The Elliptic Curve Group

Contents

1 Introduction **2**
- 1.1 Motivation 2

2 Geometry **2**
- 2.1 The Projective Plane 2
- 2.2 Curves in the Projective Plane 3

3 Defining Elliptic Curves **6**
- 3.1 The Elliptic Integrals 6
- 3.2 Weierstrass $\wp$-function 7

4 The Elliptic Curve Group **9**
- 4.1 What is a group? 10
- 4.2 The properties of $(E, +)$ 10
- 4.3 Is $(E, +)$ a group? 12

5 Conclusion **15**

1 Introduction

1.1 Motivation

The study of Elliptic Curves has been of interest to mathematicians since the invention of Calculus. From some simple attempts at integrating the arc length of an ellipse, known as elliptic integrals, mathematicians Leonhard Euler and Giulio di Fragnano were able to understand that these integrals could not be solved using elementary functions. However, an algebraic connection to the elliptic integrals was uncovered leading to the topic of my essay: The Elliptic Curve Group.
The subject is very deep and of interest to the mathematical world. One of the most famous problems in this area was recognised as one of the Millennium Problems, known as the Birch and Swinnerton-Dyer (BSD) Conjecture [1]. While much can be said about this conjecture, I will instead be focusing on the much simpler matter of why it is possible to form a group for an Elliptic Curve. In this essay, I will try to keep the results in my essay fairly general and will mostly attempt to give examples that deal with the real numbers, $\mathbb{R}$, while keeping the dimensions fairly low. This will be where I believe the idea presented can be easily generalised by the reader and I shall specify differently where needed.

2 Geometry

2.1 The Projective Plane

To begin to understand the Elliptic Curve group, we must first understand what we mean by a point at infinity, $\mathcal{O}$. To do this, let us first define algebraically what is known as a projective plane.

Definition 2.1.1. [7] The projective plane $\mathbb{P}^n$ over K is defined as

$$\mathbb{P}^n = \frac{\{[a_o, \cdots, a_n] \; ; \; a_0, \cdots, a_n \text{ are not all zero}\}}{\sim},$$

where $[a_0, \cdots, a_n] \sim [a'_0, \cdots, a'_n] \;\; \forall \lambda \in K^* \;\; a_i = \lambda a'_i$ for $i = 0, \cdots, n$.

Here, the numbers a_i are called the homogeneous coordinates for the point $[a_o, \cdots, a_n]$.
To help us understand what these homogeneous coordinates look like, let us consider the coordinates in $\mathbb{R}^2$ denoted simply by (x, y). Then we may write any point in $\mathbb{R}^2 \setminus (0, 0)$ as $[x, y]$ in $\mathbb{P}^1$(also written as $\mathbb{P}$). We may also write

for $t \neq 0$, the homogeneous coordinates $[tx, ty]$ to be another representation of the point (x, y).

Example 2.1.2. For example, take the point $(1, 2)$. Then the following are examples of homogeneous coordinates for such a point:

$$[1, 2], [2, 4], [-100, -200] \text{ and } [1/2, 1].$$

Here, the intuition is that the set of all elements in the equivalence class are the non-zero points that lie on a straight line through the origin in $\mathbb{R}^2$. However, in $\mathbb{P}^2$, we define a line to be the set of points $[a, b, c] \in \mathbb{P}^2$ whose coordinates satisfy the equation

$$\alpha X + \beta Y + \gamma Z = 0$$

for some α, β, γ which are not all zero.
To get further use out of this new coordinate system, we may define the projective plane from a more geometric standpoint. To do so, we will define the affine plane by

$$\mathbb{A}^2 = \{(x, y) : x \text{ and } y \text{ any numbers}\}.$$

Hence, we may have the following alternative definition.

Definition 2.1.3. [7] The projective plane can also defined to be

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \{\text{the set of directions in } \mathbb{A}^2\},$$

where we say that two lines have the same direction if they are parallel.

Using this, we define the points at infinity to be the set of points of $\mathbb{P}^2 \setminus \mathbb{A}^2$.

2.2 Curves in the Projective Plane

Definition 2.2.1. [7] An algebraic curve in the affine plane is the set of zeros of a polynomial equation in two variables,

$$f(x, y) = 0.$$

Simple examples of such equations are the equation of a unit circle, $g(x, y) = x^2 + y^2 - 1 = 0$, and that of a parabola, $h(x, y) = y - 2x^2 = 0$, in $\mathbb{A}^2$. For us to define the same curves in $\mathbb{P}^2$ we need to find a way of turning these functions of two variables into functions of three variables.

Therefore, we want to consider a functions $F(X, Y, Z) = 0$ with the property that

$$F(ta, tb, tc) = 0 \quad \forall t \neq 0 \text{ given } F(a, b, c) = 0.$$

We call $F(X, Y, Z)$ a homogeneous polynomial of degree d if it satisfies the condition that

$$F(tX, tY, tZ) = t^d F(X, Y, Z).$$

This is equivalent to stating that F is a linear combination of monomials of the form $X^i Y^j Z^k$ such that $i + j + k = d$, standardising the idea of degree for a polynomial to be the value of d, when in homogeneous form.

Definition 2.2.2. [7] A projective curve C in the projective plane $\mathbb{P}^2$ is the set of solutions to the equation

$$C : F(X, Y, Z) = 0,$$

where F is a non-constant homogeneous polynomial of degree d.

In this sense, we may also refer to F as an algebraic curve in $\mathbb{P}^2$, similar to f in $\mathbb{A}^2$. This can be thought of simply setting $X = x, Y = y$ and $Z = 1$ such that $F(x, y, 1)$ is a restriction of the curve $f(x, y)$.
Let us see this for the case of a previously stated curve.

Example 2.2.3. Let's consider the equation of a unit circle

$$f(x, y) = x^2 + y^2 - 1 = 0,$$

such that f is an algebraic curve of degree 2 in $\mathbb{A}^2$. Let us now take a curve $C \subset \mathbb{P}^2$ defined as

$$C : F(X, Y, Z) = X^2 + Y^2 - Z^2 = 0.$$

By setting $X = x, Y = y$ and $Z = 1$ we obtain that $F(x, y, 1) = x^2 + y^2 - 1 = 0$, which is exactly how we defined our unit circle. In other words, $f(x, y) = F(x, y, 1)$.

This, of course, gives us an easy map between our homogeneous coordinates for a curve $C \subset \mathbb{P}^2$ and our coordinates on the affine plane $\mathbb{A}^2$,

$$\begin{aligned} \{[a, b, c] \in C : c \neq 0\} &\longrightarrow \{(x, y) \in \mathbb{A}^2 : f(x, y) = 0\}. \\ [a, b, c] &\longmapsto \left(\frac{a}{c}, \frac{b}{c}\right) \end{aligned}$$

The mapping is trivially bijective for if we take any coordinate $(u, v) \in \mathbb{A}^2$, satisfying $f(x, y) = 0$, we can simply map it to the homogeneous coordinates $[u, v, 1] \in C$. We call such a function $f(x, y) = 0$ the affine part of the projective curve C. Now if we wish to consider what a point at infinity looks like, then we simply consider what happens in the case $c = 0$ on C.

Example 2.2.4. To get a better intuition for this, let us once again consider the equation from Example 2.2.3. In the previous example, we had the homogeneous curve $F(X, Y, Z) = X^2 + Y^2 - Z^2 = 0$. By setting $Z = 0$, we can do the following:

$$\begin{aligned} X^2 + Y^2 - (0)^2 &= 0 \\ X^2 + Y^2 &= 0 \\ X^2 &= -Y^2 \\ \implies X &= \pm iY. \end{aligned}$$

This gives us that there are two points at infinity, $[\pm i, 1, 0]$ if we work over $\mathbb{C}$ and none if we work over $\mathbb{R}$.

Similarly, we can find the point at infinity for a straight line $\alpha X + \beta Y + \gamma Z = 0$, where WLOG we let $\alpha \neq 0$. Then via a similar procedure, we get that $\alpha X = -\beta Y$ meaning the point at infinity is $[-\beta, \alpha, 0]$. Since γ is just some constant it means that all straight parallel lines of the form $y = mx + c$ intersect on the projective plane at the point $[1, m, 0]$.
Given its later importance, we will look at one last equation now that we have built up some understanding of projective geometry.

Example 2.2.5. We start with the equation

$$y^2 = 4x^3 - g_2x - g_3$$

(such that $g_2^3 - 27g_3^2 \neq 0$, meaning the right-hand side of the equation has distinct roots) and define our affine curve to be $f(x, y) = y^2 - 4x^3 + g_2x + g_3 = 0$, with projective curve

$$C : F(X, Y, Z) = Y^2Z - 4X^3 + g_2XZ^2 + g_3Z^3 = 0.$$

By setting $Z = 0$, we get $-4X^3 = 0$, which has the triple root $X = 0$. For this equation, we get that the point at infinity is $\mathcal{O} := [0, 1, 0]$.

Example 2.2.5 will be very important to the study of the Elliptic Curve Group, once we establish more foundational knowledge behind the equation at hand. Now, before we move on to the next section of this essay, I will introduce a final key theorem for the general study of projective geometry.

Theorem 2.2.6 (Bézout's Theorem)**.** [5] Let C_1 and C_2 be two algebraic curves of degrees d_1 and d_2 respectively and no components in common. Then

$$\#(C_1 \cap C_2) = d_1 * d_2$$

as long as the following hold:

- we are working on the complex field $\mathbb{C}$;
- we include multiplicities;
- we include points at infinity.

This theorem will become quite useful in a later section, as we will be interested in the number of intersection points between a straight line (of degree 1) and that of an Elliptic Curve (which has degree 3).
As I now conclude this section, I want to first express some interesting results that can be derived from Theorem 2.2.6, to allow a reader to become more familiarised with the theorem.

Corollary 2.2.7. [5] If instead, we were to remove any of these conditions we would have that

$$\#(C_1 \cap C_2) \leq d_1 * d_2.$$

This is similar to simply removing elements from our set of intersection points, so the inequality makes sense.

This surprisingly gives us a theorem that those familiar with *MA151: Algebra 1* are likely to remember still.

Theorem 2.2.8 (Fundamental Theorem of Algebra)**.** [3] Let $p(x) \in \mathbb{C}[x]$ be a polynomial of degree $n \geq 1$, such that

$$p(x) = a_n x^n + \cdots + a_0,$$

where $a_n \neq 0$. Then the polynomial has at most n roots in $\mathbb{C}$ if we account for their multiplicity.

3 Defining Elliptic Curves

3.1 The Elliptic Integrals

In the study of trigonometry, we would typically be introduced to the trigonometric functions by first exploring the sides of triangles and the angles between them. As one studies trigonometry further, we then realise that

this connotation between trigonometric functions and triangles is merely an oversimplification of how these functions come into existence. At its essence, trigonometry is merely the study of the arc lengths of circles.
Take for example the integral

$$a(x) = \int_0^x \frac{dy}{\sqrt{1-y^2}}.$$

It can be simplified via the substitutions $y = \sin t$ and $s = \arcsin x$:

$$a(x) = \int_0^s dt = s = \arcsin x.$$

Thus similarly, the study of Elliptic Curves originates from the study of arc lengths of an ellipse. These are integrals of the form

$$b(z) = -\int_z^\infty \frac{dx}{\sqrt{4x^3 - g_2 x - g_3}}$$

called elliptic integrals. While this might initially sound confusing, we may construct a function $\wp(z)$ that has certain properties, such that $b^{-1}(z)$ equates $\wp(z)$.[2]

3.2 Weierstrass $\wp$-function

We let $\wp(z)$ be a doubly periodic function with independent complex periods ω_1 and ω_2 such that:

- $\wp(z) = \wp(-z)$
- $\wp(z) = \wp(z + \omega_1) = \wp(z + \omega_2)$;
- $\wp'(z) = \wp'(z + \omega_1) = \wp'(z + \omega_2)$
- $(\wp'(z))^2 = 4(\wp(z))^3 - g_2\wp(z) - g_3$, where $g_2, g_3 \in \mathbb{C}$ and $g_2^3 - 27g_3^2 \neq 0$.[2]

Going back to the elliptic integrals, we can utilise the substitutions $x = \wp(t)$ and $s = \wp^{-1}(z)$ to simplify the integral.

$$b(z) = -\int_s^0 \frac{\wp'}{\sqrt{4\wp^3 - g_2\wp - g_3}} dt = -\int_s^0 \frac{\wp'}{\wp'} dt = \int_0^s dt = s = \wp^{-1}(z),$$

and so the inverse function to an elliptic integral is the function $\wp(z)$. This meromorphic function is called a Weierstrass $\wp$-function (or an elliptic function) with periods defined over a complex ladder.

Definition 3.2.1. [5] A subgroup of the complex plane is called a lattice, L, if $\exists \omega_1, \omega_2 \in \mathbb{C}$, that are linearly independent (called periods) such that

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{Z}\}.$$

We can therefore define $\wp(z)$ to be

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in L \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$

with poles of finite order at $\lambda \in L$ and its derivative to be

$$\wp'(z) = -2 \sum_{\lambda \in L} \frac{1}{(z-\lambda)^3}.$$

Hence, we may allow ourselves to establish the following map:

$$z \longmapsto \big(\wp(z), \wp'(z)\big)$$

for any complex number z as long as we allow all points in L to be sent to the point $\mathcal{O}$ from Example 2.2.5. In such a way, now we have established a formula for an Elliptic Curve, which we will call the Weierstrass Normal Form of an Elliptic Curve, which looks like

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

While now we have an equation we can work with, by simply scaling our variables x and y appropriately, to do a lot of our work in the fabrication of a group. However, Elliptic Curve equations can be generalised much further for fields of different characteristics. Hence we may also utilise the equation

$$y^2 = x^3 + ax^2 + bx + c$$

and call either of these equations the Weierstrass Normal Form.[5]
Some examples are as follows:

Example 3.2.2.

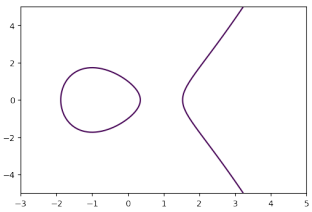

Figure 1: $y^2 = x^3 - 3x + 1$

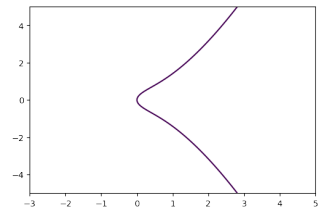

Figure 2: $y^2 = x^3 + x$

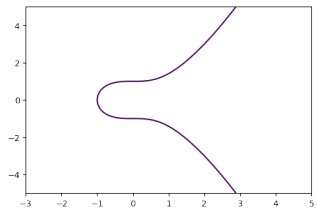

Figure 3: $y^2 = x^3 + 1$

We can also define an Elliptic Curve even more generally by the following.

Definition 3.2.3 (Elliptic Curve)**.** [6] An Elliptic Curve, E, is a smooth projective curve of genus 1 over a field K with a rational point $\mathcal{O} = [0, 1, 0]$.

In this context, we may think of the genus of a curve to be the number of "holes" for a 3D surface. When we state a curve to have genus 1, we are referring to for example a torus, which in 3 dimensions has the notion of a hole. Similarly, if we talk about a sphere, that would have genus 0 (see [6] for more). In fact, Elliptic Curves are isomorphic to the complex torus by the above mapping describing $z \mapsto (\wp(z), \wp'(z))$[5]. However, in the next section, we will be instead working with Elliptic Curves who's equation has been stated as to remove any complexity from the general idea of our group. Hence, I will utilise the Weierstrass Normal Form for an Elliptic Curve to formulate much of the theory behind the group structure.

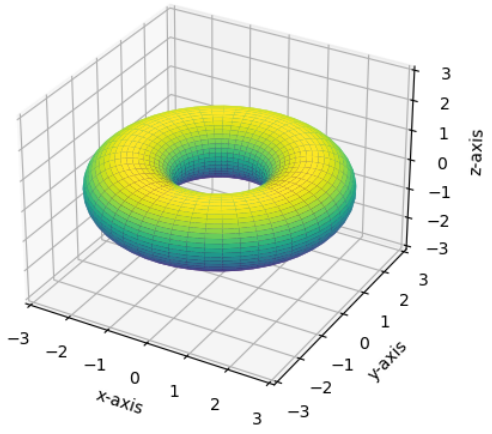

Figure 4: A simple image of a Torus

4 The Elliptic Curve Group

After much build-up, we finally have enough foundational understanding of both geometry and analysis to be able to describe what the Elliptic Curve group looks like. To do so, I quickly want to go over what exactly we define as a group, as it will aid in later explanations relating to this topic.

4.1 What is a group?

Definition 4.1.1. [3] A group, G, is a non-empty set combined with a binary operation, $\star$, such that the following holds:

- $\forall x, y \in G, x \star y \in G$ (closure);
- $\forall x, y, z \in G, (x \star y) \star z = x \star (y \star z)$ (associativity);
- $\exists e \in G$ such that $\forall x \in G, x \star e = e \star x = x$ (identity);
- $\forall x \in G, \exists y \in G$ such that $x \star y = y \star x = e$ (inverse).

We may also write a group as $(G, \star)$.

Definition 4.1.2. [3] We define a group, G, to be an Abelian group if all properties of Definition 4.1.1 hold true and also

$$\forall x, y \in G \text{ such that } x \star y = y \star x \quad \text{(commutativity)}.$$

As such, we have come across many examples of groups throughout our study of Elliptic Curves already as well as our study of mathematics.

Example 4.1.3. The following are examples of groups:

1. The set of integers under addition, $(\mathbb{Z}, +)$, is a group;
2. The set of invertible $n \times n$ real matrices, denoted $GL_n(\mathbb{R})$ or $GL(n, \mathbb{R})$, is a group under matrix multiplication;
3. The set of points on an Elliptic Curve, E, forms a group under point addition (which we shall now show to be true).

4.2 The properties of $(E, +)$

For this section, we will be utilising the Weierstrass Normal Form to establish what it means for points P and Q to be points on an Elliptic Curve, E, and to establish an understanding of what we mean when we define $P + Q$. While here we write $P + Q$, we by no means intend to describe the addition of coordinates as if P and Q were vectors, but we will get onto that shortly. For future reference, we will say $P = (x_1, y_1)$ and that $Q = (x_2, y_2)$ such that $x_1, x_2, y_1, y_2 \in E$. We define E as

$$E : y^2 = x^3 + ax^2 + bx + c \text{ such that } a, b, c \in K,$$

where K is the field we are working over with the characteristic point $\mathcal{O} = [0, 1, 0]$. We may also choose to write $E(K)$ to indicate when $x, y \in K$. This is to simply formalise the fact that P and Q are points on an Elliptic Curve. To begin to understand what the group law is of the group, we first need to describe what is meant by $P * Q$ geometrically.
We describe $P * Q$ by taking a straight line through the points P and Q. As mentioned previously, the degree of a straight line is 1 and the degree of an Elliptic Curve is 3. By Bézout's Theorem (Theorem 2.2.6), we hence know that the number of intersection points between these two algebraic curves is 3. Hence, if we take the first 2 points to be P and Q, we define this third point to be $P * Q$. We can then obtain $P + Q$ by once again taking the straight line passing through $P * Q$ and $\mathcal{O}$ and then finding the third intersection point. This third point, we define to be $P + Q$ and is equivalent by taking the point $P * Q$ and reflecting it across the x-axis. This gives rise to the equality $P + Q = \mathcal{O} * (P * Q)$. We will denote a point $P = (x, y)$ to be reflected across the x-axis by $-P = (x, -y)$[5].
Below is a simple representation of the geometrical explanation above.

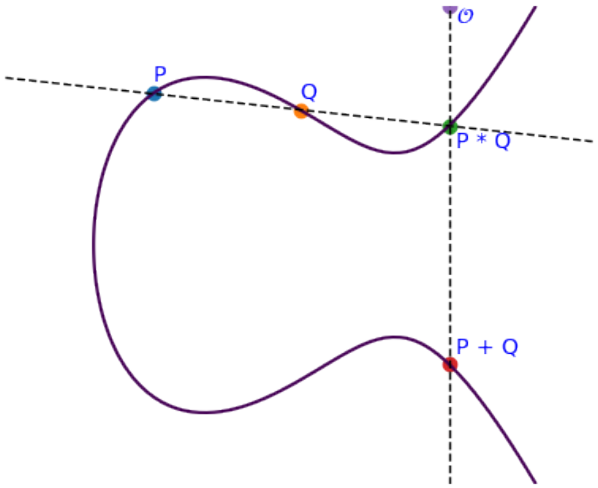

Figure 5: A simple illustration of the geometric explanation

If we take $P = Q$ then we take the tangent line to the curve at that point and let the intersection point on the Elliptic Curve be defined as $P * P$. We then define $2P$ to be the reflection over the x-axis.
The question still remains, is this a group?

4.3 Is $(E, +)$ a group?

We begin with closure. We know that $+$ is closed under "addition of points", as we shall call it, given the fact that we are dealing with intersections of two algebraic points. Then by Bézout's Theorem (Theorem 2.2.6) we know that the points $P * Q$ and $P + Q$ lie on the curve. Hence, it is fairly obvious that our operation is closed under addition, as seen by Figure 5.
Now we move to associativity. By this, we mean to show that if $P, Q, R \in E$, then $(P + Q) + R = P + (Q + R)$. To do this, we will first need a bit more groundwork.

Lemma 4.3.1 (The 9th point Lemma)**.** [4] Let $P_1, \cdots, P_9$ the intersection points for the non-singular cubics C_1 and C_2. Let's assume further that the non-singular cubic C passes through the points $P_1, \cdots, P_8$. Then C also passes through P_9.

This comes from imposing a restriction on the 10 coefficients of cubics and turning our cubics into 9-dimensional problems. By fixing a point P_i on the curves we reduce our problem down a dimension. This causes C to become a one-dimensional problem. By then writing C as a linear combination of C_1 and C_2 and evaluating this at P_9, we also see that P_9 must then lie on C.
Next, we recognise that proving $(P + Q) + R = P + (Q + R)$ is the same as showing

$$\mathcal{O} * ((P + Q)) * R) = \mathcal{O} * (P * (Q + R)).$$

Using the fact that $\mathcal{O} * A = \mathcal{O} \iff A = B$ (you may attempt to sketch this to see why it's true), we then obtain that

$$(P + Q) * R = P * (Q + R).$$

Similarly,

$$\begin{aligned} &(\mathcal{O} * (P * Q)) * R = P * (\mathcal{O} * (Q * R)) \\ \implies &(P' * Q) * (\mathcal{O} * R') = (\mathcal{O} * P') * (Q * R'). \end{aligned}$$

Where $P' = P * Q$ and $R' = R * Q$. Then, trivially, $P = P' * Q$ and $R = R' * Q$. Hence, this condition is the same with P', Q, R' and $\mathcal{O}$ in place of P, Q, R and $\mathcal{O}$.
Let's consider an Elliptic Curve, E, with the 8 points $\mathcal{O}, P, Q, R, P * Q, P * R, Q * R, \mathcal{O} * R$ and $\mathcal{O} * P$.
We now consider the 6 lines l, m, n and L, M, N defined as follows.

	L	M	N
l	P	Q	$P * Q$
m	R	$\mathcal{O}$	$R * \mathcal{O}$
n	$P * R$	$Q * \mathcal{O}$	?

By this we mean the line L passes through the points P, R and $P * R$.
We now want to use Lemma 4.3.1, and to do so we define lmn and LMN to be the union of the 8 points that define each line. Now we check that since E, LMN and lmn share 8 points, it implies that $\exists \lambda_1, \lambda_2$ such that $E = \lambda_1 lmn + \lambda_2 LMN$. Since $(P * Q) * (R * \mathcal{O})$ lies on N and E, it means that the point must then lie on lmn. But also, the point $(P * R) * (Q * \mathcal{O})$ lies on n and E, so similarly it lies on LMN. This means that via the 9th point Lemma, we get that

$$(P * Q) * (R * \mathcal{O}) = (P * R) * (Q * \mathcal{O}),$$

showing that our operation is associative. [4]
Next, we move to show that the identity element exists. In fact, we have already come across this element and that is the point $\mathcal{O} = [0, 1, 0]$.
Thus, let's assume as such and say that $P + \mathcal{O} = P = \mathcal{O} + P$. Does everything still work? Let's take P and join it to $\mathcal{O}$ giving us $P * \mathcal{O}$. Then take the line joining $P * \mathcal{O}$ and $\mathcal{O}$, giving us $\mathcal{O} * (\mathcal{O} * P)$. This intersection point is clearly

$$P = P + \mathcal{O} = \mathcal{O} * (-P) = \mathcal{O} * (-(P + \mathcal{O})) = \mathcal{O} * (\mathcal{O} * P).$$

Hence, $\mathcal{O}$ is our identity element.
Lastly, we move on to the existence of the inverse element. Once again, we have defined our inverse element of P as $-P$. We can verify this by taking the tangent line at $\mathcal{O}$ and finding the intersection point called Q (once again you can verify it yourselves through a simple sketch). By taking the line through P and Q we get the third intersection point to be $-P$. To check now that $P + (-P) = \mathcal{O}$ we consider taking the third intersection point of the line through P and $-P$, which is Q. Then taking the line through Q and $\mathcal{O}$ we get the third intersection to be $\mathcal{O}$ as the line is tangent at $\mathcal{O}$.
Does commutativity hold? We have used the fact that $P + Q = Q + P$ as we showed $(E, +)$ was a group, yet no mention of this was made as to why this is true. When we defined our operation $+$, we built our group law by taking the third intersection point of a line with our Elliptic Curve. This notion is directionless meaning that if we take the line passing through P

and Q it is the same line as the one passing through Q and P. As a result, we get that commutativity holds for $(E, +)$.
Hence, $(E, +)$ is an Abelian group.
Now it's time to have a look at an example of what we discussed in action.

Example 4.3.2. Let E be an Elliptic Curve defined by the equation

$$y^2 = x^3 - x.$$

We let $P = (0, 0)$ and $Q = (1, 0)$.

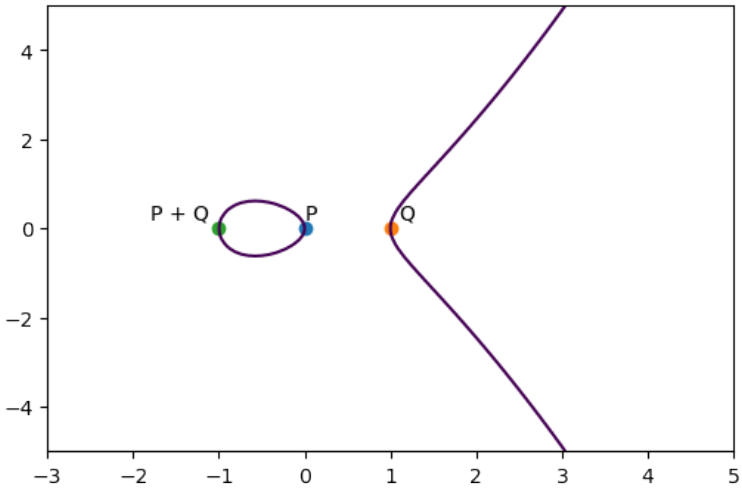

Figure 6: Illustration of the points P, Q and $P + Q$ on E

Starting with P. Let's consider what $P + P$ looks like. We begin by taking the tangent line at P. This will be the vertical line $x = 0$ with multiplicity 2 at the point $(0, 0)$. This means that the third point of intersection with the curve will be $\mathcal{O}$, so $P + P = \mathcal{O}$. We can add P more times to itself and obtain $2P = \mathcal{O}, 3P = P$, etc.
We see the same thing with Q, to obtain similar results by taking the line $x = 1$ instead.
Instead, lets focus on $P + Q$. We take the line through P and Q of the form $y = 0$. This yields the third intersection point, $P * Q$, to be the point $(-1, 0)$. By then taking the straight line through $\mathcal{O}$ and $P * Q$, we get the line $x = -1$. This line meets the Elliptic Curve with multiplicity 2 at $(-1, 0)$ meaning that the point $P + Q = (-1, 0)$.

5 Conclusion

Throughout this essay, we have spent a lot of time simply building up enough theory to get a group from our Elliptic Curves. So now some of you may wonder why this is so important. As mentioned in Section 4, we define $E(K)$ to be the set of points in K such that the points lie on the Elliptic Curve, E. The two most important sets related to this area of mathematics are $\mathbb{Q}$ and $\mathbb{F}_p$.

The Birch and Swinnerton-Dyer (BSD) conjecture I mentioned in the introduction deals with one of these fields. Now that we understand more about the group, the millennium problem attempts to prove if the set of points generating $E(\mathbb{Q})$ is finitely generated.

The other field is instead of big interest to encryption. Elliptic Curve Diffie Hellman (ECDH) [2] deals with the generation of encryption keys between two parties. This of course relies on the same group operations as $E(\mathbb{F}_p)$.

References

[1] https://www.claymath.org/millennium/birch-and-swinnerton-dyer-conjecture/, May 2023. [Accessed 21-04-2024].

[2] Ian F Blake, Gadiel Seroussi, and Nigel Smart. *Elliptic curves in cryptography*, volume 265. Cambridge University Press, 1999.

[3] Richard Lissaman. *MA151: Algebra 1 2022/23*. Unpublished, Warwick University, 1st edition, 2022. [Accessed 21-04-2024].

[4] Tim Murphy. Chapter 3: The associative law. https://www.maths.tcd.ie/pub/Maths/Courseware/EllipticCurves/2016/Associativity.pdf, 2016. [Accessed 21-04-2024].

[5] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*, volume 9. Springer, 1992.

[6] Andrew Sutherland. 18.783 elliptic curves lecture 1, Feb 2017. [Accessed 21-04-2024].

[7] Alex Tao. Projective geometry, Jun 2008. [Accessed 21-04-2024].