# The Billing-Mahler Theorem

Crystal Xie

July 9, 2024

**Abstract**

In this paper we prove that there are no rational torsion points of order 11 on an elliptic curve, which is what is known as the Billing-Mahler theorem. We will assume no prior knowledge of elliptic curves, but we will assume an understanding of group theory, number theory, and linear algebra.

## 1 Introduction

The study of Diophantine equations, i.e. the study of integer and rational solutions to polynomial equations, has an extremely rich and long history dating back to ancient Greece. For the most basic types of Diophantine equations, namely linear and quadratic equations in two variables, this topic has been studied extensively, and tools such as Hasse's principle, quadratic reciprocity, and Hensel's lemma have been developed.

The next simplest type of Diophantine equation is the elliptic curve, which are cubic equations in two variables. Elliptic curves appear naturally when finding the length of an arc on an ellipse, and the theory of elliptic curves has applications in several different areas of math, including in cryptography and in the proof of Fermat's Last Theorem. In this paper we will take a look at few results on the surface of a very deep field.

We will start with the group law on the rational points on elliptic curves, as well as briefly looking at the Nagell-Lutz theorem. After that we will prove Mordell's theorem, and finally we will use the proof of Mordell's theorem to prove the Billing-Mahler theorem. We also include appendices to cover the necessary background from projective geometry and algebraic number theory.

## 2 The Group Law and the Nagell-Lutz Theorem

An elliptic curve is a non-singular curve $E$ given by

$$E = \left\{(x, y) : y^2 = f(x) = x^3 + ax^2 + bx + c\right\} \cup \{\mathcal{O}\}.$$

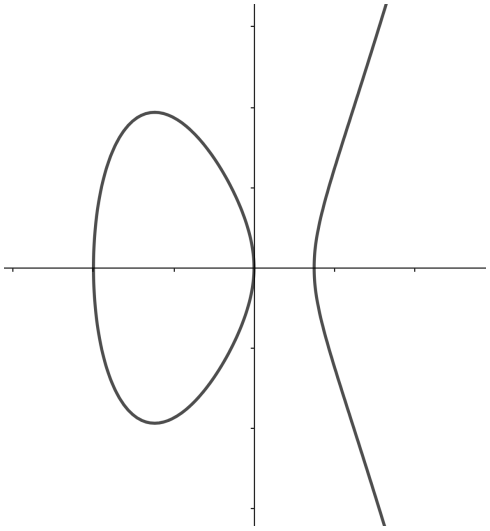

Figure 1: The elliptic curve $y^2 = x^3 - 2x^2 - 8x$.

where $a, b, c \in \mathbb{Z}$ and the point $\mathcal{O}$ is the point at infinity where vertical lines meet. Non-singular means that the partial derivatives of $f$ with respect to $x$ and $y$ are never both zero, or in other words, that the curve has a tangent line at every point. An example of an elliptic curve is shown in Figure 1.

There is a certain group structure that points on these elliptic curves satisfy. Let $\ell$ be the line through points $P$ and $Q$ on the curve $E$; then define $P * Q$ as the third intersection point of $\ell$ with $E$. Then we will define $P + Q$ as follows:

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

In other words, we take the third intersection, $P * Q$, of the line through $P$ and $Q$, and then we take the third intersection of the vertical line through $P * Q$. This is illustrated in Figure 2.

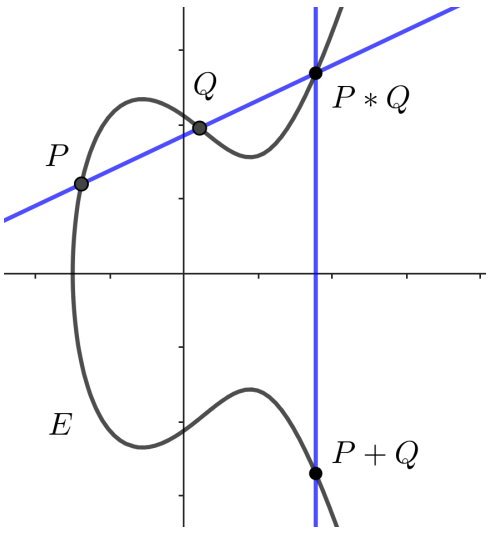


Figure 2: Adding two points $P$ and $Q$ on elliptic curve $E$.

Through some computation, we can find explicit formulas for the sum of two points. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_1 + P_2 = (x_3, y_3)$. Then if $m$ is the slope of the line through $P_1$ and $P_2$, we get

$$x_3 = m^2 - a - x_1 - x_2 \qquad \text{and} \qquad y_3 = -mx_3 - (y_1 - mx_1)\,.$$

. If $P_1 \neq P_2$, then $m = \frac{y_2 - y_1}{x_2 - x_1}$, and if $P_1 = P_2$, the slope is $m = \frac{f'(x_1)}{2y_1}$ (where $f(x) = x^3 + ax^2 + bx + c$ is the equation for the cubic). These formulas will frequently be useful to us.

**Proposition 1.** *The following properties are satisfied for points $P$, $Q$ on an elliptic curve $E$:*

*(a) Closure: $P + Q$ is in $E$.*

*(b) Commutativity: $P + Q = Q + P$.*

*(c) Identity: $P + \mathcal{O} = \mathcal{O} + P = P$.*

*(d) Inverses: $P + (-P) = \mathcal{O}$, where $-P$ is the point $P$ reflected across the $x$-axis.*

*(e) Associativity: $P + (Q + R) = (P + Q) + R$.*

*Therefore, $(E, +)$ is an abelian group.*

*Proof.* Statements (a) and (b) follow from the definition of $*$.

(c) We have $P * \mathcal{O} = -P$ (where $-P$ is $P$ reflected across the $x$-axis), and $\mathcal{O} * (-P) = P$, so $P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O}) = P$.

(d) We have $P * (-P) = \mathcal{O}$, and $\mathcal{O} * \mathcal{O} = \mathcal{O}$, so $P + (-P) = \mathcal{O} * (P * (-P)) = \mathcal{O}$.

(e) We can check that associativity is true using the explicit formulas for the addition operation. □

We now turn our attention to properties of rational points of finite order on these elliptic curves.

**Definition.** *A rational point is a point $(x, y)$ with both $x$ and $y$ in $\mathbb{Q}$. We will use the notation $E(\mathbb{Q})$ to denote the set of rational points on an elliptic curve $E$.*

**Definition.** *A point of finite order is a point such that there exists an $n$ with*

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ times}} = \mathcal{O},$$

*and $kP \neq \mathcal{O}$ for all $1 \leq k < n$.*

Note the points of order 2 are the points with $y = 0$ and $x \neq 0$, since those (together with $(0, 0)$) are the only points that are their own inverse.

Using some real and complex analysis we can obtain a very good description of the real and complex points on elliptic curves. Namely, if the group of real points on a curve is connected, then it is isomorphic to the circle group (the multiplicative group of complex numbers of magnitude 1), and if the group of real points has two connected components, then it is isomorphic to the direct product of the circle group with a group of order 2. Furthermore, the group of complex points on the elliptic curve is the direct product of two circle groups. This allows us to understand the real and complex points of finite order very well. Therefore we will only look at rational points of finite order.

One critical piece of information associated with any polynomial is the discriminant. For a cubic $f(x) = x^3 + ax^2 + bx + c$, it is

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

If $x_1$, $x_2$, and $x_3$ are the roots of $f$, then $D_f$ can be rewritten as

$$D_f = (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2.$$

It follows that $D_f$ is nonzero if and only if $f$ has distinct roots in $\mathbb{C}$. For elliptic curves it can tell us even more about the rational points, as shown by the following theorem:

**Theorem** (Nagell-Lutz)**.** *If $P = (x, y)$ is a rational point of finite order on $E$, then it has integer coordinates, and furthermore either $y = 0$ or $y$ divides the discriminant of $f(x)$.*

A proof of this is given in [2].

The Nagell-Lutz theorem allows us to find all the rational points of finite order through a finite number of operations: for each of the $\tau(D)$ values of $y$, any rational solutions to $0 = x^3 + ax^2 + bx + c - y^2$ will be integers that divide $c - y^2$ (by the rational root theorem), so testing all of them yields the set of rational solutions.

# 3 Mordell's Theorem

In order to prove the Billing-Mahler theorem we still need a little more information about the group of rational points, which will be provided by the implications of the following theorem, along with sub-results contained in its proof.

**Theorem** (Mordell)**.** *For a non-singular cubic curve $C$ defined over $\mathbb{Q}$, the group of rational points is a finitely generated abelian group.*

To prove this theorem, we will first need a property of rational numbers called the *height*, which will define an ordering on the rational points.

**Definition.** *If $x = \frac{m}{n}$ for relatively prime integers $m$ and $n$, then the height $h(x)$ is* $\log(\max\{|m|, |n|\})$.

From this we will define the height of a rational point as the height of its $x$-coordinate. Additionally, we will say $h(\mathcal{O}) = 0$, and that $h(P) = 0$ if $P$ has an $x$-coordinate of 0.

## 3.1 The Proof

To prove Mordell's theorem we will require four lemmas. We will assume the lemmas for now in order to prove Mordell's theorem, and afterwards we will take a closer look at the lemmas.

**Lemma 1.** *For every real number $M$, the set of rational points on $C$ with height at most $M$ is finite.*

**Lemma 2.** *Let $P_0$ be a fixed rational point of $C$. There is a constant $\kappa_0$ depending on $P_0$, $a$, $b$, and $c$ such that*

$$h(P + P_0) \leq 2h(P) + \kappa_0 \qquad \text{for all } P \in C(\mathbb{Q}).$$

**Lemma 3.** *There is a constant $\kappa$, depending on $a$, $b$, and $c$, so that*

$$h(2P) \geq 4h(P) - \kappa \qquad \text{for all } P \in C(\mathbb{Q}).$$

**Lemma 4.** *The index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ is finite.*

We are using $2C(\mathbb{Q})$ to denote the set of points in $C(\mathbb{Q})$ that are twice of other points in $C(\mathbb{Q})$.

*Proof.* The proof is by descent. We will find a sequence of points descending in height until we reach a certain fixed threshold.

By Lemma 4 the number of cosets of $2C(\mathbb{Q})$ in $C(\mathbb{Q})$ is finite, so suppose there are $n$ of them, and let $Q_1, \ldots, Q_n$ be representatives for the cosets. Take any point $P$ in $C(\mathbb{Q})$. It must be in one of these cosets, say the $i_1$-th coset. Then

$$P - Q_{i_1} = 2P_1 \qquad \text{for some } P_1 \in C(\mathbb{Q}).$$

Similarly, $P_1$ is in one of the cosets, so we can continue this process to get

$$\begin{aligned} P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\vdots \\ P_m - Q_{i_m} &= 2P_m, \end{aligned}$$

where the $Q_{i_j}$ are all coset representatives and the $P_j$ are elements of $C(\mathbb{Q})$. Substituting these equations back into the equation for $P$, we get

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

We want to show that eventually the height of $P_m$ is below a fixed threshold $\gamma$, since by Lemma 1 that would mean there are only a finite set of possibilities for what $P_m$ could be.

If we set $P_0$ to $-Q_i$ for $i = 1, 2, \ldots, n$ in Lemma 2, we get $h(P - Q_i) \leq 2h(P) + \kappa_i$ for some constant $\kappa_i$ and all $P \in C(\mathbb{Q})$. If we let $\kappa'$ be the largest of the $\kappa_i$'s, then we get

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

for all $P \in C(\mathbb{Q})$ and all $i \in \{1, 2, \ldots, n\}$. On the other hand, by Lemma 3 there is a constant $\kappa$ so that for each $j = 1, 2, \ldots, n$, we have

$$4h(P_j) - \kappa \leq h(2P_j) = h(P_{j-1} - Q_{i_j}),$$

therefore, combining the two inequalities,

$$4h(P_j) - \kappa \leq 2h(P_{j-1}) + \kappa'.$$

By rewriting this as

$$h(P_j) \leq \frac{3}{4}h(P_{j-1}) - \frac{1}{4}\left(h(P_{j-1}) - (\kappa + \kappa')\right),$$

we can conclude for all values of $j$ with $h(P_{j-1}) \geq \kappa + \kappa'$, we will have $h(P_j) \leq \frac{3}{4}h(P_{j-1})$. Thus the sequence of points $P_j$ has heights that are strictly descreasing, and eventually we will find an $M$ such that $h(P_M) \leq \kappa + \kappa'$. The set of points that have height less than $\kappa + \kappa'$ is finite due to Lemma 1. Therefore, $C(\mathbb{Q})$ is generated by the finite set of coset representatives together with the finite set of elements of $C(\mathbb{Q})$ with height at most $\kappa + \kappa'$. □

Now we take a closer look at the lemmas. Lemma 1 is obvious because the set of points in $C(\mathbb{Q})$ with height at most $M$ is in the set of points $(\frac{m_1}{n_1}, \frac{m_2}{n_2})$ where $m_1, n_1 \in \{\pm 1, \pm 2, \ldots, \pm M\}$. This set has finite size. Lemmas 2 and 3 relate the geometric properties of the point addition operation to the number theoretic nature of the height of points, and while their proofs are interesting, they are not so relevant to our main goal of proving the Billing-Mahler theorem, so we will not cover them in this paper. Their proofs can be found in [5].

## 3.2 $2C(\mathbb{Q})$ in $C(\mathbb{Q})$

The proof of Lemma 4 will provide us with tools that will turn out to be useful in the proof of Billing-Mahler. We restate it and then present the proof.

**Lemma 4.** *The index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ is finite.*

*Proof.* To compare $C(\mathbb{Q})$ and $2C(\mathbb{Q})$, we will study the duplication map $P \mapsto 2P$ by breaking it into two parts $\phi : C \mapsto \overline{C}$ and $\psi : \overline{C} \mapsto C$, where $\overline{C}$ is a second cubic curve defined in terms of $C$.

Suppose that the polynomial $f(x)$ has at least one rational root and translate the curve $C$ so that this rational root is at $T = (0, 0)$. The new curve is isomorphic to the old one over the rationals so we can simply study the translated curve instead. Then the cubic is

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

We will define $\overline{C}$ as follows:

$$\overline{C} : y^2 = \overline{f}(x) = x^3 + (-2a)x^2 + (a^2 - 4b)x.$$

We now show that there is a homomorphism $\phi$ from $C$ to $\overline{C}$, and similarly that there is a homomorphism $\psi$ from $\overline{C}$ to $C$, giving an automorphism on the complex points of $C$. Given a point $P = (x, y)$, we define $\phi$ as

$$\phi(P) = \begin{cases} \left( \left(\frac{y}{x}\right)^2, \frac{y}{x^2}(x^2 - b) \right) & \text{if } P \neq \mathcal{O}, T \\ \overline{\mathcal{O}} & \text{if } P = \mathcal{O} \text{ or } P = T. \end{cases}$$

Similarly, for a point $\overline{P} = (\overline{x}, \overline{y})$ on $\overline{C}$, we define $\psi$ as

$$\psi(\overline{P}) = \begin{cases} \left( \left(\frac{\overline{y}}{\overline{x}}\right)^2, \frac{\overline{y}}{\overline{x}^2}(\overline{x}^2 - (a^2 - 4b)) \right) & \text{if } P \neq \overline{\mathcal{O}}, \overline{T} \\ \mathcal{O} & \text{if } P = \overline{\mathcal{O}} \text{ or } P = \overline{T}. \end{cases}$$

Using the explicit formulas for the addition of points we can show that $\phi$ and $\psi$ satisfy the homomorphism property, and $\psi \circ \phi$ is an isomorphism from $C$ to $C$ satisfying $\psi \circ \phi(x, y) = 2(x, y)$. The kernel of $\phi$ is $\{\mathcal{O}, T\}$, since the only point with $x = 0$ is $T = (0, 0)$ and all other points with complex values of $x \neq 0$ and $y$ get mapped to points that are not $\overline{\mathcal{O}}$. Similarly, the kernel of $\psi$ is $\left\{\overline{\mathcal{O}}, \overline{T}\right\}$.

Now we look at how $\phi$ and $\psi$ affect $C(\mathbb{Q})$ and $\overline{C}(\mathbb{Q})$ (which we'll call $G$ and $\overline{G}$ for the sake of notation). For the two "exceptional" points in $\overline{G}$, namely $\overline{\mathcal{O}}$ and $\overline{T}$, we can see that $\overline{\mathcal{O}}$ is always in the image of $G$, and $\overline{T}$ is in the image of $G$ if and only if there is a point $(x, y) \in G$ with $x \neq 0$ and $y = 0$, which happens if and only if the discriminant of $0 = x^2 + ax + b$ is a perfect square. As for the remaining points in $\overline{G}$, we claim that they

are exactly the set of points where the $\overline{x}$-coordinate is a square of a rational number. We get an analagous statement for $\psi$ with a similar proof.

Let $\mathbb{Q}^\times$ denote the multiplicative group of nonzero rational numbers, and let $(\mathbb{Q}^\times)^2$ be the group of rational numbers that are the square of an element in $\mathbb{Q}^\times$. Referring to the definition of $\phi$, it is clear that anything in the image of $G$ under $\phi$ must have an $\overline{x}$-coordinate in $(\mathbb{Q}^\times)^2$, so we just need to prove that anything in $C(\mathbb{C})$ with an $\overline{x}$-coordinate in $(\mathbb{Q}^\times)^2$ is in the image of $G$.

Since the kernel of $\phi$ is $\{\mathcal{O}, T\}$, for each point of $\phi(G)$, there should be two points in $G$ that map to it. Let $(\overline{x}, \overline{y})$ be a point in $\phi(G)$, where $\overline{x} = t^2$ for a $t \in \mathbb{Q}^\times$, and we will show that the points $(x_1, y_1)$ and $(x_2, y_2)$ are both on $G$ and map to $(\overline{x}, \overline{y})$, where

$$x_1 = \frac{1}{2}\left(t^2 - a + \frac{\overline{y}}{t}\right), \qquad y_1 = x_1 t,$$

$$x_2 = \frac{1}{2}\left(t^2 - a - \frac{\overline{y}}{t}\right), \qquad y_2 = -x_2 t.$$

We can show that $(x_1, y_1)$ and $(x_2, y_2)$ lie on $C$ by simply checking that they satisfy the equation $y^2 = x^3 + ax^2 + bx$, because expanding the product $x_1 \cdot x_2$ shows that it is actually equal to $b$. So the equation $y_1^2 = x_1^3 + ax_1^2 + bx_1$ is equivalent to $t^2 = x_1 + a + x_2$ after we divide both sides by $x_1$ and substitute $b = x_1 x_2$, and we know this is true from the definitions of $x_1$ and $x_2$. We can check that $(x_2, y_2)$ satisfy the equation as well in the same way.

To show that $(x_1, y_1)$ and $(x_2, y_2)$ are in the image of $G$, we need to show that

$$\frac{y_i^2}{x_i^2} = \overline{x} \qquad \text{and} \qquad \frac{y_i}{x_i^2}(x_i^2 - b) = \overline{y}$$

are true for $i = 1$ and $i = 2$. The first one follows from the definitions of $y_1$ and $y_2$. Plugging the definitions into the second equation and using the fact that $b = x_1 x_2$ gives

$$\frac{y_1}{x_1^2}(x_1^2 - b) = \frac{x_1 t}{x_1}(x_1^2 - x_1 x_2) = t(x_1 - x_2),$$

which is true from the definitions of $x_1$ and $x_2$. We can do the same calculation for the point $(x_2, y_2)$.

We now show that $\psi(\overline{G})$ has finite index in $G$, since showing that $\phi(G)$ has finite index in $\overline{G}$ would be a similar proof. We do this by finding an injective homomorphism from the quotient group $G/\psi(\overline{G})$ to a finite group. Let the mapping $\mu : G \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$

be defined as

$$\begin{aligned}\mu(\mathcal{O}) &= 1 \pmod{(\mathbb{Q}^\times)^2},\\ \mu(T) &= b \pmod{(\mathbb{Q}^\times)^2},\\ \mu((x,y)) &= x \pmod{(\mathbb{Q}^\times)^2} \qquad \text{if } x \neq 0,\end{aligned}$$

and we claim this is a homomorphism with kernel $\psi(\overline{G})$.

If $\mu$ is indeed a homomorphism, then the statement that the kernel is $\psi(\overline{G})$ is clear due to the fact we proved earlier that the image of $\psi$ is exactly the points with $x$-coordinates in $\mathbb{Q}^\times$. To show it's a homomorphism, first note that $\mu(-(x,y)) = x = \frac{1}{x} \cdot x^2$ and thus

$$\mu(-(x,y)) \equiv \frac{1}{x} = \frac{1}{\mu(x,y)} = (\mu(x,y))^{-1} \pmod{(\mathbb{Q}^\times)^2},$$

so $\mu$ sends inverses to inverses. So, if we just show that when $P_1 + P_2 + P_3 = \mathcal{O}$ (i.e. when $P_1$, $P_2$, $P_3$ lie on a line), then $\mu(P_1)\mu(P_2)\mu(P_3) \equiv 1 \pmod{(\mathbb{Q}^\times)^2}$, and then we would get

$$\mu(P_1)\mu(P_2) \equiv \mu(P_3)^{-1} \equiv \mu(-P_3) = \mu(P_1 + P_2) \pmod{(\mathbb{Q}^\times)^2},$$

which is the homomorphism property we want to show. Let $y = mx + k$ be the line passing through $P_1$, $P_2$, and $P_3$ (which must be collinear). Substituting this for $y$ in $y^2 = x^3 + ax^2 + bx$ and rearranging means that the three points satisfy

$$0 = x^3 + (a - m^2)x^2 + (b - 2mk)x - k^2.$$

The $x$-coordinates of the three points are roots of this equation. Suppose that the $x$-coordinates are $x_1$, $x_2$, and $x_3$; then $x_1x_2x_3 = k^2$, which is in $\mathbb{Q}^2$, so we have obtained

$$\mu(P_1)\mu(P_2)\mu(P_3) = x_1x_2x_3 = k^2 \equiv 1 \pmod{(\mathbb{Q}^\times)^2}.$$

Therefore, $\mu$ is a homomorphism with kernel $\psi(\overline{G})$.

We now look at what rational numbers can occur as the $x$-coordinate of a point in $G$. If there is a point $(x,y)$ in $G$, then we can write it as $(\frac{m}{e^2}, \frac{m}{e^3})$ and substitute it into $y^2 = x^3 + ax^2 + bx$ to get

$$n^2 = m(m^2 + ame^2 + be^4).$$

Let $d$ be the greatest common divisor of the two terms on the right. Since $e$ and $m$ are relatively prime, $d \mid m^2 + ame^2 + be^4$ implies that $d \mid b$. Then every prime dividing $m$ that doesn't also divide $b$ must appear to an even power in the prime factorization of $m$, and only the primes dividing both $m$ and $b$ can appear to an odd power. Therefore

$$m = \pm(m')^2 \cdot p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_t^{\epsilon_t}$$

for some integer $m'$, where the $p_i$ are all the distinct primes dividing $b$, and $\epsilon_i \in \{0, 1\}$ for all $i$. So there are $2^{t+1}$ possibilities for $m$ (and therefore $x$) $\pmod{(\mathbb{Q}^\times)^2}$. So, the image of the quotient group $G/\psi(\overline{G})$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ under the injective homomorphism induced by $\mu$ has size at most $2^{t+1}$, hence $(G : \psi(\overline{G}))$ is at most $2^{t+1}$. We can similarly find that $(\overline{G} : \phi(G)) \leq 2^{s+1}$ where $s$ is the number of distinct prime divisors of $a^2 - 4b$.

Because these indexes are finite, we can find elements $g_1, \ldots, g_n$ to represent the cosets of $\psi(\overline{G})$ in $G$, and similarly we can find elements $\overline{g}_1, \ldots, \overline{g}_m$ to represent the cosets of $\phi(G)$ in $\overline{G}$. Then we claim that the set of representatives of the cosets of $2G$ in $G$ is contained in

$$\left\{g_i + \psi(\overline{g}_j) \mid 1 \leq i \leq n,\ 1 \leq j \leq m\right\}.$$

To show this, let $g$ be an element of $G$. Then there is a representative $g_i$ so that $g - g_i = \psi(\overline{g})$ for some $\overline{g} \in \overline{G}$. Similarly we can find a representative $\overline{g}_j$ so that $\overline{g} - \overline{g}_j = \phi(g')$ for some $g' \in G$. Then we have

$$\begin{aligned} g = g_i + \psi(\overline{g}) &= g_i + \psi(\overline{g}_j + \phi(g')) \\ &= g_i + \psi(\overline{g}_j) + \psi(\phi(g')) \\ &= g_i + \psi(\overline{g}_j) + 2g', \end{aligned}$$

so any element of $G$ can be expressed as the sum of two elements in the finite set $\left\{g_i + \psi(\overline{g}_j)\right\}$ along with an element of $2G$. Hence $2G$ has finite index in $G$. □

To summarize the proof of Lemma 4: we defined a pair of homomorphisms $\phi : C \to \overline{C}$ and $\psi : \overline{C} \to C$ so that $\phi \circ \psi = \psi \circ \phi = 2$ is an automorphism on $C(\mathbb{C})$. Then we showed that the images of $G$ and $\overline{G} = \phi(G)$ under $\phi$ and $\psi$ are exactly the points in $\overline{C}$ and $C$ with $\overline{x}$- and $x$-coordinates being in $(\mathbb{Q}^\times)^2$. After gathering this information about $\phi$ and $\psi$, we aimed to show that $(G : \psi(\overline{G}))$ and $(\overline{G} : \phi(G))$ are finite; in order to do this we defined a new homomorphism $\mu : G \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ with kernel $\psi(\overline{G})$ so that an injective homomorphism $G/\psi(\overline{G}) \hookrightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ was induced. The image of this injective homomorphism turns out to be finite, implying $(G : \psi(\overline{G}))$ and $(\overline{G} : \phi(G))$ are finite, and from there it follows that $(G : 2G)$ is finite.

## 3.3 Consequences

Mordell's theorem says that $G = C(\mathbb{Q})$ is a finitely generated abelian group, so from the fundamental theorem of finitely generated abelian groups, we know that $G$ is isomorphic to a direct sum of infinite cyclic groups and finite cyclic groups of prime power order:

$$G \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ times}} \oplus \mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu_s}}.$$

Here $r$ is called the **rank** of $G$. Also, the subgroup

$$\mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu_s}}$$

corresponds to the points of finite order, or **torsion points**, in $G$. It is accordingly called the **torsion subgroup** of $G$.

# 4 The Billing-Mahler Theorem

We will now look at the main result of this paper:

**Theorem** (Billing-Mahler)**.** *There are no rational torsion points of order* 11 *on an elliptic curve defined over* $\mathbb{Q}$*.*

To prove this theorem, we will first study what happens if there does exist a point $P$ of order 11 on an elliptic curve defined over $\mathbb{Q}$. Let

$$P_i = \underbrace{P + P + \cdots + P}_{i \text{ times}} = iP.$$

Then note that $P_i + P_j + P_k = \mathcal{O}$ if and only if $i + j + k \equiv 0 \pmod{11}$, and furthermore these statements are equivalent to saying that $P_i$, $P_j$, and $P_k$ are collinear.

## 4.1 Setup

We have $P_0 = \mathcal{O} = (0, 1, 0)$, and let $P_1 = (a, b, c)$ and $P_2 = (\alpha, \beta, \gamma)$. Since the three vectors $\{(0, 1, 0), (1, 0, 0), (0, 0, 1)\}$ in $\mathbb{Q}^3$ are linearly independent, we can apply a linear transformation (change of basis) mapping the three original points $(0, 1, 0)$, $(a, b, c)$, $(\alpha, \beta, \gamma)$ to the points $P_0' = (0, 1, 0)$, $P_1' = (1, 0, 0)$, $P_2' = (0, 0, 1)$. This is an invertible linear map from $\mathbb{Q}^3$ to $\mathbb{Q}^3$, and since it can also be considered as a bijective map from $\mathbb{P}^2(\mathbb{Q})$ to $\mathbb{P}^2(\mathbb{Q})$, it maps lines to lines. Now we look at the point $P_3' = (u, v, w)$, which is not on the same line as $P_0'$, $P_1'$, and $P_2'$, since $1+2+3 \not\equiv 0 \pmod{11}$; we can again take a linear map, this time defined by $x \mapsto x/u$, $y \mapsto y/v$, and $z \mapsto z/w$, which doesn't change $P_0'$, $P_1'$, or $P_2'$ (since they are considered points in $\mathbb{P}^2$), and maps $P_3'$ to $P_3 = (1, 1, 1)$. Thus, now we can write

$$P_0 = (0, 1, 0), \qquad P_1 = (1, 0, 0), \qquad P_2 = (0, 0, 1), \qquad P_3 = (1, 1, 1).$$

Let $P_4$ be $(x_1, x_2, x_3)$, for some $x_1, x_2, x_3 \in \mathbb{Q}$.

Using the fact that the cross product of two points in $\mathbb{P}^2$ gives the line through them, we can determine equations for lines passing through points we have written down, and then take the unique intersections of pairs of lines to find new multiples of $P$. For example,

for the point $P_{-3}$, since the equation of the line through $P_0$ and $P_3$ is $x - z = 0$, and the equation of the line through $P_1$ and $P_2$ is $y = 0$, and $P_{-3}$ is the intersection of these two lines, we have $P_{-3} = (1, 0, 1)$. Then, the equation of the line through $P_{-3}$ and $P_4$ is $-x_2x + (x_1 - x_3)y + x_2z = 0$, and $P_{-1}$ is the intersection of this line and the line through $P_0$ and $P_1$, so we get $P_{-1} = (x_1 - x_3, x_2, 0)$. Continuing with this method, we find

$$\begin{aligned} P_{-3} &= (1, 0, 1) \\ P_{-1} &= (x_1 - x_3, x_2, 0) \\ P_{-2} &= (0, x_1 - x_2 - x_3, x_1 - x_3) \\ P_{-5} &= (x_2, x_2, x_3) \\ P_5 &= ((x_1 - x_3)x_2, -x_1x_2 + x_1x_3 + x_2^2 - x_3^2, (x_1 - x_3)x_3). \end{aligned}$$

Here $x_1 \neq x_3$, as that would imply $P_{-2} = P_0$ (a contradiction since $P$ doesn't have order 2), and also $x_2 \neq 0$, as that would imply $P_{-5} = P_2$ (a contradiction since $P$ doesn't have order 7).

Since $2 + 4 + 5 \equiv 0 \pmod{11}$, we know that $P_2$, $P_4$, and $P_5$ lie on a line, which is given by

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

So we have obtained the following proposition:

**Proposition 2.** *If there exists a rational torsion point of order* 11 *on an elliptic curve defined over* $\mathbb{Q}$*, then the cubic curve* $C$ *given by*

$$u^2v - u^2w + uw^2 - v^2w = 0$$

*has more than five rational solutions.*

*Proof.* We can check that $P_0$, $P_1$, $P_2$, $P_3$, and $P_{-3}$ satisfy this equation. Furthermore, we have just found that $P_4$ is a sixth rational solution. □

## 4.2 The Elliptic Curve $E$

We reduce $C$ to Weirstrass form using the algorithm given by T. Nagell in [3], so that we can instead look at the elliptic curve $E$ given by the equation

$$y^2z = x^3 - 4x^2z + 16z^3,$$

since we get a bijection from the points on $C$ to the points on $E$. So, in order to show that Proposition 2 is false and thus obtain a contradiction on the assumption that a rational torsion point of order 11 exists, we need to show that $y^2 = x^3 - 4x^2 + 16$ has exactly five rational solutions.

**Proposition 3.** *The elliptic curve $E$ given by the equation*

$$y^2 = f(x) = x^3 - 4x^2 + 16$$

*has exactly five rational solutions.*

With the Nagell-Lutz theorem we see that the torsion subgroup of $E$ is of order 5, and is generated by $(0, 4)$. Since Mordell's theorem implies that

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$$

where $E(\mathbb{Q})_{\text{tors}}$ is the torsion subgroup and $r$ is the rank, we want to show that $r = 0$.

Let $\theta$ be the real root of $f(x)$ (an explicit value can be found with a calculator), and let $K$ be the cubic field $\mathbb{Q}[\theta]$. Also with a calculator, we can compute that the discriminant of $K$ is $-2^2 \cdot 11$, the ring of integers is

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \cdot \frac{1}{2}\theta + \mathbb{Z} \cdot \frac{1}{4}\theta^2,$$

the unit rank is 1, and a fundamental unit is $\eta = 1 - \frac{1}{2}\theta$. Then the ring of integers is $\mathcal{O}_K^\times = \langle -1 \rangle \times \langle \eta \rangle$, and the class number of $K$ is 1 (so $\mathcal{O}_K$ is a principal ideal domain).

From the proof of Mordell's theorem, there is a homomorphism $\mu$ from $E(\mathbb{Q})$ to $K^\times/(K^\times)^2$ with kernel $2E(\mathbb{Q})$, meaning $E(\mathbb{Q})/2E(\mathbb{Q})$ is isomorphic to the image of $\mu$. However, from the implications of Mordell's theorem,

$$2E(\mathbb{Q}) \cong 2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z} \oplus 2\mathbb{Z}_{p_1^{\nu_1}} \oplus \cdots \oplus 2\mathbb{Z}_{p_s^{\nu_s}},$$

so the quotient group $G/2G$ looks like

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}_{p_1^{\nu_1}}/2\mathbb{Z}_{p_1^{\nu_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu_s}}/2\mathbb{Z}_{p_s^{\nu_s}},$$

where $\mathbb{Z}_{p_i^{\nu_i}}/2\mathbb{Z}_{p_i^{\nu_i}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ if $p_i = 2$, and 0 if $p_i \neq 2$. So we actually have

$$\text{Im}(\mu) \cong E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r.$$

Hence showing that $r = 0$ is the same as showing that $\text{Im}(\mu)$ is trivial, or in other words, that every rational point on $E$ has $x$-coordinate in $K^2$.

Suppose now for the sake of contradiction that there is a rational point $(x, y)$ on $E$ so that $x - \theta$ is not in $K^2$. We can write $x = \frac{r}{t^2}$ and $y = \frac{s}{t^3}$, where $r$, $s$, $t$ are integers so that $\gcd(r, t) = \gcd(s, t) = 1$. Then since

$$\mu(x, y) = x - \theta \equiv r - t^2\theta \pmod{(K^\times)^2},$$

we know that $r - t^2\theta \notin (K^\times)^2$.

Due to Mordell's theorem, we can write the integral ideal $(r - t^2\theta)$ of $\mathcal{O}_K$ as

$$(r - t^2\theta) = \left(\prod_i \mathfrak{p}_i^{\epsilon_i}\right)\mathfrak{I}^2, \tag{1}$$

where $\epsilon_i \in \{0, 1\}$, $\mathfrak{I}$ is an integral ideal, and the $\mathfrak{p}_i$ are prime ideals of $\mathcal{O}_K$ dividing the discriminant of $f(x)$, which is $-2^8 \cdot 11$. Hence the $\mathfrak{p}_i$ divide either 2 or 11. In fact, $(2) = \mathfrak{p}^3$, and $(11) = \mathfrak{q}^2\mathfrak{q}'$ where $\mathfrak{q} \neq \mathfrak{q}'$. Furthermore, $N_{K/\mathbb{Q}}(\mathfrak{p}) = 2$, and $N_{K/\mathbb{Q}}(\mathfrak{q}) = N_{K/\mathbb{Q}}(\mathfrak{q}') = 11$.

We now have

$$\prod_i \mathfrak{p}_i^{\epsilon_i} = \mathfrak{p}^{\epsilon_1}\mathfrak{q}^{\epsilon_2}(\mathfrak{q}')^{\epsilon_3},$$

and we'd like to show that the $\epsilon_i$ are all 0. Taking the norm of both sides gives

$$\prod_i N_{K/\mathbb{Q}}(\mathfrak{p}_i^{\epsilon_i}) = 2^{\epsilon_1}11^{\epsilon_2+\epsilon_3}.$$

Taking the norm of both sides of (1) gives

$$\prod_i N_{K/\mathbb{Q}}(\mathfrak{p}_i)^{\epsilon_i} \cdot N_{K/\mathbb{Q}}(\mathfrak{I})^2 = N_{K/\mathbb{Q}}(r - t^2\theta).$$

We can compute the RHS of the above equation to be $(t^6(x-\theta_1)(x-\theta_2)(x-\theta_3))$, which is $(t^6y^2)$, a square. So we know that $\epsilon_1 = 0$, while $\epsilon_2 + \epsilon_3$ is either 0 or 2.

If $\epsilon_2 + \epsilon_3 = 2$, i.e. $\epsilon_2 = \epsilon_3 = 1$, then $\mathfrak{q}\mathfrak{q}' \mid r - t^2\theta$, and therefore $11 \mid (r - t^2\theta)^2$. This means that $\frac{r^2 - 2rt^2\theta + t^4\theta^2}{11}$ is in $\mathcal{O}_K$, so 11 divides both $r$ and $t$. This is a contradiction since we assumed $\gcd(r, t) = 1$.

So, $\epsilon_2 = \epsilon_3 = \epsilon_1 = 0$, meaning $(r - t^2\theta) = \mathfrak{I}^2$, where $\mathfrak{I} = (\alpha)$ for some $\alpha \in \mathcal{O}_K$ due to $K$ having class number 1. Then we know that

$$r - t^2\theta = u \cdot \alpha^2,$$

where $u$ is a unit that is not a square in $K$ (since we assumed $r - t^2\theta$ isn't a square in $K$). We assume that $u \in \{-1, \eta, -\eta\}$, and we choose $\alpha$ appropriately. However, since the norm of the LHS of $r - t^2\theta = u \cdot \alpha^2$ is positive (due to it being a square), we know that the norm of $u$ must also be positive, so $u$ can't be $-1$ or $-\eta$. Thus

$$r - t^2\theta = \eta \cdot \alpha^2$$

for some $\alpha \in \mathcal{O}_K$. We are still looking for a contradiction, so we look more closely at $\alpha$.

Define $\beta = \eta\alpha \in \mathcal{O}_K$ and say that $\beta = a + b \cdot \frac{1}{2}\theta + c \cdot \frac{1}{4}\theta^2$. Then

$$\left(1 - \frac{1}{2}\theta\right)(r - t^2\theta) = \beta^2 = \left(a + b \cdot \frac{1}{2}\theta + c \cdot \frac{1}{4}\theta^2\right)^2.$$

Using $\theta^3 - 4\theta^2 + 16 = 0$, some calculations give

$$r - \left(\frac{r}{2} + t^2\right) \cdot \theta + \frac{t^2}{2} \cdot \theta^2 = (a^2 - 4c^2 - 4bc) + (ab - c^2) \cdot \theta + \left(\frac{b^2}{4} + \frac{ac}{2} + bc + c^2\right) \cdot \theta^2.$$

Matching coefficients gives us the three equations

$$\begin{aligned} r &= a^2 - 4c^2 - 4bc \\ -r - 2t^2 &= 2ab - 2c^2 \\ 2t^2 &= b^2 + 2ac + 4bc + 4c^2. \end{aligned}$$

The second implies $2 \mid r$, but then from the first equation we know $2 \mid a$, so then $2 \mid b$ from the third equation. However, this means that 4 divides the RHS of the third equation, so $2 \mid t$. This is a contradiction since we assumed $\gcd(r, t) = 1$.

Hence we arrive at a contradiction in all cases, meaning the rank of $E(\mathbb{Q})$ is indeed 0. Therefore Proposition 3 is true, which contradicts Proposition 2. Thus it follows that there cannot exist a rational torsion point of order 11.

# Appendices

## A Projective Geometry

In the $(x, y)$-plane, any two distinct points uniquely define a line. Also, two distinct lines uniquely define a point where they intersect, except when the lines are parallel. To keep things consistent and remove this "non-parallel" condition, we can define the *points at infinity* as the theoretical points where parallel lines intersect. We can't just have one single point at infinity, since that would imply this single point at infinity would lie on all lines, contradicting the fact that any two lines have exactly one point of intersection. We actually need a point at infinity for every distinct direction in the ordinary plane.

We will call this plane consisting of the ordinary plane together with the added points at infinity, the *projective plane*, denoted by $\mathbb{P}^2$. We can write this as

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \left\{\text{directions in } \mathbb{A}^2\right\},$$

where $\mathbb{A}$ represents the affine (Cartesian) plane.

We can now see that in the projective plane, any two lines intersect in exactly one

point, which would be an ordinary point in $\mathbb{A}^2$ if they are not parallel, and a point at infinity corresponding to their common direction if they are parallel. So, in $\mathbb{P}^2$ we can eliminate the notion of parallel lines altogether. Additionally, all the points at infinity lie on a common line, being the *line at infinity* that consists entirely of the points at infinity. Thus, in the projective plane any two distinct points still uniquely define a line. Notationally, we can let $\mathbb{P}^1$ represent the line at infinity so that we can say $\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$.

For a point $(x, y) \in \mathbb{A}^2$, we let $[x : y : 1]$ be the coordinates of its counterpart in $\mathbb{P}^2$, and we let $[x : y : 0]$ in $\mathbb{P}^2$ represent the direction of the line passing through the origin and $(x, y)$ in $\mathbb{A}^2$. In other words, we introduce a third coordinate, letting it be 0 if the point is a point at infinity, and nonzero if it comes from $\mathbb{A}^2$. Then, we define the points $[x : y : z]$ as being equivalent to $[\frac{x}{z} : \frac{y}{z} : 1]$ in $\mathbb{P}^2$, and associate it with the point $(\frac{x}{z}, \frac{y}{z})$ in $\mathbb{A}^2$. In other words, points in $\mathbb{P}^2$ are considered up to a scalar.

This is the connection between the geometric description of $\mathbb{P}^2$ that we give above, to the algebraic description that follows. Rational solutions to the equation

$$x^n + y^n = 1$$

are of the form $(\frac{a}{c}, \frac{b}{c})$, where $a, b, c \in \mathbb{Z}$ and $\gcd(a, c) = \gcd(b, c) = 1$. We can *homogenize* this equation, or in other words, we can introduce a third variable $Z$ so that every term has the same degree, and so that the solution $(a/c, b/c)$ of the first equation corresponds to the integer solution $(a, b, c)$ to the homogenized Fermat equation.

$$X^n + Y^n = Z^n. \tag{2}$$

Homogenization is useful because, as we can see, for any $t \in \mathbb{Z}$ with $t \neq 0$, the triple $(ta, tb, tc)$ is a solution if and only if $(a, b, c)$ is. So when solving equation (2), we can consider $(ta, tb, tc)$ and $(a, b, c)$ as equivalent triples. Thus we get an equivalence relation among the non-trivial solutions to equation (2).

Let $S$ be the set of these non-trivial solutions under the equivalence relation. Then the solutions $(a, b, c)$ in $S$ with $c$ being nonzero map to the solutions $(\frac{a}{c}, \frac{b}{c})$ to the original equation $x^n + y^n = 1$, and correspond to the points $(\frac{a}{c}, \frac{b}{c})$ in $\mathbb{A}^2$, which are $[\frac{a}{c} : \frac{b}{c} : 1]$ in $\mathbb{P}^2$ from our geometric description. The solutions $(a, b, c) \in S$ with $c = 0$ don't correspond to a solution to $x^n + y^n = 1$, and so they correspond to the points $[a : b : 0]$ at infinity in $\mathbb{P}^2$. We can also check that the points in our geometric description of $\mathbb{P}^2$ map injectively to $S$, since a point $(x, y) \in \mathbb{A}^2$ corresponds to the solution $(x, y, 1)$ to equation (2), while a point $[x : y] \in \mathbb{P}^1$ corresponds to the solution $(x, y, 0)$. So $S$ and $\mathbb{P}^2$ are the same.

After developing an understanding of points, we naturally would like to move on to curves. For a curve $C$ in the projective plane, we can consider it as being the union of an ordinary curve $C_0$ in $\mathbb{A}^2$ along with the set of its points at infinity, which are the limiting directions of the tangent lines to $C_0$. For example, if $C_0$ is a hyperbola, then $C$ consists

of $C_0$ along with the directions that the asymptotes of $C_0$ have.

Through homogenization we get an injective mapping from the set of curves in $\mathbb{A}^2$ to the set of curves in $\mathbb{P}^2$ that don't contain the line at infinity. To move in the other direction, we can dehomogenize by fixing one of the variables. For example, let us take the affine cubic $y^2 = x^3 + 1$. This is degree 3, so homogenizing gives the projective curve $Y^2Z = X^3 + Z^3$. This sends the point at infinity on the original curve to the point $[0 : 1 : 0]$ on the projective curve (and lets us work with the point at infinity algebraically). Letting $Z = 1$ lets us dehomogenize and returns the affine curve $y^2 = x^3 + 1$ again. We could also dehomogenize by setting $Y = 1$ to be the line at infinity, which sends our point at infinity to the point $(x, z) = (0, 0)$ on the affine curve $z = x^3 + z^3$. Taking different lines to be the line at infinity essentially gives us overlapping affine curves, that, when taken together, form the projective curve.

I hope this brief tangent provides enough background to understand the rest of the paper. Interested readers can learn more about projective geometry using [1].

# B Algebraic Number Theory

We will list some definitions and results in algebraic number theory that are necessary for Proposition 3 of the proof of the Billing-Mahler theorem. This is only meant to be a short overview, so we will not prove anything or go into much detail; interested readers can refer to an algebraic number theory text such as [4].

**Definition.** *A **number field** is an extension $K$ of the rational numbers $\mathbb{Q}$ with degree $(K : \mathbb{Q})$ being finite. When $(K : \mathbb{Q}) = 3$ it is called a **cubic field**.*

For example, $\mathbb{Q}[\sqrt[3]{2}]$ is a cubic field.

**Definition.** *An **algebraic integer** is a number that is the root of some nonzero monic one-variable polynomial of finite degree.*

For example, $\sqrt{2}$ and $1 + i$ are algebraic integers, while $\pi$ and $e$ are not.

**Definition.** *Let $K$ be a number field. The **ring of integers** $\mathcal{O}_K$ is the set of algebraic integers of $K$. In other words, $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$, where $\overline{\mathbb{Z}}$ is the set of algebraic integers.*

**Definition.** *For a number field $K$ and its ring of integers $\mathcal{O}_K$, a **fundamental unit** is a generator for the group of units of $\mathcal{O}_K$, when this group of units has rank 1.*

By Dirichlet's unit theorem, the unit group has rank 1 if and only if the number field is either a real quadratic field, a complex cubic field, or a purely imaginary quartic field. (The number field used in our proof of Billing-Mahler is a complex cubic field.) Readers can learn more about Dirichlet's unit theorem from Section 1.7 of [4].

**Definition.** *For a commutative ring $(R, +, \times)$, an **ideal** is an additive subgroup of $R$ such that for all $r \in R$ and $x \in I$, the product $rx$ is in $I$.*

For example, the multiples of 5 in $\mathbb{Z}$ (denoted by $5\mathbb{Z}$) is an ideal of $\mathbb{Z}$.

**Definition.** *Let $R$ be a commutative ring and let $\mathfrak{p}$ be an ideal in $R$. This ideal is called **prime** if it satisfies the condition that if $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of $R$ with $\mathfrak{ab} \subset \mathfrak{p}$, then either $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$.*

**Definition.** *An ideal is **principal** if it can be generated by a single element.*

For example, the ideal $5\mathbb{Z}$ is principal (generator being 5).

**Definition.** *Let $R$ be a commutative ring with no zero divisors (product of nonzero elements is nonzero). If $I$ is an $R$-submodule of the field of fractions of $R$ such that there exists an $r \in R$ with $rI \in R$, then $I$ is a **fractional ideal**.*

In the above definition, multiplication by $r$ can be thought of as "clearing the denominators."

**Definition.** *Let $K$ be a number field, and let $\mathcal{O}_K$ be its ring of integers. Let $J_K$ be the group of fractional ideals of $\mathcal{O}_K$, and let $P_K$ be the subgroup of $J_K$ containing the principal ideals. Then the **ideal class group** of $K$ is the quotient group $J_K/P_K$. This group is finite, and its order is called the **class number** of $K$.*

If the class number of a number field $K$ is 1, then the ring of integers $\mathcal{O}_K$ is a principal ideal domain, meaning that every ideal is principal.

For example, $\mathbb{Z}$ and $\mathbb{Z}[\omega]$, where $\omega$ is a primitive third root of unity, have class number 1 and have trivial ideal class groups. On the other hand, the class group of $\mathbb{Z}[\sqrt{-5}]$ is cyclic of order 2.

Since principal ideal domains are also unique factorization domains, we also know that every ideal in a number field with class number 1 has a unique factorization (up to order) into powers of prime ideals. We may also obtain divisibility rules on the ideals from here.

Finally, we take a look at the norm of elements and ideals in a field extension. First we require some terms from Galois theory:

**Definition.** *Let the field $L$ be a finite extension of of an arbitrary field $K$. Then the **Galois group** of $L$ over $K$, denoted by $\mathrm{Gal}(L/K)$, is the group of automorphisms on $L$ that fix $K$. In other words, it is the group*

$$\{\sigma : L \hookrightarrow L \mid \sigma(x) = x \text{ for all } x \in K\}.$$

**Definition.** *For a field $K$, the finite extension $L/K$ is a **Galois extension** if the order of the Galois group is equal to the degree of the extension, i.e. $|\mathrm{Gal}(L/K)| = (L : K)$.*

**Definition.** *For a field $K$ and a finite extension $L$ of $K$, the field $L$ is a finite dimensional vector space over $K$, and multiplication by an $\alpha \in L$ is a $K$-linear transformation from $L$ to itself. Then the* ***norm*** *of $\alpha$, denoted by $N_{L/K}(\alpha)$, is defined as the determinant of this linear transformation.*

When $L/K$ is a Galois extension, the norm of $\alpha$ is the product of the roots of the minimal polynomial of $\alpha$ over $K$. This is equivalent to saying

$$N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

The norm is a group homomorphism from $L^\times$ to $K^\times$. In other words, for $\alpha$ and $\beta$ in $L^\times$, we have

$$N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta).$$

Furthermore, for $\alpha \in \mathcal{O}_K$, the norm $N_{L/K}(\alpha)$ is $\pm 1$ if and only if $\alpha$ is a unit in $\mathcal{O}_K$.

We can define a generalization of this norm for ideals in the field extension. In our conditions, where all ideals are principal and $L/K$ is a Galois extension, we have

$$N_{\mathcal{O}_L/\mathcal{O}_K}(\mathfrak{a}) = K \cap \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\mathfrak{a}),$$

for some ideal $\mathfrak{a}$ in the set of nonzero fractional ideals of $\mathcal{O}_L$. This norm for ideals is compatible with the norm for elements, so

$$|N_{L/K}(x)| = N_{\mathcal{O}_L/\mathcal{O}_K}(x\mathcal{O}_K)$$

for all elements $x \in L$ and the corresponding ideals $x\mathcal{O}_K$. By abuse of notation we write $N_{L/K}$ in the place of $N_{\mathcal{O}_L/\mathcal{O}_K}$.

# References


[1] H.S.M. Coxeter. *Projective Geometry.* Springer, 2003.

[2] É. Lutz. Sur l'équation $y^2 = x^3 - ax - b$ dans les corps p-adiques. *J. Reine Angew. Math.*, 1937.

[3] T. Nagell. Sur les propriétés arithmétiques des cubiques planes du premier genre. *Acta Mathematica*, pages 93–126, 1928.

[4] J. Neukirch. *Algebraic Number Theory.* Springer, 1999.

[5] J.H. Silverman and J.T. Tate. *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics. Springer, 2015.