Elliptic Curves Class Project

Israel Ben Aron[†]

[†]Temple University

April 15th, 2021

1 An Introduction to Elliptic Curves

Elliptic curves comprise a vast range of subjects and ideas and so in this description, we will expose the most basic properties and describe the interesting mathematical structure. We will start by focusing on cubic curves over rational numbers, and eventually describe what an elliptic curve is. This will allow us to dissect the fundamental ideas of elliptic curves by simplifying it to a description of cubic curves. We will then be able to construct what elliptic curves are, based on the understanding and framework of cubic curves.

1.1 Cubic Curves Over Rational Numbers

We begin with a basic definition about cubic polynomials.

Definition (Cubic Polynomial)**.** A *cubic polynomial* is a polynomial of the form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0. \tag{1}$$

If the coefficients of (1) are rational, we say that it is a rational cubic. This will be the focus for our description of cubic curves.

In general, we say that the solutions of a polynomial of finite degree is a curve in the plane. Linear equations, polynomials with degree 1, describe lines in the plane. Likewise, for quadratic polynomials with degree 2, solutions are conic sections in the plane. We next turn to cubic polynomials with degree 3. We call the solutions of these polynomials cubic curves.

Definition (Cubic Curves)**.** A *cubic curve* is the graph of the solutions of a polynomial with degree 3.

We will illustrate this with a simple example of a rational cubic (cubic polynomial with rational coefficients) which was plotted using Mathematica.

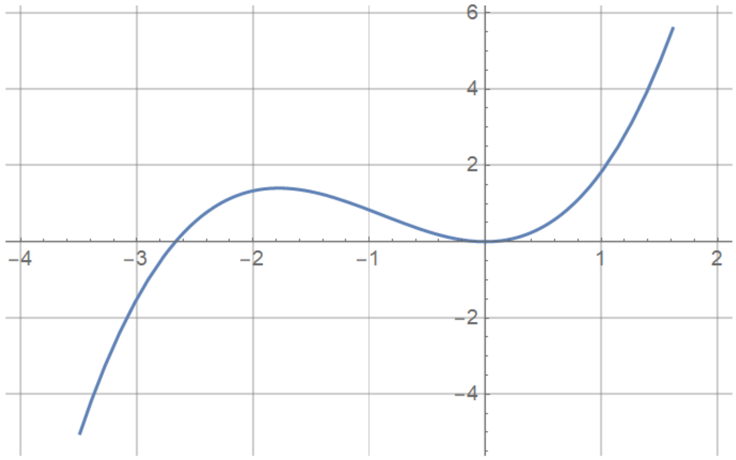

Figure 1: Plot of $y = \frac{1}{2}x^3 + \frac{4}{3}x^2$.

Example 1.1. Consider the cubic polynomial given by

$$y = \frac{1}{2}x^3 + \frac{4}{3}x^2.$$

Plotting this gives the curve in Figure 1 below.

The main concern with cubic equations is being able to find solutions (points on the curve) to them in certain fields. For instance, suppose we want to find rational solutions to the equation given in Example 2.1. To do this for cubics of the form $y^3 - x^3 = c$, suppose we have found one rational solution to it, namely, (x, y) with x and y both rational and $y \neq 0$. Then we may apply the duplication formula, which was first introduced by Claude Bachet in 1621 [1]. This is a pair that can determine another rational point given one has already been found. The formula is given by

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3} \right), \tag{2}$$

where c is an integer and not equal to 1 or -432.

It follows from (2) that if we had one rational solution to a given cubic equation of the form $y^3 - x^3 = c$, we can generally find a second solution, namely by using this formula. Likewise, we can obtain a third, fourth, and fifth solution. So given two rational solutions, we can obtain a third solution in addition to the previous two. The duplication formula provides the motivation to find more rational solutions for general cubics. That is, we want to see if we can find the next solution to a given cubic provided we already have one or two solutions. This then has a direct geometric interpretation. That is, if P and Q were rational solutions to a cubic equation, then we can form a line between the two points. This line will then produce a third point at the intersection between the line and another point on the cubic curve. We call this line a rational line. The third point of intersection is typically labelled as $P * Q$. We also note that if we only had one rational solution, i.e., point, we can obtain a second point by drawing the line tangent to the point and finding its intersection with the curve [3]. One way to think about this is to imagine that the line passes through the same point twice and intersects to find a third point (in our case second). Using the curve in Example 2.1, we can apply this geometric principle. This is shown in Figure 2. Likewise, we may also plot the case in which we only have one rational point, P, as shown in Figure 3.

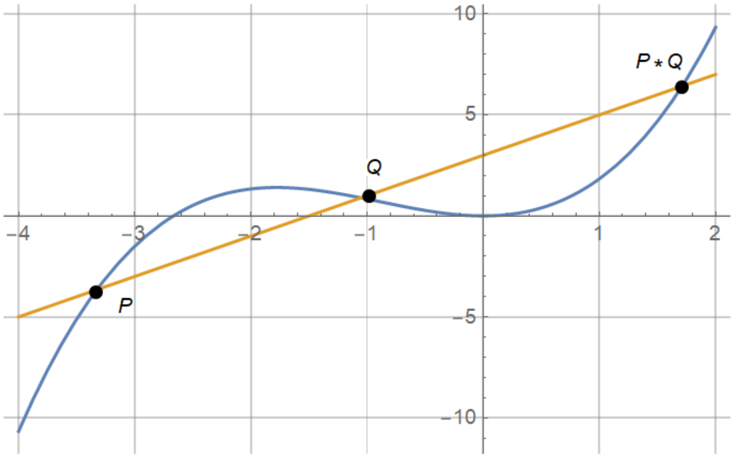

Figure 2: Intersection of Line Connecting P and Q with Curve given in Example 2.1.

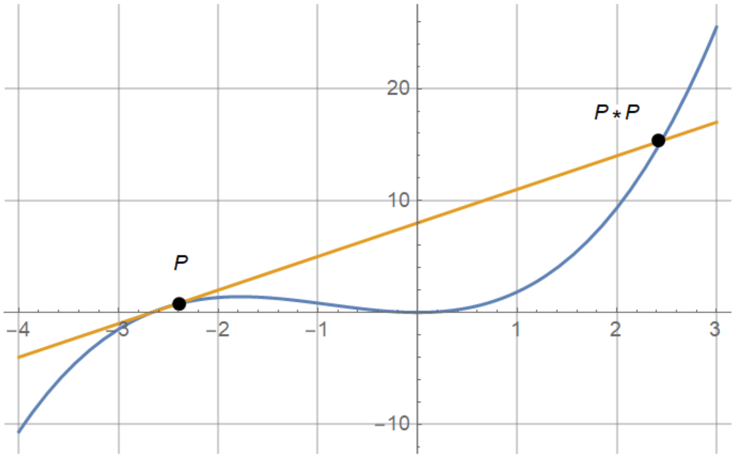

Figure 3: Given point P, we can find another point on the curve, $P * P$.

1.2 The Group Law

The duplication formula and its corresponding geometrical interpretations provide the opportunity to explore what is understood about generating rational points. That is, we can ask questions about the algebraic structure of the composition law given by '$*$' and what it does to the set of rational points on the curve [1]. When considering the underlying structure, it is best to start with simple constructions. One of the simplest algebraic structures is a group. We start with its definition.

Definition (Group)**.** A *group* is a set G with one binary operation, $\cdot$, that satisfies the following properties [2]:

- For all $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. (Associative Law)
- There exists $e \in G$ such that for all $a \in G$, $a \cdot e = e \cdot a = a$. (Existence of an Identity)
- For all $a \in G$, there exists $b \in G$ such that $a \cdot b = e = b \cdot a$. (Existence of an Inverse)

The binary operation in the definition above is typically called the *group law*. Forming a group with the properties that have since been described will allow us to push the ideas further and aid our description of elliptic curves. Then by some clever manipulations, a group can be obtained using a group law given by an operation '+'.

This operation can be described as a type of addition of cubic curves. That is, given P, Q and $P * Q$, we can obtain $P + Q$. However, we have a complication. If P, Q and $P * Q$ are given rational points on a cubic curve, then there are no other compositions that are able to be formed between the points using '$*$' since no line can intersect more than three points in a cubic. To get around this complication, we define an identity O to be the rational point in which we connect to the rational point $P * Q$. This gives us a third intersection point which we define to be $P + Q$, where '+' is the group law. This is best understood with a visualization since it is inherently geometric. Then we can consider the curve in Example 2.1. We will use the identity to illustrate the group law in Figure 4. From the plot, we can observe some basic principles about the definition of the group law. That is, from Figure 4, we can obtain the following relation

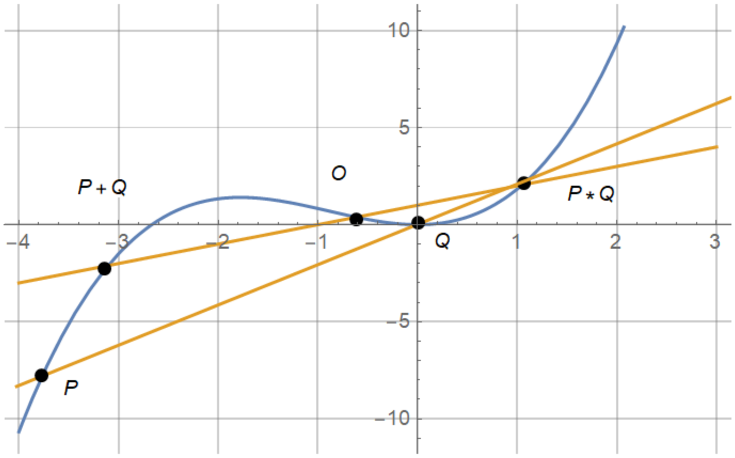

Figure 4: Illustrating the group law, '+'.

$$P + Q = O * (P * Q). \tag{3}$$

Now that we have this group law defined, we can confirm that the set of rational points along with '+' is a group. This process includes confirming each condition given in the definition of a group. This can be done with the given group and composition laws and some geometric manipulation.

1.3 Mordell's Theorem and Elliptic Curves

The construction and confirmation of this group now allows us to build up our description of cubic curves even further. As above, we have defined the group as a set of rational points on any given cubic. That is, given a group of rational points of a cubic, we are able to make conclusions about other properties of the curve. In particular, we obtain Mordell's Theorem.

Theorem (Mordell's Theorem)**.** If a non-singular rational plane cubic curve has a rational point, then the group of rational points is finitely generated [1].

Mordell's Theorem essentially says that given a particular finite set of rational points on a cubic curve, all other rational points on that curve can be obtained by repeated addition.

In proving Mordell's Theorem, we reduce the form of a general cubic into a so-called *Weierstrass normal form.* A cubic equation in this form is given by

$$y^2 = f(x) = x^3 + ax^2 + bx + c. \tag{4}$$

Solving this equation would result in at most three roots. If these roots are distinct, we obtain the definition of an elliptic curve.

Definition (Elliptic Curve)**.** An *elliptic curve* is a cubic curve in normal form such that the roots are distinct.

We note that these roots can be complex. Then there is the issue of singularity. This involves the question of how many real roots there are and how many of them repeat. If a root repeats, the cubic curve is said to be *singular.* But given that each root is distinct, we have a non-singular cubic curve, i.e., an elliptic curve.

The discovery of this property and formulation of cubic curves allowed mathematicians to explore uncharted territory and begin to solve long-standing problems in mathematics. A famous example is Andrew Wiles's proof of Fermat's Last Theorem, which makes use of elliptic curves.

References

[1] Silverman, J. H., & Tate, J. T. (2015). Rational Points on Elliptic Curves (Undergraduate Texts in Mathematics) (2nd ed. 2015 ed.). Springer.

[2] Malik, D. S., Mordeson, J. M., & Sen, M. K. (1996). Fundamentals of Abstract Algebra. McGraw-Hill College.

[3] Peeples, W. D. (1954). Elliptic curves and rational distance sets. Proceedings of the American Mathematical Society, 5(1), 29. https://doi.org/10.1090/s0002-9939-1954-0060262-1

[4] Washington, L., 2008. Elliptic curves. Boca Raton, FL: Chapman & Hall/CRC.

[5] Lozano-Robledo, A., 2011. Elliptic curves, modular forms, and their L-functions. Providence, R.I.: American Mathematical Society.

[6] Barsagade, M. W., & Meshram, S. (2014). Overview of History of Elliptic Curves and its use in cryptography. International Journal of Scientific & Engineering Research, 5(4), 467–471. http://www.ijser.org

[7] Cassels, J. W. S. (1991). Lectures on Elliptic Curves (London Mathematical Society Student Texts, Vol. 24) (1st ed.). Cambridge University Press.