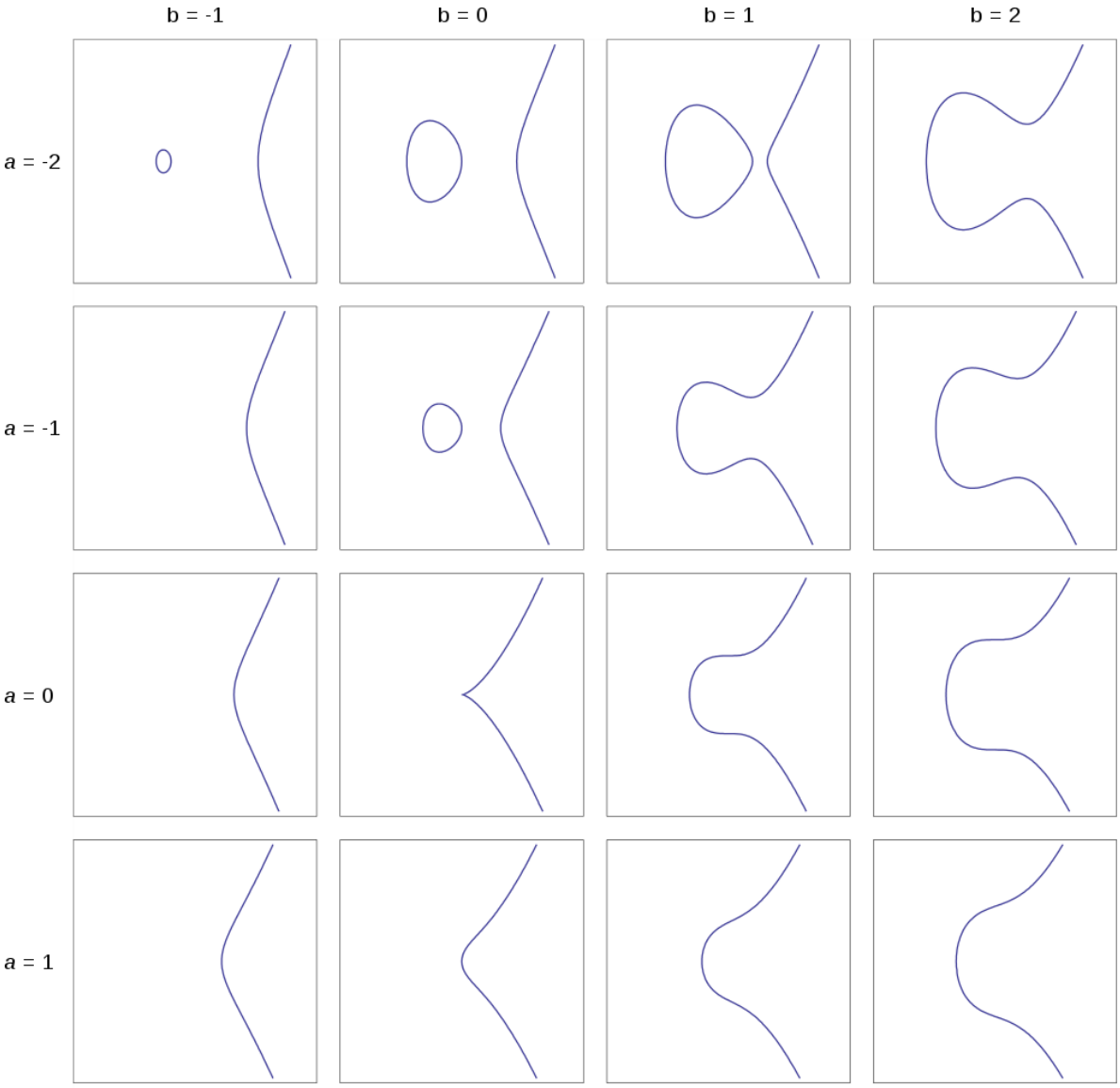
Rearranging this equation gives:

$$4a^3 + 27b^2 = 0$$

Therefore, for repeated root to exist in the equation $y = x^3 + ax + b$, it should satisfy the condition $4a^3 + 27b^2 = 0$. When the repeated root exists in the equation $y = x^3 + ax + b$, it follows that equation $y^2 = x^3 + ax + b$ is not an elliptic curve. Therefore, for a curve to be an elliptic curve, it must satisfy the discriminant $4a^3 + 27b^2 \neq 0$.

The factor -16 itself is not useful in determining whether the curve is elliptic or not, but it is said to be useful in the advanced study of elliptic curves.

The discriminant also tells you whether the curve will have two components or one component on a cartesian plane, where if the discriminant is positive, the graph has two components, and when the discriminant is negative, the graph has one component.



[2]

The diagram above shows different kinds of elliptic curves, with the exception of the case a=0, b=0 which is the case when the discriminant is zero, which indicates it is not an elliptic curve.

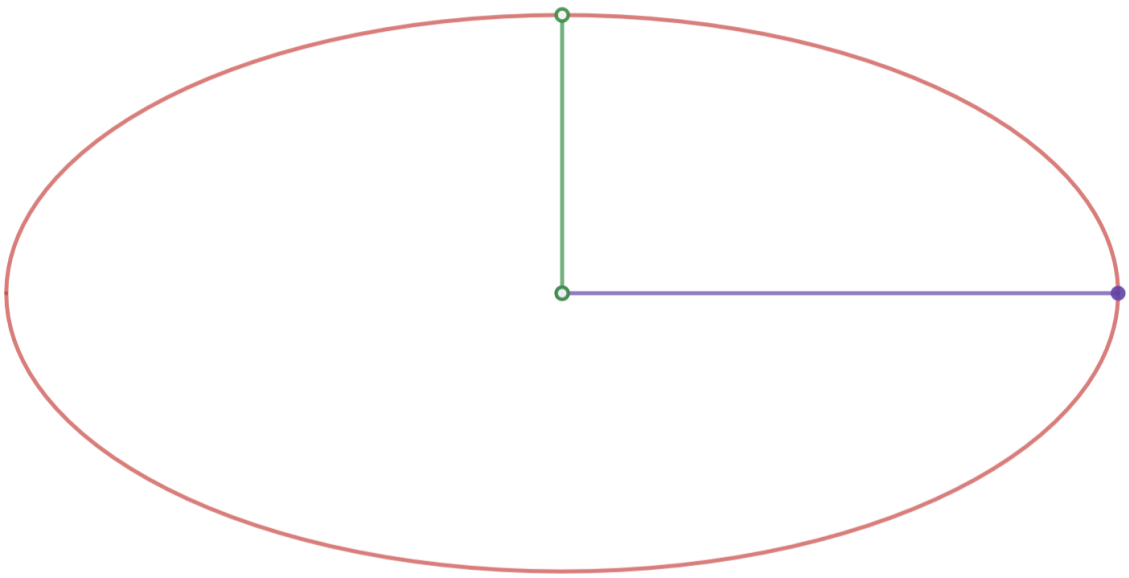
[2] https://commons.wikimedia.org/wiki/File:EllipticCurveCatalog.svg

Derivation of Elliptic Curve from Ellipse

As the name suggests, the elliptic curve originated from ellipse. The original purpose of the elliptic curve is to calculate the circumference of an ellipse. On cartesian coordinate system, ellipse is defined as:

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

And the drawing of an ellipse is shown below when a=4 and b=2. In case of a > b, a (horizontal line) is called as semi-major axis and b (vertical line) is called as semi-minor axis.



The area of an ellipse is commonly known as πab. However, it is not possible to show the circumference of ellipse, as elementary functions. Elementary functions are defined as functions that are sum and product of polynomials, exponents, logarithms, trigonometry, and other basic functions. As the circumference of an ellipse is not possible to be shown with the forms of elementary functions, arc length method should be used to calculate the circumference of an ellipse.

To calculate the circumference of an ellipse, the first step is to parameterize the function. Assuming the centre of an ellipse is (0,0), and a and b are axes of an ellipse, the parametric equation of an ellipse can be written as:

$$x = a(\cos(t)), y = b(\sin(t))$$

Where 0 ≤ t ≤ 2π.

The arc length of a function in a parametric equation is defined as:

$$L = \int_{\alpha}^{\beta} \sqrt{(\frac{dx}{dt})^2 + (\frac{dy}{dt})^2}\, dt$$

Where $\frac{dx}{dt}$ and $\frac{dy}{dt}$ denotes the derivative of each parametric equation, and alpha and beta denotes the starting and end point of the parametric equation.[3]

To find the circumference of an ellipse, first find the derivative of each parametric equation:

$$\frac{dx}{dt} = -a(\sin(t)), \frac{dy}{dt} = b(\cos(t))$$

Next, put the derivative of each parametric equation into the arc length formula:

$$L = \int_{0}^{2\pi} \sqrt{(-a(\sin(t))^2 + (b(\cos(t))^2}\, dt$$

$$= \int_{0}^{2\pi} \sqrt{a^2\sin^2(t) + b^2\cos^2(t)}\, dt$$

[3] https://tutorial.math.lamar.edu/classes/calcii/ParaArcLength.aspx

To remove one of the trigonometric functions, one of the trigonometric identities $\sin^2(t) + \cos^2(t) = 1$ is used.

$$L = \int_0^{2\pi} \sqrt{(a^2 - b^2)\sin^2(t) + b^2(\sin^2(t) + \cos^2(t))}\, dt$$

$$= \int_0^{2\pi} \sqrt{(a^2 - b^2)\sin^2(t) + b^2}\, dt$$

Take the b out of the integral:

$$L = b\int_0^{2\pi} \sqrt{\left(\frac{a^2}{b^2} - 1\right)\sin^2(t) + 1}\, dt$$

$$= b\int_0^{2\pi} \sqrt{1 + \frac{a^2 - b^2}{b^2}\sin^2(t)}\, dt$$

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

Substitute k^2 in $\frac{b^2-a^2}{b^2}$. In this case, it will be assumed that b ≥ a. This will show that 0 ≤ k ≤ 1. However, when k=0 it the integral will simply be a line, and k=1 the integral will simply be a circle. Therefore, those cases are removed, so it becomes 0 < k < 1.

$$L = b\int_0^{2\pi} \sqrt{1 - k^2\sin^2(t)}\, dt$$

When the constant b is removed, this integral is famously known as the elliptic integral, more specifically elliptic integral of a second kind, when the upper boundary of the integral is a variable instead of a constant, 2π.

Now remove the constant b and substitute $s = \sin^2(t)$. Chain rule can be used to calculate $\frac{ds}{dt} = 2\sin(t)\cos(t)$. Since $s = \sin^2(t)$:

$$\sin(t) = \sqrt{s}, \cos(t) = \sqrt{1 - s}, dt = \frac{ds}{2\sqrt{s}\sqrt{1 - s}}$$

Substitute s and dt into the equation above:

$$L = \int_0^{2\pi} \frac{\sqrt{1-k^2 s}}{2\sqrt{s}\sqrt{1-s}}\, ds$$

Take the 1/2 outside and multiply both numerator and denominator by $\sqrt{1-k^2 s}$:

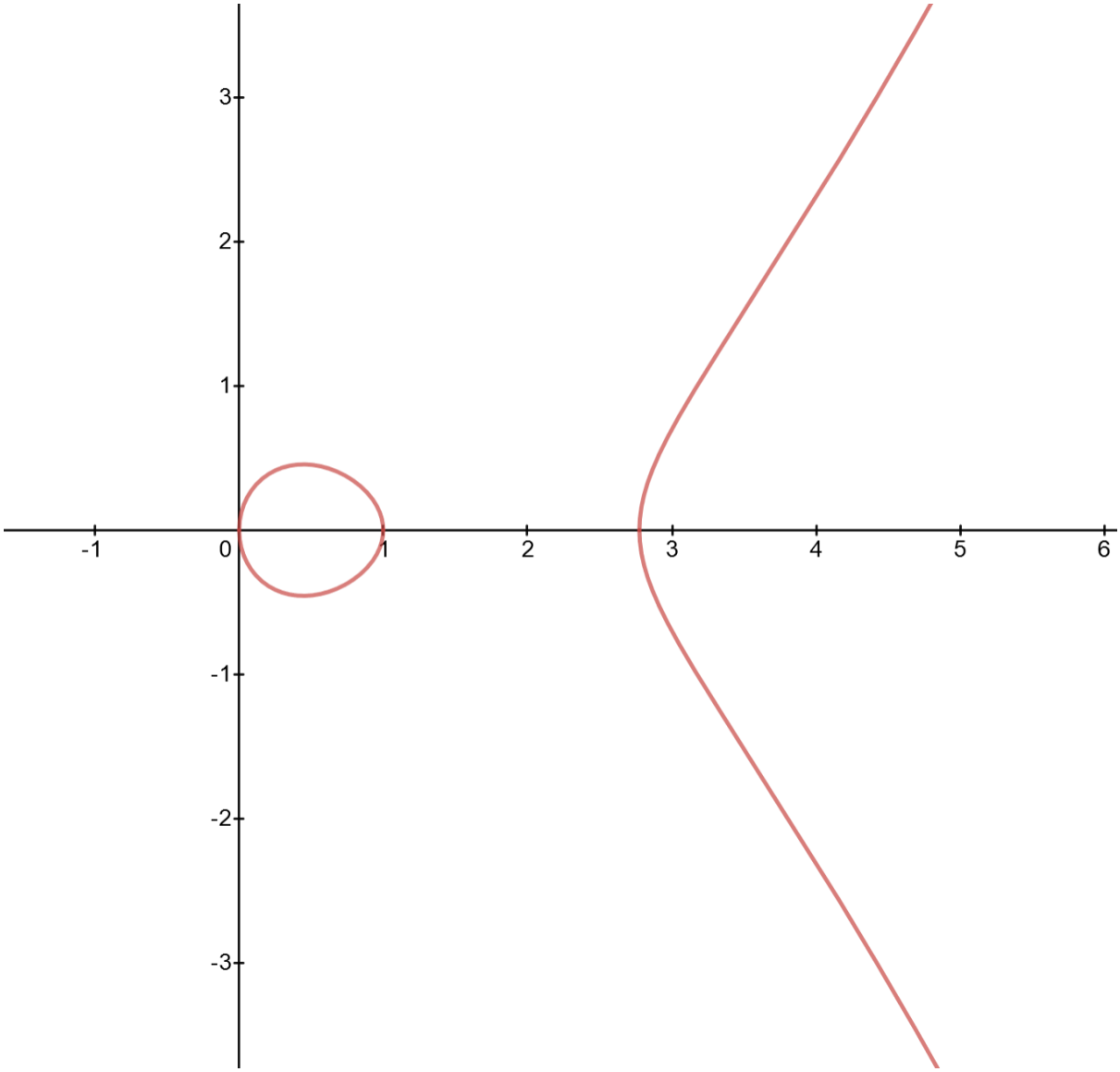
$$L = \frac{1}{2}\int_0^{2\pi} \frac{1-k^2 s}{\sqrt{s}\sqrt{1-s}\sqrt{1-k^2 s}}\, ds$$

The denominator, $\sqrt{s}\sqrt{1-s}\sqrt{1-k^2 s}$, is an expression of an elliptic curve.[4] From the calculation of circumference of an ellipse, people were able to derive a form of elliptic curve $y = \sqrt{x}\sqrt{1-x}\sqrt{1-k^2 x}$ and got interested in the graph. When both sides are squared, the form

$$y^2 = x(1-x)(1-k^2 x)$$

Which is one form of an elliptic curve. The graph of this function is shown below, in case of $k = 0.6$.

[4] https://www.unf.edu/~ddreibel/mas4932/elliptic-integrals.pdf



From this derivation of the original elliptic curve equation from an ellipse, and the current equation of elliptic curve, it can be thought that initially, the elliptic curve was used to calculate the circumference of an ellipse. However, as the mathematics developed, it can be seen that the elliptic curve is taking a different path from calculating the circumference of an ellipse and used in many different types of applications, and one such application is elliptic curve cryptography.

Elliptic Curve and Cryptography

Elliptic Curve Cryptography is one of the many usages of the elliptic curve. Elliptic Curve Cryptography is considered asymmetric encryption, as the key that is used for encryption and key that is used for decryption is different unlike symmetric encryption, which uses same key for encryption and decryption. For the cryptography, it uses the form that is introduced at the start, which is

$$y^2 = x^3 + ax + b$$

With discriminant

$$\Delta = -16(4a^3 + 27b^2)$$

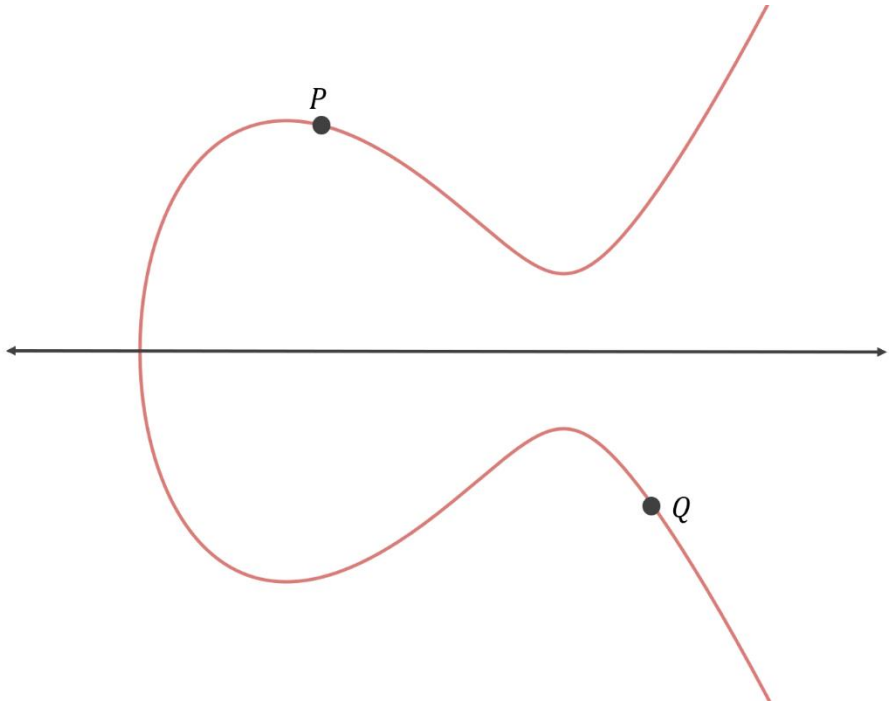
For the Elliptic Curve Cryptography, a special kind of operation is done on elliptic curves, which is called point operation.

Point Operation

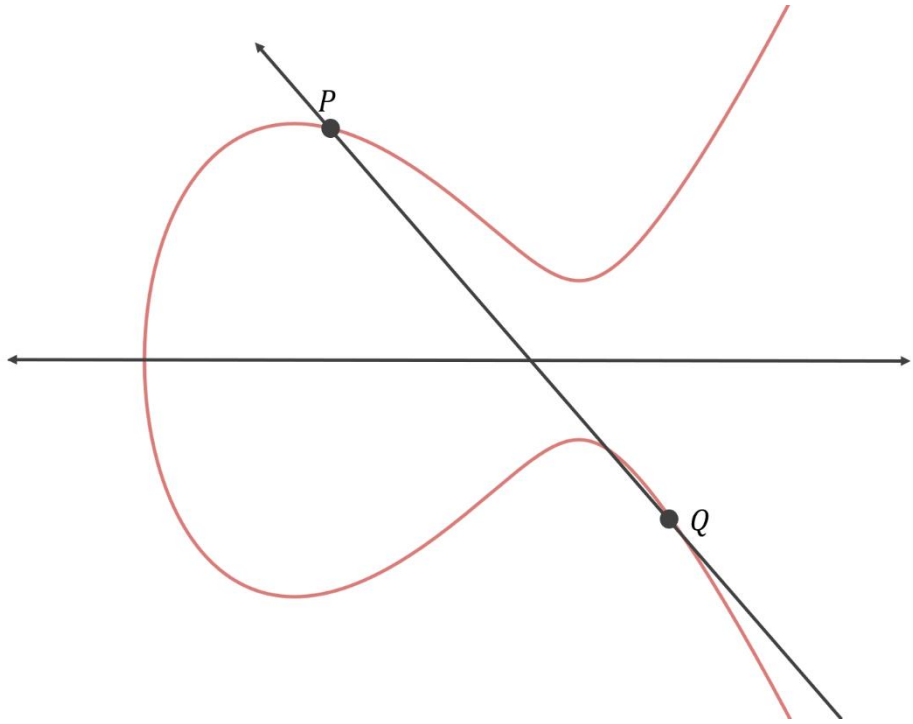
Point operation is divided into several operations, and one of them is called point addition. On an elliptic curve, the point operation is to add two points on an elliptic curve, and get a third point that is the result of the sum of two initial points. The operation is similar to adding two numbers to get a third number.

Point addition is operated as below:

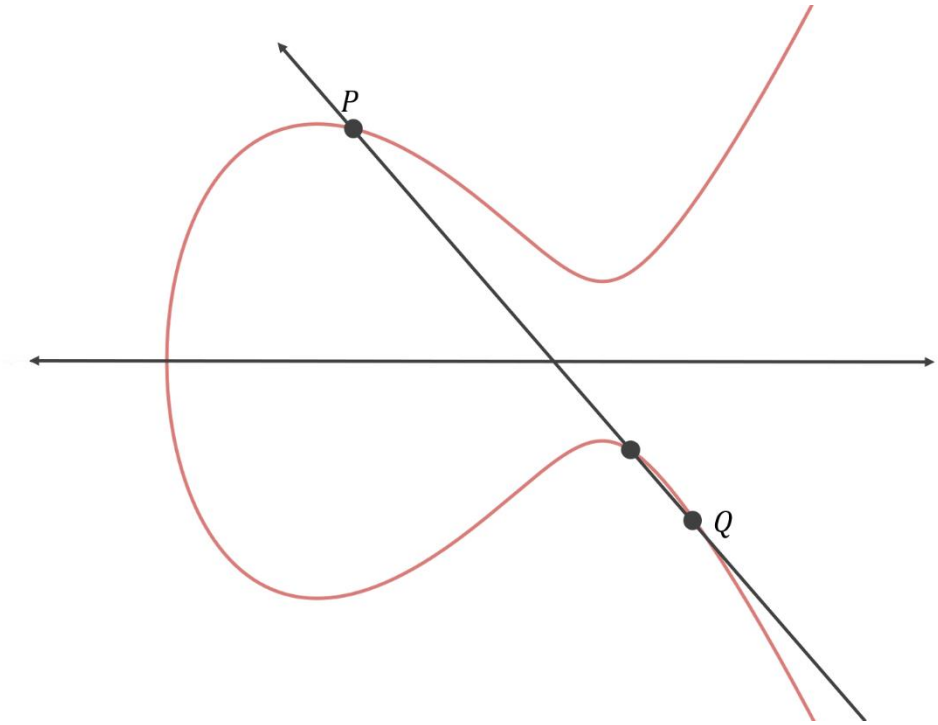
1. Find two points, P and Q to do a point addition.



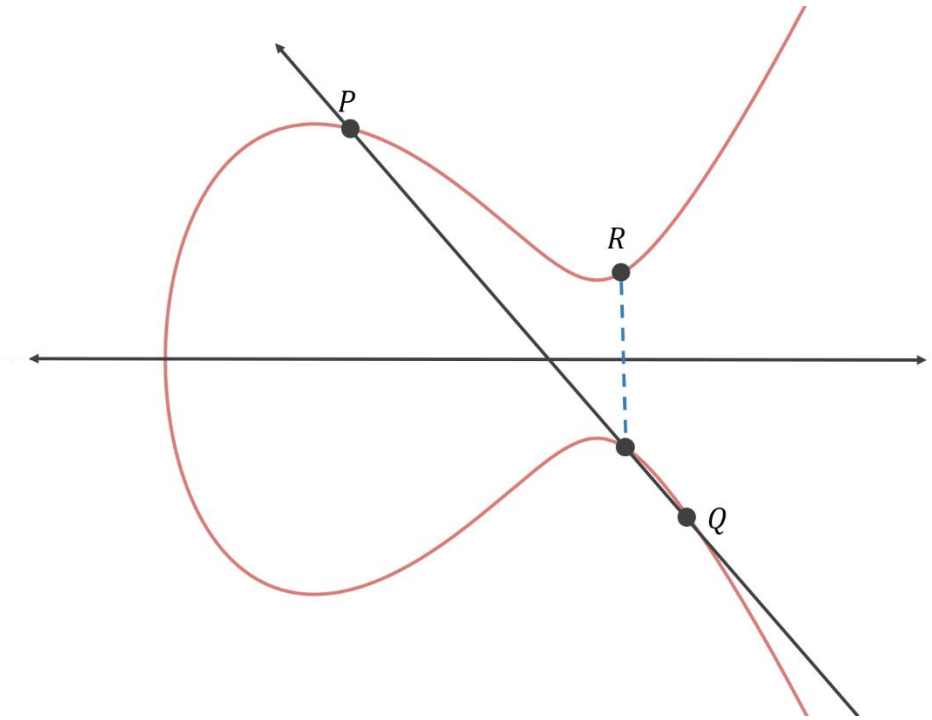
2. Draw a straight line that goes through those two points.



3. Find the third intersection that pass through the curve. This will be point -R.



4. Reflect the point to the x-axis. This will be point R.



Therefore, P + Q = R.[5]

The algebraic calculation of point addition is not very complicated. The basic is to use the equation of line, and use that to calculate the third point that will meet with the elliptic curve.

The slope of a line is

$$m = \frac{y_P - y_Q}{x_P - x_Q}$$

Which is one of a basic formula for equation of a straight line.

The x coordinate of third intersection between the line, and elliptic curve which is point -R is given by equation

$$x_R = m^2 - x_P - x_Q$$

And the y coordinate of point -R is given by equation

$$y_R = y_P + m(x_R - x_P)$$

Which is another formula based on the equation of a straight line.

Finally, $(x_P, y_P) + (x_Q, y_Q) = (x_R, -y_R)$

The part to calculate the x coordinate of -R doesn't seem like intuitive, so here is the proof of why that formula is the case.

As the elliptic curve and line intersects at three distinct points, it can be written as

$$x^3 + ax + b = (mx + c)^2$$

Expanding the right side gives

$$x^3 + ax + b = m^2x^2 + 2cmx + c^2$$

Putting everything on one side gives

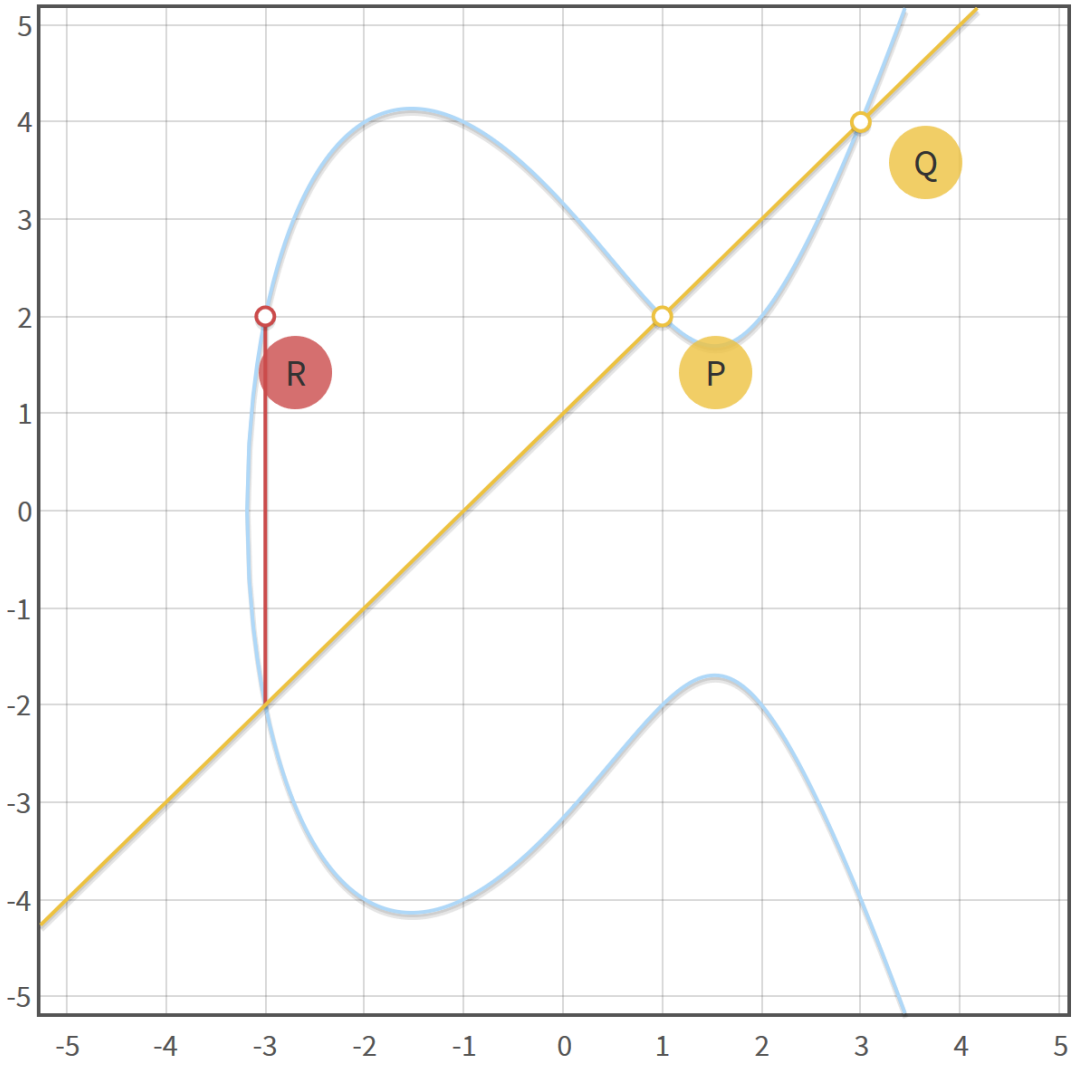
$$x^3 - m^2x^2 + ax - 2cmx + b - c^2 = 0$$

From this equation, it can be seen that $x_P + x_Q + x_R = m^2$ from the sums of roots of

[5] https://hackernoon.com/what-is-the-math-behind-elliptic-curve-cryptography-f61b25253da3

cubic equation, which is also known as Vieta's formulas. Rearranging this equation gives the formula shown above.

For the example below, the curve $y^2 = x^3 - 7x + 10$ and point P (1, 2) and Q (3, 4) is chosen.



[6]

From the geometric addition, the point R gives (-3, 2).

From the algebraic addition, the slope of a line, x co-ordinate, y co-ordinate each gives

$$m = \frac{4-2}{3-1} = 1$$

$$x_R = 1^2 - 3 - 1 = -3$$

[6] https://github.com/andreacorbellini/ecc

$$y_R = 2 + 1(-3 - 1) = -2$$

Finally, combining those two information gives

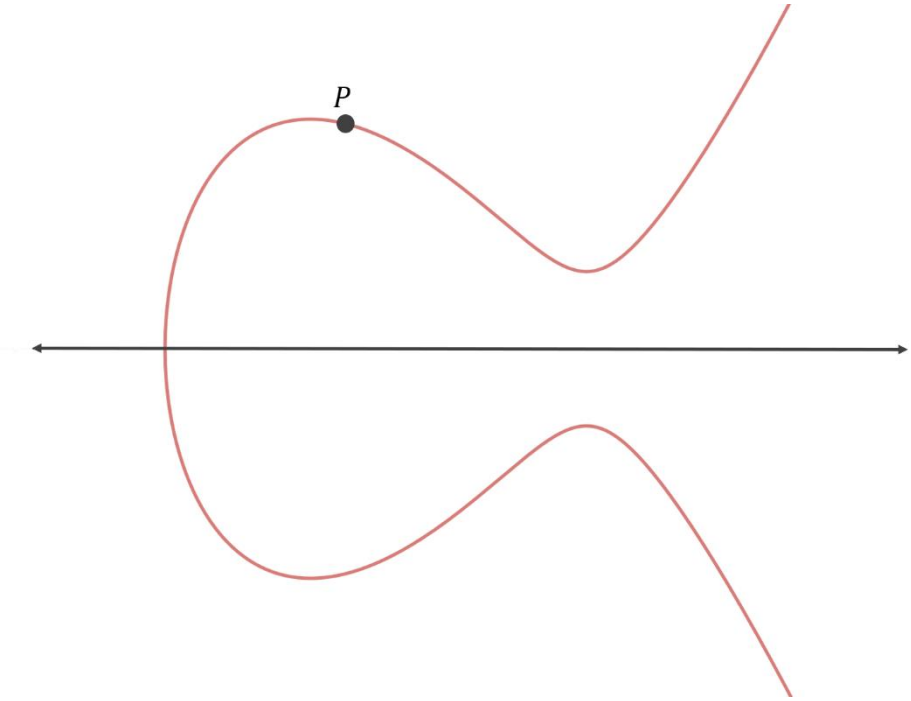
$$R = (x_R, -y_R) = (-3, 2)$$

This is how the point addition is operated on elliptic curve.[7]

Similar to point addition, point multiplication also exists. Point multiplication is defined as a case when in case of point addition, point P is equivalent to point Q. Point multiplication is done in a similar manner. However, in this case, the tangent of the elliptic curve on the original point is used to conduct the operation.

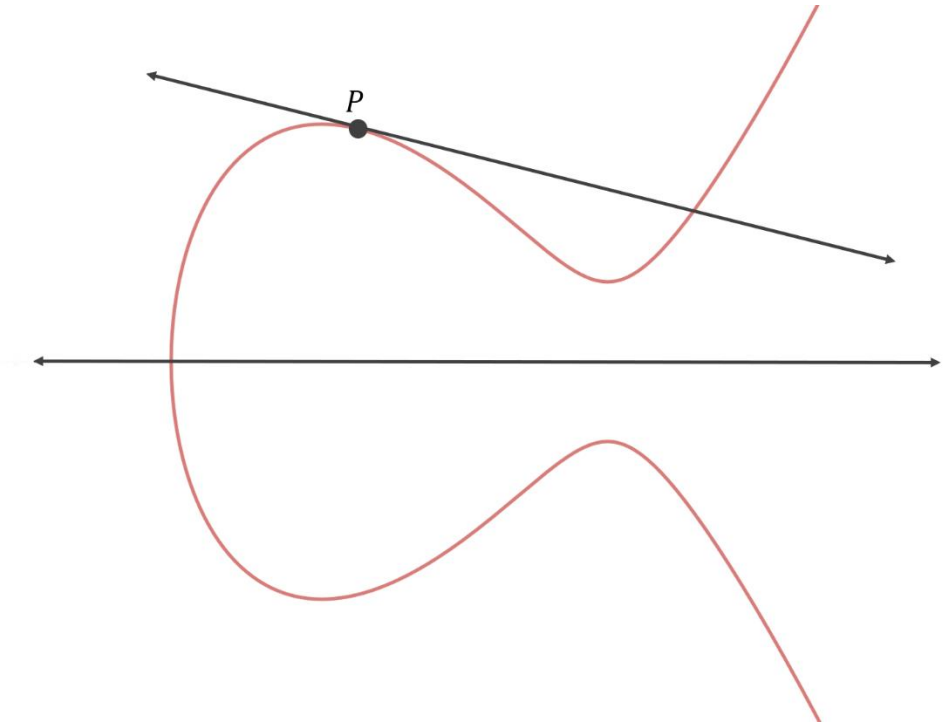
Point multiplication is operated as below:

1. Find the base point P.

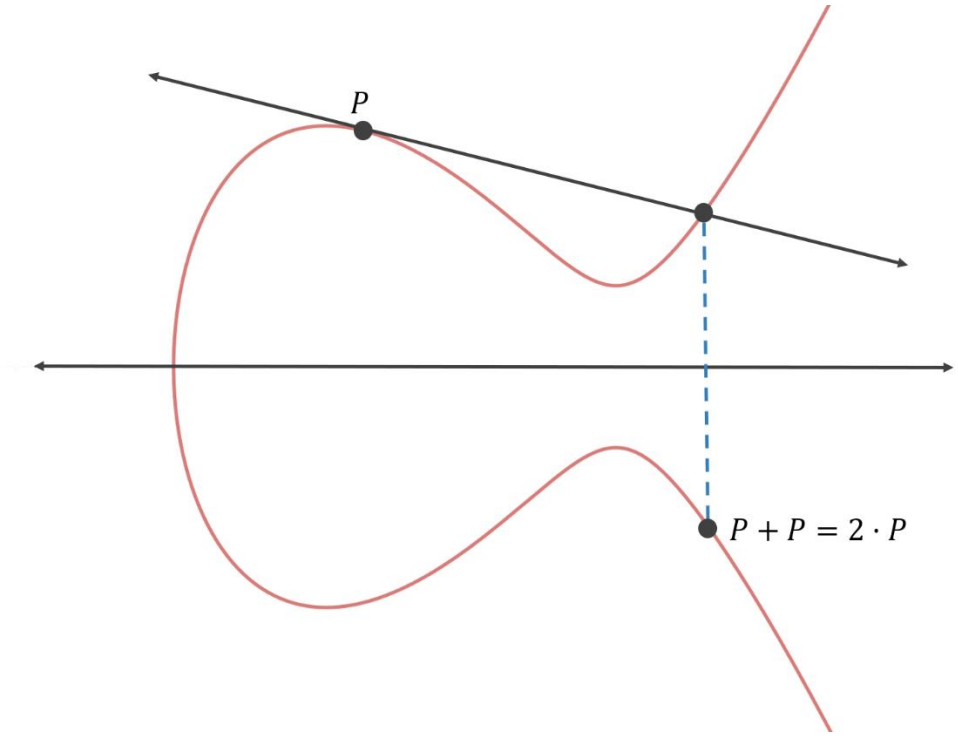


[7] https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/

2. Draw a tangent line to the elliptic curve that passes through point P.

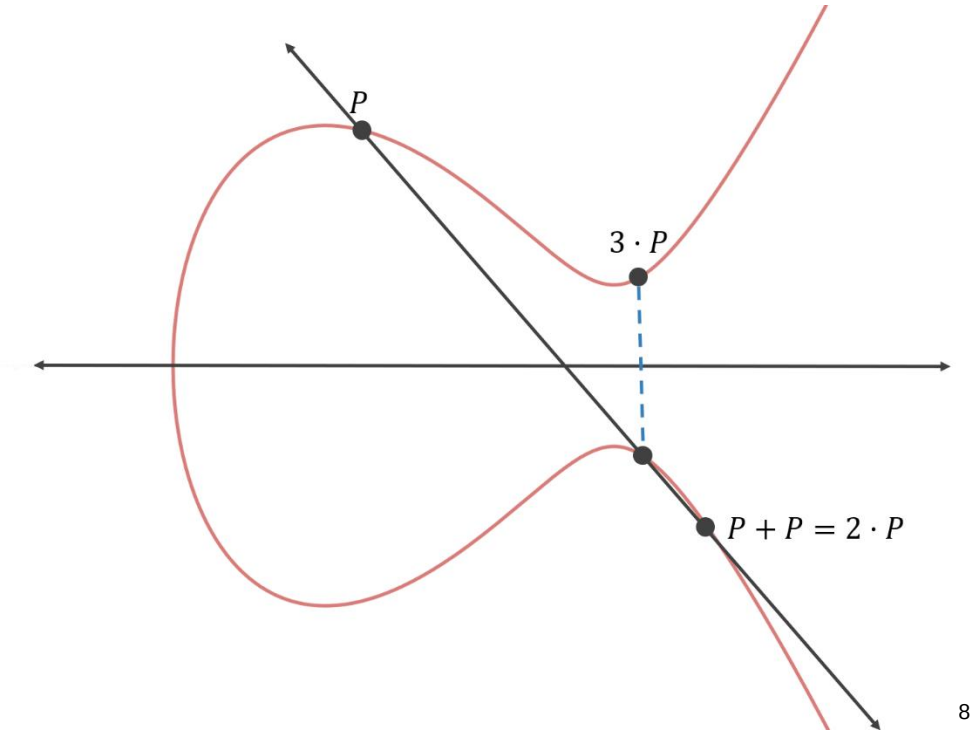


3. Find the second intersection that will pass through the curve.



4. Reflect the point to the x-axis. This will be point 2P, which is equivalent to P+P.

To compute the point 3P, conduct the point addition between point P and 2P and find the point 3P. This operation can be continued to calculate 4P, 5P and further points.



[8]

For the algebraic multiplication of a point, the derivative of elliptic curve is used.

The equation of the slope on a point is

$$m = \frac{3{x_P}^2 + a}{2y_P}$$

Which is an equation of a tangent of elliptic curve on a point.

$$y^2 = x^3 + ax + b$$

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

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

The equation for new point is same as the case when there were three distinct points on the curve.

$$x_{2P} = m^2 - x_P - x_P$$

[8] https://hackernoon.com/what-is-the-math-behind-elliptic-curve-cryptography-f61b25253da3

$$y_{2P} = y_P + m(x_{2P} - x_P)$$

For the example below, the same curve $y^2 = x^3 - 7x + 10$ and point P (1, 2) was chosen for the point multiplication.

[9]

From the geometric addition, the result is point (-1, -4).

From the algebraic addition, the result is

$$x_{2P} = m^2 - x_P - x_P = (-1)^2 - 1 - 1 = -1$$

[9] https://github.com/andreacorbellini/ecc

$$y_{2P} = y_P + m(x_{2P} - x_P) = 2 - 1(-1 - 1) = 4$$

$$2P = (x_{2P}, -y_{2P}) = (-1, -4)$$

Therefore, it can be shown that the point multiplication works.

This point operation brings some interesting properties that it satisfies commutative property which says $P + Q = Q + P$, and associated law which says $P + (Q + R) = (P + Q) + R$. The associated law property is used for the cryptography. However, it is hard to prove why the associated law works in this kind of point operation, which requires a lot of calculations that need to be done beyond the limit that this can provide. Therefore, the proof of why those properties work will be skipped.

From the point multiplication, there is a faster way to operate big point additions in a certain way. One way to do the point addition is to do double and add algorithm. The way it works is to find the power of two of a certain point, then add those points to get the final calculated point. An example works like this:

151 can be shown as 10010111_2 in binary. This representation can be turned into sums of multiples of two:

$$151 = 1 \times 2^7 + 0 \times 2^6 + 0 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$$

$$151P = 2^7P + 2^4P + 2^2P + 2^1P + 1P$$

The double and addition works like below:

- Take P.
- Double to get $2P$
- Double to get 2^2P
- Repeat the process until 2^7P

Perform point addition with $2^7P + 2^4P + 2^2P + 2^1P + 1P$

This will give $151P$ as wanted.[10]

[10] https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/

It can be seen that the operation of adding points to get $Q = nP$ where point P is multiplied by n to get a new point Q is not that very hard. However, it is not easy to find the value of n given the point of P and Q. When the elliptic curve is moved to finite field with some modulo, it is shown other than exceptional case it is very hard to find n given the point of P and Q. This part is the core of elliptic curve cryptography, and it is called discrete logarithm problem. The elliptic curve on finite field will be discussed below.

Elliptic Curve on Modular Arithmetic

Modular arithmetic is an operation that is interested in remainder of the divisor instead of the product when dividing a number to another number. Modular arithmetic is operated as below:

Addition: $(18 + 9)\ mod\ 23 \equiv 27\ mod\ 23 \equiv 4\ mod\ 23$

Subtraction: $(7 - 14)\ mod\ 23 \equiv -7\ mod\ 23 \equiv 16\ mod\ 23$

Multiplication: $(4 \times 7)\ mod\ 23 \equiv 28\ mod\ 23 \equiv 5\ mod\ 23$

Additive inverse: $-7\ mod\ 23 \equiv 16\ mod\ 23$ as $23 - 7 = 16$

Multiplicative inverse: $9^{-1}\ mod\ 23 \equiv 18\ mod\ 23$ as $9 \times 18 = 162 \equiv 1\ mod\ 23$

therefore, $\frac{1}{9}\ mod\ 23 \equiv 9 \times 18 \div 9\ mod\ 23 \equiv 18\ mod\ 23$

Now that how the modular arithmetic is done is shown, elliptic curve on modular arithmetic is defined as:

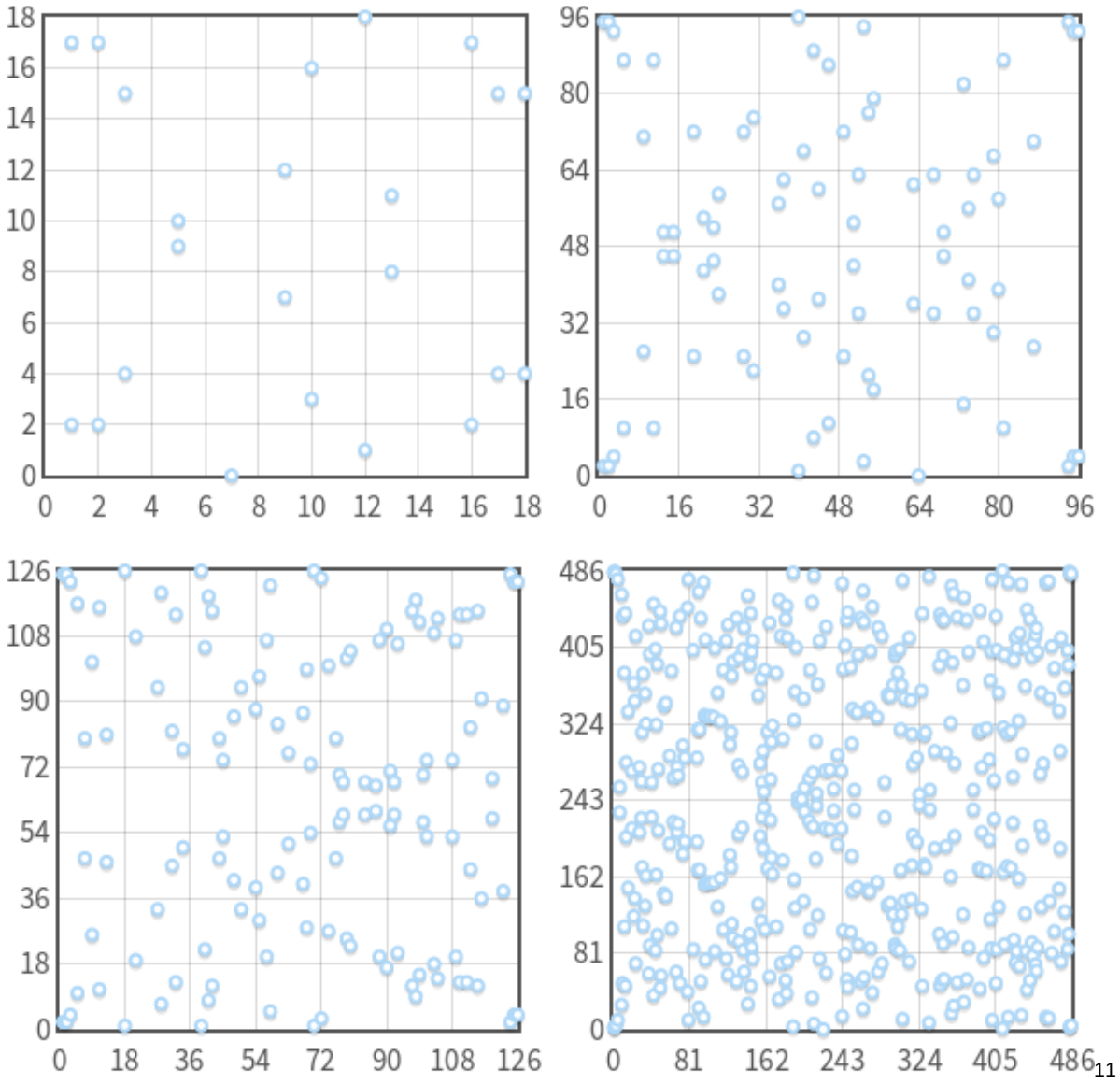
$$y^2 \equiv x^3 + ax + b\ mod\ p$$

With discriminant

$$\Delta = -16(4a^3 + 27b^2) \not\equiv 0\ mod\ p$$

Where p is a prime number.

The curve $y^2 \equiv x^3 - 7x + 10$ mod p is shown as below in case of p=19, 97, 127, 487.



[11]

Now, on this type of finite field, it is still possible to perform a point addition and multiplication, and the process is basically the same as before except calculating on modulo p. However, it is not easy to show the process geometrically, so this process will be shown only algebraically.

$$x_R = m^2 - x_P - x_Q \; mod \; p$$

$$y_R = y_P + m(x_R - x_P) \; mod \; p$$

[11] https://andrea.corbellini.name/2015/05/23/elliptic-curve-cryptography-finite-fields-and-discrete-logarithms/

If P ≠ Q,

$$m = (y_Q - y_P)(x_Q - x_P)^{-1} mod\ p$$

If P = Q,

$$m = (3x_P^2 + a)(2y_P)^{-1}\ mod\ p$$

Now, with this new finite and discrete elliptic curve, it is possible to ask a question if $Q = nP$, and given P and Q, how to find n. It turns out, this is called the discrete logarithm problem, and although there is no known mathematical proof that this problem is very hard to solve, it is believed that this problem is very hard. Additionally, this discrete logarithm problem seems to be harder than other problems that exist in cryptography. Therefore, it can be concluded that this cryptosystem requires shorter key in order to achieve the same level of security with other types of cryptography, such as Rivest–Shamir–Adleman (RSA) algorithm.[12] This discrete logarithm problem is the part that is applied to the algorithms that use Elliptic Curve Cryptography.

Elliptic Curve Diffie-Hellman

Elliptic Curve Diffie-Hellman (short for ECDH) method is one of the applications of Elliptic Curve Cryptography. It is actually a key-agreement protocol, rather than an encryption algorithm. Its main purpose is to crease and share common keys and exchange information between two parties (Alice and Bob) without third parties able to decode the information between two parties. This protocol is currently applied to many different areas, such as TLS (Transport Layer Security), which is a widely used security protocol over the internet. ECDH works like below:

1. Alice and Bob first share a base point G on same elliptic curve on same finite filed over an insecure channel.

[12] https://andrea.corbellini.name/2015/05/23/elliptic-curve-cryptography-finite-fields-and-discrete-logarithms/

2. Both Alice and Bob get their own private key d_A, d_B and public key H_A, H_B which are calculated by $H_A = d_A G, H_B = d_B G$ using point multiplication.
3. Alice and Bob exchange H_A and H_B over an insecure channel. The third party, also known as Man in the Middle, has gotten point G, H_A, H_B. However, the Man in the Middle should be able to solve the discrete logarithm problem in order to figure out d_A and d_B. This indicates that the Man in the Middle would not be easily find out their private keys.
4. Alice calculates $S = d_A H_B$ and Bob calculates $S = d_B H_A$ and they have a shared secret which is S. The point S would be same for both Alice and Bob as:

$$S = d_A H_B = d_A(d_B G) = d_B(d_A G) = d_B H_A = S$$

The Man in the Middle knows G, H_A, H_B. However, he is not able to figure out the shared secret S. This problem is known as the Diffie-Hellman problem, and it is stated as the following:

"given point P, aP, bP, what is the result of point abP?"

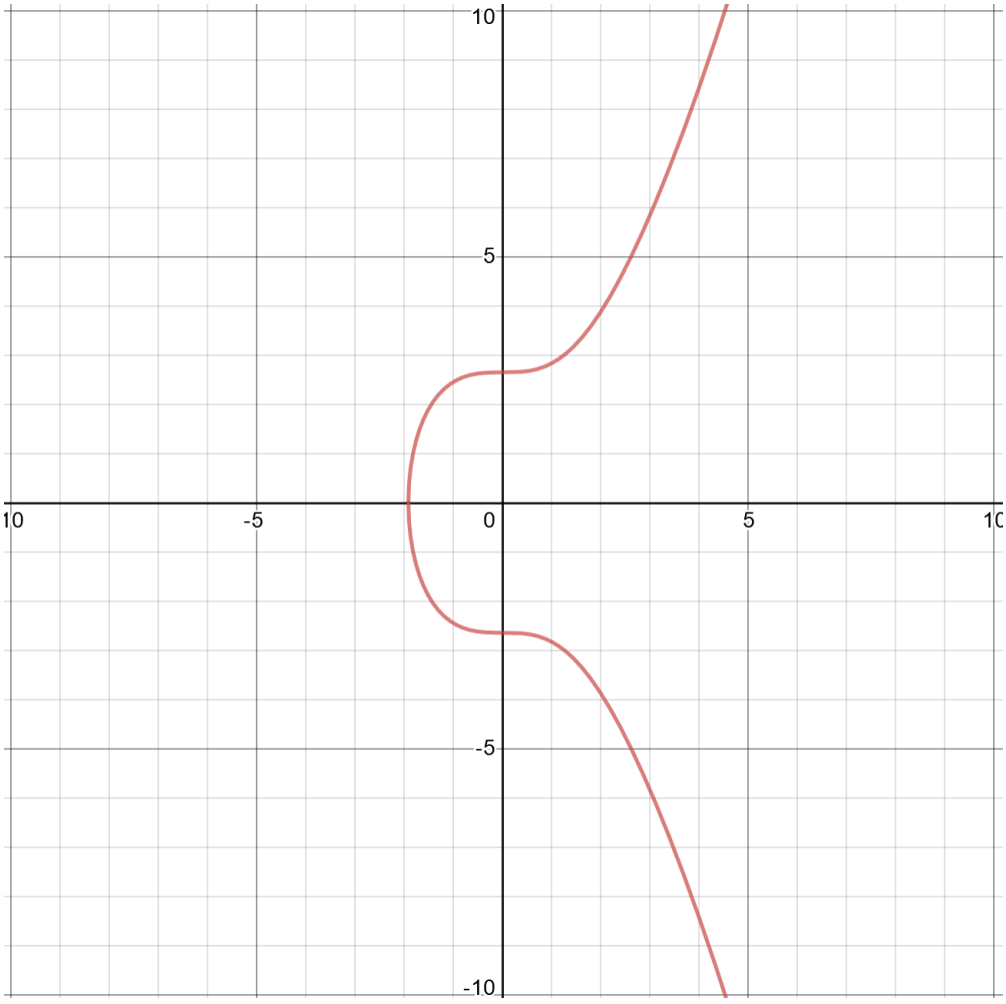
This problem is assumed to be as hard as discrete logarithm problem, although no mathematical proof is currently available. However, as this algorithm is based on discrete logarithm problem, it would be as hard as discrete logarithm problem.[13]

When Alice and Bob has gotten same key which is S, they can use that point to encrypt and send messages using symmetric encryption such as using x coordinate of point S and apply that to Advanced Encryption Standard(AES), or other symmetric encryption method, and this is what TLS in order to securely send and receive the data over the internet.

[13] https://andrea.corbellini.name/2015/05/30/elliptic-curve-cryptography-ecdh-and-ecdsa/

Current Usage

Currently, there are many usages of Elliptic Curve Cryptography around the internet. One of the usages that is mentioned is Transport Layer Security, which is established in order to securely transport data over the internet. Another famous usage of ECC is Bitcoin, which is a type of cryptocurrency, defined as the currency that exists as a form of database with highly secure cryptography method. The curve that is used on Bitcoin is called secp256k1, which is a special type of elliptic curve that is used on Standards for Efficient Cryptography Group (SECG)[14]. The curve secp256k1 has equation $y^2 = x^3 + 7$ which is shown below:



[14] https://andrea.corbellini.name/2015/05/30/elliptic-curve-cryptography-ecdh-and-ecdsa/

There are other curves such as secp256r1, secp384r1, which are also applied to other areas of applications.

Other than using ECDH as an application of elliptic curve cryptography, there are other algorithms such as Elliptic Curve Digital Signature Algorithm (ECDSA), which is to verify whether the data sent is from the specified person. These many other algorithms other than ECDH and ECDSA that are based on Elliptic Curve Cryptography. However, those algorithms are much more complicated than ECDH, therefore those will not be introduced in this section.

Conclusion

The research question aims to find the relationship between ellipse and elliptic curves, and how the properties of the curve can be applied to cryptography. For the first part of deriving the equation of elliptic curve from an ellipse, the mathematics that required was quite challenging as I had to use various properties in calculus and trigonometry to derive the equation of an elliptic curve from an ellipse. However, when I first derived the equation of elliptic curve from an ellipse, I was not able to find how the equation of elliptic curve that originally came out of ellipse is converted to the equation that is currently used on cryptography and other areas. It can be seen that the first part of my research question is somewhat distinct from the second part of the research question. For the second part, which is to find the properties of elliptic curve in order to apply it onto cryptography, I had to understand a lot of completely new kind of concepts that was never learnt in IB mathematics or any other personal courses. It was quite challenging to digest all the new concepts and knowledge that was provided in the elliptic curve cryptography such as point addition and point multiplication, elliptic curve on a finite field, and discrete logarithm problems. There are still a lot of things that can be discussed related to how the elliptic curve works, and how it can be applied to the encryption and decryption of data, which can be discussed if the research can be done more in depth. However, due to limit on this extended essay, I have limited to topics above.

Works Cited

- Weisstein, Eric W. “Elliptic Curve.” *From Wolfram MathWorld*, 24 Aug. 2020, mathworld.wolfram.com/EllipticCurve.html.

- Weisstein, Eric W. “Elliptic Integral of the Second Kind.” *From Wolfram MathWorld*, 24 Aug. 2020, mathworld.wolfram.com/EllipticIntegraloftheSecondKind.html.

- Knutson, Hans. “What Is the Math behind Elliptic Curve Cryptography?” *Hacker Noon*, 6 Apr. 2018, hackernoon.com/what-is-the-math-behind-elliptic-curve-cryptography-f61b25253da3.

- Dawkins, Paul. “Section 3-4 : Arc Length with Parametric Equations.” *Calculus II - Arc Length with Parametric Equations*, 26 May 2020, tutorial.math.lamar.edu/classes/calcii/ParaArcLength.aspx.

- Dreibelbis, Dan. “Why Are They Called ‘Elliptic’ Curves?” Department of Mathematics and Statistics, 25 Jan. 2010.

- Tos. “EllipticCurveCatalog.svg.” *Wikipedia Commons*, 14 Feb. 2008, commons.wikimedia.org/wiki/File:EllipticCurveCatalog.svg.

- Corbellini, Andrea. “Elliptic Curve Cryptography: a Gentle Introduction.” *Andrea Corbellini Atom*, 17 May 2015, andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/.

- Corbellini, Andrea. “Elliptic Curve Cryptography: Finite Fields and Discrete Logarithms.” *Andrea Corbellini Atom*, 23 May 2015, andrea.corbellini.name/2015/05/23/elliptic-curve-cryptography-finite-fields-and-discrete-logarithms/.

- Corbellini, Andrea. “Elliptic Curve Cryptography: ECDH and ECDSA.” *Andrea Corbellini Atom*, 30 May 2015, andrea.corbellini.name/2015/05/30/elliptic-curve-cryptography-ecdh-and-ecdsa/.

- Corbellini, Andrea. “Ecc.” *Https://Github.com/Andreacorbellini/Ecc*, 2020, andrea.corbellini.name/ecc/interactive/reals-add.html.

- Learning, Lumen. “College Algebra.” *Lumen*, 2020, courses.lumenlearning.com/waymakercollegealgebra/chapter/equations-of-ellipses/.