# ON THE EXISTENCE OF TORSION POINTS OF ORDER 11 ON ELLIPTIC CURVES OVER Q

ROHAN RAMKUMAR

## 1. Abstract

The goal of this expository paper is to explore the Billing-Mahler Theorem about torsion points on elliptic curves. We present two perspectives, one involving linear algebra and rational transformations, and another where we explicitly construct modular curves, and explore the differences and similarities between these methods.

## 2. Introduction

### 2.1. **Elliptic Curves.**

We shall define an elliptic curve to be a curve of the form

$$E : y^2 = x^3 + ax^2 + bx + c,$$

for some $a, b, c \in \mathbb{Z}$.

With the transformation $(x, y) \mapsto \left(x - \frac{a}{3}, y\right)$, we can remove the quadratic term and rewrite our curve as $E : y^2 = x^3 + ax + b$. With a proper scaling, we can make $a$ and $b$ integers. We call this the Weierstrass form of $E$. Now, consider the graph of the curve $E \cup \mathbb{O}$, where $\mathbb{O}$ is the point at infinity. Choose two points $P = (p_1, p_2)$, and $Q = (q_1, q_2)$

*Date*: July 22, 2024.

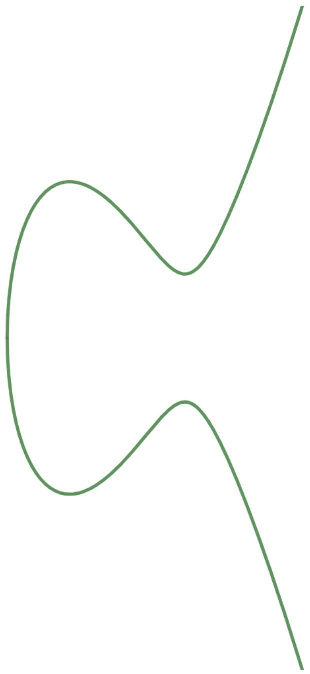

**Figure 1.** Graph of an elliptic curve $y^2 = x^3 + ax + b$.

with $p_1, p_2, q_1, q_2 \in \mathbb{Q}$ and $P, Q \in E$. Define the operation $*$ so that $R = (r_1, r_2) = P * Q$ is the intersection of $E$ and the line through $P$ and $Q$. If $P = Q$, then we will use the tangent line of $E$ at point $P$ instead. Letting the slope and $y$-intercept of this line be $\alpha$ and $\beta$ respectively, we have the following system:

$$r_2 = \alpha r_1 + \beta$$
$$r_2^2 = r_1^3 + ar_1 + b.$$

Substituting, we get

$$(\alpha r_1 + \beta)^2 = r_1^3 + ar_1 + b,$$

and

$$x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + b - \beta^2 = 0$$

after changing variables. Note that, by construction, $x = p_1$ and $x = q_1$ satisfy this equation, so $x = r_1$ must be the third root of the cubic, and

$$x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + b - \beta^2 = (x - p_1)(x - q_1)(x - r_1).$$

By Vieta, $p_1 + q_1 + r_1 = \alpha^2$, so we have $r_1 = \alpha^2 - p_1 - q_1$, and $r_2 = \alpha r_1 + \beta = \alpha^3 - \alpha p_1 - \alpha q_1 + \beta$. From this calculation, we see that $R \in \mathbb{Q}^2$, so we have found a way to generate new rational points on $E$ given two rational points on the curve. It turns out that this result holds more generally, by Bézout's Theorem, which states that the intersection of a curve of degree $m$ and a curve of degree $n$ (in the complex projective plane) are exactly $mn$ points, counting multiplicities. In this case we have a line (degree 1) intersecting our elliptic curve (degree 3), so there are 3 intersections, $P, Q$, and $P * Q$ We will now explain the basics of group theory.

### 2.2. **Group Theory.**

**Definition 2.1.** (Definition of a Group) A group $G = (X, \cdot)$ consists of a set $X$ and operation $\cdot$ such that the following is true:

(1) Associative Property: For all $a, b, c \in X$, we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c = a \cdot b \cdot c$.
(2) Identity: There exists some $e \in X$ such that $e \cdot a = a$ for all $a \in X$.
(3) Inverses: For all $a \in X$, there exists $a^{-1} \in X$ such that $aa^{-1} = e$.

*Example.* Consider the group $(\mathbb{Z}, +)$, which consists the set of integers $\mathbb{Z}$ with the operation addition, $+$.

(1) We have $a + (b + c) = (a + b) + c$, for integers $a, b, c$ so addition is associative.
(2) $0 + a = a$ for all integers $a$, so 0 is our identity element.
(3) $a + (-a) = 0$, the identity, so inverses are defined in $(\mathbb{Z}, +)$.

Note that addition is commutative, but commutativity is not a necessary condition for a group operation. We call commutative groups Abelian.

**Definition 2.2.** (Abelian Groups) A group $G = (X, \cdot)$ is Abelian if we have $a \cdot b = b \cdot a$ for $a, b \in G$.

*Nonexample.* The group of $n \times n$ matrices for some $n$ under the operation of matrix multiplication is not Abelian, since $A \cdot B$ is not necessarily equal to $B \cdot A$.

We call a group $S$ a subgroup of a group $G$ is $S \subset G$ and the operations of $S$ and $G$ are the same. Recall that a function $f : A \mapsto B$ is injective if no distinct $a_1, a_2 \in A$ have $f(a_1) = f(a_2)$ and surjective if for each $b \in B$ there exists $a \in A$ with $f(a) = b$. A bijective function is both injective and surjective.

**Definition 2.3.** (Homomorphism) A map $f : A \mapsto B$, for groups $G_1 = (A, \cdot)$, and $G_2(B, *)$ is a homomorphism if it satisfies

$$f(x \cdot y) = f(x) * f(y).$$

**Definition 2.4.** (Isomorphism) A homomorphism is an isomorphism if and only if it is bijective. We write $G \cong H$ if $G$ is isomorphic to $H$.

*Example.* Consider the function $f : \mathbb{R} \mapsto \mathbb{R}^+$ defined as $f(x) = e^x$. We can see that $f$ is a homomorphism betwen $(\mathbb{R}, +)$ and $(\mathbb{R}, \cdot)$ because

$$f(x + y) = e^{x+y} = e^x \cdot e^y.$$

Since $e^x$ is bijective, it is also an isomorphism.

*Example.* Consider the function $f : \mathbb{C} \mapsto \mathbb{R}$ defined as

$$f(a + bi) = a.$$

This is a homomorphism between the additive groups of $\mathbb{C}$ and $\mathbb{R}$ because

$$f(u + v) = f(a + bi + c + di) = a + c = f(u) + f(v)$$

for complex numbers $u = a + bi$ and $v = c + di$. However, this function isn't injective, since, for example, $f(3 + 4i) = f(3 + 2i) = 3$, so $f(x)$ is not an isomorphism. Although $f$ is surjective here, this is not true in general for homomorphisms (a surjective homomorphism is known as an epic morphism).

**Definition 2.5.** (Quotient Groups) Define $aN := \{an : n \in N\}$. Consider a subgroup $N$ of $G$. If $gN = Ng$ for $g \in G$, we call $N$ a normal subgroup of $G$. Then $N$ is normal, we can define the quotient group

$$G/N$$

to be the set $\{aN : a \in G\}$, and we define an operation on $G/N$ such that $(aN) \cdot (bN) = (a \cdot b)N$.

*Example.* Consider the additive group of $\mathbb{Z}$ and the subgroup

$$\{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\},$$

denoted $n\mathbb{Z}$, which is the set of $\mathbb{Z}$ that are multiples of $n$. Since addition is commutative, $n\mathbb{Z}$ is a normal subgroup. Then we have the quotient group $\mathbb{Z}/n\mathbb{Z}$ is the set of $a + n\mathbb{Z}$, where $a \in \mathbb{Z}$. With the isomorphism

$$f(a + n\mathbb{Z}) \mapsto a \pmod{n}$$

(one can verify that this is in fact an isomorphism), we see that the set $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to the integers modulo $n$.

**Theorem 2.6.** *(Fundamental Homomorphism Theorem) Let $f : G \mapsto H$ be a homomorphism. Then we have*

$$\mathfrak{I}(f) \cong G/\mathfrak{K}(f),$$

*where the image $\mathfrak{I}(f) \subset H$ is the set $\{f(g) : g \in G\}$ and the kernel $\mathfrak{K}(f) \subset G$ is the set $\{g : g \in G; f(g) = e\}$, where $e$ is the identity element.*

See [Pin10] for a proof and more details.

*Example.* Consider the homomorphism $f : \mathbb{Z}/100\mathbb{Z} \mapsto \mathbb{Z}/10\mathbb{Z}$ defined as

$$f(x) = x \pmod{10}.$$

This function can be thought of as extracting the units digit from a two-digit number. For example, $f(13) = 3$ and $f(\overline{ab}) = b$ for any two digit number $\overline{ab}$. We can see that $f(x + y) = f(x) + f(y)$, so $f(x)$ is a homomorphism. The kernel of this function is the set of $\overline{b0}$ for integer $b < 10$, and the image of $f$ is the set $\mathbb{Z}/10\mathbb{Z}$, as for any $n \in \mathbb{Z}/10\mathbb{Z}$, we can choose any $\overline{bn}$, as $f(\overline{bn}) = n$. The group $(\mathbb{Z}/100\mathbb{Z})/\mathfrak{K}(f)$ consists of the set $\{\tilde{0}, \tilde{1}, \dots, \tilde{9}\}$, where we define $\tilde{n} = \{\overline{0n}, \overline{1n}, \dots, \overline{9n}\}$ for each $0 \leq n \leq 9$. Clearly this group is isomorphic to $\mathfrak{I}(f) = \mathbb{Z}/10\mathbb{Z}$, as was expected by the first homomorphism theorem.

**Definition 2.7.** (Order) Given a group $G$, we define its order $|G|$ to be the number (possibly infinite) of elements in $G$. An order of an element is the smallest number $n$ (again possibly infinite) with $a^n = e$, the identity element.

**Definition 2.8.** (Index) The given a group $G$ and a subgroup $H$, we define the index to be the value $|G : H|$ (possibly infinite) such that

$$|G| = |G : H||H|.$$

*Example.* Consider the subgroup $2\mathbb{Z}$ of $\mathbb{Z}$. Since there are two elements in $\mathbb{Z}$ for every element of $2\mathbb{Z}$, we see that $|\mathbb{Z} : 2\mathbb{Z}| = 2$.

**Definition 2.9.** (Direct Sum of Two Groups) Given two groups $(G, \cdot)$ and $(H, *)$, we define the direct sum of $G$ and $H$ as

$$G \oplus H = \{(a, b) : a \in G, b \in H\},$$

under the operation $(a, b) + (c, d) = (a \cdot c, b * d)$. Sometimes the notation × is used instead of ⊕ depending on the operation of the groups. In this paper, we will use the two symbols interchangeably.

**Definition 2.10.** (Generators of a Group) For a group $G$, if for some set $S \subset G$, every element of $G$ can written as a product of finitely many elements in $S$ and their inverses, then we say that $S$ generates $G$, and we define $\langle S\rangle$ to be the smallest subgroup of $G$ containing $S$. If $G$ is generated by one element $S = \{x\}$, then we write $\langle S\rangle = \langle x\rangle$. We call a group finitely generated if $S$ is finite.

Finitely generated Abelian groups are very important in abstract algebra, due to the following theorem:

**Theorem 2.11.** *(Structure Theorem of Finitely Generated Abelian Groups) For any finitely generated Abelian group $A$,*

$$A \cong \mathbb{Z}^r \oplus \mathbb{Z}/p_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n\mathbb{Z} = \mathbb{Z}^r \oplus A_{tors},$$

*for prime $p_i$. We call $\mathbb{Z}^r$ the free part of $A$ and $A_{tors}$ the torsion part. $r$ is called the rank.*

**Definition 2.12.** (Ring) We call a set $R$ equipped with two operations $+$ and $\cdot$ a ring if the following are true

- $(R, +)$ is an abelian group,
- $(R, \cdot)$ is associative and has an identity element $e$ such that $a \cdot e = e \cdot a = a$ for all $a \in R$,
- The operation $\cdot$ distributes over $+$; i.e. $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$.

*Example.* Consider the set of integers $\mathbb{Z}$. We can see that $(\mathbb{Z}, +)$ creates an abelian group, and $(\mathbb{Z}, \cdot)$ is associative, has the identity 1, and distributes over addition, so $(\mathbb{Z}, +, \cdot)$ is a ring.

**Definition 2.13.** (Ideals of a Ring) For a ring $(R, +, \cdot)$, the subring $(I, +, \cdot)$ is called an ideal of $R$ if $rx, xr \in I$ for every $x \in I$ and $r \in R$. If $R$ is commutative (in $\cdot$), then the ideal $(a) = aR = \{ar : r \in R\}$ is called a principal ideal of $R$ generated by $a$.

*Example.* Consider the principal ideal $(3) = 3\mathbb{Z}$ of $\mathbb{Z}$. We can see that $(3)$ is an ideal because any $n \in \mathbb{Z}$ multiplied by some $m \in (3)$ will still be a multiple of 3, hence $nm \in (3)$.

**Definition 2.14.** A ring $(K, +, \cdot)$ is a field if $K$ is closed under inverses with respect to $\cdot$; or that $(K, \cdot)$ is a group.

*Example.* The ring $\mathbb{Z}$ is not a field because $\frac{1}{n}$ is not necessarily in $\mathbb{Z}$ for $n \in \mathbb{Z}$. However, $\mathbb{Q}$ is a field, as we can verify that

$$\frac{1}{\frac{p}{q}} = \frac{q}{p} \in \mathbb{Q}$$

for $\frac{p}{q} \in \mathbb{Q}$.

The set of $E(\mathbb{Q})$ under the operation $*$ has no identity element, so it does not form a group. However, we can modify this operation slightly so that creates a group.

**Definition 2.15.** (Elliptic Curve Point Addition) Define the Abelian operation $P + Q$, for rational points $P$ and $Q$ to be the reflection of $P * Q$ over the $x$-axis.

Now, note that $\mathbb{O} + P = P$ for all rational $P$, so $\mathbb{O}$ is the identity element of the group $E(\mathbb{Q})$. This also lets us define the additive inverse of $P$ as the point $-P$ such that $P + (-P) = \mathbb{O}$. We see the the negative of a point is a reflection of that point about the $x$-axis. The point addition operation is commutative, as the order of points does not change the line between them, and the operation is also associative (see [FO17] for a proof), meaning that the set of rational points, $E(\mathbb{Q})$ with an operation of point addition is an Abelian group.

### 2.3. **Projective Space.**

We will make heavy use of projective space, so we will need some definitions.

**Definition 2.16.** (Projective Space Over a Field) We define the set $\mathbb{P}^n(K)$, for some field $K$ to be the set $V \backslash \{0\}$ under the equivalence relation $x \sim y$ if $x = \lambda y$ for some $\lambda \neq 0$, where $V = K^{n+1}$.

*Example.* Consider the projective plane $\mathbb{P}^2(K)$ over a field $K$. By our definition, this is the set $K^3 \backslash \{0\}$ under the equivalence relation of scaling. We use homogeneous coordinates $(x, y, z) \in K^3 \backslash \{0\}$ to represent a point in $\mathbb{P}^2(K)$, where the point $(x, y, z)$ represents the same point as $(\lambda x, \lambda y, \lambda z)$ for $\lambda \neq 0$.

**Definition 2.17.** (Homogeneous Polynomial) A multivariate polynomial is called homogeneous if each term has the same degree.

*Example.* $x^3 + xz^2 + xyz$ is a homogeneous polynomial in three variables because each term has degree three.

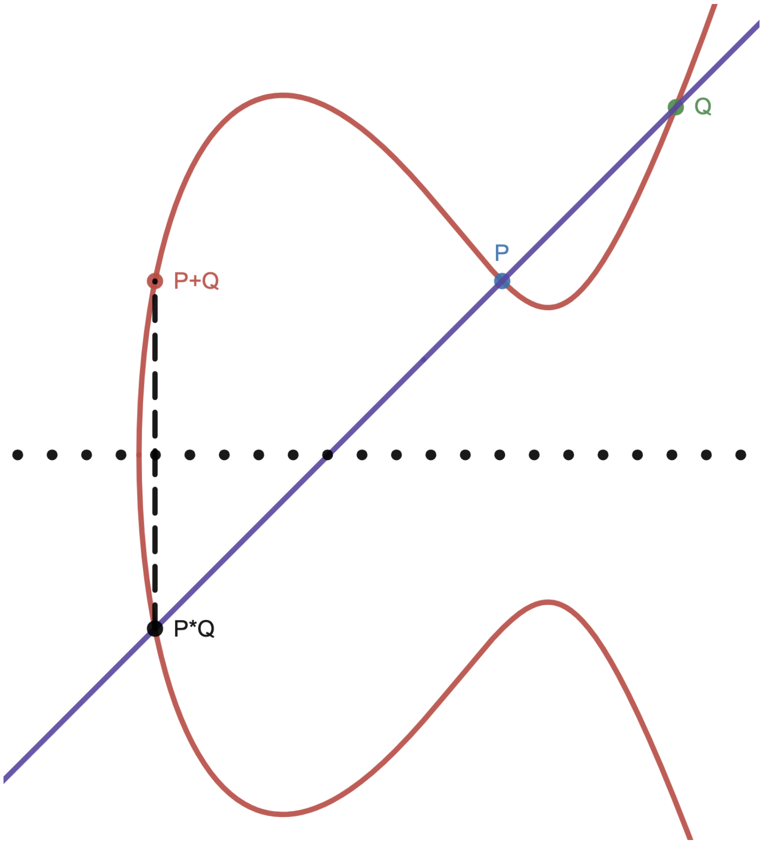

**Figure 2.** Point addition on an elliptic curve. We define $P+Q$ to be the reflection of $P*Q$ over the $x$-axis.

**Definition 2.18.** (Projective Algebraic Plane Curve) A projective algebraic plane curve, henceforth referred to as an algebraic curve, is the set of points in some projective space that satisfy $h(x, y, z) = 0$, for some homogeneous polynomial $h$ in three variables. The degree of this algebraic curve is the degree of $h$.

*Example.* Consider an elliptic curve $y^2 = x^3 + ax + b$. Letting $y = \frac{Y}{Z}$ and $x = \frac{X}{Z}$ and multiplying both sides by $Z^3$, we get $Y^2Z = X^3 + aXZ^2 + bZ^3$. Rearranging, we see that $Y^2Z - X^3 - aXY^2 - bZ^3 = 0$, so this is an algebraic curve of degree 3, called a cubic curve. Any polynomial in 2 variables can be transformed into an algebraic curve like this.

We dehomogenize a curve or a point with the substitution $(x, y, z) \mapsto (x/z, y/z, 1)$. By discarding the $z$-coordinate, we can consider it now in $2d$ space. Although this process works for most points, this transformation fails if $z = 0$. In this case, we map this point to $\mathbb{O}$, the point at infinity.

2.4. **Torsion Points.** A natural thing to analyze is the group is the order of its elements. We call a point with finite order a torsion point. We will state some major results about torsion points.

**Theorem 2.19.** *(Mordell-Weil) The additive group of rational points on an abelian variety (e.g. an elliptic curve) is finitely generated.*

So, we can write $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$. This theorem was first proved for elliptic curves by Louis Mordell in [Mor22], and was later generalized to abelian varieties by André Weil in [Wei29].

**Theorem 2.20.** *(Nagell-Lutz) All rational torsion points $P = (x, y)$ on elliptic curves satisfy the following:*

1. *$x$ and $y$ are integers.*
2. *$y = 0$ or $y^2 \mid \Delta$, where $\Delta$ is the discriminant of the cubic function of $x$ on the right-hand side of the equation for $E$.*

Similar to the discriminant of a quadratic equation, $b^2 - 4ac$, we can define an expression in terms of the coefficients of the cubic $x^3 + ax + b$. Since this cubic is in depressed form, the discriminant is $-4a^3 - 27b^2$. This theorem was proven independently by Élisabeth Lutz in [Lut37] and Trygve Nagell.

**Theorem 2.21.** *(Mazur) The torsion groups of all elliptic curves over $\mathbb{Q}$ must be isomorphic to one of the following:*

1. *$\mathbb{Z}/n\mathbb{Z}$ for $1 \geq n \geq 10$ or $n = 12$.*
2. *$\mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ for $1 \geq n \geq 4$.*

*Furthermore, there exist infinitely many elliptic curves that have each of these 15 possible torsion subgroups.*

This was proven by Barry Mazur in [Maz77] and [MG78].

We will be analyzing a specific case of Mazur's theorem, by showing that $n = 11$ is impossible.

**Theorem 2.22.** *(Billing-Mahler) There exists no elliptic curve with any rational point of order 11.*

This was first proved by Gunnar Billing and Kurt Mahler in [BM40].

In this paper, we will derive a cubic curve C which must have more than 5 rational points if there exists such an 11-torsion point, and we will turn that curve into an elliptic curve $E$, which we will prove has exactly 5 rational points using some algebraic number theory. The rest of the paper will look through at this problem through the lens of modular curves.

## 3. Implications of 11

We will assume the contrary, that there exists some rational point $P$ of order 11 on some elliptic curve $E : y^2 = x^3 + ax + b$. For convenience will will use the notation

$$P_i := iP.$$

Also, let

$$L_{P,Q}$$

denote the line connecting $P$ and $Q$ and let $L_{i,j} = L_{P_i,P_j}$.

**Lemma 3.1.** *The points $P_i, P_j$, and $P_k$ lie on a line if and only if $i + j + k \equiv 0 \pmod{11}$.*

*Proof.* We see that, by our definition of point addition, the $P_i + P_j$ must be the additive inverse of $P_k$, so we have $P_i + P_j = -P_k = P_{-k}$. So, $i + j \equiv -k \pmod{11}$ and $i + j + k \equiv 0 \pmod{11}$ as desired. ■

**Lemma 3.2.** *Let $K$ be a field and $(a_1, b_1, c_1), (a_2, b_2, c_2) \in \mathbb{P}^2(K)$ be distinct points. Then the equation of*

$$L_{(a_1,b_1,c_1),(a_2,b_2,c_2)}$$

*is*

$$\begin{vmatrix} x & y & z \\ a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{vmatrix} = 0.$$

*Proof.* Expanding out the determinant, we see that

$$(b_1c_2 - c_1b_2)x - (a_1c_2 - c_1a_2)y + (a_1b_2 - b_1a_2)z = 0.$$

Dehomogenizing by setting all $z$-coordinates to 1, we get

$$(b_1 - b_2)x - (a_1 - a_2)y = b_1a_2 - a_1b_2,$$

which is a line passing through our two desired points. ■

Consider the points $\overline{P}_0 = \mathcal{O} = (0, 1, 0), \overline{P}_1 = (a_1, b_1, c_1),$ and $\overline{P}_2 = (a_2, b_2, c_2)$. By Lemma 3.1 these points are not collinear, so $\overline{P}_1, \overline{P}_2$, and $\overline{P}_3$ as vectors are linearly independent. So, we can define a linear change of basis transformation $\phi$ such that

$$\phi(\overline{P}_0) = (0, 1, 0), \phi(\overline{P}_1) = (1, 0, 0), \text{ and } \phi(\overline{P}_2) = (0, 0, 1).$$

Let $P'_n = \phi(\overline{P}_n)$. This linear map $\phi$ is an affine transformation of $\mathbb{P}^2(\mathbb{Q})$ that preserves lines, so $P'_0, P'_1$, and $P'_2$ are not collinear. So, $P'_3 = (u, v, w)$ does not lie on $L_{P'_0,P'_1}$, which has an equation $z = 0$. Hence, $w \neq 0$. Similarly, $u, v \neq 0$ because $P'_3 \notin \{L_{P'_0,P'_2}, L_{P'_1,P'_2}\}$. Thus, define the transformation $\psi : \mathbb{P}^2(\mathbb{Q}) \mapsto \mathbb{P}^2(\mathbb{Q})$ as

$$\psi(x, y, z) = \left(\frac{x}{u}, \frac{y}{v}, \frac{z}{w}\right).$$

Now let $P_n = \psi(P'_n)$. Since homogenous coordinates are unaffected by scaling, we see that $P'_0, P'_1$, and $P'_2$ are fixed. Now, we have

$$P_0 = (0, 1, 0), P_1 = (1, 0, 0), P_2 = (0, 0, 1), \text{ and } P_3 = (1, 1, 1).$$

Let $P_4 = (x_1, x_2, x_3)$. By Lemma 3.2, we have

$$L_{0,1} : z = 0,$$
$$L_{0,2} : x = 0,$$
$$L_{0,3} : x - z = 0,$$
$$L_{1,2} : y = 0,$$
$$L_{1,4} : x_3y - x_2z = 0,$$
$$L_{2,3} : x - y = 0.$$

We have that $P_{-3}$ is the intersection of $L_{0,3}$ and $L_{1,2}$, which is the point

$$P_{-3} = (1, 0, 1).$$

Similarly, we can calculate

$$P_{-1} = (x_1 - x_3, x_2, 0), P_{-2} = (0, x_1 - x_2 - x_3, x_1 - x_3).$$

We see that

$$L_{-2,-3} : (x_1 - x_2 - x_3)x + (x_1 - x_3)y - (x_1 - x_2 - x_3)z = 0.$$

$$P_{-5} = L_{1,4} \cap L_{2,3} = (x_2, x_2, x_3),$$

and

$$P_5 = L_{0,-5} \cap L_{-2,-3} = ((x_1 - x_3)x_2, -x_1x_2 + x_1x_3 + x_2^2 - x_3^2, (x_1 - x_3)x_3).$$

$2 + 4 + 5 \equiv 0 \pmod{11}$, so $P_2, P_4, P_5$ are collinear and

$$\begin{vmatrix} 0 & 0 & 1 \\ x_1 & x_2 & x_3 \\ (x_1 - x_3)x_2 & -x_1x_2 + x_1x_3 + x_2^2 - x_3^2 & (x_1 - x_3)x_3 \end{vmatrix} = 0.$$

Calculating this determinant, we see that

$$x_1^2x_2 - x_1^2x_3 + x_1x_3^2 - x_2^2x_3 = 0.$$

Consider the curve $C : u^2v - u^2w + uw^2 - v^2w = 0$. This curve has the following points:

$$P_0 = (0, 1, 0), P_1 = (1, 0, 0), P_2 = (0, 0, 1), P_3 = (1, 1, 1), P_{-3} = (1, 0, 1).$$

However, the existence of a point of order 11 implies that some other rational $P_4 = (x_1, x_2, x_3)$ satisfies it as well, so this equation must have more than 5 rational points. We shall show that this is impossible.

## 4. The Cubic Curve C

**Proposition 4.1.** *The cubic curve $C : u^2v - u^2w + uw^2 - v^2w = 0$ has only 5 rational points: (0,1,0),(1,0,0),(0,0,1),(1,1,1), and (1,0,1).*

**Lemma 4.2.** *The cubic curve $C$ is equivalent to the curve $y^2 + y = x^3 - x^2$.*

*Proof.* We will use an algorithm outlined in [ST92] to do this. We will use the curve

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

Note that the tangent line at any point $P_0$ is given by the equation

$$\left.\frac{\partial F}{\partial X}\right|_{P_0} X + \left.\frac{\partial F}{\partial Y}\right|_{P_0} Y + \left.\frac{\partial F}{\partial Z}\right|_{P_0} Z = 0. \tag{4.1}$$

The tangent line at $\mathcal{O}$ is given by $Y - Z = 0$. By making the substitution

$$X_1 = X, Y_1 = Y, Z_1 = Y - Z,$$

we have set the line $Z_1 = 0$ to the tangent at point $\mathcal{O} = (1, 0, 0)$ (note that the coordinates of $\mathcal{O}$ have not changed under this transformation). Our new curve is

$$X_1Y_1^2 - Y_1^3 + X_1^2Z_1 - 2X_1Y_1Z_1 + Y_1^2Z_1 + X_1Z_1^2 = 0.$$

Now, we substitute $Z_1 = 0$ into this equation to find the intersection of our tangent line at $\mathcal{O}$ to the curve, as we get $X_1Y_1^2 - Y_1^3 = Y_1^2(X_1 - Y_1) = 0$, so $X_1 = Y_1 \neq 0$, since the point $(x, 0, 0) = (1, 0, 0) = \mathcal{O}$. From this, we can see that the point $\mathcal{O} * \mathcal{O} = (1, 1, 0)$. We want to move this point to the point $(0, 1, 0)$, which we can do with the transformation

$$X_2 = X_1 - Y_1, Y_2 = Y_1, Z_2 = Z_1,$$

to get the new cubic equation:

$$X_2Y_2^2 + X_2^2Z_2 + X_2Z_2^2 + Y_2Z_2^2 = 0.$$

We try to apply the same process again, but we now try to move the line $X = 0$ to the tangent at the point $\mathcal{O} * \mathcal{O} = (0, 1, 0)$, but we find from 4.1 that this tangent line is already

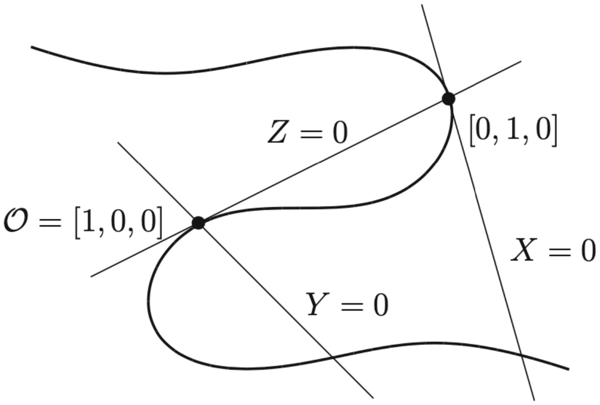

**Figure 3.** Changing the axes of C to convert it into a Weierstrass form.

be $X_2 = 0$, so we have no work to do. Now, we dehomogenize our equation, by letting $x = \frac{X_2}{Z_2}$ and $y = \frac{Y_2}{Z_2}$. Since our curve has degree 3, we divide it by $Z_2^3$ to get

$$\frac{X_2Y_2^2}{Z_2^3} + \frac{X_2^2}{Z_2^2} + \frac{X_2}{Z_2} + \frac{Y_2}{Z_2} = 0.$$

Substituting $x$ and $y$, we see that

$$xy^2 + x^2 + x + y = 0.$$

Multiplying by $x$ and making the substitution $x_1 = x, y_1 = xy$ we get $y_1^2 + y_1 = -x_1^3 - x_1^2$. Substituting $x_2 = -x_1, y_2 = y_1$, we arrive at $y_2^2 + y_2 = x_2^3 - x_2^2$ as desired. ■

The five rational points mentioned in Proposition 4.1 become the points

$$\{\mathbb{O}, (0, -1), (0, 0), (1, -1), (1, 0)\}.$$

With the translation $(x, y) \mapsto (x, y - \frac{1}{2})$, we can complete the square on the left-hand side to arrive at $y^2 = x^3 + x^2 - \frac{1}{4}$. Finally, we scale variables with the transformation $(x, y) \mapsto (\frac{x}{2^2}, \frac{y}{2^3})$ to get

$$y^2 = x^3 - 4x^2 + 16. \tag{4.2}$$

For the rest of this section, we will call this curve $E$. Note that we could depress this cubic with a simple affine transformation by using Tartaglia's method to arrive at a more familiar yet more unwieldy form as $y^2 = x^3 - 432x + 8208$.

We are left to show that Equation 4.2 has exactly 5 rational points. By Mordell-Weil, we know that $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$. We wish to show that $E(Q) \cong \mathbb{Z}/5\mathbb{Z}$, so we must prove that both $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/5\mathbb{Z}$ and $r = 0$.

**Proposition 4.3.** *The torsion group of $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.*

*Proof.* We will be using Nagell-Lutz. Recall that the square of the $y$-coordinate must divide the discriminant of the cubic function of $x$, which happens to be $\Delta = -2816 = -2^8 \cdot 11$. Clearly $11 \nmid y$, because otherwise $11^2 \mid y$, implying that $11^2 \mid \Delta$, which is false. So, we have that $y^2 \mid 2^8$ and thus $|y| \mid 2^4$. By checking all of these values of $|y|$, namely $1, 2, 4, 8$, and $16$, we can find that $|y| = 4$ is the only value for which there exists integer $x$ that solves Equation 4.2.

Thus, we end up with a group with exactly five torsion points: $\mathbb{O}, (0,4), (0,-4), (4,4), (4,-4)$, isomorphic to $\mathbb{Z}/5\mathbb{Z}$, as desired. ■

Now we need to prove that the rank of $E$ is 0, which turns out to be the hardest part of this proof.

### 4.1. **Field Theory.**

**Definition 4.4.** (Ring of Polynomials) For a commutative ring $R$, we define $R[x]$ to be the ring of polynomials:

$$p(x) = p_0 + p_1 x + \cdots + p_n x^n$$

for all nonnegative integer $n$.

*Example.* We can define substitution of a number into some ring of polynomials. For example, consider the substitution of $\sqrt{2}$ into $\mathbb{Z}[x]$, denoted $\mathbb{Z}[\sqrt{2}]$, which is

$$p_0 + p_1(\sqrt{2}) + p_2(\sqrt{2})^2 \ldots$$

But, since $(\sqrt{2})^2 = 2$, all the terms of degree 2 and higher can be collapsed into terms of lower degree, so we have

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

**Definition 4.5.** (Field Extension) Given a field $K$, we call $L$ an extension field over $K$ (denoted $L/K$) if $K$ is a subfield of $L$.

**Definition 4.6.** (Vector Space and Degree of a Field Extension) Given a field extension $L/K, L$ is a vector space over $K$; i.e. each element of $L$ can be represented as $k_1 b_1 + k_2 b_2 + \cdots + k_n b_n$ for each $k_i \in K$. The set $B = \{b_i\}$ is called the basis of this vector space, and the degree of $L/K$ is equal to the dimension of this vector space, or the number of elements in $B$.

We will be mostly concerned with extensions over $\mathbb{Q}$, the rationals. Choose a monic irreducible polynomial in $\mathbb{Z}[x]$ of degree $n$ and choose a root $\alpha$.

**Definition 4.7.** (Minimum Polynomial) The minimum polynomial of an algebraic number $\alpha$ is the lowest degree function $f(x)$ with leading coefficient 1 such that $f(\alpha) = 0$. Since $\alpha$ is algebraic, the coefficients of $f(x)$ must be integers, so $f(x) \in \mathbb{Z}[x]$.

*Example.* Consider the algebraic number $\rho = \frac{1}{2} + \frac{i\sqrt{3}}{2}$. Clearly $\rho$ satisfies the polynomial $f(x) = x^2 + x + 1 = 0$. Since this function is irreducible over $\mathbb{Z}$, it must be the lowest possible degree polynomial, and since the leading coefficient of $f(x)$ is 1, $f(x)$ is the minimum polynomial of $\rho$.

We define the field extension $\mathbb{Q}(\alpha)$ as follows:

**Definition 4.8.** (Finite Field Extensions over $\mathbb{Q}$) A field extension $K = \mathbb{Q}(\alpha)$ is the vector space spanned by $\{1, \alpha, \alpha^2, \ldots \alpha^{n-1}\}$ where $n$ is the degree of the minimum polynomial of $\alpha$ in $\mathbb{Z}[x]$. We refer to $n$ as the degree of the field extension of $L/K$, denoted $[L : K]$.

*Example.* Consider the field $K = \mathbb{Q}(\sqrt{2})$. It is easy to see that the minimum polynomial of $\sqrt{2}$ is $f(x) = x^2 - 2$. So, we have that $K/\mathbb{Q}$ is spanned by the basis $\{1, \sqrt{2}\}$; in other words, each element of $K$ can be written as $a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$. It can easily be verified that this is indeed a field.

**Definition 4.9.** (Ring of Integers of a Field) We define $\mathcal{O}_K$ as the set of elements of $K$ that are roots of some monic polynomial over $\mathbb{Z}$. This is called the ring of integers of $K$.

**Theorem 4.10.** *(Unique Factorization of Ideals of Ring of Integers) Every ideal $\mathfrak{a} = a\mathcal{O}_K$ has a unique prime decomposition:*

$$\mathfrak{a} = \prod_i \mathfrak{p_i}^{a_i}.$$

**Definition 4.11.** (Norm of an Algebraic Number and Principal Ideals of Ring of Integers) The norm of an algebraic number $\alpha$ with respect to a field extension is defined as:

$$N_{L/K} = \left( \prod_j \sigma_j(\alpha) \right)^{[L:K(\alpha)]},$$

where each $\sigma_j$ is a root of the minimum polynomial of $\alpha$. For $L = K(\alpha)$, the norm is exactly the product of the roots of the minimum polynomial. Since this product is equal to $\pm 1$ times the constant term of the minimum polynomial, by Vieta, the norm of an algebraic number is always an integer.

The norm of the principal ideal $(\alpha) = \alpha\mathcal{O}_K$ is defined as $N_{L/K}((\alpha)) = |N_{L/K}(\alpha)|$. Additionally, we have that $N_{K/Q}(a) = a^{[K:Q]}$ for $a \in \mathbb{Q}$ and

$$N_{K/Q}(\alpha, \beta) = N_{K/Q}(\alpha) \cdot N_{K/Q}(\beta)$$

for $\alpha, \beta \in K$.

The ideal generated by a prime number in $\mathbb{Z}$ may not necessarily be prime in $K$. We call a prime $p$ ramified in $L$ if we have

$$p\mathcal{O}_k = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_s^{e_s},$$

and some $e_i > 1$.

**Theorem 4.12.** *A prime $p$ is ramified in $K$ if and only if $p \mid D_K$, where $D_K$ is the discriminant of $K$.*

**Theorem 4.13.** *(Sum of Two Prinicpal Ideals is GCD) Given two principal ideals of some ring of integers $\mathcal{O}_K$, $(a) = a\mathcal{O}_K$ and $(b) = b\mathcal{O}_K$, then the ideal $(a) + (b) = (\gcd(a, b))$.*

*Proof.* We have that $(a) + (b)$ consists of the set of $x \in \mathcal{O}_K$ such that $x = ma + nb$ for $m, n \in \mathbb{Z}$. But, by Bézout's identity, this is the set of $x = l \gcd(a, b)$ for $l \in \mathbb{Z}$. Hence, $(a) + (b) = (\gcd(a, b))$. ■

### 4.2. Rank of E.

**Proposition 4.14.** *E has a rank of 0.*

Our polynomial is $f(x) = x^3 - 4x^2 + 16$. As mentioned earlier, $\text{Disc}(f) = \Delta = -2^8 \cdot 11 < 0$, so $f(x)$ has three roots, $\theta_1, \theta_2, \theta_3$, only one of which is real. Choose one arbitrarily to be called $\theta$. Consider the number field $K = Q(\theta)$. With the use of a CAS, we find that the discriminant of $K$ is $-44$. We also find that the ring of integers of $K$ is $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \cdot \frac{1}{2}\theta + \mathbb{Z} \cdot \frac{1}{4}\theta^2 = \mathbb{Z}\left[\frac{\theta}{2}\right]$. We see that the class number is $h_K = 1$, meaning that all ideals of $\mathcal{O}_K$ are principal.

**Theorem 4.15.** *(Dirichlet Unit Theorem) Let $K$ be a finite field extension of $\mathbb{Q}$ with $r_1$ real embeddings and $2r_2$ complex embeddings ($r_2$ pairs of complex embeddings). Then the the abelian unit group of $\mathcal{O}_K$, denoted $\mathcal{O}_K^\times$, is finitely generated and has rank $r = r_1 + r_2 - 1$.*

For our cubic field $K$, we have $r_1 = 1$ and $r_2 = 1$, since there are one real and two complex roots, so the rank of $\mathcal{O}_K^\times$ is 1, which means there is only one fundamental unit group (not $\pm 1$). We can calculate that $\mathcal{O}_K^\times = \langle -1 \rangle \oplus \langle \eta \rangle = (-1)^{e_0} \cdot (\eta)^{e_1}$, where $\eta = 1 - \frac{1}{2}\theta$ and $e_0, e_1 \in \mathbb{Z}$.

**Proposition 4.16.** *Let $K^\times$ be the multiplicative group of $K$, and let $(K^\times)^2$ be the subgroup of $K^\times$ containing the elements $a^2$ for every $a \in K$. Then the map $\mu : E(\mathbb{Q}) \mapsto K^\times/(K^\times)^2$ defined by*

$$\mu(\mathbb{O}) := 1, \mu(x, y) := x - \theta \mod (K^\times)^2$$

*is a homomorphism with kernel $2E(\mathbb{Q})$.*

*Proof.* Note that $\mu(P) = \mu(-P)$ because $P$ and $-P$ have the same $x$-coordinate. Since any element $\nu \in (K^\times)/(K^\times)^2$ satisfies $\nu^2 = 1$ and thus $\nu = \frac{1}{\nu}$, so we have $\mu(-P) = \mu(P) = \frac{1}{\mu(P)} = \mu(P)^{-1}$. Next, we have to show that $P_1 + P_2 + P_3 = \mathbb{O} \implies \mu(P_1)\mu(P_2)\mu(P_3) = 1$. If any of the $P_i = \mathbb{O}$, then the other two must be negatives of each other, so $\mu(P_1)\mu(P_2)\mu(P_3) = 1$. So, assume that none of the $P_i = (x_i, y_i)$ are $\mathbb{O}$. Since the $P_i$ sum to $\mathbb{O}$, they are the intersection of some line $y = \lambda x + \nu$ and $E$. Thus, we must have

$$f(x) - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3),$$

where $f(x) = x^3 - 4x^2 + 16$. Substituting $x = \theta$, we see that

$$(x_1 - \theta)(x_2 - \theta)(x_3 - \theta) = (\lambda\theta + \nu)^2 + f(\theta) = (\lambda\theta + \nu)^2 \equiv 1 \mod (K^\times)^2,$$

since $f(\theta) = 0$. But the left-hand side is precisely $\mu(P_1)\mu(P_2)\mu(P_3)$, so we are done. Now, we must show that the kernel of this homomorphism is $2E(\mathbb{Q})$, or the set of all points on $E(\mathbb{Q})$ that are multiples of 2. Any point $P_k \in \mathfrak{K}(\mu)$ can be written as $2P_n$ for some $P_n \in E(\mathbb{Q})$, so $\mu(P_k) = \mu(2P_n) = \mu(P_n)^2 \equiv 1 \mod (K^\times)^2$, so we see that $2E(\mathbb{Q}) \subset \mathfrak{K}(\mu)$. Let $P_0 = (x_0, y_0) \in \mathfrak{K}(\mu)$. Then, $x_0 - \theta$ must be a square of some element in $K$, and, treating $K$ as a vector space of dimension three, we must have

$$x_0 - \theta = (u\theta^2 + v\theta + w)^2.$$

Since the degree of the minimum polynomial of $\theta$ is 3, we cannot have $u = 0$, as otherwise there would exist a quadratic polynomial with root $\theta$. Now define the following:

$$r = \frac{4u + v}{u}, s = \frac{4uv + v^2}{u} - w, t = \frac{4uw + vw}{u} + 16u.$$

Noting that $-\theta^3 = -4\theta^2 + 16$, we see that

$$(r - \theta)(u\theta^2 + v\theta + w) = s\theta + t,$$

so

$$(s\theta + t)^2 = (r - \theta)^2(u\theta^2 + v\theta + w)^2 = (r - \theta)^2(x_0 - \theta).$$

Note that the function $g(x) = (sx + t)^2 - (r - x)^2(x_0 - x)$ is a monic cubic polynomial with roots $\theta_1, \theta_2, \theta_3$, so it must be equal to $f(x) = x^3 - 4x^2 + 16$. The intersections of the elliptic curve and the line $y = sx + t$ are the roots to the equation

$$f(x) - (sx + t)^2 = -(r - x)^2(x_0 - x).$$

We see that the point $\pm P = (x_0, \pm y_0)$ must be an intersection point, and since the point with $x$-coordinate $r$ is a double root of this function, the line $y = sx + t$ must be tangent to $E$ at the some point $R = (r, y_1)$. But this means that $2R = \mp P$, so $P$ is a multiple of 2, and thus $\mathfrak{K}(\mu) = 2E(\mathbb{Q})$. ■

Recall that by Mordell-Weil,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}^r.$$

By the first homomorphism theorem,

$$\mathfrak{I}(\mu) \cong E(\mathbb{Q})/\mathfrak{K}(\mu) \cong E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}^r)/(2\mathbb{Z}/5\mathbb{Z} \times 2\mathbb{Z}^r) \cong (\mathbb{Z}/2\mathbb{Z})^r,$$

where $\mathfrak{I}$ and $\mathfrak{K}$ are image and kernel respectively, since $\mathbb{Z}/5\mathbb{Z}$ is a finite field, so $2\mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z}$. Since we want to show that $r = 0$, we need to show that $\mathfrak{I}(\mu)$ has a trivial image. Assume the contrary, that there exists some $P = (x, y)$ such that $\mu(P) \neq 1$. In other words, $x - \theta$ is not a perfect square in $K$.

**Proposition 4.17.** *For any rational $x$ and $y$ such that $(x, y) \in E(\mathbb{Q})$, $x$ can be written in the form*

$$x = \frac{n}{t^2},$$

*for $n, t \in \mathbb{Z}$ and $t \neq 0$ such that* $\gcd(n, t) = 1$.

*Proof.* Let $x = \frac{a_1}{b_1}$ and $y = \frac{a_2}{b_2}$ in simplest terms. Consider the transformation of $E(\mathbb{Q})$ defined: $(p, q) \mapsto (p \cdot b_1, q \cdot b_1^{3/2})$. This maps $E$ to a different curve, call it $E_1 : y^2 = x^3 + \alpha x^2 + \beta x + \gamma$. The point $(x, y) = (\frac{a_1}{b_1}, \frac{a_2}{b_2})$ is sent to $\left(a_1, \frac{a_2\sqrt{b_1^3}}{b_2}\right)$. This new point must lie on $E_1$, so we have

$$\frac{a_2^2 b_1^3}{b_2^2} = a_1^3 + \alpha a_1^2 + \beta a_1 + \gamma.$$

The RHS must be integral, since we have just scaled each coefficient by some power of $b_1$, so the LHS must also be an integer, and we must have $b_2^2 \mid a_2^2 b_1^3$. Since $\frac{a_2}{b_2}$ is in simplest form, we must have $b_2^2 \mid b_1^3$, so $b_1$ must be a perfect square, and thus $x = \frac{a_1}{b_1}$ can be written as $\frac{n}{t^2}$ with $n = a_1$ and $t^2 = b_1$. ■

Thus,

$$\mu(P) = \mu(x, y) = x - \theta \mod (K^\times)^2 = n - t^2\theta \mod (K^\times)^2.$$

**Proposition 4.18.** *Consider the integral ideal $(n - t^2\theta)$.*

$$(n - t^2\theta) = \left(\prod_i \mathfrak{p}_i^{e_i}\right)\mathfrak{A}^2,$$

*where $\mathfrak{A}$ is an integral ideal, each $e_i \in \{0, 1\}$, and each $\mathfrak{p}_i$ divides the discriminant*

$$\Delta(f) = \prod_{j \neq k}(\theta_j - \theta_k)^2 = -2^8 \cdot 11.$$

*Proof.* For this proof, we will work in the field $L = \mathbb{Q}(\theta_1, \theta_2, \theta_3)$. Consider each root $\theta_j$. Factoring out the even powers of ideals in the factorization of $(n - t^2\theta_j)$, we have

$$\left(\prod_i \mathfrak{p}_i^{e_{ij}}\right)\mathfrak{A}_j^2$$

for some ideal $\mathfrak{A}_j$, prime ideals $\mathfrak{p}_i$ and $e_{ij} \in \{0, 1\}$. If $\mathfrak{p}_i \mid \mathfrak{A}$, then $\mathfrak{p}_i$ ramifies, so it must divide the discriminant. Thus, we only need to consider unramified prime ideals which do not appear in $\mathfrak{A}$. We must have $e_{ij} = 1$ for some $j$, otherwise the corresponding $\mathfrak{p}_i$ term would not appear in any of the factorizations. Since $y^2 = (x-\theta_1)(x-\theta_2)(x-\theta_3)$, we have $y^2t^6 = (n-\theta_1t^2)(n-\theta_2t^2)(n-\theta_3t^2)$. Let $m = yt^3$. Since the product of the ideals $(n-\theta_1t^2)(n-\theta_2t^2)(n-\theta_3t^2)$ is a perfect square, then the sum of the exponents for each $i$ over $j$ must be even, or

$$e_{i1} + e_{i2} + e_{i3} \equiv 0 \pmod 2.$$

Fix some $i$. Then, we must have some $j, k \in \{1,2,3\}, j \neq k$ with $e_{ij} = e_{ik} = 1$, since they cannot all be 0.

Consider the ideal $\mathfrak{u} = (n-\theta_jt^2) + (n-\theta_kt^2)$.

Notice that since we have the equivalence between the numbers:

$$-1 \cdot (n-\theta_jt^2) + 1 \cdot (n-\theta_kt^2) = t^2(\theta_j - \theta_k),$$

we must have that the number $(\theta_j - \theta_k)t^2$ is contained in the ideal $(n-\theta_jt^2) + (n-\theta_kt^2)$, since $-1, 1 \in \mathcal{O}_L$. Additionally, since $m^2 = (n-\theta_1t^2)(n-\theta_2t^2)(n-\theta_3t^2)$, we see that $n-\theta_jt^2 \mid m^2$ and $n-\theta_kt^2 \mid m^2$, so $\gcd(n-\theta_jt^2, n-\theta_kt^2) \mid m^2$, and $m^2$ lies in the ideal $(n-\theta_jt^2) + (n-\theta_kt^2)$. Since any multiple of $m^2$ by an element in $L$ will also lie in this ideal, $m^2(\theta_j - \theta_k)$ lies in $\mathfrak{u}$. Since $\gcd(m,t) = 1$ and both $t^2(\theta_j-\theta_k)$ and $m^2(\theta_j-\theta_k)$ lie in $\mathfrak{u}$, we must have that $\theta_j - \theta_k$ is in $\mathfrak{u}$. But, since $\mathfrak{u} = \gcd((n-\theta_jt^2),(n-\theta_kt^2))$, we see that $\mathfrak{p}_i \mid (\theta_j - \theta_k) \mid \Delta$, as desired. ■

**Theorem 4.19.** *(Dedekind-Kummer) Let $K = \mathbb{Q}(\alpha)$ and let $f$ be the minimum polynomial of $\alpha$ over $\mathbb{Z}[x]$. Then for each prime number $p$ not dividing the index $|\mathcal{O}_K : \mathbb{Z}[\alpha]|$, factor $f(x)$ into monic irreducible polynomials as*

$$f(x) \equiv \pi_1(x)^{e_1} \cdot \pi_2(x)^{e_2} \dots \pi_n(x)^{e_n} \pmod p.$$

*Then, $(p) = p\mathcal{O}_K$ can be factored as*

$$(p) = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdot \dots \cdot \mathfrak{p}_n^{e_n},$$

*such that $N_{K/\mathbb{Q}}(\mathfrak{p}_i) = p^{\deg \pi_i}$.*

Recall that $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \cdot \frac{1}{2}\theta + \mathbb{Z} \cdot \frac{1}{4}\theta$, so the index $|\mathcal{O}_K : \mathbb{Z}[\theta]| = 1 \cdot 2 \cdot 4 = 8$, since $\mathbb{Z}[\theta] = \mathbb{Z} + \mathbb{Z} \cdot \theta + \mathbb{Z} \cdot \theta^2$. Since 11 does not divide this index, we can write

$$f(x) = x^3 - 4x^2 + 16 \equiv (x+1)^2(x+5) \pmod{11}.$$

Thus, we see that

$$(11) = \mathfrak{q}^2 \cdot \mathfrak{q}'$$

for prime ideals $\mathfrak{q} \neq \mathfrak{q}'$ and $N_{K/\mathbb{Q}}(\mathfrak{q}) = N_{K/\mathbb{Q}}(\mathfrak{q}') = 11^1 = 11$. However, $2 \mid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. Since $\mathcal{O}_K = \mathbb{Z}\left[\frac{\theta}{2}\right]$, consider the ring $\mathbb{Q}\left(\frac{\theta}{2}\right)$. But, the basis of this field is $\left\{1, \frac{\theta}{2}, \frac{\theta^2}{4}\right\}$, which spans the same vector space as $\mathbb{Q}(\theta)$, which has basis $\{1, \theta, \theta^2\}$, so $K = \mathbb{Q}(\theta) = \mathbb{Q}\left(\frac{\theta}{2}\right)$. Since

$$\theta^3 - 4\theta^2 + 16 = 0,$$

we find that

$$\left(\frac{\theta}{2}\right)^3 - 2\left(\frac{\theta}{2}\right)^2 + 2 = 0,$$

so $g(x) = x^3 - 2x^2 + 2$ is the minimum polynomial of $\frac{\theta}{2}$. Now, since $2 \nmid \left|\mathcal{O}_K : \mathbb{Z}\left[\frac{\theta}{2}\right]\right| = 1$, we can apply Dedekind-Kummer:

$$g(x) = x^3 - 2x^2 \equiv x^3 \pmod 2.$$

So, $(2) = \mathfrak{p}^3$, for some prime ideal $\mathfrak{p}$ with $N_{K/\mathbb{Q}}(\mathfrak{p}) = 2^1 = 2$.

Next, note that

$$\begin{aligned}\left(\prod_i N_{K/\mathbb{Q}}(\mathfrak{p}_i)^{e_i}\right) \cdot N_{K/\mathbb{Q}}(\mathfrak{A})^2 &= N_{K/\mathbb{Q}}\left(\left(\prod_i \mathfrak{p}_i^{e_i}\right)\mathfrak{A}^2\right)\\ &= N_{K/\mathbb{Q}}((n - t^2\theta))\\ &= N_{K/\mathbb{Q}}(n - t^2\theta),\end{aligned}$$

where we have used the multiplicative property of the norm. The minimum polynomial of $n - t^2\theta$ is $(x - (n - t^2\theta_1))(x - (n - t^2\theta_2))(x - (n - t^2\theta_3))$, and the product of its roots is $(n - t^2\theta_1)(n - t^2\theta_2)(n - t^2\theta_3)$, so

$$\begin{aligned}N_{K/\mathbb{Q}}(n - t^2\theta) &= (n - t^2\theta_1)(n - t^2\theta_2)(n - t^2\theta_3)\\ &= t^6(n/t^2 - \theta_1)(n/t^2 - \theta_2)(n/t^2 - \theta_3)\\ &= t^6(x - \theta_1)(x - \theta_2)(x - \theta_3).\end{aligned}$$

But recall that $(x - \theta_1)(x - \theta_2)(x - \theta_3) = x^3 - 4x^2 + 16 = y^2$, so

$$N_{K/\mathbb{Q}}(n - t^2\theta) = t^6y^2,$$

a perfect square. Hence,

$$\prod_i N_{K/\mathbb{Q}}(\mathfrak{p}_i)^{e_i} = \frac{N_{K/\mathbb{Q}}(n - t^2\theta)}{(N_{K/\mathbb{Q}}(\mathfrak{A}))^2} = \left(\frac{t^3y}{N_{K/\mathbb{Q}}(\mathfrak{A})}\right)^2.$$

Since $N_{K/\mathbb{Q}}(\mathfrak{p}) = 2$ and $N_{K/\mathbb{Q}}(\mathfrak{q}) = N_{K/\mathbb{Q}}(\mathfrak{q}') = 11$, and since

$$\prod_i N_{K/\mathbb{Q}}(\mathfrak{p}_i^{e_i}) = N_{K/\mathbb{Q}}(\mathfrak{p}^{e_1}\mathfrak{q}^{e_2}\mathfrak{q}'^{e_3}) = 2^{e_1}11^{e_2}11^{e_3}$$

is a perfect square, we must have $e_1 = 0$ or $e_2 = e_3 = 0$ or 1.

If $e_2 = e_3 = 1$, then from Proposition 4.18, $\mathfrak{q}\mathfrak{q}' \mid n - t^2\theta$, so $(\mathfrak{q}\mathfrak{q}')^2 \mid (n - t^2\theta)^2 = n^2 - 2nt^2\theta + t^4\theta^2$. But recall that $\mathfrak{q}^2\mathfrak{q}' = 11$, so

$$\frac{n^2 - 2nt^2\theta + t^4\theta^2}{11} \in \mathcal{O}_K.$$

This means that $11|r$ and $11|t$, contradicting the fact that $\gcd(r, t) = 1$. So, we have $e_1 = e_2 = e_3 = 0$ and $(n - t^2\theta) = \mathfrak{A}^2$. Since $K$ has class number 1, $\mathfrak{A}$ is generated by some $a \in \mathcal{O}_K$. Then, we have $n - t^2\theta = u \cdot a^2$, where $u$ is a non-square element of the units $\mathcal{O}_K^\times$ ($u$ clearly cannot be a square since otherwise $n - t^2\theta$ would be a perfect square in $K$ which we assumed to be false).

After factoring all even powers of $\eta$ into $a$, we find that $u \in \{-1, -\eta, \eta\}$, where $\eta$ is the fundamental unit $1 - \frac{1}{2}\theta$ as mentioned earlier. We see that $N_{K/\mathbb{Q}}(u)N_{K/\mathbb{Q}}(a)^2 = N_{K/\mathbb{Q}}(n - t^2\theta) = t^6y^2$, as calculated earlier, so

$$N_{K/\mathbb{Q}}(u) = \frac{t^6y^2}{N_{K/\mathbb{Q}}(a)^2} = \left(\frac{t^3y}{N_{K/\mathbb{Q}}(a)}\right)^2 \geq 0,$$

and since $N_{K/\mathbb{Q}}(-1) = N_{K/\mathbb{Q}}(-\eta) = -1 < 0$, we know that $u = \eta$ and $n - t^2\theta = \eta \cdot a^2$. Since $\eta a \in \mathcal{O}$, we can write

$$\eta a = u + v \cdot \frac{1}{2}\theta + w \cdot \frac{1}{4}\theta^2,$$

for $u, v, w \in \mathbb{Z}$, from our equation for $\mathcal{O}_K$. Thus,

$$\begin{aligned}\eta(n - t^2\theta) &= \left(1 - \frac{1}{2}\theta\right)(n - t^2\theta)\\ &= (\eta a)^2\\ &= \left(u + v \cdot \frac{1}{2}\theta + w \cdot \frac{1}{4}\theta^2\right)^2\\ &= \theta^4\left(\frac{w^2}{16}\right) + \theta^3\left(\frac{vw}{4}\right) + \theta^2\left(\frac{uw}{2}\right) + \theta^2\left(\frac{v^2}{4}\right) + \theta(uv) + u^2.\end{aligned}$$

But, recall that $\theta^3 - 4\theta^2 + 16 = 0$, so $\theta^3 = 4\theta^2 - 16$ and $\theta^4 = 4\theta^3 - 16\theta = 16\theta^2 - 16\theta - 64$. Making these substitutions and expanding $\left(1 - \frac{1}{2}\theta\right)(n - t^2\theta)$, we arrive at

$$\theta^2\left(\frac{t^2}{2}\right) - \theta\left(t^2 + \frac{n}{2}\right) + n = \theta^2\left(\frac{v^2}{4} + \frac{uw}{2} + vw + w^2\right) + \theta(uv - w^2) + (u^2 - 4wv - 4w^2). \tag{4.3}$$

Any of the $\theta = \theta_1, \theta_2, \theta_3$ satisfy this equation, so we can choose the matrix

$$A = \begin{pmatrix} 1 & \theta_1 & \theta_1^2 \\ 1 & \theta_2 & \theta_2^2 \\ 1 & \theta_3 & \theta_3^2 \end{pmatrix},$$

so that Equation 4.3 is equivalent to

$$A \cdot \begin{pmatrix} n \\ -t^2 - \frac{n}{2} \\ \frac{t^2}{2} \end{pmatrix} = A \cdot \begin{pmatrix} u^2 - 4wv - 4w^2 \\ uv - w^2 \\ \frac{v^2}{4} + \frac{uw}{2} + vw + w^2 \end{pmatrix}.$$

The matrix $A$ turns out to be the Vandermonde matrix $V(\theta_1, \theta_2, \theta_3)$, which is a matrix with a special property that the square of its determinant is the discriminant of the monic polynomial with roots $\theta_1, \theta_2, \theta_3$, which we found to be the cubic $x^3 - 4x^2 + 16$, which has discriminant $\Delta = -2816 \neq 0$, so the determinant of $A$ is non-zero and $A$ is invertible. Multiplying both sides by $A^{-1}$ equates the vectors

$$\begin{pmatrix} n \\ -t^2 - \frac{n}{2} \\ \frac{t^2}{2} \end{pmatrix} = \begin{pmatrix} u^2 - 4wv - 4w^2 \\ uv - w^2 \\ \frac{v^2}{4} + \frac{uw}{2} + vw + w^2 \end{pmatrix}.$$

From equating the second entries of each vector, we see that

$$-2t^2 - n = 2uv - 2w^2,$$

so $n$ must be even. Equating the first entries gives us

$$n = u^2 - 4wv - 4w^2,$$

and since $n$ is even, $u$ must also be even. Equating the third entries tells us that

$$2t^2 = v^2 + 2uw + 4vw + 4w^2,$$

so $v$ is even. But, since $u$ is even, $4 \mid v^2 + 2uw + 4vw + 4w^2 = 2t^2$, so $t$ is even. But, $\gcd(n, t) = 1$, so this is impossible and we have arrived at a contradiction. Thus, there exists no point $P$ such that $\mu(P) \neq 1 \mod (K^\times)^2$, and thus the image $\mathfrak{I}(\mu) = 1$. But, since $\mathfrak{I}(\mu) \cong (\mathbb{Z}/2\mathbb{Z})^r$, we must have $r = 0$, as desired. Thus there exists exactly 5 rational points on $E$, so there cannot exist any elliptic curves with torsion points of order 11.

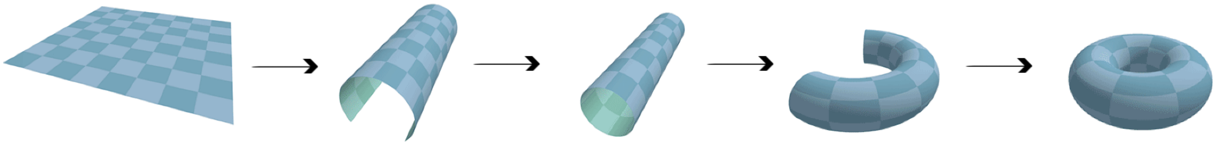

**Figure 4.** Transformation between $\mathbb{C}/\Lambda$ and the surface of a torus. Since a torus has genus one, it can be mapped to an elliptic curve, which also has genus one, because of Theorem 5.9. Edited from https://upload.wikimedia.org/wikipedia/commons/6/60/Torus_from_rectangle.gif.

## 5. A Different Approach: Modular Curves

Although we have successfully proven the theorem of Billing-Mahler, we still have unanswered questions, such as how the elliptic curve $y^2-y=x^3-x^2$ has any relation to $11-$torsion elliptic curves. We seek to explain this by deriving this equation from a different angle, by using modular curves.

**Definition 5.1.** (Lattice $\Lambda$ Definition) Define a lattice $\Lambda \subset \mathbb{C}$ with basis $\langle \omega_1, \omega_2 \rangle$, with $\frac{\omega_1}{\omega_2} \notin \mathbb{Q}$, to be an additive subgroup of $\mathbb{C}$ to be $\mathbb{Z}\cdot\omega_1+\mathbb{Z}\cdot\omega_2$. In other words, it consists of all integer combinations of $\omega_1$ and $\omega_2$.

Consider the quotient group $\mathbb{C}/\Lambda$. This group consists of all the complex numbers within the parallelogram spanned by $\omega_1$ and $\omega_2$, where the operation, addition, between two complex numbers $z_1$ and $z_2$ is defined as normal complex addition $z_1+z_2$ modulo $\omega_1, \omega_2$. This parallelogram is called a complex torus, as the paralleogram can be morphed into the surface of a torus. It turns out that there is a connection between elliptic curves and complex tori, but we first need to define a function on $\mathbb{C}/\Lambda$.

**Definition 5.2.** (Weierstrass $\wp$-function) Let $\Lambda$ be a complex lattice. Define the Weierstrass $\wp$-function on $\Lambda$ to be

$$\wp(z)=\frac{1}{z^2}+\sum_{\omega\in\Lambda,\omega\neq 0}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right).$$

We can calculate the derivative

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

**Theorem 5.3.** *For any lattice $\Lambda$, there exists an elliptic curve $E/\mathbb{C}$ such that the map $\phi:\mathbb{C}/\Lambda\mapsto\mathbb{P}^2(\mathbb{C})$ defined as*

$$\phi(z):=[\wp(z),\wp'(z),1]$$

*is both an isomorphism between the Riemann surface of the complex torus $\mathbb{C}/\Lambda$ and that of the elliptic curve $E/\mathbb{C}$ and an isomorphism between the additive groups of $\mathbb{C}/\Lambda$ and $E(\mathbb{C})$.*

*Proof.* A property of the function $\wp(z)$ is that it satisfies the differential equation

$$\wp'(z)^2=4\wp(z)^3-60G_4\wp(z)-140G_6,$$

where $G_k$ is an Eisenstein series of weight $k$ with respect to $\Lambda$ defined by

$$G_k=\sum_{\omega\in\Lambda,\omega\neq 0}\omega^{-k}$$

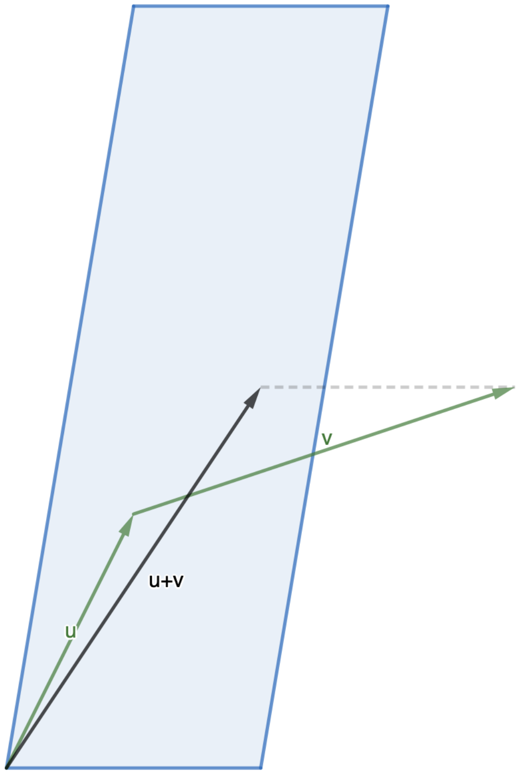

**Figure 5.** Addition in a complex torus.

(see VI.3.5 of [Sil09] for a deeper discussion of this). For convenience, let $g_2 = 60G_4(\Lambda)$ and $g_3 = 140G_6(\Lambda)$. We see that this differential equation is in a very similar form to that of an elliptic curve; in fact, if we let $y = \wp'(z)$ and $x = \wp(z)$, as is the case under $\phi$, then we have

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

an elliptic curve. It requires some more work to show that $\phi$ is surjective and is truly an isomorphism between $\mathbb{C}/\Lambda$ and $E(\mathbb{C})$ (see VI.3.6 of [Sil09] for more details), but it can be shown that complex addition on a complex torus $\mathbb{C}/\Lambda$ corresponds to point addition on $E(\mathbb{C})$. ■

It turns out that this relationship works both ways, as is evidenced by the uniformization theorem. We call two lattices $\Lambda_1$ and $\Lambda_2$ homothetic if $\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbb{C}^* = \mathbb{C}\backslash\{0\}$.

**Theorem 5.4.** *(Uniformization Theorem of Elliptic Curves) For any elliptic curve $E/\mathbb{C}$, there exists a lattice $\Lambda \subset \mathbb{C}$, unique up to homothety, such that the map $\phi$, as defined earlier, maps $\mathbb{C}/\Lambda$ to $E(\mathbb{C})$.*

See [Par16] for a proof. This theorem tells us that there is a bijection between equivalence classes of lattices under homothety and the set of all $E/\mathbb{C}$. Thus, we have turned the problem of analyzing elliptic curves into analyzing lattices.

A natural question to ask about lattices over $\mathbb{C}$ is when two bases span the same lattice. We only need to consider lattices spanned by $\langle 1, \tau\rangle = \left\langle 1, \frac{\omega_2}{\omega_1}\right\rangle$, as any lattice will be homothetic to one of this form. Additionally, we want to take this basis to be positively oriented, or that $\operatorname{im}(\tau) > 0$. If this is not the case, then we can just switch $\omega_1$ and $\omega_2$, which clearly will not affect the lattice. This orientation makes it so that we only have to consider $\tau$ in the upper half plane $\mathcal{H} = \{z = a + bi | b > 0; a, b \in \mathbb{R}\}$.

**Definition 5.5.** (Special Linear Group) Define $\mathrm{SL}(n, F)$ or $\mathrm{SL}_n(F)$, where $n \in \mathbb{Z}^+$ and $F$ is a field, to be the group of $n \times n$ matrices over $F$ with determinant 1.

*Example.* ($\mathrm{SL}_2(\mathbb{Z})$) In this paper we will be concerned with the group and subgroups of $\mathrm{SL}_2(\mathbb{Z})$, or $2 \times 2$ integer matrices with determinant 1. We define the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane $\mathcal{H}$ to be Möbius transformation (fractional transformation of a complex number)

$$\gamma(z) = \frac{az+b}{cz+d}$$

for some

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

that is $a, b, c, d \in \mathbb{Z}$ such that $ad - bc = 1$. We can verify that the group action of functional composition is equivalent to that of matrix multiplication by defining $\gamma_1, \gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$ as

$$\gamma_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \text{ and } \gamma_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

We see that

$$(\gamma_1 \circ \gamma_2)(z) = \frac{(a_1a_2 + b_1c_2)z + (a_1b_2 + b_1d_2)}{(c_1a_2 + c_2d_1)z + (c_1b_2 + d_1d_2)} = (\gamma_1 \cdot \gamma_2)(z),$$

where $\circ$ is functional composition and $\cdot$ is matrix multiplication, so our action of functional composition of Möbius transformations is isomorphic to that of matrix multiplcation in $\mathrm{SL}_2(\mathbb{Z})$, with the caveat that $\gamma$ is considered the same matrix as $-\gamma$, as $\gamma(z) = -\gamma(z)$.

Consider the mapping

$$\phi : \Lambda \mapsto \mathbb{Z}^2$$

by the transformation

$$\phi(n\omega_1 + m\omega_2) = (n, m)$$

for $n, m \in \mathbb{Z}$. Clearly this is an isomorphism, as $\phi(z_1) + \phi(z_2) = \phi(z_1 + z_2)$ for $z_1, z_2 \in \Lambda$. Our question about different bases for the same lattice $\Lambda$ has turned into a question about different bases for $\mathbb{Z}^2$. But this is just the set of pairs of vectors $((a, b), (c, d))$ that are linearly independent, which is the same as the set of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with nonzero determinant. To preserve our positive orientation, we can choose matrices with positive determinant. Since we want to create a group of integer matrices, the inverses of all of these matrices must be over $\mathbb{Z}$, so the determinant must be $\pm 1$. Since we require a positive determinant, we see that all automorphisms of $\mathbb{Z}^2$ that preserve orientation and have integral inverses are exactly the group $\mathrm{SL}_2(\mathbb{Z})$.

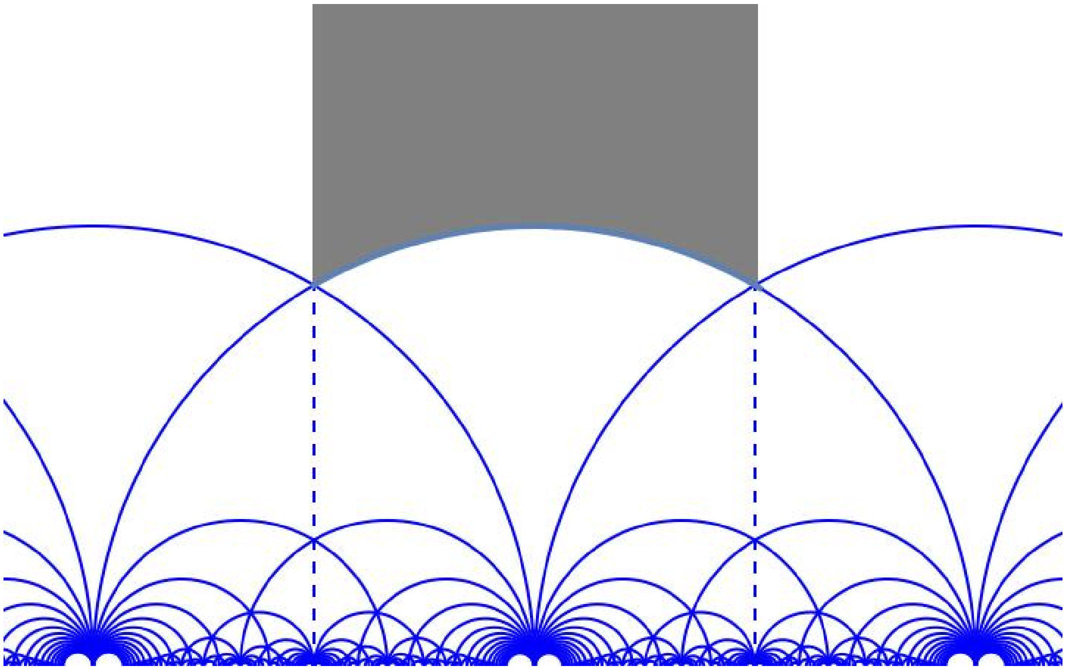

**Figure 6.** The fundamental domain (in gray) of $Y(1)$ and the its images under $\Gamma(1)$. Each "triangle" corresponds to the image of the fundamental domain under some transformation $\gamma \in \Gamma(1)$. This pattern is known as the Dedekind tessellation of the upper half plane.

*Example.* The vectors $\hat{\mathbf{i}} = (1,0)$ and $\hat{\mathbf{j}} = (0,1)$ clearly span $\mathbb{Z}^2$. We can choose any matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, such as

$$A = \begin{pmatrix} 7 & -6 \\ 6 & -5 \end{pmatrix},$$

and we see that $A^T \cdot \hat{\mathbf{i}} = (7,-6)$ and $A^T \cdot \hat{\mathbf{j}} = (6,-5)$ are our new basis vectors of $\mathbb{Z}^2$.

Temporarily reversing the order of the basis of our lattice $\Lambda$, we see that if $\Lambda = \langle \tau, 1 \rangle$, then $\phi(\tau) = (1,0)$ and $\phi(1) = (0,1)$. Applying a matrix

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

to these vectors, we get the new basis vectors

$$A^T \cdot (1,0) = (a,b) \text{ and } A^T \cdot (0,1) = (c,d),$$

which corresponds to a new basis of our lattice, after reversing our basis again to bring it back to its original form, $\Lambda = \langle c\tau + d, a\tau + b \rangle$. Scaling, we see that

$$\Lambda = \langle 1, \tau \rangle = \left\langle 1, \frac{a\tau + b}{c\tau + d} \right\rangle.$$

Thus, to study the equivalence classes of lattices over $\mathbb{C}$, we need to study the equivalence classes of the upper half plane defined by the equivalence relation $z_1 \sim z_2$ if $z_2 = \gamma(z_1)$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, which is also the equivalence class of lattices up to homothety. From here, we will refer to the group $\mathrm{SL}_2(\mathbb{Z})$ as $\Gamma(1)$, the name of which we shall soon explain.

We are concerned with the quotient $\mathcal{H}/\Gamma(1)$; that is, the set of $\mathcal{H}$ under the aformentioned equivalence relation. We call this quotient $Y(1)$. The curve $Y(1)$ is known as a modular curve. Each point of $Y(1)$ corresponds to an equivalence class mentioned earlier, and thus corresponds to an elliptic curve by Theorem 5.4. We will use the notation $\Re(z)$ and $\Im(z)$ to represent the real and imaginary parts of $z$ respectively.

**Lemma 5.6.** *(Fundamental Domain)*

*(i)* $\Gamma(1)$ *is generated by* $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *and* $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

*(ii) The region bounded by defined by* $\mathcal{D} = \{z : -\frac{1}{2} \leq \Re(z) \leq \frac{1}{2}; |z| \geq 1\}$ *is a fundamental domain; i.e. each point in* $\mathcal{D}$ *corresponds to a unique orbit of* $\mathcal{H}$ *under* $\Gamma(1)$, *except for boundary points of* $\mathcal{D}$.

*Proof.* We see that the matrices $S$ and $T$ have very intuitive actions on a complex number. $T(z) = z + 1$, which corresponds to a linear shift to the right by one, and $S(z) = -\frac{1}{z}$, which corresponds to an inversion about the unit circle followed by a reflection about the $y$-axis. These two matrices explain the translational and circular symmetry in Figure 6.

(i) We will proceed with casework.

Case 1: $a = 0$.

$bc = ad - 1 = -1$, and since $b, c \in \mathbb{Z}$, we must have $b = -c = \pm 1$. Thus,

$$\gamma(z) = \frac{\pm 1}{\mp \tau + d} = -\frac{1}{\tau \mp d} = (S \cdot T^{\mp d})(\tau).$$

Case 2: $a = \pm 1$.

Since $\gamma = -\gamma$, we can multiply by $-1$ if needed so that $a = 1$. Then

$$\gamma(z) = \frac{z + b}{cz + d},$$

and

$$(\gamma \cdot S)(z) = \frac{-cz - d}{z + b},$$

and

$$(\gamma \cdot S \cdot T^{c})(z) = \frac{-cz - d}{z + b} + c = \frac{bc - d}{z + b} = -\frac{1}{z + b}$$

because the determinant $d - bc = 1$. This transformation has matrix $\begin{pmatrix} 0 & 1 \\ 1 & b \end{pmatrix}$, which reduces to Case 1 since $a = 0$.

Case 3: $|a| > 1$.

WLOG, let $|a| \geq |c|$. If this is not the case, apply $S$ to $\gamma$. Choose $n = \left\lfloor \frac{a}{c} \right\rfloor$. Then we have $|a - nc| < |c|$. We see that

$$(\gamma \cdot T^{-n})(z) = \frac{az + b}{cz + d} - n = \frac{(a - nc)z + (b - nd)}{cz + d},$$

and

$$(\gamma \cdot T^{-n} S)(z) = -\frac{cz + d}{(a - nc)z + (b - nd)}.$$

We can repeat this process, each time decreasing both $|a|$ and $|c|$. But notice that this is the same as applying the procedure of the Euclidean algorithm to $a$ and $c$. Thus, we must eventually reach $a = 0$, if $\gcd(a, c) \neq 1$, or $a = \pm 1$, if $\gcd(a, c) = 1$, which reduce to Case 1 and Case 2 respectively.

(ii) We will show that the mapping $\pi : \mathcal{D} \mapsto Y(1)$ is a surjection, or that any $\tau \in \mathcal{H}$ is equivalent to some point in $\mathcal{D}$. First, we can repeatedly apply $T$ or $T^{-1}$ to shift $\tau$ such that $|\Re(\tau)| \leq \frac{1}{2}$. If $|\tau| \geq 0$, then $\tau \in \mathcal{D}$ as desired. Otherwise, we have

$$\Im(S\tau) = \Im\left(-\frac{1}{\tau}\right) = \Im\left(-\frac{\bar{\tau}}{|\tau|^2}\right) = \Im\left(\frac{\tau}{|\tau|^2}\right) > \Im(\tau),$$

so we can repeatedly apply $T^{\pm 1}$ to $S(\tau)$ again until it is between the lines $|\Re(z)| = \frac{1}{2}$. Now, we will derive a formula for $\Im(\gamma(z))$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$. Let $\tau = u + vi$. Then we have

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d} = \frac{au + avi + b}{cu + cvi + d} = \frac{(au + avi + b)(cu - cvi + d)}{|cu + cvi + d|^2}.$$

Taking the imaginary part, we see that

$$\Im(\gamma(\tau)) = \Im\left(\frac{(au + avi + b)(cu - cvi + d)}{|cu + cvi + d|^2}\right) = \frac{advi - bcvi}{|c\tau + d|^2}.$$

But, since $ad - bc = 1$, we have

$$\Im(\gamma(\tau)) = \frac{vi}{|c\tau + d|^2} = \frac{\Im(\tau)}{|c\tau + d|^2}.$$

Since there can only be a finite number of lattice points inside the unit disk, there are only a finite number of matrices $\gamma$ such that $\Im(\gamma(\tau)) > \Im(\tau)$. So the algorithm must terminate at some $\tau \in \mathcal{D}$. It turns out that the map $\pi$ is injective only for non-boundary points of $\mathcal{D}$ and we have the following for distinct points $\tau_1, \tau_2$ in the boundary $\partial\mathcal{D}$ with $\tau_2 = \gamma(\tau_1)$ :

$$\Re(\tau_1) = \pm\frac{1}{2} : \tau_2 = T^{\pm 1}(\tau_1),$$

$$|\tau_1| = 1 : \tau_2 = -\frac{1}{\tau_1}.$$

See Lemma 2.3.2 of [DS05] for a proof of injectivity and boundary conditions. ■

**Definition 5.7.** (Riemann Surface) A Riemann surface is a connected complex manifold of complex dimension 1.

Intuitively, this means that the neighborhood of each point in a Riemann surface is homeomorphic to to the complex plane $\mathbb{C}$, or that it "looks like" the complex plane near every point. It turns out that $Y(1)$ is a Riemann surface (see section 2.1 of [DS05] for more details). We need the following definition:

**Definition 5.8.** (Compact Set) A set $X$ is compact if every open cover of $X$ has a finite subcover.

In other words, $X$ contains all limiting points.

*Example.* For example, the interval $[0, 1)$ is not compact since it does not contain the point 1. In fact, all compact subsets of Euclidean space $\mathbb{R}^n$ must be bounded and closed (this is known as the Heine-Borel Theorem).

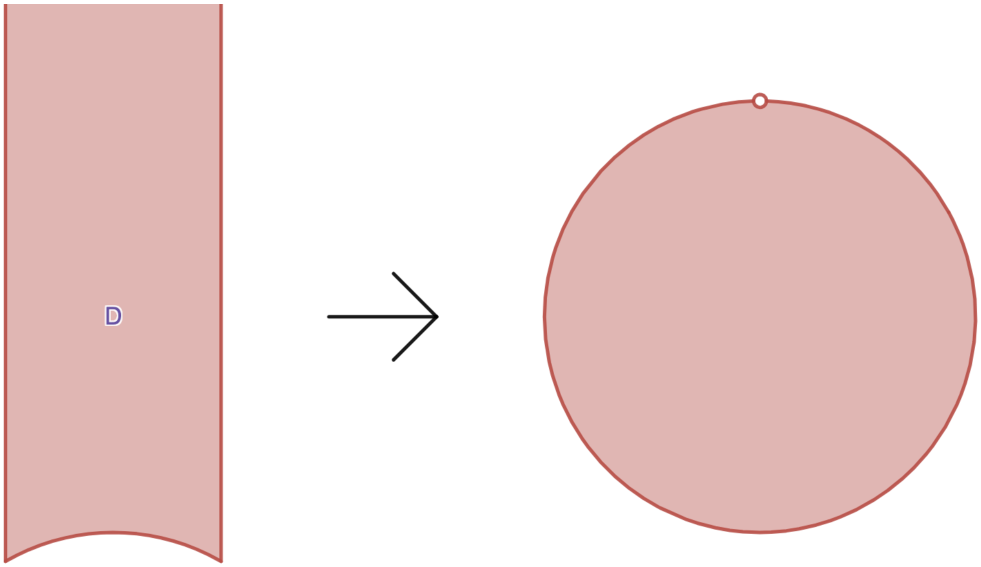

**Figure 7.** By thinking in the Riemann sphere $\mathbb{P}^1(\mathbb{C})$, the fundamental domain D can be thought of as a sphere missing a point, hence it is not compact.

*Example.* The set $\mathbb{C}$ is not compact. We can see this by applying a stereographic projection to turn it into a sphere missing one point. If we add the point at infinity to our complex plane, we arrive at the complex projective line $\mathbb{P}^1(\mathbb{C})$, which is now in bijection with the sphere, which is compact. This sphere is known as the Riemann sphere.

The reason why compactness is important is because of the following theorem:

**Theorem 5.9.** *Every compact Riemann surface is isomorphic to an algebraic curve.*

See [Smi15] for a proof and details. Note that we have already seen this theorem in action. A torus is a compact Riemann surface, so it must be isomorphic to an algebraic curve. But from 5.3, we know that the Weierstrass $\wp$-function does exactly that, converting a complex torus into an algebraic curve, specifically an elliptic curve.

Now, consider the fundamental domain $\mathcal{D}$. We would like it to be compact so that we can determine an equation for its algebraic curve. If we consider the extended complex plane $\mathbb{C}_\infty$, we can think of $\mathcal{D}$ as a disk missing a point (see Figure 7).

This is not compact because it is missing a limiting point. Thus, we can add the point $\infty$ to compactify $D$. However, by doing this, we must add all the the points $\gamma(\infty)$ for some

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1).$$

We see that

$$\lim_{x\to\infty} \frac{ax+b}{cx+d} = \frac{a}{c},$$

so naturally, we let $\gamma(\infty) = \frac{a}{c}$. Similarly, choosing any $q = \frac{a}{c} \in \mathbb{Q}$ in lowest terms we can find $b$ and $d$ such that $ad - bc = 1$, and thus there will exist $\gamma \in \Gamma(1)$ with $\gamma(\infty) = q$. This

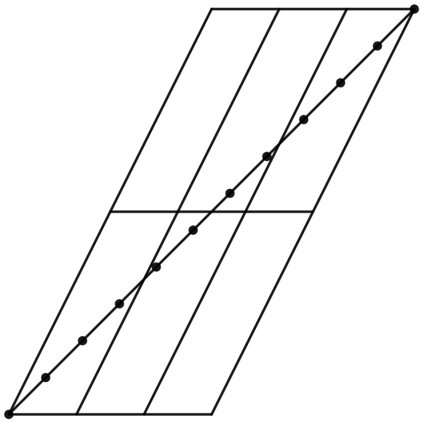

**Figure 8.** Any point $P$ of order 11 corresponds to a complex number $z \in \mathbb{C}/\Lambda$ such that $11z \equiv 0 \mod \Lambda$. In this figure, we have $11z = 3 + 2\tau$. With a change of basis $\langle 1, \tau\rangle \mapsto \langle 3 + 2\tau, \tau\rangle$, we transform the set $nz \mapsto \frac{\mathbb{Z}}{11}$.

means that we must add both $\infty$ and $\mathbb{Q}$ to $\mathcal{H}$ to create a compact modular curve. This leads to the definition $\mathcal{H}^* = \mathcal{H} \cup \infty \cup \mathbb{Q}$. This leads to the following definition:

$$X(1) = \mathcal{H}^*/\Gamma(1).$$

For now, the set $\mathbb{Q} \cup \infty$, called cusps, lie in the same orbit under $\Gamma(1)$. But, using different subgroups of $\Gamma(1)$ instead, we can have multiple orbits, the number of which is related to the structure of elliptic curves.

Now, let there exist a cycle of order 11 on an elliptic curve $E/\mathbb{Q}$. From Theorem 5.3, for a lattice $\Lambda = \langle 1, \tau\rangle$ corresponding to $E$, we must have that there exists $z \in \mathbb{C}/\Lambda$ such that $11z \equiv 0 \mod \Lambda$, so $11z = n + m\tau$ for some $n, m \in \mathbb{Z}$. We can change our basis to $\langle n + m\tau, \omega\rangle$ where $\omega$ is some lattice point positively oriented from $n + m\tau$ (see Figure 8). Dividing by $n + m\tau$, we get the lattice $\Lambda' = \langle 1, \tau'\rangle$, for which the cyclic subgroup of order 11 is represented by the additive group $\frac{1}{11}\mathbb{Z} \in \mathbb{C}/\Lambda'$. Since $\Lambda'$ is homothetic to $\Lambda$, they represent the same elliptic curve $E$. Consider the pair $(\mathbb{C}/\Lambda, P)$, called a refined moduli pair. If we choose a point $P$ be of order 11, we see that, on the complex torus, $P = \frac{n}{11}$ for some integer $n$. Choosing the basis $\langle \frac{n}{11}, \tau'\rangle$ and rescaling lets us choose $P = \frac{1}{11}$.

We have just shown that for any point $P$ of order 11,

$$(\mathbb{C}/\Lambda, P) \cong \left(\mathbb{C}/\Lambda, \frac{1}{11}\right).$$

We wish to determine for which what subset $\gamma \in \Gamma(1)$ we have $\left(\mathbb{C}/\Lambda_\tau, \frac{1}{11}\right) \cong \left(\mathbb{C}/\Lambda_{\tau'}, \frac{1}{11}\right)$. Recall that the homothety of $\Lambda_{\tau'}$ is given by $c\tau + d$. Hence, we have

$$\frac{c\tau + d}{11} \equiv \frac{1}{11} \mod \Lambda_{\tau'}.$$

We must have that $\frac{c\tau}{11}$ is a multiple of $\tau$, or that $c \equiv 0 \pmod{11}$. Additionally, we must have $d \equiv 1 \pmod{11}$. So, we have $\gamma(\frac{1}{11}) = \frac{a}{11} + b$. We want this to be congruent to $\frac{1}{11} \mod \Lambda_{\tau'}$. But,

$$\frac{a}{11} + b \equiv \frac{1}{11} \mod \Lambda_{\tau'},$$

so $a \equiv 1 \pmod{11}$. So,

$$\gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{11},$$

where $*$ represents any other number. We denote the set of $\gamma$ that satisfy this as $\Gamma_1(11)$. In general, for $N > 0$,

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

We see that $\Gamma(1) = \Gamma_1(1) = \mathrm{SL}_2(\mathbb{Z})$, as all integer matrices are equivalent $\pmod 1$. We can define the modular curves $Y(N) = \mathcal{H}/\Gamma(N)$ and $Y_1(N) = \mathcal{H}/\Gamma_1(N)$, compactifying them into $X(N)$ and $X_1(N)$ respectively.

We have the following in general:

**Theorem 5.10.** *For $N > 0$,*

*(i)There exists a surjective mapping between the pair $(E, P)$ and a point on $Y_1(N)$, where $P$ is a rational point on elliptic curve $E$ of order $N$. Two pairs $(E_1, P_1)$ and $(E_2, P_2)$ correspond to the same point on $Y_1(N)$ if and only if there exists an isomorphism between $E_1$ and $E_2$ that maps $P_1$ to $P_2$.*

*(ii)There exists a surjective mapping between the pair $(E, P, G)$ and a point on $Y(N)$, where $P$ is a rational point on elliptic curve $E$ and $G$ is a cyclic subgroup of $E$ both of order $N$. Two pairs $(E_1, P_1, G_1)$ and $(E_2, P_2, G_2)$ correspond to the same point on $Y(N)$ if and only if there exists an isomorphism between $E_1$ and $E_2$ that maps $P_1$ to $P_2$ and $G_1$ to $G_2$.*

See [DS05] for more details.

It turns out that, unlike in the case of $X(1)$, where we added a single orbit of cusps to compactify $Y(1)$, we need to instead adjoin a set $\mathcal{C}$ of 10 orbits of cusps, 5 of which lie in $\mathbb{Q}$ and 5 of which lie in the maximal real subfield $\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ of the cyclotomic field $\mathbb{Q}(\zeta_{11})$. See example 9.3.5 of [DI95] for more details. Additionally, there exists a bijection

$$X_1(11)_{\mathbb{Q}} \longleftrightarrow Ell(\mathbb{Q}) \cup \mathcal{C}_{\mathbb{Q}},$$

where $Ell(\mathbb{Q})$ is the set of elliptic curves over $\mathbb{Q}$ with 11-torsion points, $\mathcal{C}_{\mathbb{Q}}$ is the set of five cusps in $\mathbb{Q}$, and $X_1(11)_{\mathbb{Q}}$ represents the algebraic curve over $\mathbb{Q}$ representing $X_1(11)$. Such an algebraic curve exists because of Theorem 5.9, since $X_1(11)$ is compact. From example 9.1.6 of [DI95], we see that the genus of $X_1(11)$ is given by

$$g = 1 + \frac{11^2}{24}\prod_{p|N}\left(1 - \frac{1}{p^2}\right) - \frac{11}{4}\prod_{p|N}\left(1 - \frac{1}{p^2} + v_p(N)\left(1 - \frac{1}{p}\right)^2\right) = 1,$$

since the only prime factor of 11 is itself, with the p-adic valuation $v_{11}(11) = 1$. From the genus-degree formula for algebraic curves, which states that

$$g = \frac{(d-1)(d-2)}{2},$$

we see that for a curve to have genus 1 it must have a degree $d$ satisfying

$$d^2 - 3d = 0.$$

Since our curve has positive degree, we must have $d = 3$. By applying the procedure from Lemma 4.2, we can turn this cubic curve into an elliptic curve, so the modular curve $X_1(11)$ has an elliptic curve equation.

**Proposition 5.11.** *The modular curve $X_1(11)$ as an algebraic curve has the equation*

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

*Proof.* Consider the refined moduli pair $(E, P)$, where $P$ is a rational point of order 11 on $E$. We can rewrite $E$ it as

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2,$$

with $a_2, a_3 \neq 0$, if we transform $P$ into $(0, 0)$ and the tangent line to $P$ be the line $x = 0$ after a linear transformation (see [Rei86] for details). With the transformation

$$X = \left(\frac{a_3}{a_2}\right)^2 X'$$

and

$$Y = \left(\frac{a_3}{a_2}\right)^3 Y',$$

and substituting $(1 - c) = \frac{a_1a_2}{a_3}$ and $b = -\frac{a_2^3}{a_3^2}$, which is valid since $a_3 \neq 0$, we arrive at

$$E : y^2 + (1 - c)xy - by = x^3 - bx^2.$$

Since $P$ has order 11, we see that $5P = -6P$, so $x_{5P} = x_{6P} = x_{-6P}$, where $x_{nP}$ is the $x$-coordinate of $nP$. We can calculate the following:

- $P = (0, 0)$
- $2P = (b, bc)$
- $3P = (c, b - c)$
- $4P = (r(r - 1), r^2(c + r - 1))$, where $r = \frac{b}{c}$
- $5P = (rs(s - 1), rs^2(r - s))$, where $s = \frac{c}{r-1}$
- $6P = (-mt, m^2(m + 2t - 1))$, where $m = \frac{s(1-r)}{1-s}$ and $t = \frac{r-s}{1-s}$.

Equating $x$-coefficients of $5P$ and $6P$, we have

$$rs(s-1) = -mt.$$

Reversing the substitutions of $6P$, we have

$$r^2 - 4sr + 3s^2r - s^3r + s = 0.$$

With the transformation $(s, r) \mapsto \left(\frac{1}{s+1}, \frac{1}{r+1}\right)$ to bring $(1, 1)$ to $(0, 0)$ and remove the singularity there, we arrive at

$$r^2 + s^2r + r - s^3 = 0.$$

Finally, substituting $y = \frac{s}{r}$ and $x = \frac{1}{r}$, we have

$$y^2 + y = x^3 - x^2,$$

which parameterizes our pair $(E, P)$ and thus is an equation for $X_1(11)$. ■

Notice that this is exactly the same equation we found earlier in Lemma 4.2. Of course, this is no coincidence, as we were implicitly parameterizing all 11-torsion elliptic curves without realizing it. We have already proven that this elliptic curve has exactly 5 torsion points, but we expected exactly 5 cusps to lie in $\mathbb{Q}$. Thus, there are no non-cusp rational points on $X_1(11)$, so there cannot be any elliptic curves over $\mathbb{Q}$ with torsion points of order 11.

## 6. Further Exploration

A lot of our work with modular curves did not require that $P$ had order 11. In fact, we could have used a similar procedure to describe a point with $N$-torsion. By analyzing the curves $X_1(N)$ for higher values of $N$, Mazur in [Maz77] and [MG78] was able to prove that there are only 15 different possibilities for torsion groups, and that infinitely must exist of each kind.

Elliptic curves in general are also important in cryptography. The previously most popular cryptography algorithm, RSA, is weak to quantum algorithms, which are able to efficiently factor large numbers in theory. So, a new technique has been developed called ECC, or elliptic curve cryptography, where an elliptic curve is considered over the finite field $\mathbb{F}_p$ instead of $\mathbb{Q}$. In this finite field, given a point $P$ and another point $nP$, it is difficult to calculate the value of $n$. So, we can publicly hand out $P$ and $nP$, keeping our value of $n$ secret.

## 7. Acknowledgements

I would like to thank Dr. Rubinstein-Salzedo and Ryan Catullo for the helpful discussions regarding this paper.

## References

[BM40] G. Billing and K. Mahler. On exceptional points on cubic curves. *J. Lond. Math. Soc.*, 15:32–43, 1940.

[DI95] Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem, Providence, RI*, pages 39–133, 1995.

[DS05] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[FO17] Kazuyuki Fujii and Hiroshi Oike. An algebraic proof of the associative law of elliptic curves. *Advances in Pure Mathematics*, 07(12):649–659, 2017.

[Lut37] Elisabeth Lutz. Sur l'équation $y^2 = x^3 - ax - b$ dans les corps p-adiques. *crll*, 1937(177):238–247, 1937.

[Maz77] B. Mazur. Modular curves and the eisenstein ideal. *Publications mathématiques de l'IHÉS*, 47(1):33–186, December 1977.

[MG78] B. Mazur and D. Goldfeld. Rational isogenies of prime degree. *Inventiones Mathematicae*, 44(2):129–162, June 1978.

[Mor22] Louis Joel Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Mathematical Proceedings of the Cambridge Philosophical Society*, 1922.

[Par16] Peter S Park. Uniformization theorem for elliptic curves over c. *Harvard Scholar*, 2016.

[Pin10] Charles C Pinter. *A book of abstract algebra*. Courier Corporation, 2010.

[Rei86] Markus A. Reichert. Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields. *Mathematics of Computation*, 46(174):637–658, 1986.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[Smi15] Zachary Smith. Compact riemann surfaces: A threefold categorical equivalence. *University of Chicago Mathematics REU*, 2015.

[ST92] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*, volume 9. Springer, 1992.

[Wei29] André Weil. L'arithmétique sur les courbes algébriques. *Acta Mathematica*, 52(0):281–315, 1929.

Euler Circle
*Email address*: ramkumar.rohan@gmail.com