Group Theory and its Connection to Elliptic Curve Cryptography

Thomas Baisley

May 2021

0.1 Preface

Our goal is to introduce the reader to elliptic curves and their use in elliptic curve cryptography. Elliptic curves are interesting to study in their own right, as they have applications in number theory. One notable example is Andrew Wiles' proof of Fermat's Last Theorem. After viewing this, we hope the reader will be able to both recognize and construct elliptic curves and finite fields, as well as be able to implement an cryptographic system based on these ideas, in this case the Elliptic-curve Diffie-Hellman protocol.

The new Setting: Alice, Bob, and Eve are back at it again. Alice still wants to share a secret with Bob without Eve knowing it. However, Alice wants to spice it up, so she wants to use a different form of Diffie-Hellman key exchange using elliptic curves.

1 Basic Definitions

1.0.1 Groups

A group G is a set with a binary operator, $\times$, such that

1. $\times$ is associative
2. $\times$ has an identity element, i.e. $\exists 1 \in G, \forall x \in G, x1 = 1x = x$
3. every element in G is invertable, i.e. $\forall x \in G, \exists y \in G, xy = yx = 1$

Notes

1. When the binary operator is commutative, the group is said to be abelian.
2. Although groups can be infinite, we mainly deal with finite groups.
3. The order of a group is its cardinality
4. One example of a group, specifically an abelian group, is $(\mathbb{Z}, +)$

1.0.2 Rings

A Ring is a set R with two binary operators $+$ and $\times$ such that

1. R is a commutative group with respect to $+$
2. $\times$ is associative and has its own identity element unique from the identity element of $+$
3. $\times$ distributes over $+$

Notes

1. If $\times$ is commutative, we say R is commutative
2. $(\mathbb{Z}, +, \times)$ is a well known example of a ring

1.0.3 Exercise 1

Prove that the set $\mathbb{Z}[X]$, the set of polynomials with integer coefficients along with addition and multiplication of polynomials is a ring.

1.0.4 Fields

A field F is a commutative ring such that every nonzero element is invertible.

Notes

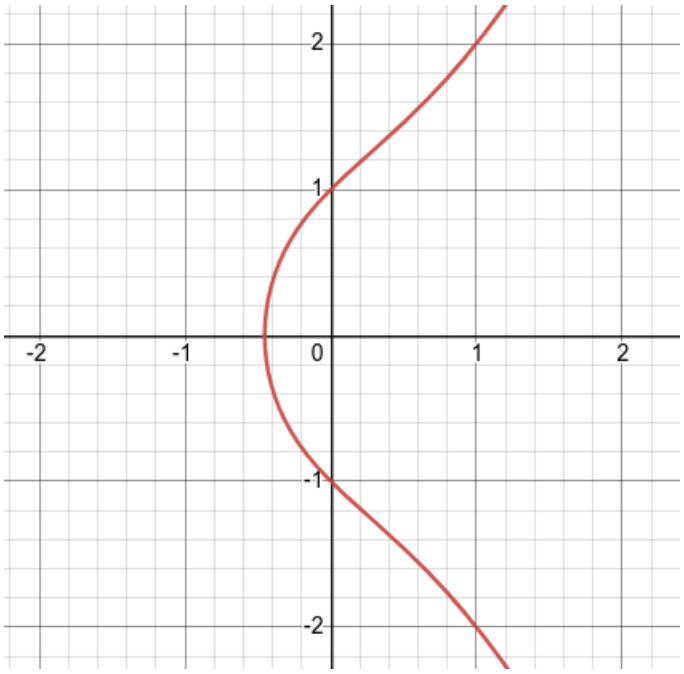
1. Notable examples of fields include $\mathbb{Q}$ with normal addition and multiplication and $\mathbb{Z}_p^*$ for any prime p
2. $\mathbb{Z}_p^*$ is specifically a finite field, since its order, or cardinality, is finite.

1.0.5 Elliptic Curves

An elliptic curve E is the set of all $x, y \in \mathbb{R}$ such that the relationship

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

, where $a, b \in \mathbb{R}$, is satisfied.
The elliptic curve $y^2 = x^3 + 2x + 1$ is graphed below.



Notes

1. We generally also include a point $\mathbb{O} \in E$, where intuitively $\mathbb{O}$ represents a point at infinity. The purpose of this point will become clear later, when we formally define a ring on elliptic curves.

2. We also note that if $4a^3 + 27b^2 \neq 0$ then the curve defined by those a, b is said to be non-singular i.e. $x^3 + ax + b = 0$ has three distinct roots. We can actually prove this with some algebra and calculus.

1.0.6 Non-Singular Elliptic Curve Proof

We want to show that $4a^3 + 27b^2 = 0 \Leftrightarrow x^3 + ax + b = 0$ does not have three distinct roots.
We prove the first direction of implication, so we first assume $4a^3 + 27b^2 = 0$:

$$
\begin{aligned}
& 27b^2 = -4a^3 \\
\implies & \frac{27b^3}{8} = -\frac{a^3 b}{2} \\
\implies & 3b/2 = -a\sqrt[3]{\frac{b}{2}} \\
\implies & b/2 + a\sqrt[3]{\frac{b}{2}} + b = 0 \\
\implies & k^3 + ak + b = 0 \qquad \text{(setting } k = \sqrt[3]{\frac{b}{2}}\text{)}
\end{aligned}
$$

Thus, we have our first root $k = \sqrt[3]{\frac{b}{2}}$
We can then do polynomial division to find the other roots.

$$
\begin{array}{r|l}
x^3 + 0x^2 + ax + b & x - \sqrt[3]{\frac{b}{2}} \\
\hline
-\ x^3 - \sqrt[3]{\frac{b^2}{4}}x^2 & x^2 + \sqrt[3]{\frac{b}{2}}x + (a + \sqrt[3]{\frac{b^2}{4}}) \\
\hline
-\sqrt[3]{\frac{b}{2}}x^2 + ax + b & \\
-\ \sqrt[3]{\frac{b}{2}}x^2 - \sqrt[3]{\frac{b^2}{4}}x & \\
\hline
(a + \sqrt[3]{\frac{b^2}{4}})x + b & \\
-\ (a + \sqrt[3]{\frac{b^2}{4}})x + a\sqrt[3]{\frac{b}{2}} + b/2 & \\
\hline
b/2 + a\sqrt[3]{\frac{b}{2}} + b = 0 &
\end{array}
$$

Now, we can plug $\sqrt[3]{\frac{b}{2}}$ into our resulting polynomial to see if $\sqrt[3]{\frac{b}{2}}$ is a double root.

$$x^2 + \sqrt[3]{\frac{b}{2}}x + (a + \sqrt[3]{\frac{b^2}{4}}) = m \tag{1}$$

$$\implies \sqrt[3]{\frac{b^2}{4}} + \sqrt[3]{\frac{b^2}{4}} + a + \sqrt[3]{\frac{b^2}{4}} = m \tag{2}$$

$$\implies a + 3\sqrt[3]{\frac{b^2}{4}} = m \tag{3}$$

$$4a^3 + 27b^2 = 0 \tag{4}$$

$$\implies a^3 = \frac{-27b^2}{4} \tag{5}$$

$$\implies a = -3\sqrt[3]{\frac{b^2}{4}} \tag{6}$$

$$\implies 0 = m \qquad \text{(plug (6) into (3))}$$

Therefore, we see that $\sqrt[3]{\frac{b}{2}}$ is, in fact, a double root, and we conclude that $4a^3 + 27b^2 = 0 \implies x^3 + ax + b = 0$ does not have three distinct roots.
Now we prove the other direction, so we first assume that $x^3 + ax + b = 0$ does not have three distinct roots.
Note that the derivative of the polynomial is zero at that duplicate root.

$$3x^2 + a = \frac{dy}{dx} \tag{7}$$
$$\implies k^2 + a = -2k^2 \tag{8}$$
$$\text{let } k \text{ be the value at the duplicate root} \tag{9}$$
$$\implies k^3 + ak + b = 0 \tag{10}$$
$$\implies k(k^2 + a) + b = 0 \tag{11}$$
$$\implies k(-2k^2) + b = 0 \tag{12}$$
$$\text{plug (8) into (11)} \tag{13}$$
$$\implies -2k^3 + b = 0 \tag{14}$$
$$\implies k = \sqrt[3]{\frac{b}{2}} \tag{15}$$
$$\implies \frac{b}{2} + a\sqrt[3]{\frac{b}{2}} + b = 0 \tag{16}$$
$$\implies \frac{3b}{2} = -a\sqrt[3]{\frac{b}{2}} \tag{17}$$
$$\implies \frac{27b^3}{8} = -a^3\frac{b}{2} \tag{18}$$
$$\implies 27b^2 = -4a^3 \tag{19}$$
$$\implies 4a^3 + 27b^2 = 0 \tag{20}$$
$$\tag{21}$$

Thus, we conclude that $x^3 + ax + b = 0$ not having three distinct roots implies $4a^3 + 27b^2 = 0$. Therefore, we have proven both directions of the proof and thus $4a^3 + 27b^2 = 0 \Leftrightarrow x^3 + ax + b = 0$ does not have three distinct roots.

1.1 Exercise 2

Use your favorite graphing program to generate a couple of elliptic curves. Get a sense of what they look like and try to find patterns in how they look!

2 Elliptic Curves as a Finite Field

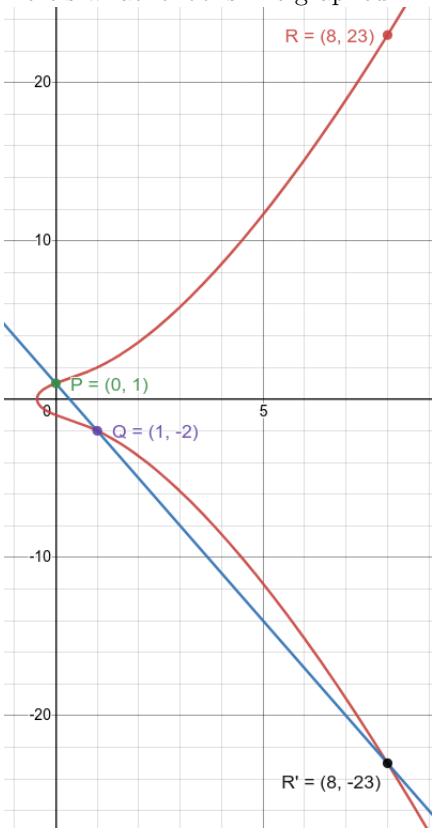
In order to construct a crypto-system using elliptic curves, we must construct a field where the "home" set are the points E which satisfy some generic non-singular elliptic curve. The first step in this process is to build up an abelian group with E.

We can define a binary operation which, with E, makes an abelian group. We define the operation + like so,

Consider two points $P, Q \in E$ where $P = (x_1, y_1)$ and $Q = (x_2, y_2)$

0. We treat $\mathbb{O}$ as the identity element, i.e. $\mathbb{O} + P = P + \mathbb{O} = P$
1. if $x_1 \neq x_2$, then we define line L to be the point made from P and Q. On an elliptic curve this line will intersect a third point R'. We thus define $P + Q = R$ where R is R' reflected over the x-axis.
2. if $x_1 = x_2$ and $y_1 = -y_2$, then we define $P + Q = \mathbb{O}$, thus, in this case, Q would be the inverse of P
3. if $x_1 = x_2$ and $y_1 = y_2$, then $P = Q$ and we are "adding" a point P to itself. In this case, we find the line tangent to P and then do the same operations as we did in case 1

It helps to visualize these operations, so we do an example of each case. Let's start with $y^2 = x^3 + 2x + 1$ and use the points $P = (0, 1)$ and $Q = (1, -2)$. Here's what it looks like graphed.



We start by finding L, the slope

$$\frac{1 - -2}{0 - 1} = -3$$

and the line

$$y = -3x + 1$$

we then substitute the line equation into the curve

$$(-3x + 1)^2 = x^3 + 2x + 1$$

which can be formulated as

$$x^3 - 9x^2 + 8x = 0$$

which can trivially be factored into

$$x(x - 8)(x - 1) = 0$$

giving us $R' = (8, -23)$ and $R = (8, 23)$

What about generalizing this calculation? We can use some simple algebra to find a nice equation which solves for R in terms of P and Q.
Consider $P = (x_1, y_1)$ and $Q = (x_2, y_2)$
the slope is still

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

denote the y-intercept as c
We can then do the same algebra as before, plugging in the line into the curve,

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

rearranged as

$$x^3 - m^2x^2 + (a - 2mc)x + b - m^2 = 0$$

by the binomial theorem, the sum of the roots is equal to the coefficient to the x^2 term. Thus,

$$m^2 = x_1 + x_2 + x_3$$

and

$$x_3 = m^2 - x_1 - x_2$$

and we can use the point-slope form of the line to compute

$$y_3 = m(x_1 - x_3) - y_1$$

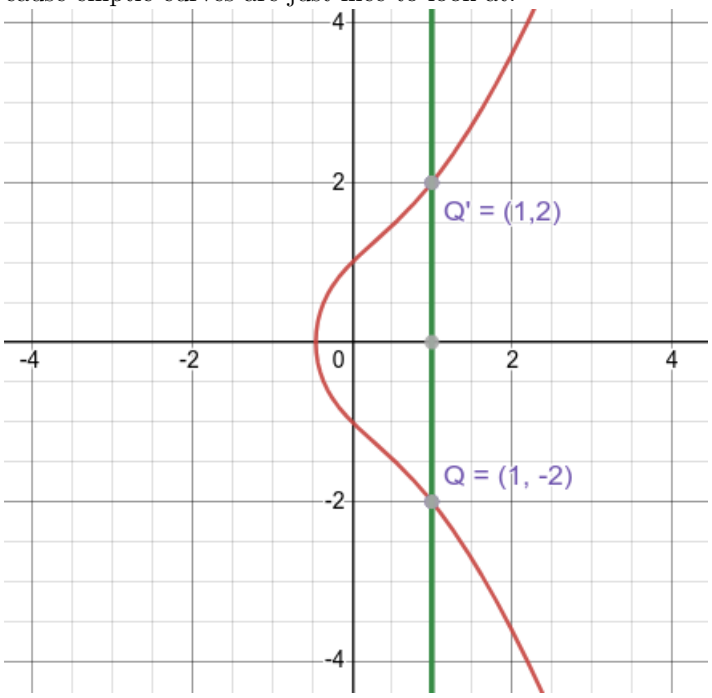
. Thus, $R = (x_3, y_3)$ and we have a set of formulae to compute $P + Q$.

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

$$x_3 = m^2 - x_1 - x_2$$

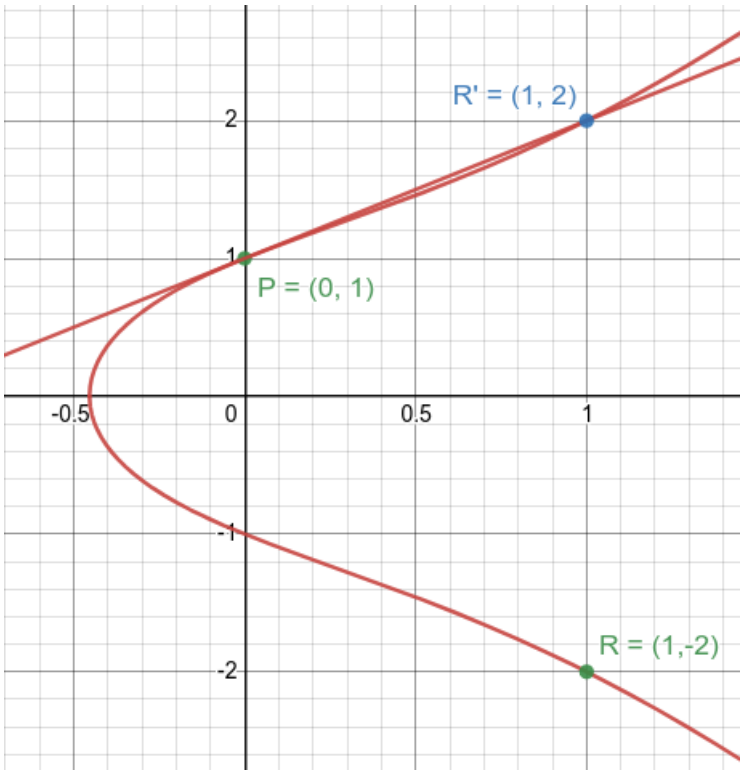
$$y_3 = m(x_1 - x_3) - y_1$$

The second case requires no calculation, but we will graph it anyway, because elliptic curves are just nice to look at.



Looking at a graphical representation makes the inclusion of $\mathbb{O}$ as the identity element more intuitive, since the line produced by a point and its inverse doesn't intersect any other portion of the curve, but rather approaches our theoretical "point at infinity".

For the third case, we will use $y^2 = x^3 + 2x + 1$ and the point $P = (0, 1)$. This problem has been graphed below as well.



To find the tangent line at that point, we have to use implicit differentiation on the elliptic curve.

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

so

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

The slope of the tangent line is $m = \frac{2}{2} = 1$ We then can use the formulas we derived in case 1 to compute R.

$$x_3 = 1^2 - 0 - 0 = 1$$

and

$$y_3 = 1(0 - 1) - 1 = -2$$

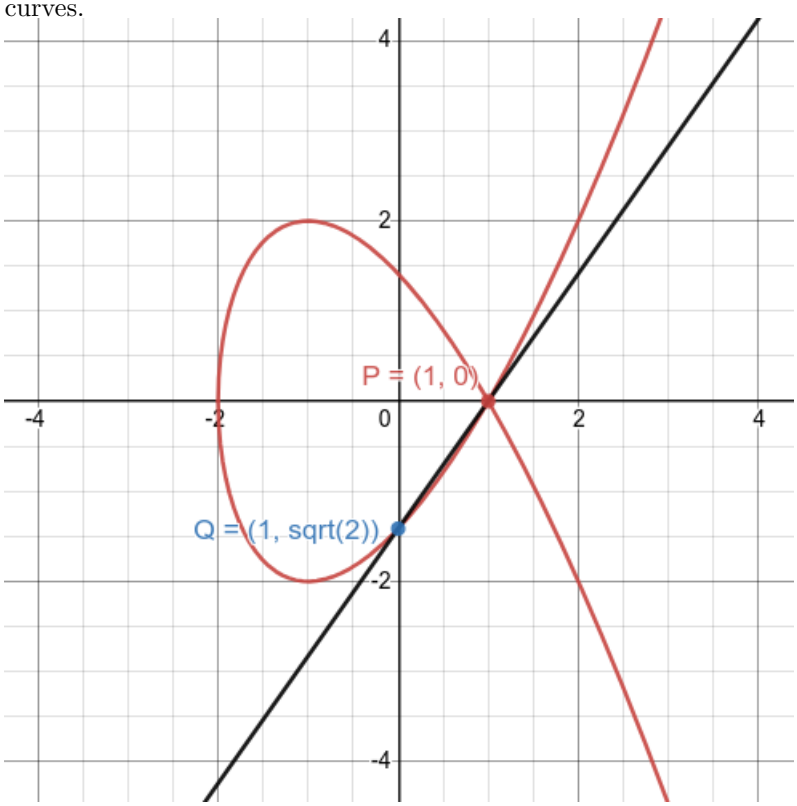
So $R = (1, -2)$. Since the formula for the derivative is the same across all elliptic curves of this form, we also have a set of formulae to compute $P + P$.

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

$$x_3 = m^2 - 2 * x_1$$

$$y_3 = m(x_1 - x_3) - y_1$$

As a final note, after defining this operator on elliptic curves, the fact that we can only construct abelian groups on non-singular curves becomes clear. Consider the curve $y^2 = x^3 - 3x + 2$. The points $(1, 0)$ and $(0, -\sqrt{2})$, if we try to add these points, we get $(1, 0)$. In fact, since $(1, 0)$ is the intersection point in the singular elliptic curve, any point on the ellipse plus $(1, 0)$ will equal $(1, 0)$. This is a problem for us, because a property of abelian groups are the uniqueness of the identity element, but every element acts as an identity element for $(1, 0)$, therefore, singular elliptic curves can't be turned into a commutative group. This arrangement has been graphed below, to further show that our intuitive definition of the binary operator on elliptic curves breaks down under singular curves.



After explaining the elliptic curve group and its associated operator, it should be clear that elliptic curves form an abelian group (doing this formally has been left as an excersise to the reader :P).

2.1 Exercise 3

Use the formula to compute $(0, \sqrt{251}) + (1, \sqrt{237})$ for the elliptic curve $y^2 = x^3 - 15x + 251$

2.2 Exercise 4

Formally prove all the properties necessary to show that non-singular elliptic curves and the operator we defined form an abelian group.

3 Elliptic Curves and Finite Fields

Now that we have an abelian group, we have to make a finite field. We can do this by taking the modulus of an elliptic curve.

3.1 Modular Elliptic Curves

Let $p > 3$ be prime. The elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Z}_p$ is the set of solutions $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ to the congruence

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

where $a, b \in \mathbb{Z}_p$ are constants such that $4a^3 + 27b^2 \equiv 0 \mod p$ (note that the curve includes $\mathbb{O}$)

Modifying the calculations for our operator under this new universe isn't actually that difficult.
Consider $P = (x_1, y_1)$ and $Q = (x_2, y_2)$
Case 2, i.e. when $x_1 = x_2$ and $y_2 = -y_1$, doesn't change $P + Q = \mathbb{O}$
and Case 0 doesn't change, $P + \mathbb{O} = P$
Case 1, however does change in the calculation of the "slope"

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = m(x_1 - x_3) - y_1$$
$$(y_2 - y_1)(x_2 - x_1)^{-1}$$

where the -1 power denotes finding the modular inverse of $(x_2 - x_1)$ since we can't divide in a modular universe.
The same applies for Case 3,

$$x_3 = m^2 - 2x_1$$
$$y_3 = m(x_1 - x_3) - y_1$$
$$m = (3x_1^2 + a)(2y_1)^{-1}$$

3.2 Euler's Criterion

If we think back to RSA, when we constructed our modular universe, we had to pick generator elements, elements that could generate the entire universe just by repeated exponentiation. The set of these elements was denoted $\mathbb{Z}_p^*$. We need to do the same thing for our modular elliptic curve field. The easiest way to do this is to solve the equivalence for various x values and see if the resulting value has a quadratic residue, which just means their exists some $y \in \mathbb{Z}_p$ such that $y^2 \equiv x^3 + ax + b \mod p$ for our chosen x. Luckily, Euler came up with criterion that determine whether a given number has a quadratic residue in some odd prime modular universe. Formally, Euler's criterion are,

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1, & \text{a quadratic residue exists} \\ -1, & \text{otherwise} \end{cases}$$

As an example, let's consider $y^2 \equiv x^3 + 2x + 1 \mod 17$
We test if $x = 4$ has a quadratic residue

$$\begin{aligned} & 4^3 + 2 * 4 + 1 \mod 17 \\ \equiv & 64 + 8 + 1 \mod 17 \\ \equiv & 73 \mod 17 \\ \equiv & 5 \mod 17 \\ & 5^8 \mod 17 \\ \equiv & 25^4 \mod 17 \\ \equiv & 8^4 \mod 17 \\ \equiv & 64^2 \mod 17 \\ \equiv & 13^2 \mod 17 \\ \equiv & 169 \mod 17 \\ \equiv & -1 \mod 17 \end{aligned}$$

Thus, $x = 4$ doesn't fall in our field.
We test if $x = 5$

$$\begin{aligned} & 5^3 + 2 * 5 + 1 \mod 17 \\ \equiv & 125 + 10 + 1 \mod 17 \\ \equiv & 136 \mod 17 \\ \equiv & 0 \mod 17 \end{aligned}$$

Funnily enough, 0 trivially has the residue 0, so $(5, 0)$ is a point on our field.

A table has been placed below that shows all the possible points on our test field.

x	$x^3 + 2x + 1 \mod 17$	quadratic residue?	y
0	1	yes	1, 16
1	4	yes	2, 15
2	13	yes	8, 9
3	0	yes	0
4	5	no	
5	0	yes	0
6	8	yes	5, 12
7	1	yes	1, 16
8	2	yes	6, 11
9	0	yes	0
10	1	yes	1, 16
11	11	no	
12	2	yes	6, 11
13	14	no	
14	2	yes	6, 11
15	6	no	
16	15	yes	7, 10

If we count the number of elements in our field, we have 24 including $\mathbb{O}$. This is where the efficiency of elliptic curve cryptography is revealed. With the same modulus, our elliptic curve field is able to have more generator points than Z_{17} would have on its own.

One last notational detail to point out is that we represent "powers" of point addition on an elliptic curve as multiplication. For example, adding point P to itself three times would be represented as $3P$.

3.3 Exercise 5

Create a small python program that can check Euler's Criterion for a given elliptic curve and test x value.

4 Elliptic Curve Diffie-Hellman Exchange

Finally, Let's go back to Alice and Bob. Alice and Bob need to agree on an elliptic curve and field parameters to use for their exchange. Fortunately for them, NIST as well as other organizations have gone through the computationally lengthy process of generating pseudo-random curves, so they can agree on using one of those. Alice and Bob's key pairs are (d_A, Q_A) and (d_B, Q_B) respectively where d is the private key and Q is the public key. Alice and Bob each start off with some generator point on the curve G. Alice and Bob then take the generator point to the power of their private key, i.e. $Q_A = d_A G$ and $Q_B = d_B G$. Alice and Bob then exchange their public keys. Alice and Bob

then take each other's public key and take it to the power of their private key. By the properties of an elliptic curve finite field, $d_A d_B G = d_B d_A G$, and Alice and Bob have the same shared secret. However, let's say Eve has intercepted the communications between Alice and Bob. To find the shared secret, Eve just needs to "undo" the point multiplication done by Alice and Bob to find their private keys. Unfortunately for Eve, this is equivalent to solving the discrete log problem, as undoing point multiplication in a modular elliptic field is analogous to taking a root or log in a modular integer universe. This is the fundamental property by which elliptic curve cryptography gets its security from.

5 Conclusions

With modular elliptic curves, we can make secure cryptographic systems that use shorter keys than traditional cryptographic systems. Besides their utility, elliptic curves are fascinating in their own right, in terms of number theory and demonstrating how group theory is integral to both cryptography and computer science.

6 Sources

The graphs came from Desmos.

`https://web.archive.org/web/20090117023500/http://www.nsa.gov/business/programs/elliptic_curve.shtml`

The information about elliptic curve key efficiency came from this nsa article.

Cryptographic Theory and Practice, by Douglas R. Stinson

This is the source of the Elliptic Curve and Finite Field Elliptic Curve implementation and information.

Handbook of Elliptic and Hyperelliptic Curve Cryptography, by Henri Cohen and Gerhard Frey

This is the source of the number theory relating to abelian groups and the like.