Topics on Elliptic Curves

Avram Silberztein and Anwyn Woodyatt

December 29, 2023

Abstract

This paper summarizes an undergrad research project\reading course (MATH 470) at McGill University under the supervision of Dr. Jonathan Love. It mostly follows chapters 1-3, 4.1, 4.5 and A1-A2 of *Rational Points on Elliptic Curves* by Silverman and Tate [4]. It is presented as an undergraduate friendly introduction to elliptic curves and applications of the topic.

Contents

1 An Introduction to Projective Geometry

There are two ways to introduce $\mathbb{P}^2$, the *Projective Plane* — algebraically and geometrically. We will motivate both and explore their relationship.

1.1 Geometric Projective Plane

Imagine you are standing between train tracks, line of sight parallel to the tracks. Notice how the tracks seem to converge far in the distance? You may describe this place they "converge" at the horizon. This concept motivates something called a *point at infinity*.

Geometrically, we are taught in high school that two distinct lines in $\mathbb{R}^2$ can either never intersect (parallel lines) or intersect once. What if we want every distinct line to intersect once? We make this possible by extending the real plane. We say two parallel lines intersect at a point at infinity, like the train tracks. Two non-parallel lines still intersect once on the real plane. So, we have extended $\mathbb{R}^2$ to $\mathbb{R}^2 \cup P$ where P is a point at infinity. Is this sufficient?

We cannot have only one point at infinity since that implies any two distinct non-parallel lines have two points of intersection. So each equivalence class of parallel lines defines a unique point at infinity, sometimes called a *direction*. Since there are infinitely many equivalence classes of parallel lines as there are infinite values of slope (think about rotating the familiar line $x = y$ in $\mathbb{R}^2$ around the origin), there are infinite points at infinity.

You may like to visualize it the following way. If we think of $\mathbb{R}^2$ as an open disk of infinite radius, then the collection of points at infinity is the border (or horizon from train track analogy), mod the equivalence relation of antipodal points. This is because whichever direction you travel along a line, it associates to the same point at infinity (otherwise parallel lines would have two intersection points).

We can now define the projective plane, geometrically:

Definition 1. $\mathbb{P}^2 = \mathbb{R}^2 \cup \{\textit{points at infinity}\}$

We call the line connecting all points at infinity the *line at infinity*, denoted L_∞.

1.2 Algebraic Projective Plane

To define the projective plane algebraically, we need some definitions to start.

Define an equivalence relation on the set of triples in $\mathbb{R}^3 \backslash \{(0,0,0)\}$ by setting $(a,b,c) \sim (a',b',c')$ if there exists non-zero t in $\mathbb{R}$ such that

$$ta = a', tb = b', tc = c'$$

This is easily seen to be an equivalence relation:

$$Reflexivity : (a,b,c) = 1(a,b,c)$$
$$Transitivity : (a,b,c) = t(d,e,f), (d,e,f) = s(g,h,i) \Rightarrow (a,b,c) = t \cdot s(g,h,i)$$
$$Symmetry : (a,b,c) = t(d,e,f) \Rightarrow (d,e,f) = \frac{1}{t}(a,b,c)$$

Where we recall that t is a unit of $\mathbb{R}$, so it has an inverse $\frac{1}{t}$.

We write an equivalence class as

$$[a,b,c] = \{(x,y,z) : \exists\, t \in \mathbb{R}\backslash\{0\} \text{ with } t(x,y,z) = (a,b,c) \text{ and } x,y,z \in \mathbb{R} \text{ not all zero}\}$$

and call $[a,b,c]$ a *homogeneous coordinate*. We define $\mathbb{P}^2$ as the set of such equivalence classes.

Definition 2.

$$\mathbb{P}^2 = \mathbb{R}^3\backslash\{(0,0,0)\}/\sim$$

Remark 1. *More generally,*

$$\mathbb{P}^n = \mathbb{R}^{n+1}\backslash\{\bar{0}\}/\sim$$

In the case of $n = 1$, we call this the projective line, denoted $\mathbb{P}^1$.

Definition 3. *A line in $\mathbb{P}^2$ is the set*

$$\{[x,y,z] : Ax + By + Cz = 0\}$$

where A,B,C are real constants, not all zero.

Note that since the equation itself is homogeneous, it is sufficient to check if a point lies on a line using a representative of the homogeneous coordinate.

We can also define L_∞ algebraically:

Definition 4. $L_\infty = \{[x,y,z] \,:\, z = 0\}$

1.3 Geometric and Algebraic Connection

Now that we have established two ways to define the projective plane, it would be ideal to understand their equivalence. To do this, we backtrack to the geometric definition and concept of direction. As discussed, any line is parallel to a line through the origin with the same slope. Lines through the origin in $\mathbb{R}^2$ are categorized by equations of the form

$$Ax = By$$

with A,B real constants, not both zero. If $A' = tA, B' = tB$ for some non-zero t in $\mathbb{R}$, then $A'x = B'y$ is the same line as above.

So $[A, B]$ is a homogeneous coordinate in $\mathbb{P}^1$ which defines a line through the origin. Since each point at infinity is uniquely determined by the equivalence class of lines through the origin in $\mathbb{R}^2$, it follows that each point at infinity is uniquely determined by some $[A, B]$ in $\mathbb{P}^1$. Thus, we can write

Definition 5. $\mathbb{P}^2 = \mathbb{R}^2 \cup \mathbb{P}^1$

as our new geometric definition of the projective plane.

We now have the understanding to transfer between our two definitions easily, and when convenient. The following table, which defines the one-to-one correspondence, can be used for reference. It is not hard to show the one-to-one correspondence with these mappings.

Algebraic $\mathbb{P}^2$		**Geometric** $\mathbb{P}^2$
$[a, b, c]$	$\rightarrow$	$\begin{cases} (a/c, b/c) \in \mathbb{R}^2 & \text{if } c \neq 0 \\ [a, b] \in \mathbb{P}^1 & \text{if } c = 0 \end{cases}$
$[x, y, 1]$	$\leftarrow$	$(x, y) \in \mathbb{R}^2$
$[A, B, 0]$	$\leftarrow$	$[A, B] \in \mathbb{P}^1$

Table 1: Maps between definitions of points in $\mathbb{P}^2$

1.4 Projective Geometry in Arbitrary Dimension

Even though we work in $\mathbb{P}^2$ with elliptic curves, it is enlightening to explore the extension to arbitrary dimension n.

Definition 6. $U_i = \{[x_0 : x_1 : \cdots : x_n] : x_i \neq 0\}$ *for* $i \in \{0, ..., n\}$

Proposition 1.1. U_i *is in one-to-one correspondence with* $\mathbb{R}^n$

Proof. WLOG, we prove this for U_0.

Consider the map which sends $[x_0, ..., x_n]$ to $(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0})$.
It is well-defined since $x_0 \neq 0$ and representatives of homogeneous coordinates differ by a non-zero scalar which is cancelled in the division. Equivalently, we can write
$[x_0, ..., x_n] = [1, \frac{x_1}{x_0}, ..., \frac{x_n}{x_0}] \coloneqq [1, x_1^{'}, ..., x_n^{'}]$ by definition of homogeneous coordinates, so WLOG we can take $x_0 = 1$.
Surjectivity: For $(x_1, ..., x_n)$ in $\mathbb{R}^n$, choose $[1, x_1, ..., x_n]$ in U_0.
Injectivity: Let $[1, x_1, ..., x_n]$ and $[1, y_1, ..., y_n]$ in U_0. If $(x_1, ..., x_n) = (y_1, ..., y_n)$, trivially
$[1, x_1, .., x_n] = [1, y_1, ..., y_n]$.

Alternatively, suppose $[x_0, ..., x_n]$ and $[y_0, ..., y_n]$ in U_0 and $x_0 \neq 0 \neq y_0$. If $(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0}) = (\frac{y_1}{y_0}, ..., \frac{y_n}{y_0})$ then $\frac{x_i}{x_0} = \frac{y_i}{y_0}$ for $i \in \{\mathbf{1}, .., n\}$. Since x_0 and y_0 are non-zero, either $x_i = y_i = 0$, or $x_i \neq 0$ and $y_i \neq 0$. In the latter case, $\frac{x_i}{y_i} = \frac{x_0}{y_0} \coloneqq t$, a non-zero constant, so $x_i = ty_i$. This trivially holds in the former case, so it is true for all i in $\{\mathbf{0}, ..., n\}$. Thus, $(x_0, ..., x_n) = t(y_0, ..., y_n)$ and $[x_0, ..., x_n] = [y_0, ..., y_n]$.

□

Proposition 1.2. *$\mathbb{P}^n \backslash U_i$ is in one-to-one correspondence with $\mathbb{P}^{n-1}$*

Proof. Again, WLOG, we prove this for U_0.
Consider the map sending $[0, x_1, ..., x_n]$ to $[x_1, ..., x_n]$, which is easily shown to be bijective.

□

Remark 2. *In fact, as topological spaces, the above one-to-one correspondences are actually homeomorphisms (isomorphisms of topological spaces).*

Indeed, if we define a map from $\mathbb{R}^{n+1} \backslash \{(0, x_1, ..., x_n)\}$ to $\mathbb{R}^n$ in exactly the same way as a representative from the quotient subspace U_i (continuous via calculus), then by

Lemma 1.1 (Universal Property of Quotients)**.** *Let X, Z be a topological spaces and $\sim$ be an equivalence relation on X. Denote the quotient space by X'. Let $\pi : X \to X'$ be the usual surjective map. Then for all continuous $f : X \to Z$ such that $x \sim y$ implies $f(x) = f(y)$, there exists a unique continuous map $\overline{f} : X' \to Z$ such that $f(x) = \overline{f}(\pi(x))$ for all x in X.*

the map from U_i is a continuous map to $\mathbb{R}^n$. Its predictable inverse is continuous by composition of continuous functions, first lifting $(x_1, ..., x_n)$ to $(1, x_1, ..., x_n)$ and then (continuously) surjecting onto U_0.

Corollary 1.1.1. $\mathbb{P}^n = \mathbb{R}^n \cup \mathbb{P}^{n-1}$

Proof. Write $\mathbb{P}^n = U_i \cup (\mathbb{P}^n \backslash U_i)$, a disjoint union. The rest follows directly from the above.

□

1.5 Projective Curves

We introduce curves in $\mathbb{P}^2$ both top down and bottom up.

Top down starts with a *projective curve* and separates it into its real part and points at infinity. Using our algebraic definition of $\mathbb{P}^2$, we need three variables to define a projective curve. A projective curve is defined by the set of solutions to

$$C_{\mathbb{P}^2} : F(X, Y, Z) = 0$$

with real coefficients. In particular, this curve needs to be well-defined with respect to homogeneous coordinates, i.e. $F(a, b, c) = 0$ if and only if $F(ta, tb, tc) = 0$ for non-zero t. Thus we are restricted to *homogeneous* polynomials in three variables.

Recall that $F(X, Y, Z)$ is called *homogeneous of degree* d if it is a linear combination of monomials $X^i Y^j Z^k$ such that $i + j + k = d$.

It follows that to check if a point in $\mathbb{P}^2$ is on $C_{\mathbb{P}^2}$, it is sufficient to check with any representative of the homogeneous coordinate.

We can relate this algebraic definition of a projective curve to a geometric one using the same maps between our algebraic and geometric definition of the projective plane.

Given a point $[a, b, c]$ on $C_{\mathbb{P}^2}$ with $c \neq 0$, we get the point $\left(\frac{a}{c}, \frac{b}{c}\right)$ on the real plane. Combining this with the fact that F is homogeneous of degree d, we get

$$F\left(\tfrac{a}{c}, \tfrac{b}{c}, 1\right) = \tfrac{1}{c^d} F(a, b, c) = 0$$

and we define $f(x, y) = F(x, y, 1)$ as the *dehomogenization* of $F(X, Y, Z)$.

Remark 3. *Note that we dehomogenize with respect to Z by convention, as we consider $Z = 0$ the line at infinity. But we can also dehomogenize with respect to X or Y by taking $X = 0$ or $Y = 0$ as the line at infinity. Dehomogenizing with respect to X, Y or Z associates to U_0, U_1 and U_2 respectively.*

Now $f(x, y) = 0$ if and only if $F(x, y, 1) = 0$. We call $f(x, y) = 0$ the *affine part of the projective curve* or simply the *affine curve* and denote it by $C_{\mathbb{R}^2}$.

Remark 4. *The $\mathbb{R}^2$ notation is inspired by maps in 1.3: $[x, y, 1]$ is a point in $\mathbb{P}^2$ satisfying $F(x, y, 1) = 0$ if and only if (x, y) is a point in $\mathbb{R}^2$ satisfying $f(x, y) = 0$.*

The points $[a, b, 0]$ on $C_{\mathbb{P}^2}$ associate to points at infinity/classes of parallel lines in $\mathbb{P}^1$. It is true and intuitive that these points "complete" the affine curve by corresponding to the points at infinity/class of limiting tangent lines as the real curve travels to infinity. The reader is referred to [4] A2 for convincing examples.

Bottom up is quick, now knowing what a projective curve is. Suppose we are given a curve in $\mathbb{R}^2$, denote it

$$C_{\mathbb{R}^2} : f(x, y) = 0.$$

We would like to find a projective curve such that its affine part is $C_{\mathbb{R}^2}$; that is, find a homogeneous polynomial $F(X, Y, Z)$ such that $F(x, y, 1) = f(x, y)$ but $F(X, Y, 0) \not\equiv 0$ (otherwise the projective curve would contain the entire line at infinity). To do so, we *homogenize* $f(x, y)$.

The degree of

$$f(x, y) = \sum_{i,j} a_{ij} x^i y^j$$

is defined as the largest $i + j$ such that a_{ij} is non-zero.

Let the degree of f be d. Then the *homogenization* of f is

$$F(X,Y,Z) = \sum_{i,j} a_{ij} X^i Y^j Z^{d-i-j}$$

which has degree d by observation, $F(x,y,1) = f(x,y)$ and $F(X,Y,Z) \not\equiv 0$ since d ensures there will be a monomial in F without Z.

In conclusion, to move from a projective curve to an affine curve, we dehomogenize (in one of three ways). To construct a projective curve from a curve on the real plane, we homogenize.

We wrap up this section with some terminology which will arise in the discussion of elliptic curves.

A projective curve is called *rational* if F has rational coefficients. Since the set of solutions to a polynomial with rational coefficients is the same as the set of solutions to the same polynomial multiplied by a scalar, we can clear the coefficient denominators and equivalently say that a projective curve is rational if F has integer coefficients.

The *rational points* of a projective curve, denoted by the set $C(\mathbb{Q})$, is the set of points on the curve with rational coordinates. It is an important observation that a homogeneous coordinate can be rational despite a non-rational representative. That is, $[a,b,c]$ is rational if and only if there exists non-zero t such that ta, tb and tb are rational.

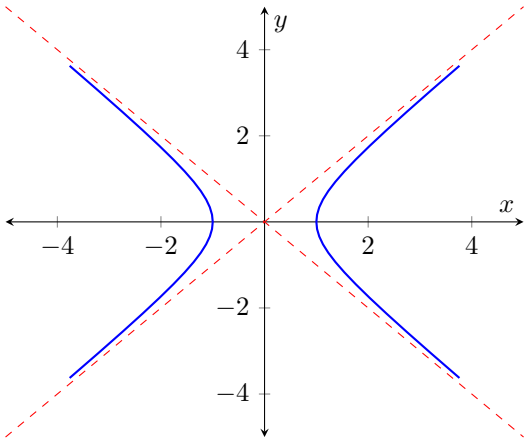
A point on a projective curve is called *non-singular* if its affine points are non-singular as normally defined in calculus and analysis (see appendix B), and its points at infinity are non-singular. We denote points at infinity non-singular if they are non-singular when dehomogenized in an alternative way in which the point is affine. Such a dehomogenization exists from the "not all zero" condition of a homogenous coordinate. If there are multiple ways to dehomogenize, either way is sufficient since a point being non-singular is a local property and U_i are open sets. In particular, if a point lies in the open intersection of U_i and U_j and is non-singular in one, then it must be non-singular in the other.

Lastly, a *tangent line* at a point P on a projective curve is defined by dehomogenizing the curve, finding the tangent to P on the real plane, and homogenizing the tangent equation to get a projective line.

1.6 Worked Example

Finally, we work through an example to see the magic all come together.

We start with the familiar unit hyperbola in $\mathbb{R}^2$



[2]

given by the equation

$$C : x^2 - y^2 = 1.$$

We translate to a curve in $\mathbb{P}^2$ by homogenizing:

$$X^2 - Y^2 = Z^2.$$

Now, given the projective curve

$$F(X, Y, Z) = X^2 - Y^2 - Z^2 = 0$$

we can project it onto U_0 by taking $F(1, y, z)$, U_1 by taking $F(x, 1, z)$ and U_2 by taking $F(x, y, 1)$. On U_2, this curve is our original hyperbola. Taking $Z = 0$ as the line at infinity, we find the points at infinity from U_2:

$$X^2 - Y^2 = 0$$

which implies

$$(X - Y)(X + Y) = 0.$$

That is, $X = Y$ or $-X = Y$, or $[1 : 1]$ and $[1 : -1]$ in $\mathbb{P}^1$. Notice that these are the asymptotes of our hyperbola (limiting tangents).

Now projecting onto U_0 via $F(1, y, z)$, we get the curve

$$y^2 + z^2 = 1.$$

This is a circle! In particular, if $X = 0$ then we get

$$Y^2 + Z^2 = 0$$

whose only solution (over reals) is $[0, 0]$, which is not a point in $\mathbb{P}^1$. This is intuitive since the unit circle does not tend to infinity in any direction on the real plane.

We can visualize the points at infinity by projecting them onto U_0. For example, take $[1 : 1]$ which is associated to the asymptote $L(X, Y, Z) = Y - X = 0$. What does this line look like when projected onto U_0? This line is already homogenized, so taking $L(1, y, z)$ we get the line $y = 1$. Now where does

this line intersect our projective curve? Substituting $y = 1$ into $y^2 + z^2 = 1$ gives that $[1 : 1]$ is the same as the point $(1, 0)$ on the real plane associated to U_0.

Projecting onto U_1 is identical to projecting onto U_2.

2 Rational Points on Conics

We first wish to find rational points on conics which are curves of the form:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \tag{1}$$

where the coefficients are rational. For one of these curves $\mathcal{C}$, suppose we have one rational point on it, $\mathcal{O}$. Then, for any line L in the plane with rational slope, $\forall x_P \in \mathbb{Q}$, let $P = (x_P, y_L)$ with y_L chosen such that $P \in L$.

Proposition 2.1. *The line $L_P^{\mathcal{O}}$ passing through $\mathcal{O}$ and P will intersect $\mathcal{C}$ at another point $\mathcal{Q} \in \mathbb{Q}^2$.*

Proof. $L_P^{\mathcal{O}}$ is given by

$$y = \frac{y_{\mathcal{O}} - y_P}{x_{\mathcal{O}} - x_P} x + \left(y_{\mathcal{O}} - \frac{y_{\mathcal{O}} - y_P}{x_{\mathcal{O}} - x_P} x_{\mathcal{O}} \right).$$

Plugging this y into $\mathcal{C}$, and using projective coordinates, the result will be a quadratic in x. Since one of the solution is $(x_{\mathcal{O}}, y_{\mathcal{O}}) \in \mathbb{Q}^2$ the other, $\mathcal{Q}$, must also be rational by equation 17 of appendix A. □

So $\forall r_P \in \mathbb{Q}$, $\exists \mathcal{Q} \in \mathcal{C} \cap L_P^{\mathcal{O}}$ such that $\mathcal{Q} \in \mathbb{Q}^2$. Which means there is a bijection between $\mathbb{Q}$ and $\mathcal{C} \cap \mathbb{Q}^2$ in projective coordinates. If normal coordinates are used, for the point R such that $L_R^{\mathcal{O}} \parallel L$, the lines will not intersect without projective coordinates.

For this to work we first need a rational point $\mathcal{Q} \in \mathcal{C}$, in general this is not always possible as the conic may not have a single rational point. We look at when this is the case.

Suppose there is such a rational point $(x, y) \in \mathcal{C}$. Since the coefficients of $\mathcal{C}$ are rational we can clear denominators and homogenize $\mathcal{C}$ and get

$$AX^2 + BXY + CY^2 + DXZ + EYZ + FZ^2 = 0 \tag{2}$$

over the integers X, Y, Z where the coefficients are also integers. By Hasse's local-global principal, the above has a solution if and only if it has a real solution and a p-adic solution for all primes p. Therefore, $\mathcal{C}$ has no rational points if and only if the transformed version of $\mathcal{C}$, given by equation 2, does not meet these requirements.

3 Rational Points on Cubics

3.1 Finding Rational Points on Cubics

We now wish to look at rational points on rational cubics of the form

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

where the coefficients are rational. Let $\mathcal{C}$ be a rational cubic, we want to check if $\exists P \in \mathbb{Q}^2 \cap \mathcal{C}$. But now a similar technique to Hasse's for conics fails as this method leads to integer polynomial equations of degree 3 which are much harder to solve.

Now suppose we have a rational point on $\mathcal{C}$. If we try to build a bijection between $\mathbb{Q}$ and $\mathcal{C}$ as we did for conics we quickly encounter an issue as our line $L_P^{\mathcal{O}}$ will intersect $\mathcal{C}$ in two new points instead of one. And in general the two new intersection points of $L_P^{\mathcal{O}}$ and $\mathcal{C}$ will not be rational. This is because plugging in the $y = mx + b$ of $L_P^{\mathcal{O}}$ into $\mathcal{C}$ will yield a cubic equation for which we know one rational solution, $x_{\mathcal{O}}$, but by appendix A, this doesn't impose any condition for the other two roots to also be rational.

So we wish to find new rational points on a degree 3 polynomial from existing ones. From appendix A, we see that we need to already know 2 rational points. So if we have two rational points Q and P on $\mathcal{C}$ then the intersection of the line L_P^Q with $\mathcal{C}$ will be in 3 points, and this third point R, using the notation $R = P * Q$, must also be rational.

Proof. L_P^Q is given by

$$y(x) = \frac{y_Q - y_P}{x_Q - x_P}x + \left(y_Q - \frac{y_Q - y_P}{x_Q - x_P}x_Q\right).$$

Plugging this y into $\mathcal{C}$, the result will be a cubic in x. Let r_3 be this third root. From equation 19 of appendix A we have, $r_3 = \frac{a_0}{-r_1 r_2}$ for $a_0,\ r_1,\ r_2 \in \mathbb{Q}$. So $r_3 \in \mathbb{Q}$ and $R = (r_3, y(r_3)) \in \mathbb{Q}^2$. □

Therefore, the * operation acting between two rational points on a cubic is closed. It is also abelian since the order in which we choose the points clearly doesn't matter.

3.2 Intersections of Cubics

By appendix A.4 of [4], two cubics (polynomials of degree 3) with no common components, will intersect in 9 complex points allowing for multiplicity. We want to prove the following.

Proposition 3.1. *Let $\mathcal{C},\ \mathcal{C}_1,\ \mathcal{C}_2$ be three rational cubics such that $|\mathcal{C} \cap (\mathcal{C}_1 \cap \mathcal{C}_2)| \geq 8$. Then $|\mathcal{C} \cap (\mathcal{C}_1 \cap \mathcal{C}_2)| = 9$.*

Proof. Let $F(x, y) = 0,\ F_1(x, y) = 0,$ and $F_2(x, y) = 0,$ be the equations which describe the rational cubics $\mathcal{C},\ \mathcal{C}_1,$ and $\mathcal{C}_2$ respectively with the coefficient of their first non zero power of x and y in common

is 1. So F, F_1, and F_2 are each uniquely determined by 8 rational numbers. We wish to determine the 8 coefficients of F. For each point in $\mathcal{C} \cap (\mathcal{C}_1 \cap \mathcal{C}_2)$ that we specify, we have a linear equation that must hold for $\mathcal{C}$. So we have 8 linear equations and 8 unknowns. So we can solve for the 8 coefficients of $F(x, y)$. But we notice that for $G = \lambda_1 F_1 + \lambda_2 F_2$, with constants λ_1, λ_2 such that the coefficient of the first non zero power of x and y is 1, G also solves these 8 linear equations. By uniqueness of these 8 coefficients, we must have $F = G$. And the 9th point is clearly a root of G as it is a root of F_1 and F_2. So $\mathcal{C}$ passes through the 9th point. □

3.3 Weierstrass Normal Form and Elliptic Curves

The general form of a cubic is given by equation 1 and is very cumbersome to work with. Through a series of clever substitutions it can be transformed into *Weierstrass normal form*,

$$y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Crucially this transformation is bijective on rational points. For the rest of this paper we can therefore only consider cubics in this form. For more details about this transformation see section 1.3 of [4]. An important property of cubics in this form is that they are symmetric across the y axis.

Such a curve is called an *elliptic curve* if $f(x)$ has distinct complex roots.

3.4 Group of Rational Points

An abelian group of rational points on an elliptic curve C can be formed. It is labeled $C(\mathbb{Q})$. We define $\mathcal{O}$ to be the neutral element at infinity, and consider it a rational point. Then addition is defined by

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

which is a closed and commutative operation as the * operation is closed and commutative (see section 3.1). In Weierstrass normal form the symmetry across the x axis means that for $Q = (x, y), -Q = (x, -y)$. Since we are in the projective plane this shows that we indeed have $-\mathcal{O} = \mathcal{O}$. And $P - P = \mathcal{O} * (P * -P) = \mathcal{O} * \mathcal{O} = \mathcal{O}$. So all elements have inverses. For associativity, let P, Q, R be distinct points.

$$\begin{aligned} P + (Q + R) &= \mathcal{O} * (P * (\mathcal{O} * (Q * R))) = -(P * (-(Q * R))) = -(P * ((-Q) * (-R))) \\ &= (-P) * (Q * R) \\ (P + Q) + R &= \mathcal{O} * ((\mathcal{O} * (P * Q)) * R) = -((-(P * Q)) * R) = -(((-P) * (-Q)) * R) \\ &= (P * Q) * (-R) \end{aligned}$$

We have that

$$(-P)*(Q*R) \in \left(L_{-P}^{Q*R} \cap \mathcal{C}\right) \quad \text{and} \quad (P*Q)*(-R) \in \left(L_{P*Q}^{-R} \cap \mathcal{C}\right)$$

so showing that these points are equal is equivalent to showing that

$$L_{-P}^{Q*R} \cap L_{P*Q}^{-R} \in \mathcal{C}.$$

Let L_{A^B} be the line that goes through the points A and B of the form $y = mx + b$. Set $g_{L_{A^B}}(x) = (mx + b) - y$, then let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the curves with points satisfying the following equations.

$$\mathcal{C}_1 : \; g_{L_{-P}^{Q*R}}(x) \times g_{L_{-R}^{-Q}}(x) \times g_{L_{Q*P}^{-(Q*P)}}(x) = 0$$

$$\mathcal{C}_2 : \; g_{L_{P*Q}^{-R}}(x) \times g_{L_{-P}^{-Q}}(x) \times g_{L_{Q*R}^{-(Q*R)}}(x) = 0$$

Then the eight points, $-P,\ -Q,\ -R,\ Q*P,\ Q*R,\ -(Q*P),\ -(Q*R),\ \mathcal{O}$ are on $\mathcal{C}_1$ and $\mathcal{C}_2$ and $\mathcal{C}$. So by Proposition 3.1 the 9th intersection point of $\mathcal{C}_1$ and $\mathcal{C}_2$ which is given by $L_{-P}^{Q*R} \cap L_{P*Q}^{-R}$ must be on $\mathcal{C}$. Which is what we wanted to show.

The requirements for a group are met so $(C(\mathbb{Q}), +)$ is a group.

4 Points of Finite Order

4.1 Points of Order 2

We consider a non-singular cubic $\mathcal{C}$ in Weierstrass normal form $y^2 = F(x)$ where F is a cubic polynomial. For $ord(P) = 2$ we need $P + P = 2P = \mathcal{O} \iff P = -P \iff y_P = 0 \iff F(x) = 0$. So these points are the 3 complex roots of F. We notice that for these points, $P_1,\ P_2,$ and P_3 we have for $i, j, k = 1, 2, 3,\ i \neq j \neq k,\ P_i + P_j = P_k$ and $P_i + P_i = \mathcal{O}$. So addition of these elements with the identity element is closed. They therefore form a subgroup.

4.2 Points of Order 3

We need $3P = \mathcal{O} \iff P = -2P \iff x_{2P} = x_{-P} = x_P$. We find an expression for x_{2P}. We have $x_{2P} = x_{\mathcal{O}*(P*P)} = x_{-(P*P)} = x_{P*P}$. And $P*P$ is given by the tangent line at P of the form $y = mx+b$. We have $f(x) = x^3 + ax^2 + bx + c$. The slope m is $\frac{dy}{dx}\big|_P$. So by differentiating we get

$$y^2 = f(x) \quad \implies \quad 2y\,\frac{dy}{dx} = f'(x) \quad \implies \quad m = \frac{f'(x_P)}{2y_P}. \tag{4}$$

The intercept β is given by $y_P = mx_P + \beta$.

We plug this into $y^2 = f(x)$ to get

$$y^2 = (mx_P + \beta)^2 = x^3 + ax^2 + bx + c$$
$$0 = x^3 + (a - m^2)x^2 + (b - 2m\beta)x + (c - \beta^2). \tag{5}$$

From appendix A, since we know the double root, x_P, we have:

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

$$\implies x_{2P} = -2x_p - a + m^2$$

$$x_{2P} = -2x_p - a + \left(\frac{f'(x_P)}{2y_P}\right)^2$$

$$x_{2P} = -2x_p - a + \frac{(3x_P^2 + 2ax_P + b)^2}{4(x_P^3 + ax_P^2 + bx_P + c)}$$

$$x_{2P} = \frac{-8x_P(x_P^3 + ax_P^2 + bx_P + c) - 4a(x_P^3 + ax_P^2 + bx_P + c) + (3x_P^2 + 2ax_P + b)^2}{4(x_P^3 + ax_P^2 + bx_P + c)}$$

$$x_{2P} = \frac{x_P^4(-8 + 9) + x_P^3(-8a - 4a + 12a) + x_P^2(-8b - 4a^2 + 4a^2 + 6b) + x_P(-8c - 4ab + 4ab) + (-4ac + b^2)}{4(x_P^3 + ax_P^2 + bx_P + c)}$$

$$x_{2P} = \frac{x_P^4 - 2bx_P^2 - 8cx_P + b^2 - 4ac}{4(x_P^3 + ax_P^2 + bx_P + c)} \tag{6}$$

Let P be a point of order three, then we must have $x_{2P} = x_P$.

$$0 = -x_P + \frac{x_P^4 - 2bx_P^2 - 8cx_P + b^2 - 4ac}{4x_P^3 + 4ax_P^2 + 4bx_P + 4c}$$

$$0 = \frac{-x_P(4x_P^3 + 4ax_P^2 + 4bx_P + 4c) + x_P^4 - 2bx_P^2 - 8cx_P + b^2 - 4ac}{4x_P^3 + 4ax_P^2 + 4bx_P + 4c}$$

$$\iff \psi(x_P) := 3x_P^4 + 4ax_P^4 + 6bx_P^2 + 12cx_P + 4ac - b^2 = 0$$

So the x coordinates of points of order 3 must be roots of $\psi(x)$. As deg $\psi(x) = 4$, $\psi(x)$ has 4 complex roots, which each lead to 2 points on the curve. We look at whether these roots are distinct as this would lead to 8 distinct points of order 3.

Remark 5. *Let $g(x)$ be a polynomial with a double root r, then $g'(r) = 0$. Since for another polynomial $g_2(x)$:*

$$g(x) = (x - r)^2 g_2(x) \quad \implies \quad g'(x) = 2(x - r)g_2(x) + g_2'(x)(x - r)^2 \quad \implies \quad g'(r) = 0.$$

So we need to determine whether $\exists\, x_0$ such that $\psi(x_0) = \psi'(x_0) = 0$.

We can write $\psi(x) = 0$ in the following form using $f''(x) = 6x + 2a$ and $f'''(x) = 6$.

$$\begin{aligned}
\psi(x) = 0 \implies \quad x &= -2x - a + \left(\frac{f'(x)^2}{4f(x)}\right) \\
0 &= 12f(x)x + 4af(x) - f'(x)^2 \\
0 &= f(x)(12x + 4a) - f'(x)^2 \\
0 &= 2f(x)f''(x) - f'(x)^2 \\
\implies \psi(x) &= 2f(x)f''(x) - f'(x)^2 \\
\implies \psi'(x) &= 2f'(x)f''(x) + 2f(x)f'''(x) - 2f'(x)f''(x) \\
\psi'(x) &= 2f(x)f'''(x) = 12f(x)
\end{aligned}$$

So suppose $\exists\, x_0$ such that $\psi(x_0) = \psi'(x_0) = 0$, then

$$\begin{aligned}
\psi'(x_0) = 0 \implies \quad & f(x_0) = 0 \\
\psi(x_0) = 0 \implies \quad & 2f(x_0)f''(x_0) = f'(x_0)^2 = 0 \implies f'(x_0) = 0.
\end{aligned}$$

By B.1, this implies that $\mathcal{C}$ is non-singular, which is a contradiction. So no such x_0 exists and $\psi(x)$ has no double roots. Thus, there are 8 distinct points of order 3.

4.3 Exercise 2.1 [4]

Let A be an abelian group and, for every integer $m \geq 1$, let

$$A_m = \{P \in A : mP = \mathcal{O}\}$$

be the set of elements of order dividing m.

(a) *Prove that A_m is a subgroup of A.*

Proof. A_m is a subgroup if it is non-empty and closed under products and inverses.
It is non-empty since it contains $\mathcal{O}$.
If P, Q are elements of A_m, then $mP = mQ = \mathcal{O}$. Then since rational points are abelian,
$m(P + Q) = mP + mQ = \mathcal{O} + \mathcal{O} = \mathcal{O}$.
Let $-P$ be the inverse of P. We claim that $m(-P)$ is the inverse of mP, i.e. $m(-P) = -(mP) = \mathcal{O}$, so A_m is closed under inverses. The result follows using commutativity of rationals:
$m(-P) + mP = m(-P + P) = m\mathcal{O} = \mathcal{O}$.

□

(b) *Suppose that A has order M^2, and further suppose that for every integer m dividing M, the subgroup A_m has order m^2. Prove that A is the direct product of two cyclic groups of order M.*

Proof. Our goal is to show that $A \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}$, since for groups G and H, $|G \times H| = |G||H|$.
By the *Structure Theorem*, as A is a finitely generated (it is finite) abelian group, it can be expressed as the direct product of finitely many cyclic groups.
So $A \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$, for natural number k, and $m_1|m_2|...|m_k$ (by the Structure Theorem). Hence $|A| = M^2 = m_1 \cdots m_k$.

Claim 1. $A \ncong \mathbb{Z}/M^2\mathbb{Z}$, *thus* $k > 1$.
Suppose for contradiction that $A \cong \mathbb{Z}/M^2\mathbb{Z} = \{0, 1, ..., M, ..., 2M, ..., (M-1)M, ..., M^2 - 1\}$. Then $A_M = \{0, M, 2M, ..., (M-1)M\}$ has order M. Contradiction.

Claim 2. $k = 2$.
$m_1|m_k$, so we write $m_k = m_1 n$ for some natural number n.
Then $M^2 = m_1 \cdots m_k = m_1 \cdots m_n n = m_1^2 \cdots m_{k-1} n$ gives $m_1^2 | M^2$, so $m_1 | M$. This verifies A_{m_1} exists.
Since A_{m_1} is a subgroup of A, we have
$A_{m_1} \cong \{x = (x_1, ..., x_k) \in \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} : m_1 x = \bar{0}\}$. By Lagrange's Theorem, $(\mathbb{Z}/m_1\mathbb{Z}, \bar{0})$ is contained in A_{m_1}.
Now, $m_1|m_2|\cdots|m_k$ gives $\mathbb{Z}/m_1\mathbb{Z} \subseteq \mathbb{Z}/m_2\mathbb{Z} \subseteq \cdots \subseteq \mathbb{Z}/m_k\mathbb{Z}$, so in fact $(\mathbb{Z}/m_1\mathbb{Z})^k$ (shorthand notation for direct product k-times) is contained in A_{m_1}.
By assumption, $|A_{m_1}| = m_1^2$, thus $A_{m_1} \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_1\mathbb{Z}$, forcing $k = 2$.

Claim 3. $m_1 = m_2$
Write m_1 in its prime factorization as $m_1 = p_1^{a_1} \cdots p_d^{a_d}$ for primes p_i and natural numbers a_i.
Since $m_1|m_2$ and $m_1 m_2 = M^2$ implies M^2 has even prime powers, we get
$m_2 = p_1^{a_1+2b_1} \cdots p_d^{a_d+2b_d} \cdot q_1^{2a'_1} \cdots q_{d'}^{2a'_{d'}}$, where $b_i \geq 0$ and $gcd(p_i, q_j)$ for all i in $\{1, ..., d\}$ and j in $\{1, ..., d'\}$.
We proceed to show that $q_j = 1$ for all j. Let q be any arbitrary q_j.
Since q is prime, $q|M^2$ gives $q|M$, which verifies that A_q exists. Now, elements of $\mathbb{Z}/m_1\mathbb{Z}$ have order dividing some combination of $p_i^{a_i}$; in particular, they do not have order dividing q since $gcd(p_i, q) = 1$. Thus $A_q \subseteq \{(0, \mathbb{Z}/m_2\mathbb{Z}\}$. Now how many elements of $\mathbb{Z}/m_2\mathbb{Z}$ have order dividing q? Exactly q. Indeed, recall from a course in group theory,

Lemma 4.1. *For each divisor d of n, there exists a unique subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d. By Lagrange, each element of this subgroup has order dividing d.*

This gives $|A_q| = q$, but by assumption $|A_q| = q^2$ which forces $q = 1$.
Since q was an arbitrary q_j, we have reduced to $m_2 = p_1^{a_1+2b_1} \cdots p_d^{a_d+2b_d}$. It remains to show that $b_i = 0$ for all i. To this end, let $m = p_1^{a_1+b_1}$, dividing M since M^2 has $p_1^{2a_1+2b_1}$ in its prime factorization. Then following how we argued above,
$|A_m| =$ (number of elements of order m in $\mathbb{Z}/m_1\mathbb{Z}$) $\cdot$ (number of elements of order m in $\mathbb{Z}/m_2\mathbb{Z}$),

$\mathbb{Z}/m_1\mathbb{Z}$ has $p_1^{a_1}$ such elements and $\mathbb{Z}/m_2\mathbb{Z}$ has $p_1^{a_1+b_1}$ such elements. By assumption $|A_m| = m^2$. But then $p_1^{a_1} \cdot p_1^{a_1+b_1} = p_1^{2a_1+2b_1} = m^2$ if and only if $b_1 = 0$. The same argument holds for remaining b_i.

It follows from claim 3 that $m_1 = m_2 = M$ since $m_1 m_2 = M^2$.

□

(c) *Find an example of a non-abelian group G and an integer m such that the set $G_m = \{g \in G : g^m = e\}$ is not a subgroup of G.*

Proof. Consider the dihedral group D_3 of order six, the symmetry group of an equilateral triangle. Then G_2 is the set of reflections, but reflections do not form a subgroup since the composition of two reflections is a rotation.

□

5 Complex Points on Elliptic Curves

5.1 Relation to Doubly Periodic Complex Functions

In this section we consider complex points on elliptic curves. These are the points $(x, y) \in \mathbb{C}^2$ such that,

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

for rational coefficients a, b, c. For the cubic

$$y^2 = x^3 + x^2 - x \tag{7}$$

we plot the modular surface, $|y|$ in terms of $x \in \mathbb{C}$ in figure 1.

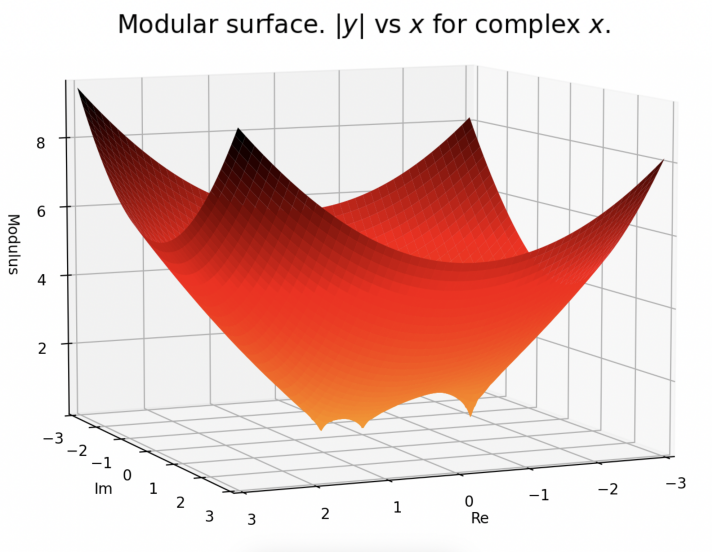


Figure 1: Modular surface of the cubic in equation 7.

Figure 2 shows a zoomed in view where we focus on the points where $|y| = 0$. As $|x| \to \infty$ we can see from figure 1 that $|y| \to \infty$, and for $x \in \mathbb{R}$ we can be more specific as $|y| \to \mathcal{O}$. Therefore if we place $\mathcal{O}$ on the plane (using a transformation in the complex projective plane) as seen in figure 2, the blue curve which contains the real points of the cubic with $y > 0$ will be bent to the black curve such that as $x \to \infty$, $y \to \mathcal{O}$.

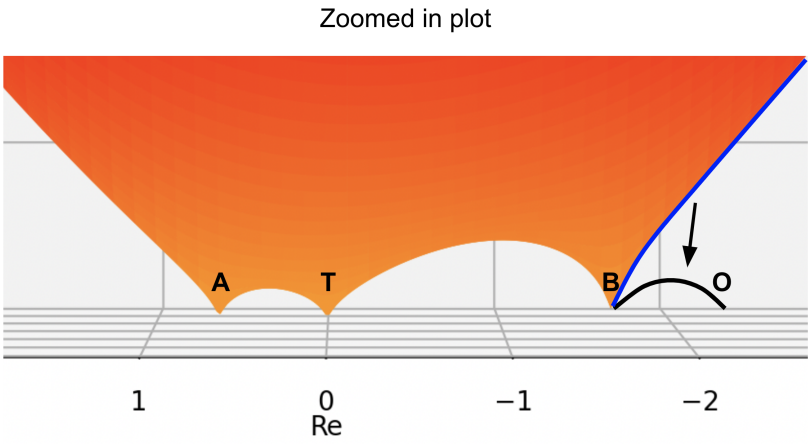


Figure 2: Zoomed in version of Figure 1. We identify the 3 points of order 2 by A, B and $T = (0, 0)$.

By placing $\mathcal{O}$ such that $\text{dist}(A, T) = \text{dist}(B, \mathcal{O})$ our image looks like a slice of through center of the top half of a torus as in figure 3, with $r = \text{dist}(A, T)/2$ and $R = \text{dist}(T, B)/2 + r$. And for each $x \in \mathbb{C}$, both the positive and negative roots of y are on the complex elliptic curve, these negative points correspond to the bottom half of the torus. The complex projective plane is in fact topologically equivalent to a torus. A bijection between the two will be given in the next section.

As seen in figure 3 torus is uniquely determined by the radii of the two circles. These radii can be thought as periods since going around one of the circles gets you back to the same place. A torus can thus be created from a parallelogram in the complex plane with sides R and r. This can be seen visually by gluing the opposite sides of the parallelogram together.

So all parallelograms on $\mathbb{C}$ map to a torus and thus an elliptic curve. To study functions on this parallelogram we require complex functions that are doubly periodic.

5.2 Doubly Periodic Complex Functions

We want a function $f : \mathbb{C} \longrightarrow \mathbb{C}$ such that for w_1, $w_2 \in \mathbb{C}$,

$$f(z + w_1) = f(z) \quad \text{and} \quad f(z + w_2) = f(z).$$

This condition is extremely restrictive, for instance a polynomial would clearly not work nor would any trig function as these only have 1 period. To create such a function we can first notice that an

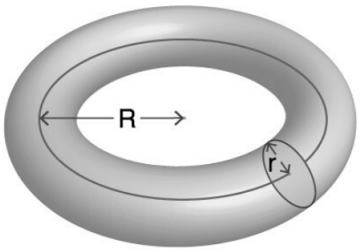


Figure 3: Torus with radii R and r.

infinite sum in both directions is invariant to a simple shift. For example,

$$g(z) = \sum_{n=-\infty}^{\infty} \frac{1}{z+n} \quad \Longrightarrow \quad g(z+1) = g(z).$$

So for our function to be doubly periodic we therefore need to include two infinite sums, meaning that we sum over the following lattice: $\mathcal{L} = \{nw_1 + mw_2 : \forall n, m \in \mathbb{N}\}$. We therefore try

$$f(z) = \sum_{w \in \mathcal{L}} \frac{1}{(z-w)}$$

This function is indeed doubly periodic however it is boring as the sum diverges. The standard function of this type that converges is the Weierstrass $\wp$ function,

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in \mathcal{L}-0} \frac{1}{(z-w)^2} - \frac{1}{w^2}.$$

It is doubly periodic as for $a \in \mathcal{L}$, we have

$$\begin{aligned}
\wp(z+a) &= \frac{1}{(z+a)^2} + \sum_{w \in \mathcal{L}-0} \frac{1}{(z+a-w)^2} - \frac{1}{w^2} \\
&= \frac{1}{(z+a)^2} + \frac{1}{(z+a-a)^2} - \frac{1}{a^2} + \sum_{w \in \mathcal{L}-\{0,a\}} \frac{1}{(z+a-w)^2} - \frac{1}{w^2} \\
&= \frac{1}{z^2} + \frac{1}{(z+a)^2} - \frac{1}{a^2} + \sum_{w \in \mathcal{L}-\{0,a\}} \frac{1}{(z-w)^2} - \frac{1}{w^2} \\
&= \frac{1}{z^2} + \sum_{w \in \mathcal{L}-0} \frac{1}{(z-w)^2} - \frac{1}{w^2} \\
&= \wp(z).
\end{aligned}$$

And it can be shown [1] that for $g_2 = 60 \sum_{w \in \mathcal{L}-0} \frac{1}{w^4}$, and $g_4 = 140 \sum_{w \in \mathcal{L}-0} \frac{1}{w^6}$, $\wp$ satisfies,

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

We define the period parallelogram $P(w_1, w_2)$ as seen in Fig 4 where we include the black boundary and not the red points. We can now define a map from the inside of the parallelogram $P(w_1, w_2)$ onto the complex points on the elliptic curve given by $y^2 = 4x^3 - g_2x - g_3$.

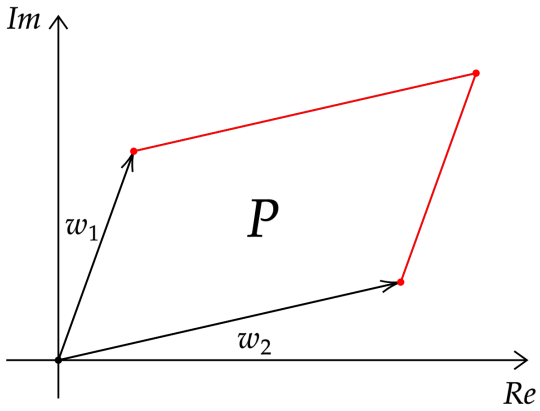


Figure 4: $P(w_1, w_2)$, the red points are not included in $P(w_1, w_2)$.

Let $\phi : P(w_1, w_2) \longrightarrow C(\mathbb{C})$ such that

$$\phi(z) = \begin{cases} (\wp(z), \wp'(z)) & z \in P(w_1, w_2) \setminus 0 \\ \mathcal{O} & z = 0 \end{cases}$$

then ϕ is bijective and

$$\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2) = (\wp(z_1), \wp'(z_1)) + (\wp(z_2), \wp'(z_2))$$

where $+$ in this last line is addition on the elliptic curve.

Finding complex points of finite order on $C(\mathbb{C})$ is now equivalent to finding points of finite order on $P(w_1, w_2)$. Figure 5 shows the points of orders 1, 2, 3 and 4. In general the number of points dividing M is simply M^2 so the number of points of order exactly M is $M^2 - \sum_{d|M,\, d<M} d^2$.

6 Nagell-Lutz Theorem

We wish to find all points of finite order, for this we first transform our cubic equation into an integer equation. Our cubic is

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

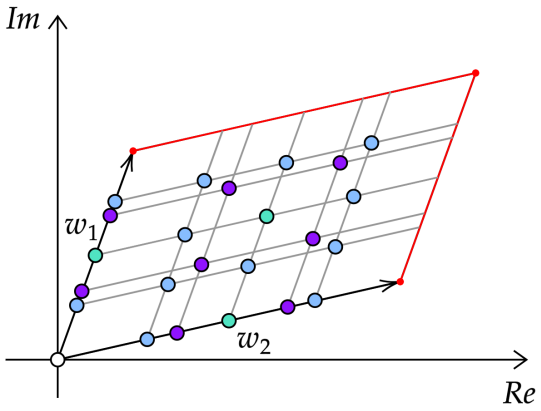


Figure 5: Points of finite order. White = order 1, Cyan = order 2, Purple = order 3, Blue = order 4.

where the coefficients are rational. Since we are looking at rational points, $x, y \in \mathbb{Q}$ so we can clear denominators. So for this section the our cubic equations is over the integers with integer coefficients.

We will prove the following theorem characterizing rational points of finite order.

Theorem 6.1 (Nagell-Lutz)**.** *For* $(x, y) \in C(\mathbb{Q})$.

1. $ord(x, y) < \infty \implies x, y \in \mathbb{Z}$
2. $ord(x, y) < \infty \implies y = 0 \text{ or } y|D.$

Where D is the *discriminant* of the polynomial which can be written in terms of the complex roots $\alpha_1, \alpha_2, \alpha_3$ as

$$D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2.$$

From appendix A, D can be expressed in terms of the coefficients as

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

6.1 Part 1 of Nagell-Lutz Theorem

We wish to prove that if $P = (x, y)$ is of finite order then $x, y \in \mathbb{Z}$. We first develop some results. For m, $n \in \mathbb{Z}$ such that $x = m/n$,

$$x = \frac{m}{n} \in \mathbb{Z} \iff n = 1 \iff \forall p \text{ prime}, p \nmid n. \tag{8}$$

We will thus want to examine the exponent of p in the prime factorization of n. To this end we define the order of a rational number with respect to a prime.

Definition 7. *For a prime p, let m, n, $\nu \in \mathbb{Z}$ such that $\gcd(m,n) = 1$, let*

$$ord\left(\frac{m}{n}p^{\nu}\right) = \nu.$$

This order of a rational number is not to be confused with the order of a point $P = (x, y)$. Next we establish a relation between the order of the coordinates of a point. For m, n, μ, w, u, $\nu \in \mathbb{Z}$ such that $x = \frac{m}{n}p^{\mu}$ and $y = \frac{w}{u}p^{\sigma}$, from the cubic we get that

$$\left(\frac{w}{u}p^{\sigma}\right)^2 = \left(\frac{m}{n}p^{\mu}\right)^3 + a\left(\frac{m}{n}p^{\mu}\right)^2 + b\frac{m}{n}p^{\mu} + c$$

$$\implies \frac{u^2}{w^2p^{2\sigma}} = \frac{m^3 + am^2 + np^{\mu} + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}.$$

And $p \nmid n$, m, w, u so no factor of p can be added or removed to either side. By matching the orders on both sides of the equation we get that $-2\sigma = -3\mu$, which implies that $\exists\, \nu \in \mathbb{Z}$, such that

$$\mu = 2\nu \quad \text{and} \quad \sigma = 3\nu.$$

The exponents of the prime of the coordinate obey this important relation. Next we define a subset of $C(\mathbb{Q})$ based on the order of the coordinates.

Definition 8. *Let*

$$C(p^{\nu}) = \{(x, y) \in C(\mathbb{Q}) : ord(x) \leq -2\nu \text{ and } ord(y) \leq -3\nu\} \cup \mathcal{O}.$$

Since we have inequalities, these sets have the following nesting property.

$$C(p^{\nu}) \subset C(p^{\nu-1}) \subset C(p^{\nu-2}) \subset \ldots \subset C(p^2) \subset C(p) \subset C(\mathbb{Q}) \tag{9}$$

Using this set in combination with the equation 8, part 1 of the theorem says that

$$P \in C(\mathbb{Q}) \text{ and } \operatorname{ord}(P) < \infty \quad \implies \quad \forall p \text{ prime}, P \notin C(p). \tag{10}$$

To this end we first show that $\forall \nu \in \mathbb{N}$, $C(p^{\nu}) \leq C(\mathbb{Q})$.

Proposition 6.1. $C(p^{\nu}) \leq C(\mathbb{Q})$

Proof. We start by changing variables from x, y to t, s where

$$t = \frac{x}{y} \quad \text{and} \quad s = \frac{1}{y}.$$

The cubic transforms from

$$y^2 = x^3 + ax^2 + bx + c \quad \text{to} \quad s = t^3 + at^2 s + bts^2 + cs^3.$$

The map between (x, y) and (t, s) is a bijection for all points such that $\text{ord}(x, y) \neq 2$ and $(t, s) \neq \mathcal{O}$. To add points on the (t, s)-plane we first look at what a line in the (x, y)-plane looks like in the (t, s)-plane. Let $y = \lambda x + \nu$, after dividing by νy we get,

$$\frac{1}{\nu} = \frac{\lambda x}{\nu y} + \frac{1}{y} \quad \Longrightarrow \quad s = -\frac{\lambda}{\nu} t + \frac{1}{\nu}$$

which is also a line. Let $(x, y) \in C(p^\nu)$, we look at $\text{ord}(t, s)$. For $\ell \geq \nu$,

$$x = \frac{m}{np^{2\ell}}, \;\; y = \frac{u}{wp^{3\ell}} \quad \Longleftrightarrow \quad t = \frac{mw}{nu} p^\ell, \; s = \frac{w}{u} p^{3\ell} \quad \Longleftrightarrow \quad \text{ord}(t) = \ell, \;\; \text{ord}(s) = 3\ell. \tag{11}$$

Crucially by the definition of $C(p^\nu)$,

$$\text{ord}(t) \geq \nu \text{ and } \text{ord}(s) \geq 3\nu \quad \Longleftrightarrow \quad (t, s) \in C(p^\nu). \tag{12}$$

Closure of $C(p^\nu)$:

Next we look at the closure of $C(p^\nu)$. Due to the bijection between the (x, y) and (t, s) planes we can work with the the (t, s)-plane. For $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$ (excluding the point at infinity), we find $P_3 = -(t_3, s_3) = P_1 + P_2$. The negative of a point in (t, s)-plane is simply $(-t, -s)$ since,

$$-(x, y) = (x, -y) \quad \Longrightarrow \quad -(t, s) = -\left(\frac{x}{y}, \frac{1}{y}\right) = \left(\frac{x}{(-y)}, \frac{1}{-y}\right) = (-t, -s).$$

So $P_1 + P_2 = (-t_3, -s_3)$.

Case 1: $t_1 = t_2$.

We first consider the case where $t_2 = t_1$. Then $L_{t_1}^{t_2}$ is vertical so $t_3 = t_1$ and P_3 must be P_1 or P_2 so $s_3 = s_2$ or $s_3 = s_1$. Thus, $\text{ord}(-t_3) \geq \nu$ and $\text{ord}(-s_3) \geq 3\nu$ so by equivalence 12, $P_3 = (-t_3, -s_3) \in C(p^\nu)$.

Case 2: $t_1 \neq t_2$ and $P_1 \neq P_2$.

As lines are still lines in the (t, s) plane, $-P_3 \in L_{P_1}^{P_2}$ which is given by, $s = \alpha t + \beta$ with

$$\alpha = \frac{s_1 - s_2}{t_1 - t_2} \quad \text{and} \quad \beta = s_1 - \alpha t_1 = s_2 - \alpha t_2.$$

We solve for α and β using the cubic.

$$\begin{aligned}
s_2 - s_1 &= (t_2 - t_1)^3 + a(t_2^2 s_2 - t_1^2 s_1) + b(t_2 s_2^2 - t_1 s_1^2) + c(s_2^3 - s_1^3) \\
&= (t_2^3 - t_1^3) + a((t_2^2 - t_1^2)s_2 + t_1^2(s_2 - s_1)) + b((t_2 - t_1)s_2^2 + t_1(s_2^2 - s_1^2)) + c(s_2^3 - s_1^3) \\
\implies \alpha = \frac{s_2 - s_1}{t_2 - t_1} &= \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_2 + t_1)s_2 + b s_2^2}{1 - a t_1^2 - b t_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)}. \qquad (13)
\end{aligned}$$

By construction of the line, t_1, t_2, t_3 are roots of the following polynomial in t,

$$\begin{aligned}
\alpha t + \beta = s &= t^3 - a t^2(\alpha t + \beta) + b t(\alpha t + \beta)^2 + c(\alpha t + \beta)^3 \\
\implies 0 &= (1 + a\alpha + b\alpha^2 + c\alpha^3)t^3 + (\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta)t^2 + \dots \\
&= \gamma(t - t_1)(t - t_2)(t - t_3)
\end{aligned}$$

for $\gamma = (1 + a\alpha + b\alpha^2 + c\alpha^3)$, by the Fundamental Theorem of Algebra. From equation 18 of appendix A,

$$\begin{aligned}
-\gamma(t_1 + t_2 + t_3) &= (\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta) \\
\implies t_3 &= \frac{-(\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta)}{(1 + a\alpha + b\alpha^2 + c\alpha^3)} - t_2 - t_1 \qquad (14)
\end{aligned}$$

Since our goal is showing that $(t_3, s_3) \in C(p^\nu)$, we determine $\mathrm{ord}(t_3)$. We have that $\mathrm{ord}(t_1) \geq \nu$, $\mathrm{ord}(t_2) \geq \nu$, and using equation 11,

$$\begin{aligned}
\mathrm{ord}(\alpha) &= \mathrm{ord}\left(\frac{s_1 - s_2}{t_1 - t_2}\right) = \mathrm{ord}(s_1 - s_2) - \mathrm{ord}(t_1 - t_2) = 3\ell - \ell = 2\ell \geq 2\nu \\
\implies \mathrm{ord}(\beta) &= \mathrm{ord}(s_1 - \alpha t_1) \geq 3\nu \\
\implies \mathrm{ord}(t_3) &\geq \min\left\{\min\left\{\mathrm{ord}\left(\frac{-(\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta)}{(1 + a\alpha + b\alpha^2 + c\alpha^3)}\right)\right\},\ \min\{\mathrm{ord}(t_2)\},\ \min\{\mathrm{ord}(t_3)\}\right\} \\
&\geq \min\left\{\min\left\{\mathrm{ord}(-(\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta)\right\} - 0,\ \nu,\ \nu\right\} = \nu \\
\implies \mathrm{ord}(s_3) &= \mathrm{ord}(\alpha t_3 + \beta) \geq 3\nu.
\end{aligned}$$

Therefore by equivalence 12, $(t_3, s_3) \in C(p^\nu)$.

Case 3: $P_1 = P_2$**.**

As $P_1 = P_2$ we use the tangent line at t_1, $\frac{ds}{dt}(t_1)$. Implicit differentiation gives,

$$\frac{ds}{dt} = 3t^2 + a\left(2ts + t^2\frac{ds}{dt}\right) + b\left(s^2 + 2s\frac{ds}{dt}t\right) + 3cs^2\frac{ds}{dt}$$

$$\implies \frac{ds}{dt}(t_1) = \frac{3t_1^2 + 2at_1s + bs^2}{1 - at_1^2 - 2bst_1 - 3cs^2}.$$

But this is the same as equation 13 for $t_1 = t_2$, so this collapses to the previous case.

So in all cases $P_3 \in C(p^\nu)$ which shows that $C(p^\nu)$ is closed under addition. Furthermore, $\forall P \in C(p^\nu)$, $-P \in C(p^\nu)$, $P + (-P) = \mathcal{O} \in C(p^\nu)$. Thus all the requirements for a subgroup are satisfied,

$$C(p^\nu) \leq C(\mathbb{Q}).$$

□

Furthermore, from equation 14 we see that,

$$\begin{aligned}\text{ord}(t_1 + t_2 + t_3) &= \text{ord}\left(\frac{-(\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta)}{(1 + a\alpha + b\alpha^2 + c\alpha^3)}\right) \\ &= \text{ord}(-(\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta) - \text{ord}(1 + a\alpha + b\alpha^2 + c\alpha^3) \\ &\geq (2\nu + 3\nu) - 0 = 5\nu \geq 3\nu.\end{aligned}$$

So in terms of the set,

$$R_m = \{a \in \mathbb{Q} : \text{ord}(a) \geq m\}$$

we have that

$$t_1 + t_2 + (-t_3) \in R_{3\nu} \quad \implies \quad t_3 \equiv t_1 + t_2 \mod R_{3\nu}. \tag{15}$$

So we can define the following homomorphism.

Definition 9. *Let* $g : \frac{C(p^\nu)}{C(p^{3\nu})} \longrightarrow \frac{R_\nu}{R_{3\nu}}$ *such that*

$$g((x, y)) = t = \frac{x}{y} \quad \textit{and} \quad g(\mathcal{O}) = 0.$$

We are now able to prove part 1 of the Nagell-Lutz theorem which as previously mentioned is equivalent to proving implication 10. By contradiction, suppose that $\exists P$ of order m in $C(p)$. So by the nesting property 9, $\exists \nu \geq 1$ such that $P \in C(p^\nu)$ but $P \notin C(p^{\nu+1})$.

Case 1: $p \nmid m$

If $p \nmid m$ then, for $n \in \mathbb{N}$ let t_n be the t coordinate of nP. From equation 15.

$$\begin{aligned} t_2 &\equiv t_1 + t_1 && \mod R_{3\nu} \\ t_3 &\equiv t_2 + t_1 \equiv 3t_1 && \mod R_{3\nu} \\ &\vdots \\ t_n &\equiv nt_1 && \mod R_{3\nu} \end{aligned}$$

But $mP = \mathcal{O}$ so $g(mP) = t_m = g(\mathcal{O}) = 0$. And $\gcd(m, p) = 1$ so $m \equiv 1 \mod R_{3\nu}$, thus

$$\begin{aligned} t_m = 0 \equiv mt_1 \equiv t_1 && \mod R_{3\nu} \\ \implies t_1 \equiv 0 && \mod R_{3\nu} \\ \implies P \in C(p^{3\nu}) \\ \implies P \in C(p^{\nu+1}). \end{aligned}$$

by nesting property 9, since $\nu + 1 < 3\nu$. But this is a contradiction since $P \notin C(p^{\nu+1})$.

Case 2: $p \mid m$

Let $m = np$ and $P' = nP$ so P' has order p and $C(p)$ is closed so $P' \in C(p)$. As in the previous case let $\nu \geq 1$ such that $P' \in C(p^\nu)$ but $P' \notin C(p^{\nu+1})$. As before, $t'_n \equiv nt'_1 \mod R_{3\nu}$ so

$$\begin{aligned} g(pP') = g(\mathcal{O}) = 0 = t'_p \equiv pt'_1 && \mod R_{3\nu} \\ \implies t'_1 \equiv 0 && \mod R_{3\nu-1} \\ \implies P' \in C(p^{3\nu-1}) \\ \implies P' \in C(p^{\nu+1}) \end{aligned}$$

by nesting property 9, as $\nu + 1 < 3\nu - 1$. But this is a contradiction since $P' \notin C(p^{\nu+1})$.

Therefore in both cases, for $P \in C(\mathbb{Q})$ such that $\text{ord}(P) < \infty$,

$$P = (x, y) \notin C(p) \quad \implies \quad x, y \in \mathbb{Z}.$$

Which completes the proof of part 1 of the Nagell-Lutz theorem.

6.2 Part 2 of Nagell-Lutz Theorem

For $P = (x_P, y_P)$, we suppose that $\text{ord}(x_P, y_P) < \infty$, and by part 1 of the theorem, $x, y \in \mathbb{Z}$. We wish to show that $y_P = 0$ or $y_P \mid D$. Since P has finite order, so does $2P$ which therefore also has integer coordinates. From equations 4, 5 and appendix A, for $m = \frac{f'(x_P)}{2y_P}$,

$$a - m^2 = -(2x_P + x_{2P}).$$

And $a, x_P, x_{2P} \in \mathbb{Z} \implies m^2 \in \mathbb{Z}$. But we also have that $f'(x_P), y_P \in \mathbb{Z} \implies m \in \mathbb{Q}$. So the denominator of m must be 1, thus $m \in \mathbb{Z}$. Hence, $y_P \mid f'(x_P)$. And $y_P^2 = f(x_P) \implies y_P \mid f(x_P)$. So if $D = r(x)f(x) + s(x)f'(x)$ for $r(x), s(x) \in \mathbb{Z}[x]$, then $y_P \mid D$ as y_P can be factored out of $f(x_P)$ and $f'(x_P)$. We therefore need $r(x), s(x)$ such that,

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = r(x)f(x) + s(x)f'(x).$$

We can solve for the coefficients of r and s using Mathematica (see appendix C). Since we require the coefficients to be integers, we find that the smallest polynomials for which this works is with $\deg(r) = 1$ and $\deg(s) = 2$. We find the solutions,

$$\begin{aligned} r(x) &= -4a^3 + 15ab - 27c + x(-6(a^2 - 3b)) \\ s(x) &= a^2b - 4b^2 + 3ac + x(2a^3 - 7ab + 9c) + x^2(2(a^2 - 3b)). \end{aligned}$$

Thus $y_P \mid D$ or $y_P = 0$ in which case P has order 2.

This completes the proof of part 2 of the Nagell-Lutz theorem. Points of finite order in $C(\mathbb{Q})$ thus have integer coordinates and their y coordinate is 0 or one of the divisors of D.

7 Rational Points are Finitely Generated

In this section we aim to prove

Theorem 7.1 (Mordell's Theorem for curves with a rational point of order two)**.** *For a non-singular cubic curve*

$$C : y^2 = x^3 + ax^2 + bx$$

with integer coefficients, the group of rational points is a finitely generated abelian group.

and do so as a direct corollary of the tailored *Descent Theorem* for non-singular cubic curves, and our prior knowledge that $C(\mathbb{Q})$ is an abelian group.

Theorem 7.2 (Descent Theorem)**.** *For an abelian group Γ, suppose there exists a function*

$$h : \Gamma \to [0, \infty)$$

satisfying

1. *For real number M, the set $\{P \in \Gamma : h(P) \leq M\}$ is finite (i.e. h satisfies the "Finiteness Property")*
2. *For every fixed P_0 in Γ, there exists constant k_0 such that for all P in Γ*

$$h(P + P_0) \leq 2h(P) + k_0$$

3. *There exists constant k such that for all P in Γ*

$$h(2P) \geq 4h(P) - k$$

and the further condition

4. The subgroup $2\Gamma = \{2P : P \in \Gamma\}$ *has finite index in* Γ

holds.
Then Γ *is finitely generated.*

The conditions of the Descent Theorem holding in the setting of Mordell's Theorem are lemmas themselves, and we will only briefly mention their proofs. However, we refer the reader to [4] 3.1-3.5 for complete proofs.

The conditions of the Descent Theorem also refer to a function h, which we define now.

7.1 Height

It is useful to have a function that defines the complexity of a number, which motivates the concept of *height*.

For a rational point $x = \frac{p}{q}$ with integer numerator and denominator, we define the big height function H as

$$H(x) = max\{|p|, |q|\}.$$

We further define the little height function h as

$$h(x) = \ln(H(x))$$

Big H defines the complexity by norm whereas little h defines the complexity of a number by the number of digits. Hence, a number with small h height would take less space to store than a number with big h height.

By observation, $\{x \in \mathbb{Q} : H(x) \leq k\}$ is a finite set. This follows from the fact that then $|p|, |q| \leq k$, so there are finite choices for both p and q.

For a point $P = (x, y)$ in $C(\mathbb{Q})$, we define

$$H(P) \coloneqq H(x)$$

and by convention, we set $H(\mathcal{O}) = 1$.

7.2 Exercise 3.1 [4]

Part (a). *Prove that the set of rational numbers* x *with height* $H(x)$ *less than or equal to* k *contains at most* $2k^2 + k$ *elements.*

Proof. This is a combinatorics argument.
Write $x = \frac{p}{q}$ with $p, q \in \mathbb{Z}$ in reduced form. Suppose $H(x) = max\{|p|, |q|\} \leq k$. Then in particular

$|p| \leq k$ and $|q| \leq k$, so we write $-k \leq p, q \leq k$. Since p, q take integer values, we see that there are $2k+1$ choices for p and $2k$ choices for q (since q cannot be zero). Thus we get $(2k+1)(2k)$ total pairings of p and q. But note, since a negative in the numerator is equivalent to a negative in the denominator, we can, WLOG, say there are actually only k choices for q. Other equivalencies, like reducing fractions, would only reduce the number of unique combinations, so we conclude that there are at most $(2k+1)(k) = 2k^2 + k$ reduced rational numbers with height less than or equal to k.

□

Part (b). *Let $R(k)$ be the set of rational numbers with height $H(x) < k$. Prove that*

$$\lim_{k\to\infty} \frac{|R(k)|}{k^2} = \frac{12}{\pi^2}. \tag{16}$$

Proof. Let $0 \leq m, n < k$. We start by finding an expression for $|\{\gcd(m,n) = 1\}|$ in terms of $|R(k)|$. We can write,

$$|R(k)| = \left|\left\{\frac{m}{n} \in \mathbb{Q}^+\right\}\right| + \left|\left\{\frac{m}{n} \in \mathbb{Q}^-\right\}\right| - |\{0\}|$$

since these two sets are disjoint except for 0, so we must subtract 1. Noting that the numerator and denominator of a rational number in lowest terms are coprime, we have that

$$|\{\gcd(m,n) = 1\}| = \left|\left\{\frac{m}{n} \in \mathbb{Q}^+\right\}\right| = \frac{|R(k)|+1}{2}.$$

Given a list of N_{total} outcomes, the probability of the event E is

$$P(E) = \frac{N_E}{N_{total}}.$$

Let E_k be the event:

$$\gcd(m,n) = 1 \text{ for } 0 \leq m, n < k.$$

To determine $P(E_k)$, we have that $N_{total} = k^2$ as there are k choices for both m and n. And $N_{E_k} = |\{\gcd(m,n) = 1\}| = \dfrac{|R(k)|+1}{2}$. So

$$P(E_k) = \frac{N_{E_k}}{N_{total}} = \frac{|R(k)|+1}{2k^2}.$$

We now compute $P(E_\infty)$ directly and then we can equate it to $\lim_{k\to\infty} P(E_k)$. We calculate the probability that for $n, m \in \mathbb{N}_0$, $\gcd(m,n) = 1$. But

$$\gcd(m,n) = 1 \quad \iff \quad \forall p,\, \neg(p|m \text{ and } p|n)$$

so we compute $P(\neg(p|n \text{ and } p|m))$. For a prime p, every p integers are divisible by p so

$$P(p|n) = \frac{1}{p} \quad \implies \quad P(p \nmid n) = 1 - \frac{1}{p}$$

$$P((p|n \text{ and } p|m)) = \frac{1}{p^2} \quad \implies \quad P(\neg(p|n \text{ and } p|m)) = 1 - \frac{1}{p^2}.$$

The events for each prime p are independent as no prime divides another prime. Thus, $P(E_\infty)$, the probability that $\gcd(m, n) = 1$ is,

$$P(E_\infty) = \prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\prod_p \left(\frac{1}{1 - \frac{1}{p^2}}\right)} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Where the ζ function is defined for $s \in \mathbb{C}$, such that $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. The link between ζ and the infinite product is called the Euler's product. It says that for p prime,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}}.$$

since we can expand each term in the product to get

$$\prod_p \frac{1}{1 - \frac{1}{p^s}} = \left(\frac{1}{2^{s\cdot 0}} + \frac{1}{2^{s\cdot 1}} + \frac{1}{2^{s\cdot 2}} + ...\right)\left(\frac{1}{3^{s\cdot 0}} + \frac{1}{3^{s\cdot 1}} + \frac{1}{3^{s\cdot 2}} + ...\right)...$$

We can then expand this into a sum, where each term will be the product,

$$\prod_p \frac{1}{p^{sa_p}}$$

for a unique sequence $\{a_p\}$ of exponents. By the Fundamental Theorem of Arithmetic this covers all natural numbers so we get

$$\sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Combining these results we get that,

$$\lim_{k\to\infty} P(E_k) = \lim_{k\to\infty} \frac{|R(k)| + 1}{2k^2} = \lim_{k\to\infty} \frac{|R(k)|}{2k^2} = P(E_\infty) = \frac{6}{\pi^2}$$

$$\implies \lim_{k\to\infty} \frac{|R(k)|}{k^2} = \frac{12}{\pi^2}$$

as required. □

This result leads is connected to an interesting property of Euler's totient function φ. We start by establishing a recurrence relation for $|R(k)|$. For $k > 1$, let A be a set such that $|R(k + 1)| =$

$|R(k)| + 2|A|$, where A includes only positive rational numbers. Then

$$A = \left\{ \frac{k}{y} : 1 \leq y \leq k, (k, y) = 1 \right\} \bigcup \left\{ \frac{x}{k} : 1 \leq x \leq k, (k, x) = 1 \right\}.$$

The cardinality of A is thus, $2\varphi(k)$. So,

$$\begin{aligned} |R(k+1)| &= |R(k)| + 4\varphi(k) = |R(k-1)| + 4(\varphi(k) + \varphi(k-1)) = ... \\ &= |R(1)| + 4\sum_{n=2}^{k} \varphi(k) \\ &= 4\sum_{n=1}^{k} \varphi(n). \end{aligned}$$

Thus we can express our limit in terms of φ,

$$\lim_{k\to\infty} \frac{|R(k)|}{k^2} = \lim_{k\to\infty} \frac{4}{k^2} \sum_{n=1}^{k} \varphi(n) = \frac{12}{\pi^2}.$$

Which yields an interesting asymptotic relationship. As $k \to \infty$,

$$\sum_{n=1}^{k} \varphi(n) \approx \frac{3}{\pi^2} k^2.$$

7.3 Proof of Mordell's Theorem

We proceed in the following way given by [4] 3.1-3.5. We first assume the conditions of the Descent Theorem for $\Gamma = C(\mathbb{Q})$ and h the little height function, and prove the Descent Theorem. We then observe how the stated case of Mordell's Theorem follows *if* the conditions of the Descent Theorem hold under the conditions of Mordell's Theorem. We conclude by sketching the proofs of the conditions with h being the little height function.

Proof. (*Descent Theorem*)
Since there are finite cosets of 2Γ in Γ, we let $[\Gamma : 2\Gamma] = n$ and take a representative from each coset, denoted $Q_1, ..., Q_n$. Then for every P in Γ, since P is in one of the cosets, there exists $i_1 \in \{1, ..., n\}$ such that

$$P - Q_{i_1} = 2P_1$$

for some P_1 in Γ. We repeat the same argument for P_1, finding i_2 and P_2. Recursively,

$$\begin{aligned} P - Q_{i_1} &= 2P_1 \\ P_1 - Q_{i_2} &= 2P_2 \\ &\vdots \end{aligned}$$

$$P_{m-1} - Q_{i_m} = 2P_m$$
$$\vdots$$

Now backtracking through this set of equations from step m and substituting for $P_{m-1}, ..., P_1$ we get

$$P = Q_{i_1} + 2Q_{i_2} + ... + 2^{m-1}Q_{i_m} + 2^m P_m$$

and observe that P is an element of the subgroup generated by the coset representatives and P_m. It remains to show that by choosing large enough m, the height of P_m will be less than some real K, independent of P. Then since $\{R \in \Gamma : h(R) \leq K\}$ is a finite set, we conclude that

$$\{Q_1, ..., Q_n\} \cup \{R \in \Gamma : h(R) \leq K\}$$

is a finite generating set for Γ.

We proceed to find K. We do so by showing that height significantly decreases along the sequence $P, P_1, ...$ using conditions 2 and 3.

Applying condition 2 to the set $\{Q_1, ..., Q_n\}$, there exists a constant k_i for $i \in 1, ..., n$ such that

$$h(P - Q_i) \leq 2h(P) + k_i$$

for all points P in Γ. Since the set of coset representatives is finite, taking $k' = \max\{k_i : i \in \{1, ..., n\}\}$, we have

$$h(P - Q_i) \leq 2h(P) + k'$$

for all P and i. Now letting k be the constant from condition 3 for arbitrary j and combining with the definition of P_j and above equation, we get

$$4h(P_j) \leq h(2P_j) + k = h(P_{j-1} - Q_{i_j}) + k \leq 2h(P_{j-1}) + k + k'.$$

Equivalently,

$$h(P_j) \leq \tfrac{3}{4}h(P_{j-1}) - \tfrac{1}{4}\left(h(P_{j-1}) - (k + k')\right).$$

Hence, when $h(P_{j-1}) \geq k + k'$, $h(P_j) \leq \frac{3}{4}h(P_{j-1})$.

Now if $h(P_j) \leq k + k'$ for all j, we are already done by defining $K \coloneqq k + k'$. So assuming that there exists $h(P_{j-1}) \geq k + k'$, we get that $h(P_j) \leq \frac{3}{4}h(P_{j-1})$. If $h(P_{j-1}) \geq k + k'$, we apply the same argument. Thus, since multiplying a real number continuously by $\frac{3}{4}$ converges to zero, there exists some P_m such that $h(P_m) \leq k + k' \coloneqq K$, and we are done.

□

We now observe the proof of Mordell's Theorem as a corollary to the Descent Theorem:

Proof. (*Mordell's Theorem*)
Assuming that the conditions for the Descent Theorem hold in the setting of Mordell's Theorem, we get that $\Gamma \coloneqq C(\mathbb{Q})$ is finitely generated. From 3.4, we already know that $C(\mathbb{Q})$ is abelian, so we are done. □

We now outline the proofs of the Descent Theorem conditions holding in the setting of Mordell's Theorem as given in [4] 3.2-3.5.

The proof of condition 1 with $\Gamma = C(\mathbb{Q})$ follows from our observation that $\{R \in \Gamma : H(R) \leq K\}$ is a finite set.

The proof of condition 2 is rather direct and uses the explicit equations for rational points found in 4.

The proof of condition 3 also uses equations from 4 and is reduced to a more general result.

The proof of condition 4 is more involved, requiring the definition of two homomorphisms and several lemmas itself. The general outline from [4] is as follows:

We would like to show

Lemma 7.3. *For a non-singular elliptic curve C,*

$$[C(\mathbb{Q}) : 2C(\mathbb{Q})] < \infty$$

Now we are assuming there is a rational point of order two. Assuming that the curve is in Weierstrass form, by a change of coordinates, we can assume C is in the form

$$C : y^2 = f(x) = x^3 + ax^2 + bx,\ a, b \in \mathbb{Z}.$$

with rational point of order two, $R = (0, 0)$. Now we claim

Lemma 7.4. *For abelian groups A, B and homomorphisms $\Phi : A \to B$, $\Psi : B \to A$ such that $\Psi(\Phi(a)) = 2a$ for all a in A, if $[B : \Phi(A)] < \infty$ and $[A : \Psi(B)] < \infty$ then $[A : 2A] < \infty$.*

So it remains to find such homomorphisms with $A = C(\mathbb{Q})$.

To define such homomorphisms, we define two new elliptic curves

$$\overline{C} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x$$
$$\overline{\overline{C}} : y^2 = x^3 + \overline{\overline{a}}x^2 + \overline{\overline{b}}x$$

where $\overline{a} = -2a$, $\overline{b} = a^2 - 4b$ and recursively with double bar so that $\overline{\overline{a}} = 4a$ and $\overline{\overline{b}} = 16b$. Then it is easy to define an isomorphism, Λ, between $\overline{\overline{C}}$ and C.

Now we define

$$\Phi : C \to \overline{C}$$
$$(x,y) \mapsto \begin{cases} \left(\frac{y^2}{x^2}, y\left(\frac{x^2-b}{x^2}\right)\right) & \text{if } x \neq 0 \\ \overline{\mathcal{O}} & \text{if } (x,y) \in \{R, \mathcal{O}\} \end{cases}$$

and likewise

$$\overline{\Phi} : \overline{C} \to \overline{\overline{C}}.$$

Finally we define

$$\Phi = \Phi$$
$$\Psi = \Lambda \circ \overline{\Phi}$$

as per the above lemma.

We then continue to show that Φ is a homomorphism and $\Psi \circ \Phi$ is the multiplication by two map. Along with $\ker(\Phi) = \{R, \mathcal{O}\}$ and a couple lemmas, we get that $[\Gamma : \Psi(\overline{\Gamma})] \leq 2^{t+1}$, for $\Gamma = C(\mathbb{Q})$ and t, the number of unique primes in the factorization of b. The desired result follows from the above lemma.

8 Elliptic Curves Over Finite Fields

8.1 Finite Fields and Rational Points on Lines and Quadratics

Up until now, we have worked over elliptic curves with rational coefficients. However, $\mathbb{Q}$ is not of particular importance; in fact, everything above holds for any field. In cryptography, $\mathbb{F}_p$ is utilized where $\mathbb{F}_p$ is the field of integers mod prime p.

That is, we look at curves of the form

$$C : F(x,y) = 0$$

with coefficients in $\mathbb{F}_p$. We call a point *rational* if it is a solution to C and its coordinates are in $\mathbb{F}_p$. The complete set of rational points is denoted by $C(\mathbb{F}_p)$. Just like the rational points over curves with rational coefficients, we include points at infinity in $C(\mathbb{F}_p)$, and recall that cubics only have one point at infinity, denoted $\mathcal{O}$. With the same group law as before, $C(\mathbb{F}_p)$ forms a group.

We are left with the question: what is the size of $C(\mathbb{F}_p)$ and what group is it? We first notice that since $\mathbb{F}_p$ is finite, $C(\mathbb{F}_p)$ is also finite and trivially finitely generated. To explicitly find the size of $C(\mathbb{F}_p)$, we first we look at lines, then conics, and finally cubics. Knowing the size, we can describe the group structure using group theory, as is demonstrated by an example in the following subsection.

A line takes the form $y = ax + b$, so for any input of x in $\mathbb{F}_p$, y is uniquely determined (and in $\mathbb{F}_p$). As a projective curve, this line is defined by $Y = aX + bZ$. The single point at infinity is found by taking $Z = 0$, which gives the point $[1, a]$ in $\mathbb{P}^1$. In total, for a line C, $|C(\mathbb{F}_p)| = p + 1$.

It turns out that non-singular conics also have exactly $p+1$ rational points. The method for finding rational points on conics with coefficients in $\mathbb{Q}$ from section 2 also applies to coefficients in $\mathbb{F}_p$. That is, given one rational point P on our conic C, then by drawing any line with coefficients in $\mathbb{F}_p$ and projecting the conic onto this line from P, we get a bijection between rational points on the cubic and rational points on the line.

To make this argument more clear, we provide an example for the unit circle over $\mathbb{F}_{13}$:

$$C : x^2 + y^2 = 1$$

We project this conic onto the $y-axis$ from the point $(-1,0) = (12,0)$. A line connecting $(12,0)$ and $(m,0)$ on the $y-axis$ for some m in $\mathbb{F}_{13}$ is given by $y = m(1+x)$, and so substituting this into C gives us the rational parametrization of a circle:

$$x = \frac{1-m^2}{1+m^2}$$
$$y = \frac{2m}{1+m^2}$$

Now we can substitute values for m and find the second point of intersection with the conic, which will itself be rational. Note that a line of slope 12 is a line of slope -1 as we are working in $\mathbb{F}_{13}$.

Take $m = 2$. This gives $x = \frac{-3}{5}$, and since $\mathbb{F}_{13}$ is a field, $\frac{1}{5}$ does indeed exist as $-5 \equiv_{13} 8$.
Now $-3 \cdot 8 = -24 \equiv_{13} 2$. The second calculation yields $y \equiv_{13} 3$. So we have found a second rational point on C: $(2,3)$.

What happens if we take $m = 5$ or $m = 8$? In this case, following our explicit formulas for x and y, we get $x = \frac{2}{0}$. So what is happening here? Let's view our circle in the projective plane. Homogenizing gives

$$X^2 + Y^2 = Z^2$$

and substituting $Y = 5(X+Z)$ gives, after explanding and simplifying,

$$(X+Z)(11Z) = 0.$$

If $X = -Z$, it follows that $Y = X = 0$, which is not a point on the projective plane. So we must have $Z = 0$, in which case $Y = 5X$, giving the point at infinity $[1:5]$. Indeed, $1^2 + 25^2 \equiv_{13} 0$.

The same argument can be applied for $m = 8$.

So we get $p-2$ rational points from our explicit formulas, two points at infinity and our original point $(-1,0)$ — a total of $p+1$ rational points.

As for cubics, the number of rational points can vary, as is demonstrated by the example in the following subsection. However, the number of rational points can be approximated by a result known as the *Hasse-Weil Theorem*, refined to the setting of an elliptic curve over a finite field $\mathbb{F}_p$.

Theorem 8.1. *(Hasse-Weil) For an elliptic curve over a finite field $\mathbb{F}_p$,*

$$-2\sqrt{p} \leq \#C(\mathbb{F}_p) - p - 1 \leq 2\sqrt{p}.$$

This theorem is motivated by the fact that mod an odd prime ($\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$) the non-zero elements are equally divided between quadratic residues (defined in following subsection) and non-quadratic residues. So for a cubic given by

$$C : y^2 = f(x),$$

and substituting values of x from $\mathbb{F}_p$, we either get $y^2 = 0$ or $y^2 \neq 0$. In the former case, this gives only one solution, $y = 0$. In the latter case, there is a fifty-fifty chance that there are two solutions for y or no solutions for y (the split of quadratic residues). Thus, the number of rational points should be relatively close to $p + 1$ by counting the probable $\frac{p-1}{2} \cdot 2$ solutions from quadratic residues and $y = 0$, and of course the (single) point at infinity for a cubic.

8.2 Exercise 4.2 [4] — Rational Points on Cubics

Compute the group $C(\mathbb{F}_p)$ for the curve

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

and the primes $p = 3, 7, 11$ and 13.

Proof. Since our curve is cubic, we will need to compute quadratic residues, which are introduced in an algebraic number theory course.

Definition 10. *a is a quadratic residue mod n if there exists x in $\mathbb{Z}$ such that $x^2 \equiv_n a$.*

Definition 11. *Let n in $\mathbb{Z}$ and p prime. The Legendre symbol is defined as*

$$\left(\frac{n}{p}\right) = \begin{cases} -1 & \text{if } n \text{ not quadradic residue mod } p \\ 0 & \text{if } n \equiv_p 0 \\ 1 & \text{if } n \not\equiv_p 0, \text{ quadratic residue mod } p \end{cases}$$

To compute quadratic residues, we use Euler's Criterion:

Theorem 8.2. ***Euler's Criterion.*** *For any odd prime p and $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.*

We are now ready to start *exercise 4.2.*
Recall our curve

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

We start with $p = 3$, which is easy to compute by hand.

- $\mathbb{F}_p = \{0, 1, 2\}$

- $x = 0 \Rightarrow y = \pm 1$

  $\{(0,1),(0,-1)\} = \{(0,1),(0,2)\}\ (mod\ 3)$

- $x = 1 \Rightarrow y^2 = 3\ (mod\ 3) \Rightarrow y^2 = 0\ (mod\ 3)$

  $\{(1,0)\}\ (mod\ 3)$

- $x = 2 \Rightarrow y^2 = 11\ (mod\ 3) \Rightarrow y^2 = 2\ (mod\ 3)$

  $\left(\frac{2}{3}\right) = 2^{\frac{3-1}{2}} = 2\ (mod\ 3) = -1\ (mod\ 3)$

  2 is not a quadratic residue $(mod\ 3)$

- $C(\mathbb{F}_3) = \{(0,1),(0,2),(1,0),\mathcal{O}\}$

We compute $p = 7, 11$ and 13 the same way:

x	$y^2\ (mod\ 7)$	**QR**	**Solutions**	**Points**
0	$1\ (\Rightarrow y = \pm 1)$			$(0,1),(0,6)$
1	3	-1		
2	$4\ (\Rightarrow y = \pm 2)$			$(2,2),(2,5)$
3	3	-1		
4	6	-1		
5	5	-1		
6	6	-1		

$$C(\mathbb{F}_7) = \{(0,1),(0,6),(2,2),(2,5),\mathcal{O}\}$$

x	$y^2\ (mod\ 11)$	**QR**	**Solutions**	**Points**
0	$1 \Rightarrow y = \pm 1$			$(0,1),(0,10)$
1	3	1	$5,6$	$(1,5),(1,6)$
2	0			$(2,0)$
3	9	1	$3,8$	$(3,3),(3,8)$
4	3	1	$5,6$	$(4,5),(4,6)$
5	10	-1		
6	3	1	$5,6$	$(6,5),(6,6)$
7	10	-1		
8	$4 \Rightarrow y = \pm 2$			$(8,2),(8,9)$
9	2	-1		
10	10	-1		

$$C(\mathbb{F}_{11}) = \{(0,1),(0,10),(1,5),(1,6),(2,0),(3,3),(3,8),(4,5),(4,6),(6,5),(6,6),(8,2),(8,9),\mathcal{O}\}$$

x	$y^2 \ (mod\ 11)$	**QR**	**Solutions**	**Points**
0	$1 \Rightarrow y = \pm 1$			$(0,1),(0,12)$
1	3	1	$4,9$	$(1,4),(1,9)$
2	11	-1		
3	5	-1		
4	$4 \Rightarrow y = \pm 2$			$(4,2),(4,11)$
5	$1 \Rightarrow y = \pm 1$			$(5,1),(5,12)$
6	2	-1		
7	0			$(7,0)$
8	$1 \Rightarrow y = \pm 1$			$(8,1),(8,12)$
9	11	-1		
10	10	1	$6,7$	$(10,6),(10,7)$
11	$4 \Rightarrow y = \pm 2$			$(11,2),(11,11)$
12	12	1	$5,8$	$(12,5),(12,8)$

$$C(\mathbb{F}_{13}) = \{(0,1),(0,12),(1,4),(1,9),(4,2),(4,11),(5,1),(5,12),(7,0),(8,1),(8,12),(10,6),$$
$$(10,7),(11,2),(11,11),(12,5),(12,8),\mathcal{O}\}$$

From this exercise we can conclude a couple things. Firstly, unlike with lines and quadratics who, as we have shown, have exactly $p+1$ points in $C(\mathbb{F}_p)$, cubics appear to have an unpredictable amount of points. However, the Hasse-Weil Theorem 8.1 gives the estimate

$$-2\sqrt{p} \leq \#C(\mathbb{F}_p) - p - 1 \leq 2\sqrt{p}$$

Indeed, we see in $p = 13$, for example, that $\#C(\mathbb{F}_p) = 18$, and

$$6.8 \approx -2\sqrt{13} + (13+1) \leq 18 \leq 2\sqrt{13} + (13+1) \approx 21.2.$$

Secondly, we can analyze the group structure on $C(\mathbb{F}_p)$ by recalling that rational points of order two have y-coordinate zero. For example, $C(\mathbb{F}_3)$ is a group of order four with only one point of order two, so it is the cyclic group of order four. $C(\mathbb{F}_{11})$ on the other hand contains fourteen elements. As it is a finite abelian group, by the Structure Theorem it is either isomorphic to $\mathbb{Z}/14\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. But note, since the lowest common multiple of seven and two is fourteen, there is an element of order fourteen in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. So these two groups are actually the same, and $C(\mathbb{F}_{11})$ is the cyclic group of order fourteen.

□

8.3 Introduction to Elliptic Curve Cryptography

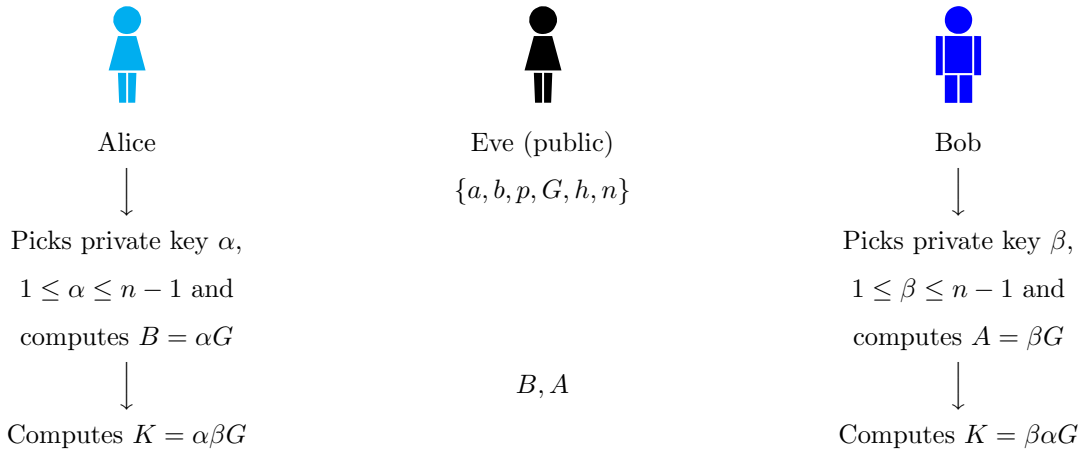
The *public key cryptosystem* is a method of encryption such that the two parties involved in the transfer of a message, classically referred to as Alice and Bob, can agree on a secret key, entirely publicly. The punchline is that anyone can encrypt a message with this public key, but only Alice and Bob can decrypt the message. So an encrypted message can be sent to each other publicly, without a hacker getting this information. This idea relies on on a mathematical function known as a *trapdoor function*: a relatively easy to use function with a nearly impossible to find (with our current technology) inverse.

It turns out that scalar multiplication of rational points on elliptic curves over $\mathbb{F}_p$, using the additive group law, is an excellent trapdoor function. That is, given a point G on an elliptic curve, it is relatively easy to compute nG for some natural number n, but it is extremely difficult to find n, given nG. So starting with an elliptic curve C over $\mathbb{F}_p$ and rational basepoint G of order n, we can use the formulas from 4 to compute the cyclic subgroup $\{kG : 1 \leq k \leq n\}$.

To begin the development of a secret key, some information is published publicly: $\{a, b, p, G, h, n\}$ where

$$a, b : \text{curve parameters}$$
$$p : \text{field mod } p$$
$$G : \text{generator point}$$
$$n : \text{order of } G$$

The following diagram outlines the subsequent steps.



By commutativity of $\mathbb{Z}/n\mathbb{Z}$, Alice and Bob share the same key K, which they can encode public messages with. In particular, Eve needs α or β to solve for K, or needs to solve the infamous *discrete logarithm problem*.

A more commonly used cryptosystem is the RSA (Rivest–Shamir–Adleman) cryptosystem. The trapdoor function is based on prime number factorization: multiplying two random large primes together is easy, but factoring this new number is hard.

ECC is advantageous for a couple reasons. Defining a *bit* as a unit of information storage, a 256 bit key in ECC is equivalent to a 3072 bit RSA key. It is also more efficient as bit size (security) is increased: a 384 bit ECC key is equivalent to a 7680 bit RSA key. So ECC requires less storage space for significantly higher security [3].

We note that as computers are improved and the possibility of quantum computers evolves, the discrete logarithm problem is at threat of being solved. Although far away, mathematicians are improving and developing secure cryptosystems for this new era.

Author Contributions

Anwyn Woodyatt wrote sections 1, 7, and 8 as well as exercises 2.1 and 3.1(a). Avram Silberztein wrote sections 2, 3, 4, 5, and 6 as well as exercise 3.1(b).

Acknowledgements

We would like to extend a warm thank you to Dr. Jonathan Love for his supervision on this project, enlightening meetings, and overall support as we take our first steps into research.

Appendix

A Rational Roots of Polynomials

For $P(x) = \sum_{n=0}^{N} a_n x^n$ for $a_n \in \mathbb{Q}$, $a_N = 1$, by the Fundamental Theorem of Algebra, for $r_1, ..., r_N \in \mathbb{C}$ we have:

$$P(x) = (x - r_1)(x - r_2)...(x - r_N)$$

So by expanding $P(x)$ out we get:

$$\begin{aligned}
a_N &= 1 \\
a_{N-1} &= -(r_1 + \cdots + r_n) \\
a_{N-2} &= r_1r_2 + r_1r_3 + \cdots + r_1r_n + r_2r_3 + \cdots + r_{n-1}r_n \\
a_{N-3} &= -\big(r_1r_2r_3 + r_1r_2r_4 + \cdots + r_1r_2r_n + r_1r_3r_4 + \cdots + r_{n-2}r_{n-1}r_n\big) \\
&\vdots \\
a_1 &= (-1)^{N-1}\big(r_1r_2\cdots r_{n-1} + r_1r_2\cdots r_{n-2}r_n + \cdots + r_2\cdots r_n\big) \\
a_0 &= (-1)^N\big(r_1\cdots r_n\big).
\end{aligned}$$

In general for $1 \leq n \leq N$,

$$a_n = (-1)^{N-n} \sum_{S \in \binom{\{1,2,\ldots,N\}}{N-n}} \prod_{k \in S} r_k.$$

Suppose we wish to solve for a root knowing that the other roots and the coefficients which are all rational. For $N = 2$,

$$a_0 = r_1 r_2 \text{ so if } a_0, r_0 \in \mathbb{Q} \Rightarrow r_2 = \frac{a_0}{r_1} \in \mathbb{Q}. \tag{17}$$

For $N = 3$,

$$\begin{aligned} a_0 &= -r_1 r_2 r_3 \\ a_1 &= r_1 r_2 + r_1 r_3 + r_2 r_3 \\ a_2 &= -(r_1 + r_2 + r_3). \end{aligned} \tag{18}$$

Suppose we know that the coefficients are rational and that r_1 is rational then:

$$\begin{aligned} r_2 r_3 &= \frac{-a_0}{r_1} \in \mathbb{Q} \\ r_2 + r_3 &= a_2 - r_1 \in \mathbb{Q}. \end{aligned} \tag{19}$$

For $b_1 \in \mathbb{Q}$, $r_2(b_1 - r_2) = r_2 b_1 - r_2^2 = b_2$. So r_2 is the root of a rational quadratic which doesn't restrict r_2 to be rational. So there is no requirement for r_2 and r_3 to be rational. So to guarantee that r_3 is rational we must have that r_1 and r_2 are already rational.

B Non-singular Curves

Definition 12. *A curve described by $F(x, y) = 0$ is non-singular if*

$$\forall (x_0, y_0), \quad \left(\left.\frac{\partial F}{\partial x}\right|_{(x_0,y_0)} = 0 \Longrightarrow \left.\frac{\partial F}{\partial y}\right|_{(x_0,y_0)} \neq 0 \right) \text{ and } \left(\left.\frac{\partial F}{\partial y}\right|_{(x_0,y_0)} = 0 \Longrightarrow \left.\frac{\partial F}{\partial x}\right|_{(x_0,y_0)} \neq 0 \right).$$

Proposition B.1. *Let $F(x, y) = f(x) - y^2 = 0$, where $f(x)$ is a polynomial, then*

$$F \text{ is non-singular} \iff f(x) \text{ and } f'(x) \text{ have no roots in common.}$$

Proof. Suppose F is non-singular at (x_0, y_0) then $\left.\frac{\partial F}{\partial x}\right|_{(x_0,y_0)} = f'(x_0) = 0$ and $\left.\frac{\partial F}{\partial y}\right|_{(x_0,y_0)} = -2y_0 = 0 \implies y_0 = 0$. But then $F(x_0, y_0) = F(x_0, 0) = f(x_0) = 0$ so $f(x_0) = f'(x_0) = 0$. Now suppose $\exists\, x_0$ such that $f(x_0) = f'(x_0) = 0$, so $\left.\frac{\partial F}{\partial x}\right|_{(x_0,0)} = f'(x_0) = 0$ and $\left.\frac{\partial F}{\partial y}\right|_{(x_0,0)} = 0$. So F is non singular at $(x_0, 0)$. □

C Discriminant code

```
ClearAll[a, b, c, s1, s0, s2, r0, r1]
F[x_] := x^3 + a*x^2 + b*x + c
R[x_] := r1*x + r0
S[x_] := s2*x^2 + s1*x + s0
Dis = -4 a^3*c + a^2 * b^2 + 18*a*b*c - 4*b^3 - 27*c^2;
sol = SolveAlways[{Dis == R[x]*F[x] + S[x]*F'[x] }, {x}];
val = sol[[4]]
s0 = FullSimplify[val[[1]][[2]] ];
s1 = FullSimplify[val[[2]][[2]] ];
s2 = FullSimplify[val[[3]][[2]]];
r0 = FullSimplify[val[[4]][[2]]];
r1 = FullSimplify[val[[5]][[2]]];
R2[x_] := r1*x + r0;
S2[x_] := s2*x^2 + s1*x + s0;
M := R2[x]*F[x] + S2[x]*F'[x]
FullSimplify[M]
```

References

[1] Lars Valerian Ahlfors and Lars V Ahlfors. *Complex analysis*, volume 3. McGraw-Hill New York, 1979.

[2] cmhughes. *How to draw the unit hyperbola in LaTex*. Stack Exchange, 6 February 2014. https://tex.stackexchange.com/questions/158968/how-to-draw-the-unit-hyperbola-in-latex.

[3] Robert Pierce. *Elliptic Curve Diffie-Helman*. YouTube, 10 December 2014. https://www.youtube.com/watch?v=F3zzNa42-tQ&t=852s.

[4] Joseph H. Silverman and John Torrence Tate. *Rational Points on Elliptic Curves*, volume 9. Springer, 1992.