Classification of Torsion Subgroups for Mordell Curves

By

Zachary Porat

* * * * * * * * *

Submitted in partial fulfillment of the requirements for

Honors in the Department of Mathematics

Union College

March 2020

Abstract

PORAT, ZACHARY Classification of Torsion Subgroups for Mordell Curves

Department of Mathematics, March 2020

ADVISOR: HATLEY, JEFFREY

Elliptic curves are an interesting area of study in mathematics, laying at the intersection of algebra, geometry, and number theory. They are a powerful tool, having applications in everything from Andrew Wiles' proof of Fermat's Last Theorem to cybersecurity. In this paper, we first provide an introduction to elliptic curves by discussing their geometry and associated group structure. We then narrow our focus, further investigating the torsion subgroups of elliptic curves. In particular, we will examine two methods used to classify these subgroups. We finish by employing these methods to categorize the torsion subgroups for a specific family of elliptic curves known as Mordell curves.

Acknowledgement

A special thank you to my advisor, Jeff Hatley. Without your guidance, both mathematically and on the rock climbing wall, this thesis would not have been possible. I am immensely grateful for your patience and mentorship throughout this process and beyond. Merci!

Notation

We shall use the following notation throughout this paper:

$\mathbb{N} = \{1, 2, 3, \ldots\}$ is the set of natural numbers.

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is the group of integers.

$\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\}$ is the field of rational numbers.

$\mathbb{R}$ is the field of real numbers.

$\mathbb{C} = \{a + bi : a, b \in \mathbb{R},\ i^2 = -1\}$ is the field of complex numbers.

Contents

1. Introduction to Elliptic Curves

Elliptic curves are an interesting area of study, laying at the intersection of algebra, geometry, and number theory. They are a powerful tool, famously being used in Andrew Wiles' proof of Fermat's Last Theorem [Wil95] for example, while remaining relatively accessible for junior mathematicians. The aim of this paper is to first provide an overview of elliptic curves and then dive more deeply into their characteristics, primarily focusing on their so-called torsion subgroups for a specific family of curves known as Mordell curves.

1.1. **Definition and Geometry.**

In order to begin our discussion of elliptic curves, we must first construct them. Let's start with an arbitrary cubic curve in the following form:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \tag{1.1}$$

We will assume this cubic is rational, meaning that its coefficients are rational numbers. Even with this constraint, the generalized equation (1.1) is still unwieldy to work with. We need ten (rational) coefficients just to define the curve! It would be nice if we could find a method to simplify the equation for a cubic curve. Enter **Weierstrass normal form**. Curves in this form have the following general equation:

$$y^2 = x^3 + ax^2 + bx + c \tag{1.2}$$

We obtain this simplified form from (1.1) by performing a series of transformations. These transformations also allow us to depict the cubic curve in the

affine plane such that the curve is always oriented symmetrically with respect to the x-axis.

Note, in order to obtain this symmetry, we actually have to work with curves in the projective plane defined over the field of rational numbers, $\mathbb{P}^2(\mathbb{Q})$. As a result, we pick up an additional rational point on the curve called the **point at infinity**, denoted by $\mathcal{O}$.[1] A complete explanation of the transformation process can be found in [ST15, §1.3].

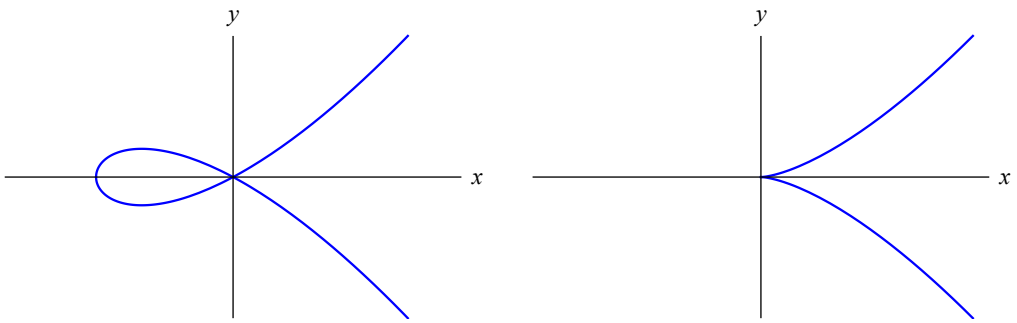
Remark 1.1.1. Any cubic with at least one rational point can be expressed in this form. Thus, for the remainder of this paper, we will assume all curves are presented in Weierstrass normal form.

Before we introduce the definition of an elliptic curve, we also need to make the following distinction. We consider a projective curve $C : F(X, Y, Z) = 0$ to be **singular** at a point $P \in C$ if and only if

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

In other words, C is singular at a point P if the tangent line at the point vanishes. Equivalently, P is a singular point on C if F has a repeated root at P. Otherwise, we say that C is **nonsingular** at P. If C is nonsingular at every point, we say that C is a **smooth** (or nonsingular) curve. Geometrically speaking, smooth curves have no cusps or self-intersections, which is why every point on the curve has a well-defined tangent line.

[1] In projective space, lines that are parallel in the affine plane actually intersect at a so-called point at infinity. For a cubic, we have one such point, which corresponds to the projective point $[0 : 1 : 0]$ on the projectivized curve. Shortly, we will understand the importance of this point in relation to the group structure of elliptic curves.



(A) $y^2 = x^3 + 3x^2$ (B) $y^2 = x^3$

FIGURE 1. Two of the three possible types of singular curves.

In contrast, there also exist singular curves, the opposite of smooth curves. Singular curves come in three variants, two of which are shown in Figure 1. Unlike smooth curves, singular curves have drastically different behavior because of their unsavory properties.

Motivated by our simplifications of the general cubic equation and with this distinction dispatched, we arrive at the following definition:

Definition 1.1.2. An **elliptic curve** is the set of solutions, including the point at infinity $\mathcal{O}$, which satisfy the following equation:

$$y^2 = x^3 + ax^2 + bx + c \tag{1.3}$$

where $a, b, c \in \mathbb{Z}$ and the curve is nonsingular. An example of an elliptic curve is shown in Figure 2.

The condition that the curve be smooth is vital when defining an elliptic curve. While we could look at a curve graphically to determine smoothness and consequently, elliptic curve eligibility, an efficient computational test would be a helpful tool. (Of course, we could compute the partial derivatives, set them

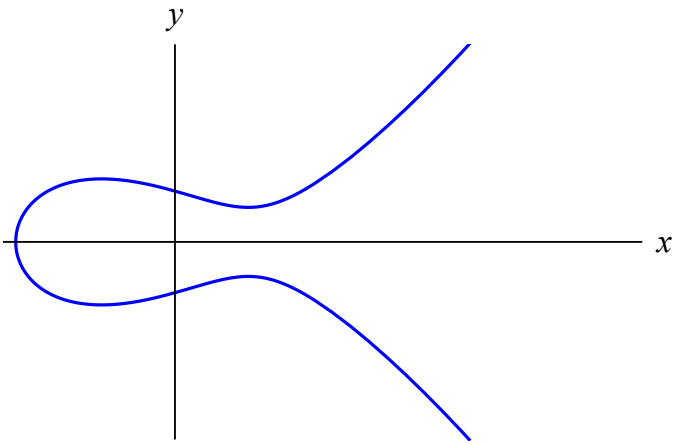


FIGURE 2. The elliptic curve $y^2 = x^3 - 5x + 8$.

equal to zero, and solve for potential singular points, but doing so is hardly efficient.) Such a test exists and involves the discriminant of the equation for a cubic curve.

This notion of a discriminant for a curve should not be wholly unfamiliar. Recall that there exists such a quantity for a quadratic curve with equation $ax^2 + bx + c = 0$ and $a \neq 0$. For this type of curve, the discriminant is the quantity given by

$$b^2 - 4ac.$$

The discriminant can be positive, zero, or negative, and this determines how many solutions there are to the given quadratic equation. In particular, a discriminant of zero indicates that the quadratic has a repeated real number solution.

The discriminant for a cubic curve plays the same role; if it is zero, then the cubic has a repeated root. We know that if the curve has a repeated root, then there is at least one point at which the partial derivatives simultaneously vanish and therefore, the curve is not smooth. Thus, the discriminant offers

an alternative to calculating the partial derivatives when verifying smoothness for a given curve.

Definition 1.1.3. The **discriminant** of a curve E is defined as the following quantity:

$$\Delta_E = -16(4a^3c - a^2b^2 - 18abc + 4b^3 + 27c^2)$$

A curve is smooth if and only if $\Delta_E \neq 0$.

1.2. **Binary Operations.** The previous section laid the groundwork for understanding elliptic curves by providing a geometric interpretation of their structure. In this section, we dive more deeply into their geometry, while hinting at their algebraic connection. In particular, we can define a binary operation between points on elliptic curves. Doing so allows us to relate curves back to group theory, a subject area we understand well.

Let P and Q be two rational points on an elliptic curve, i.e. $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are solutions to (1.3). Then, the secant line that passes through both P and Q, call it $\mathcal{L}$, must intersect the cubic at a third point. We let $P * Q$ denote this third point of intersection. Importantly, $P * Q$ is also a rational point. We explicitly find the relationship between the coordinates of P, Q, and $P * Q$ in Section 1.3, which supports these claims. See (1.5) for confirmation.

If $P = Q$, then we define $\mathcal{L}$ to be the tangent line to the curve at P. Thus, $P * P$ is the point of intersection of the tangent line with the curve. Note, this tangent line is always defined because we previously established that elliptic curves are always smooth curves, which have well-defined tangent lines for every point. The binary operation $*$ is shown in Figure 3.

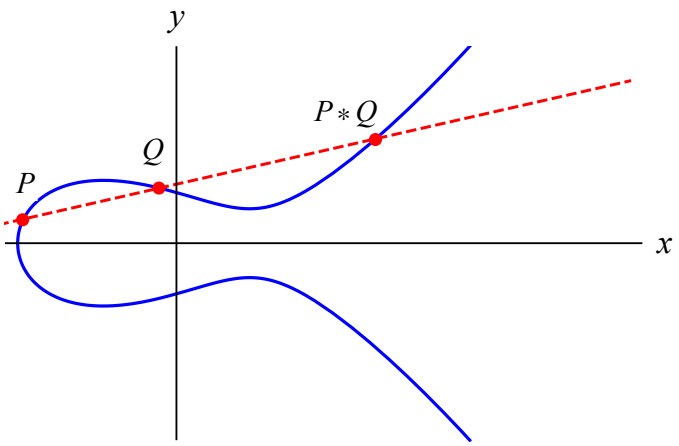


FIGURE 3. The binary operation $*$ on points P and Q.

Now we are going to define another binary operation $+$ in terms of the previously-established operation $*$. Again, let P and Q be rational points on an elliptic curve. Then, define $P + Q = \mathcal{O} * (P * Q)$ where $\mathcal{O}$ is the point at infinity. Graphically, we can interpret drawing a line through $\mathcal{O}$ and $P * Q$ as drawing a vertical line through the point $P * Q$. We define the point of intersection between the vertical line and the elliptic curve to be $P + Q$. Since our curves are symmetric about the x-axis, this is equivalent to simply reflecting $P * Q$ across the x-axis. The process of finding $P + Q$ graphically is shown in Figure 4.

1.3. **Duplication Formula.** While the process for finding $P + Q$ graphically is fairly straightforward, it would be helpful to have a method for finding it computationally. Let us start by explicitly defining points on our elliptic curve. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points on an elliptic curve. Let $P * Q = (x_3, y_3)$. Then, because of our earlier graphical argument, we also have $P + Q = (x_3, -y_3)$. Our goal is to calculate x_3 and y_3 in terms of known quantities, so that we can easily determine $P + Q$. We define the line through

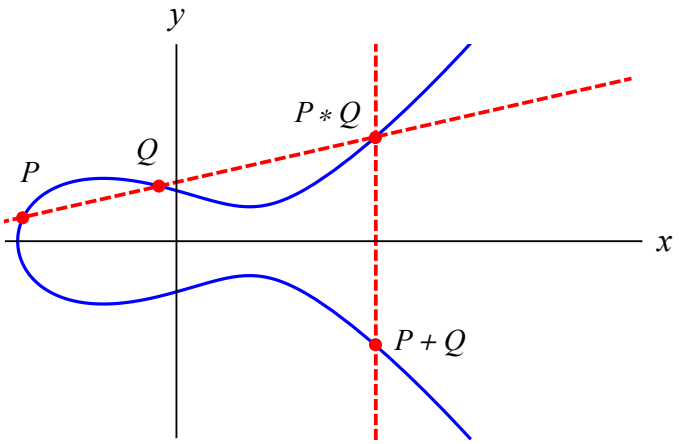


FIGURE 4. The process for defining the point $P + Q$.

P and Q, which we previously called $\mathcal{L}$, as follows:

$$\mathcal{L} : y = \lambda x + \nu, \quad \text{where} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2. \tag{1.4}$$

To find the third point of intersection with the elliptic curve, we substitute the equation for $\mathcal{L}$ from (1.4) into (1.3) to find

$$y^2 = (\lambda x + \nu)^2 = x^3 + ax^2 + bx + c.$$

Moving everything to one side and expanding the binomial, we have

$$0 = x^3 + ax^2 + bx + c - (\lambda^2 x^2 + 2\lambda\nu x + \nu^2).$$

Factoring and rearranging, we find

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2).$$

Note, this is just a cubic in x. Therefore, its three roots, x_1, x_2, x_3 give us the x-coordinates of the three intersection points with $\mathcal{L}$. Thus, we can rewrite

the left side of the equation as

$$(x - x_1)(x - x_2)(x - x_3) = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2). \quad (1.5)$$

To find x_3, we can equate the coefficients for each term in the polynomial on the left side and the right side of (1.5). After expanding the left side, we determine that the coefficients for the x^2 terms in particular give the following equality:

$$a - \lambda^2 = -x_1 - x_2 - x_3.$$

Thus, we arrive at an equation for x_3:

$$x_3 = \lambda^2 - a - x_1 - x_2.$$

This value for x_3 can then be substituted into $\mathcal{L}$, the equation for y in terms of x, to find an equation for y_3:

$$y_3 = \lambda x_3 + \nu.$$

Thus, we have found a method for computing x_3 and y_3 using known quantities. Let's see a brief example.

Example 1.3.1. Examine the curve $y^2 = x^3 + 9$ with rational points $P = (-2, 1)$ and $Q = (0, 3)$. First, we find the line $\mathcal{L}$ through P and Q:

$$y = x + 3, \quad \text{so} \quad \lambda = 1 \quad \text{and} \quad \nu = 3.$$

Now we have all we need to solve for x_3 and y_3. So, we have

$$x_3 = \lambda^2 - x_1 - x_2 = 3 \quad \text{and} \quad y_3 = \lambda x_3 + \nu = 6.$$

Thus, we find $P + Q = (x_3, -y_3) = (3, -6)$. ■

While this general method is helpful, we more specifically want to focus on the case when $P = Q$ so that we can find a finite multiple of P. In this case, we will derive a formula to find the x-value for $P + P = 2P$.

Let us start with the point $P = (X, Y)$. We want to find $2P = P + P = \mathcal{O} * (P * P)$. We can no longer find λ as in the previous case where we had distinct points, because the value would be undefined. Instead, recall that when we apply the $*$ binary operation to a single point, the resulting point $P * P$ is the point of intersection of the tangent line with the elliptic curve. We can find an equation for this tangent line to the cubic by using the curve's equation:

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

If we implicitly differentiate, we can find the slope of the tangent line:

$$\lambda = \frac{dy}{dx}(P) = \frac{f'(X)}{2Y}.$$

Let's return to our previous example.

Example 1.3.2. Again we will look at the curve $y^2 = x^3 + 9$, but this time, we will only work with $P = (-2, 1)$. Our goal is to compute $2P$. First, we find the slope of the tangent line:

$$\lambda = \frac{f'(X)}{2Y} = \frac{f'(-2)}{2} = \frac{12}{2} = 6$$

Since the tangent line passes through P, we can find ν:

$$\nu = Y - \lambda X = 1 - (6)(-2) = 13$$

With values for λ and ν, we have the needed information to compute x_3 and y_3. Plugging in, we find

$$x_3 = \lambda^2 - x_1 - x_2 = 36 - (-2) - (-2) = 40 \quad \text{and}$$

$$y_3 = \lambda x_3 + \nu = (6)(40) + 13 = 253.$$

Thus, we find $P + P = 2P = (x_3, -y_3) = (40, -253)$. ■

For our purposes, it will be helpful to have an explicit expression for $2P$ in terms of the coordinates of P. Substituting $\lambda = f'(X)/2Y$ into the formulas from above, simplifying over a common denominator, and replacing Y^2 with $X^3 + aX^2 + bX + c$, we arrive at the following:

$$x\text{-coordinate of } 2(X, Y) = \frac{X^4 - 2bX^2 - 8cX + b^2 - 4ac}{4(X^3 + aX^2 + bX + c)}.$$

This formula for $x(2P)$ is called the **duplication formula**. Let us quickly verify our result from the previous example. Since $y^2 = x^3 + 9$, we have coefficients $a = b = 0$ and $c = 9$. Thus, we have

$$x\text{-coordinate of } 2P = \frac{X^4 - 8cX}{4(X^3 + c)} = \frac{(-2)^4 - 8(9)(-2)}{4\left((-2)^3 + 9\right)} = \frac{160}{4} = 40$$

which is indeed the same value. With the duplication formula in hand, finding the formula for $y(2P)$ is straightforward and left to the reader.

1.4. **Group Structure.** Recall that we are searching for an algebraic interpretation of elliptic curves. Ideally, we want to connect them back to groups, a well-understood subject. So, it would be nice to show that the binary operation $+$, with the rational points on the curve E, form a group. In order to

form a group, four properties must be satisfied. We will show that $+$ on the curve does in fact satisfy all these properties.

1. **Closure:** From the previous examples, it is easy to see that $(E, +)$ is closed. So long as we start with a point on the elliptic curve in a specific field, the binary operation, when applied to two points on the curve, produces another point on the curve.
2. **Identity:** As one might suspect, the identity element is the point at infinity, $\mathcal{O}$. For points P and Q on the elliptic curve, $P + Q = \mathcal{O} * (P * Q)$. Thus, for an arbitrary point P on the elliptic curve, $\mathcal{O} + P = \mathcal{O} * (\mathcal{O} * P)$. The right-hand-side of this equation simply reflects P over the x-axis twice, which returns it to its original position. Thus, $\mathcal{O}+P = P$ for any P on the elliptic curve. Therefore, an identity element exists for the group.
3. **Inverse:** To show the existence of inverses, we start with an arbitrary point P on the elliptic curve. Then, we reflect P across the x-axis and suggestively notate this new point $-P$. Applying the binary operation, we have $P + (-P) = \mathcal{O} * (P * (-P))$. $P * (-P)$ is just a vertical line graphically. This implies that $P * (-P)$ only intersects the point at infinity. Therefore, $P * (-P) = \mathcal{O}$. Since $\mathcal{O} * \mathcal{O} = \mathcal{O}$, $P + (-P) = \mathcal{O}$. Thus, $-P$ is the inverse of P.
4. **Associativity:** Proving associativity is much more difficult than the previous three properties. So instead, we will present a graphical demonstration of the property in Figure 5. This provides a fairly convincing argument that is easier to understand than the proof. For those unsatisfied, the complete proof can be found in [ST15, §1.2]. Note, it

suffices to show that $P*(Q+R) = (P+Q)*R$ because we can simply reflect this point over the x-axis to obtain $P+(Q+R) = (P+Q)+R$. (Thankfully this is the case, as it prevents adding yet another line to the figure.)

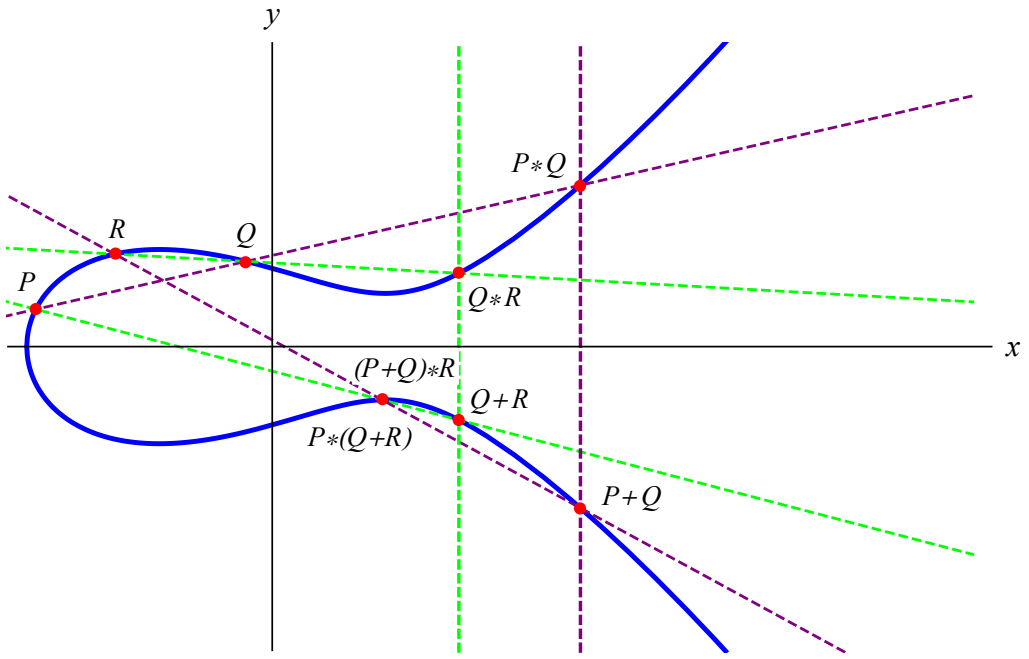


FIGURE 5. A graphical interpretation of the associativity property.

While knowing that an elliptic curve E with the binary operation $+$ forms a group is a helpful piece of information, we can in fact conclude something even more remarkable. Since we analyze the set of points on the curve over the field of rational numbers, denoted $E(\mathbb{Q})$, the set of points form an abelian group that is finitely generated. This idea was conjectured by Henri Poincaré in 1908 [Poi08], and proved by Louis Mordell in 1922 [Mor22], with a generalization provided by André Weil in 1928 [Wei28].

Theorem 1.4.1 (Mordell-Weil)**.** *$E(\mathbb{Q})$ is a finitely generated abelian group. In other words, there are points $P_1, \ldots, P_n$ such that any other point Q in $E(\mathbb{Q})$ can be expressed as a linear combination*

$$Q = a_1P_1 + a_2P_2 + \cdots + a_nP_n$$

for some $a_i \in \mathbb{Z}$.

While the complete proof of this theorem is not in the scope of this paper, it is easy to show commutativity for $+$, thus proving $E(\mathbb{Q})$ is an abelian group. Clearly, $*$ is commutative. There exists one secant line between two points on the curve, so the intersection between this line and the curve always occurs at the same point. Since $+$ simply takes these intersection points and reflects them across the x-axis, it immediately follows that $+$ is commutative too. We still present the theorem in its entirety because the result is useful. A complete proof can be found in [Sil86, Thm. VIII.6.7].

1.5. **Torsion Subgroup.** With this information, we can now start discussing particularly interesting points on the elliptic curve called torsion points.

Definition 1.5.1. The **torsion points** of an elliptic curve are defined as follows:

$$E(\mathbb{Q})_{\text{tors}} = \{P \in E(\mathbb{Q}) \,:\, \text{there is } n \in \mathbb{N} \text{ such that } nP = \mathcal{O}\}.$$

Here, n is known as the **(finite) order** of the point P.

First, we note that $E(\mathbb{Q})_{\text{tors}} \subset E(\mathbb{Q})$. Since $E(\mathbb{Q})$ is a finitely generated abelian group from the Mordell-Weil theorem, we recognize that $E(\mathbb{Q})_{\text{tors}}$ must

be finite, in addition to being abelian. Recall from group theory that any finite abelian group is isomorphic to a cyclic group $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$ or a direct sum of these cyclic groups. Naturally, the following question arises:

Question 1.5.2. What are the possible groups to which $E(\mathbb{Q})_{\text{tors}}$ can be isomorphic?

Throughout this paper, we aim to answer this question for one specific (infinite) family of curves. By doing so, we hope to gain an understanding of what this question entails and what the answer might look like generally. With our background in elliptic curves complete, let's begin investigating the subgroups formed by torsion points.

2. Methods for Classifying Torsion

In order to classify the torsion of specific elliptic curves, we use two main strategies: the Nagell-Lutz Theorem and the Reduction Modulo ℓ Method. Both have distinct purposes, so we will introduce each individually. However, when used in conjunction, these two methods can help us efficiently understand torsion for different families of curves.

2.1. Nagell-Lutz Theorem.

Discovered by Trygve Nagell and Élisabeth Lutz, two mathematicians working independently in the 1930s, the Nagell-Lutz theorem is a powerful tool when analyzing torsion subgroups as it provides a framework for rational points of finite order. Importantly, it provides torsion-point candidates.

Before we state the Nagell-Lutz theorem, we need some additional information. First, we will use the following proposition, also proved by both Nagell [Nag35] and Lutz [Lut37].

Proposition 2.1.1. *On an elliptic curve E, a rational point (X, Y) that has finite order must have integer coordinates.*

The proof of this proposition is quite long. Additionally, while the result is interesting, we care more about the computational benefits of the Nagell-Lutz theorem. Thus, we will merely state this proposition to use in our proof. For the curious reader, [ST15, §2.4] covers how to prove this result.

In order to prove the Nagell-Lutz theorem, we still need one other piece of information provided in the following theorem.

Theorem 2.1.2. *Let E be an elliptic curve given by the equation*

$$E : y^2 = x^3 + ax^2 + bx + c \qquad a, b, c \in \mathbb{Z}.$$

A point $P = (X, Y) \neq \mathcal{O}$ on E has order two if and only if $Y = 0$.

Proof. We begin the proof by assuming $P = (X, Y) \neq \mathcal{O}$ on E has order two. Recalling the definition of order, this is equivalent to $2P = \mathcal{O}$. By the definition of inverse elements, $2P = \mathcal{O}$ if and only if $P = -P$. From our discussion of the group structure, we know that $-P$ is just the reflection of P across the x-axis. Therefore, $y(-P) = -Y$. Since $P = -P$, we also have $Y = y(-P)$. By substitution, $Y = -Y$, which can only occur when $Y = 0$. □

With these two preliminary results, we now can state and prove the Nagell-Lutz Theorem.

Theorem 2.1.3 (Nagell-Lutz, [Nag35], [Lut37]). *Let E be an elliptic curve given by the equation*

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

Let $P = (X, Y)$ be a point of finite order on E. Then, $2P = \mathcal{O}$ or $Y^2 \,\big|\, \Delta_E$.

Proof. Let E be an elliptic curve as defined above. Let $P = (X, Y)$ be a rational point of finite order on E. By Prop. 2.1.1, P must have integer coefficients, i.e. $X, Y \in \mathbb{Z}$. Let P be of finite order greater than 2; by Thm. 2.1.2, $Y \neq 0$. By the duplication formula, we have:

$$x(2P) = \frac{\phi(X)}{4f(X)} = \frac{X^4 - 2bX^2 - 8cX + b^2 - 4ac}{4(X^3 + aX^2 + bX + c)}$$

Since P is a rational point of finite order, so too is $2P$. Thus by Prop. 2.1.1, $x(2P) \in \mathbb{Z}$. Substituting $Y^2 = f(X)$, we see that since $x(2P) \in \mathbb{Z}$ and is equivalent to a fraction, the numerator must divide denominator. So, $Y^2 \,\big|\, \phi(X)$. Since $P = (X, Y)$ is on the curve $y^2 = f(x)$, in particular $Y^2 = f(X)$. Therefore, we clearly have that $Y^2 \,\big|\, f(X)$. By a generalized version of Bézout's theorem from basic number theory, there exist polynomials $F(x)$ and $\Phi(x)$ with integer coefficients so that

$$F(x)f(x) + \Phi(x)\phi(x) = \Delta_E.$$

Given that these polynomials exist for all $x \in E$, they exist for $x = X$ in particular. So, we have

$$F(X)f(X) + \Phi(X)\phi(X) = \Delta_E.$$

Since $F(x), f(x), \phi(x), \Phi(x)$ all have integer coefficients, the values $F(X)$, $f(X), \phi(X), \Phi(X)$ are all integers. Thus, since $Y^2 \,\big|\, f(X)$ and $Y^2 \,\big|\, \phi(X)$, then $Y^2 \,\big|\, \Delta_E$ as desired. $\square$

For the remainder of this paper, we will only be looking at curves of the form $y^2 = x^3 + Ax + B$. This simplifies the statement of the Nagell-Lutz Theorem.

Corollary 2.1.4. *Let E be an elliptic curve in short Weierstrass form:*

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}.$$

Then, every torsion point $P = (X, Y) \neq \mathcal{O}$ of E satisfies:

(1) If P is a point of order $n \geq 3$, then Y^2 divides $4A^3 + 27B^2$.

(2) If P is of order 2, then $Y = 0$ and $X^3 + AX + B = 0$.

Proof. The first result is easily obtained by substituting $a = 0, b = A, c = B$ into the discriminant equation and applying Thm. 2.1.3. The second result follows immediately from Thm. 2.1.2 and the fact that $Y^2 = X^3 + AX + B$. $\square$

2.2. **Reduction Modulo ℓ Method.** The Nagell-Lutz Theorem is useful when looking at specific curves, as it allows us to find potential torsion points. What if we want to examine torsion more generally, say for a family of curves? In this case, we use the Reduction Modulo ℓ Method.

Up until this point, we have defined elliptic curves over the field of rational numbers $\mathbb{Q}$. However, we are not restricted to only defining them over this field. In fact, elliptic curves can be defined over any field, including $\mathbb{F}_\ell$, the finite field of size ℓ, i.e.

$$\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z} = \{a \mod \ell \,:\, a = 0, 1, 2, \ldots, \ell - 1\}.$$

As with elliptic curves over $\mathbb{Q}$, when defined over $\mathbb{F}_\ell$, the curve needs to be given by a cubic equation and the curve needs to be smooth.

So long as these conditions are met, we can still ask for solutions to our cubic equation. Furthermore, the algebraic equations for the group operation will also still hold in $\mathbb{F}_\ell$ provided that ℓ is a **prime of good reduction**. A prime is considered to be of good reduction if and only if $\Delta_E \not\equiv 0 \mod \ell$, i.e. $\ell \nmid \Delta_E$. One way to obtain an elliptic curve defined over $\mathbb{F}_\ell$ is to take an elliptic curve given by an equation with integer coefficients and reduce it modulo ℓ.

For example, let E be an elliptic curve with equation $y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{Z}$, and let $\ell \geq 2$ be a prime number. If we reduce A and B modulo ℓ, then we obtain the equation of a curve $\widetilde{E}$ given by a cubic curve and defined over the field $\mathbb{F}_\ell$. However, just because E is smooth, does not guarantee that the same holds for $\widetilde{E}$ over $\mathbb{F}_\ell$. Only if the reduction curve $\widetilde{E}$ is smooth do we have an elliptic curve over $\mathbb{F}_\ell$. If this is the case, we say that E has **good reduction** modulo ℓ.

Reducing equations modulo primes is a powerful tool because doing so often provides a simpler framework for problem-solving. This, as it turns out, is the case in the realm of elliptic curves, hence the introduction! However, before we see exactly how these reduced curves can help us, we need a bit of notation. First, as previously mentioned, there exist points that provide solutions to the equation for $\widetilde{E}/\mathbb{F}_\ell$. We will denote the set of points which give solutions $\widetilde{E}(\mathbb{F}_\ell)$, where all the coordinates are elements of $\mathbb{F}_\ell$. Second, if we have the abelian group $E(\mathbb{Q})$ and m is a natural number greater than 1, then the points of $E(\mathbb{Q})$ with order dividing m will be denoted $E(\mathbb{Q})[m]$.

Theorem 2.2.1. *Let $E/\mathbb{Q}$ be an elliptic curve, ℓ a prime number, and m a natural number not divisible by ℓ. Suppose that $E/\mathbb{Q}$ has good reduction at ℓ. Then the reduction map modulo ℓ,*

$$E(\mathbb{Q})[m] \longrightarrow \widetilde{E}(\mathbb{F}_\ell),$$

is an injective homomorphism of abelian groups. In particular, the number of elements of $E(\mathbb{Q})[m]$ divides the number of elements of $\widetilde{E}(\mathbb{F}_\ell)$.

Note, the size of the set $\widetilde{E}(\mathbb{F}_\ell)$ is finite. There are at most ℓ choices for X and ℓ choices for Y. Including the point at infinity, this gives us a maximum of $\ell^2 + 1$ possible points. Because of this finite bound on $\widetilde{E}(\mathbb{F}_\ell)$, the latter half of Thm. 2.2.1 is of particular interest to us. Essentially, the reduction map allows us to conclude information about the size of $E(\mathbb{Q})_{\text{tors}}$, while only having to perform a finite number of computations. In turn, we can lessen the workload associated with finding the size of the torsion subgroup for a particular curve (or family of curves) by reducing said curve(s) over a finite field. Since we are focusing primarily on the computation associated with this theorem, we will not present the proof. However, for those interested, a complete proof can be found in [Sil86, Prop. VII.3.1].

3. Torsion Subgroups for Mordell Curves

This section is where we begin to put our strategies to use. Henceforth, we will devote our focus on **Mordell curves**, which are elliptic curves of the form $E_D : y^2 = x^3 + D$, where D is a fixed, nonzero integer. In particular, we are interested in the cases where $D = \pm 1, \pm p, \pm p^2, \pm p^3$ for a prime p.

3.1. **Concrete Examples.** We start with a couple of concrete examples. Once we get a handle on how to work through these problems, we will transition to working more generally with Mordell curves.

Example 3.1.1. Let us start by setting $D = 1$, so we are examining the curve

$$E_1 : y^2 = x^3 + 1.$$

Let $P = (X, Y)$ be a point on the curve; we see if $Y = 0$, then $X = -1$. By Thm. 2.1.2, this is the only non-trivial point of order 2, so all other torsion points must be of order $n \geq 3$. Thus, from Cor. 2.1.4, if P is a torsion point, then $Y \in \mathbb{Z}$ and Y^2 divides the discriminant, so we have $Y^2 \,\big|\, 27$. We find $Y = \pm 1, \pm 3$ as potential Y-values for torsion points. For our equation, $X = 0$ provides a solution when $Y = \pm 1$ and $X = 2$ provides a solution when $Y = \pm 3$. Therefore, we have shown that

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (-1, 0), (2, \pm 3), (0, \pm 1)\}.$$

Thus, $E(\mathbb{Q})_{\text{tors}}$ is an abelian group of order 6, which implies $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/6\mathbb{Z}$.

■

Example 3.1.2. Next, we examine when $D = -1$, which gives us the curve

$$E_{-1} : y^2 = x^3 - 1.$$

By inspection, we see that if $Y = 0$, then $X = 1$. Just like the previous example, this is the only solution with $Y = 0$. By Thm. 2.1.2, this is the only point of order 2, which means all other torsion points must be of order $n \geq 3$.

We find, from Cor. 2.1.4, that in this case too $Y^2 \,\big|\, 27$. Thus, the potential Y-values for torsion points are $Y = \pm 1, \pm 3$.

With so few options, we can simply plug these values into the equation for E_{-1} and solve by hand. Doing so, we do not find any integer solutions for X. Thus, none of the potential values for Y yield torsion points other than $Y = 0$. The torsion subgroup of $E(\mathbb{Q})$ is thus

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (1, 0)\} \simeq \mathbb{Z}/2\mathbb{Z} \qquad \blacksquare$$

3.2. **Results for Distinct Choices of D.** As shown in the previous two examples, computing the torsion subgroup for specific curves is a fairly straightforward process. With these concrete examples under our belt, we now turn our attention to classifying the torsion subgroups for the entire family of curves. This is where the reduction mod ℓ method becomes useful.

Thm. 2.2.1 involves the number of elements of $\widetilde{E}(\mathbb{F}_\ell)$. Since we will be working with this number extensively, we will denote it N_ℓ. Heuristically, we expect N_ℓ to be $\ell + 1$. Consider a generic Mordell curve with equation $y^2 = x^3 + D$. There are ℓ choices of x in $\mathbb{F}_\ell$. For each value X, the polynomial $f(x) = x^3 + D$ gives a value for $f(X) \in \mathbb{F}_\ell$. The probability that a random element in $\mathbb{F}_\ell$ is a perfect square in $\mathbb{F}_\ell$ is $1/2$. If $f(X)$ is a nonzero square mod ℓ, i.e. if there is a $Y \in \mathbb{F}_\ell$ such that $f(X) \equiv Y^2 \not\equiv 0 \mod \ell$, then this gives two points $(X, \pm Y)$ in $\widetilde{E}(\mathbb{F}_\ell)$. If $f(X)$ is not a square modulo ℓ, then there are no points in $\widetilde{E}(\mathbb{F}_\ell)$ with x-coordinate equal to X. Thus,

$$N_\ell \approx \ell \cdot \left(\frac{1}{2} \cdot 2 + \frac{1}{2} \cdot 0 \right) + 1 = \ell + 1,$$

where we have to add 1 in order to account for the point at infinity.

Notice, we assumed that $f(X)$ is random for the sake of our heuristic argument. However, this is not the case because $f(X)$ is in fact given by a specific formula. Consequently, we would expect the estimate to hold true in some, but not all, instances. Ideally, we would have a method for determining at which primes the estimate does actually hold. This motivates the following proposition.

Proposition 3.2.1. *Let $\widetilde{E}$ be the curve $y^2 = x^3 + D$ over $\mathbb{F}_\ell$, and assume that $\ell \nmid \Delta_{\widetilde{E}}$, $\ell \geq 5$, and $\ell \equiv 2 \mod 3$. Then, $\widetilde{E}(\mathbb{F}_\ell)$ has exactly $\ell + 1$ points.*

Proof. Let $\ell \equiv 2 \mod 3$. We know infinitely many such primes exist by Dirichlet's theorem on primes in arithmetic progressions. Let $\mathbb{F}_\ell^\times$ denote the multiplicative group of nonzero elements of the field $\mathbb{F}_\ell$. We note that $\mathbb{F}_\ell^\times$ has $\ell - 1$ elements. Because of our choice for ℓ, $3 \nmid (\ell - 1)$. Thus, $\mathbb{F}_\ell^\times$ has no element of order 3. Therefore, the homomorphism $a \mapsto a^3$ on $\mathbb{F}_\ell^\times$ is one-to-one and onto. Hence, we can use the reverse mapping to conclude that each nonzero element in $\mathbb{F}_\ell$ has a unique cube root. We note that $0 \equiv 0^3 \mod \ell$, so in fact *every* element in $\mathbb{F}_\ell$ has a unique cube root. This implies that for each $Y \in \mathbb{F}_\ell$, the element $Y^2 - D$ in particular has a unique cube root. We cleverly call this root X, which gives a solution (X, Y) satisfying our equation for $\widetilde{E}$. Given the size of $\mathbb{F}_\ell$, we obtain ℓ solutions in this way. Adding the point at infinity, we find that $\widetilde{E}(\mathbb{F}_\ell)$ has $\ell + 1$ points. □

With this proposition in mind, we want to work with the smallest primes ℓ that give us $N_\ell = \ell + 1$. By Prop. 3.2.1, we may take $\ell = 5$.[2] Recall

[2] Naturally, we might be inclined to start with the smallest prime, 2, or the perhaps the first odd prime, 3. However, recalling the definition of the discriminant, we note that for a Mordell curve, $\Delta_{\widetilde{E}} = -16(27D^2) = -2^4(3^3)(D^2)$. Thus, no matter the choice of D, for $\ell = 2$ or $\ell = 3$, ℓ always divides $\Delta_{\widetilde{E}}$, so $\widetilde{E}$ has bad reduction at these primes.

that Thm. 2.2.1 requires curves of good reduction at ℓ. Thus, since we are particularly interested in $D = \pm p, \pm p^2, \pm p^3$, we have to exclude the curves $y^2 = x^3 \pm 5^k$ for $k \in \{1, 2, 3\}$ because the discriminant for these curves is congruent to 0 mod 5.

Since primes (and their squares and cubes) are relatively prime to one another, Thm. 2.2.1 allows us to conclude that the number of elements in $E(\mathbb{Q})[q]$, denoted $\#E(\mathbb{Q})[q]$, for primes $q \neq 5$, divides $N_5 = 6$. We note that the Fundamental Theorem of Finitely Generated Abelian Groups tells us that if $E(\mathbb{Q})[q]$ and $E(\mathbb{Q})[p]$ inject into $\widetilde{E}(F_\ell)$, then so too does $E(\mathbb{Q})[m]$ where $m = pq$ because $E[m] \simeq E[p] \times E[q]$. Thus, it suffices to study $E(\mathbb{Q})[q]$ for each prime q. Therefore, the only remaining group we have to check is $E(\mathbb{Q})[5]$. If we can determine $\#E(\mathbb{Q})[5]$, then we will be able to make an overarching statement about the size of $E(\mathbb{Q})_{\text{tors}}$ for Mordell curves with $D = \pm p, \pm p^2, \pm p^3$, minus the six bad-reduction curves.

The easiest way to evaluate $\#E(\mathbb{Q})[5]$ is by using another prime ℓ where N_ℓ is easily computable. According to Prop. 3.2.1, the next smallest such prime is $\ell = 11$. By Thm. 2.2.1, we know that $\#E(\mathbb{Q})[5]$ divides $N_{11} = 12$, so long as $11 \nmid D$. By Lagrange's theorem, if $E(\mathbb{Q})[p]$ is non-trivial, then p divides $\#E(\mathbb{Q})[p]$.[3] In this case, this implies that 5 divides $N_{11} = 12$. Obviously, this is not true, thus $E(\mathbb{Q})[5]$ must be trivial.

Remark 3.2.2. By invoking N_{11}, we have introduced six more curves of bad reduction, namely those with $D = \pm 11, \pm 11^2, \pm 11^3$. For these values of D, we find that $\Delta_E \equiv 0 \mod 11$, which prohibits us from invoking Thm. 2.2.1. As

[3] This result stems from the fact that for an elliptic curve $E(\mathbb{C})[p] \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Then, since $E(\mathbb{Q})[p]$ is a subgroup of $E(\mathbb{C})[p]$, Lagrange's theorem can be applied.

a result, we have to exclude these six curves, plus the previous six curves of bad reduction with $D = \pm 5, \pm 5^2, \pm 5^3$, when we make our conclusion. We will return to these twelve curves to ensure they agree with the conclusions after completing our analysis.

Based on the previous work, we conclude that the size of the torsion subgroups for Mordell curves with $D = \pm p, \pm p^2, \pm p^3$ and $p \neq 5, 11$ must divide $N_5 = 6$. Note, this result is in line with our two concrete examples. We found $\#E(\mathbb{Q})_{\text{tors}} = 6$ for the Mordell curve with $D = 1$ and $\#E(\mathbb{Q})_{\text{tors}} = 2$ for the curve with $D = -1$, both of which divide $N_5 = 6$.

To divide $N_5 = 6$, if there is any nontrivial torsion, then the size of the torsion subgroup must either be 2, 3, or 6. We want to determine what values of D yield torsion subgroups of these sizes. We can equivalently ask: When does $y^2 = x^3 + D$ have a point of order 2, a point of order 3, or a point of order 6? These two questions are equivalent because the only abelian groups of orders 2, 3, and 6 are cyclic. Note, there exists a point of order 6 if and only if there exists a point of order 2 and a point of order 3.

To classify the torsion subgroups, we start by looking at when a point of order 2 occurs. From Thm. 2.1.2, we know that a point has order two if and only if $Y = 0$. So, setting $Y = 0$, we find:

$$0^2 = X^3 + D \quad \Leftrightarrow \quad X^3 = -D$$

This implies that D must be a cube. So, we conclude that D is a cube if and only if 2 divides the size of the torsion subgroup, i.e. $E(\mathbb{Q})_{\text{tors}}$ has a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Note, this result is in line with both of our concrete

examples. For the case where $D = -1$, we found $\#E(\mathbb{Q})_{\text{tors}} = 2$ and obviously 2 divides 2. For the $D = 1$ case, $\#E(\mathbb{Q})_{\text{tors}} = 6$ and 2 divides 6.

To find when a point of order 3 occurs, we will use the division polynomial $\phi_3 = 3x^4 + 12Dx$. This polynomial is generated by taking the fact that $3P = \mathcal{O}$, which implies $2P = -P$ by the uniqueness of inverse elements, and then using the duplication formula to equate the X-value for $2P$ with that of $-P$. The division polynomial is helpful because its roots give the x-coordinates for points of order 3 over an appropriate field extension of $\mathbb{Q}$. We factor the polynomial and set it equal to zero to find

$$\phi_3 = 0 = 3X(X^3 + 4D).$$

So, $X = 0$ or $X^3 + 4D = 0$. Plugging $X = 0$ into the original equation for the Mordell curve, we find

$$Y^2 = 0^3 + D \quad \Rightarrow \quad Y^2 = D.$$

This implies that if the curve possesses a rational point of order 3 with $X = 0$, then D must be a rational square. The other factor gives us $X^3 = -4D$. By substitution, we have

$$Y^2 = -4D + D = -3D. \tag{3.1}$$

The only values of D that give integer solutions for Y in (3.1) are negative and contain a factor of 3. Since we are focusing on $D = \pm p, \pm p^2 \pm p^3$ and no prime (or its square or cube) contains a factor of 3, this rules out all values except for $D = -3, -27, -81$. However, none of these three D-values give integer solutions for X. So, this factor yields no additional rational points of order 3.

Note, only when D is both a square and a cube can we simultaneously have points of order 2 and order 3. Given our restrictions on D, the only value where this occurs is $D = 1$. Therefore, we conclude the following:

For an elliptic curve E with equation $y^2 = x^3 + D$ with $D = \pm 1, \pm p, \pm p^2, \pm p^3$ and $p \neq 5, 11$ a prime,

$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/6\mathbb{Z} & \text{if } D = 1 \text{ because both 2 and 3 divide } \#E(\mathbb{Q})_{\text{tors}} \text{ which is at most 6} \\ \mathbb{Z}/3\mathbb{Z} & \text{if } D = \square \text{ and } D \neq 1 \text{ because } 3 \mid \#E(\mathbb{Q})_{\text{tors}} \text{ but } 2 \nmid \#E(\mathbb{Q})_{\text{tors}} \\ \mathbb{Z}/2\mathbb{Z} & \text{if } D = \text{cube and } D \neq 1 \text{ because } 2 \mid \#E(\mathbb{Q})_{\text{tors}} \text{ but } 3 \nmid \#E(\mathbb{Q})_{\text{tors}} \\ 0 & \text{otherwise} \end{cases}$$

Now, we return to the twelve bad-reduction curves to confirm that they follow the above result. These are simply concrete curves, so again we will just use the Nagell-Lutz theorem to provide us with candidates for Y and then check these in the equation for the curve. These calculations are tedious, so we will not go through them individually, but the information for the curves with $D = \pm 5, \pm 5^2, \pm 5^3$ can be found in Table 1 below.

D	Possible Y-values	Tors. Points	$\#E(\mathbb{Q})_{\text{tors}}$
5	$\{\pm 1, \pm 3, \pm 5, \pm 15\}$	None	1
-5	$\{\pm 1, \pm 3, \pm 5, \pm 15\}$	None	1
25	$\{\pm 1, \pm 3, \pm 5, \pm 15, \pm 25, \pm 75\}$	$(0, \pm 5)$	3
-25	$\{\pm 1, \pm 3, \pm 5, \pm 15, \pm 25, \pm 75\}$	None	1
125	$\{0, \pm 1, \pm 3, \pm 5, \pm 15, \pm 25, \pm 75, \pm 125, \pm 375\}$	$(-5, 0)$	2
-125	$\{0, \pm 1, \pm 3, \pm 5, \pm 15, \pm 25, \pm 75, \pm 125, \pm 375\}$	$(5, 0)$	2

TABLE 1

We see that these results do indeed match our general conclusion regarding the classification of the torsion subgroups. For D neither a square nor a cube, the torsion is trivial. For D a square, $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z}$. For D a cube, $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$.

We can show the same for the curves with $D = \pm 11, \pm 11^2, \pm 11^3$. Table 2 shows these results.

D	Possible Y-values	Tors. Points	$\#E(\mathbb{Q})_{\text{tors}}$
11	$\{\pm 1, \pm 3, \pm 11, \pm 33\}$	None	1
-11	$\{\pm 1, \pm 3, \pm 11, \pm 33\}$	None	1
121	$\{\pm 1, \pm 3, \pm 11, \pm 33, \pm 121, \pm 363\}$	$(0, \pm 11)$	3
-121	$\{\pm 1, \pm 3, \pm 11, \pm 33, \pm 121, \pm 363\}$	None	1
1331	$\{0, \pm 1, \pm 3, \pm 11, \pm 33, \pm 121, \pm 363, \pm 1331, \pm 3993\}$	$(-11, 0)$	2
-1331	$\{0, \pm 1, \pm 3, \pm 11, \pm 33, \pm 121, \pm 363, \pm 1331, \pm 3993\}$	$(11, 0)$	2

TABLE 2

These too agree with our more general results. Again, we find trivial torsion when D is neither a square nor a cube. When D is a square, we have $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z}$ and when D is a cube, $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$.

Thus, we have completed classifying the torsion for Mordell curves when $D = \pm 1, \pm p, \pm p^2, \pm p^3$ for a prime p. To recap, we found

$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/6\mathbb{Z} & \text{if } D = 1 \\ \mathbb{Z}/3\mathbb{Z} & \text{if } D = \square \text{ and } D \neq 1 \\ \mathbb{Z}/2\mathbb{Z} & \text{if } D = \text{cube and } D \neq 1 \\ 0 & \text{otherwise} \end{cases}$$

This brings us to the final section. Up to this point, we have focused on particular flavors of D because we had insider knowledge. We knew that investigating these specific D-values would yield an array of torsion subgroup classifications. Moreover, they lead us to the conjecture that in general for all D's, a similar pattern will hold.

3.3. **General Results for All Mordell Curves.** To conclude, let's prove this conjecture for all Mordell curves. First, we will state the idea formally, and then prove it using a similar strategy to that found in [Kna92, Thm. 5.3].

Theorem 3.3.1. *Let E be the elliptic curve $y^2 = x^3 + D$ with $D \in \mathbb{Z}$ and with D assumed sixth-power free. Then*

$$E(\mathbb{Q})_{tors} \simeq \begin{cases} \mathbb{Z}/6\mathbb{Z} & \text{if } D = 1 \\ \mathbb{Z}/3\mathbb{Z} & \text{if } D = -432 = -2^4 3^3, \text{ or if } D = \square \text{ and } D \neq 1 \\ \mathbb{Z}/2\mathbb{Z} & \text{if } D = \text{cube and } D \neq 1 \\ 0 & \text{otherwise} \end{cases}$$

Note, the requirement that D be sixth-power free is just a technicality that ensures D is as simple as possible. If an elliptic curve E over a field K is in short Weierstrass form with equation $y^2 = x^3 + Ax + B$, the only change of variables that preserves this form is $x = u^2 x'$ and $y = u^3 y'$ for $u \in \overline{K}^\star$ where $\overline{K}^\star$ is an extension of K. This change of variables implies $B = u^6 B'$ and $\Delta_E = u^{12} \Delta'_E$. So, if B is not sixth-power free and therefore the discriminant is not minimal, we could use this change of variables to reduce them. With this technicality addressed, we can now begin the proof of Thm. 3.3.1.

Proof. The main step in the proof is to show that $\#E(\mathbb{Q})_{\text{tors}}$ divides 6. We will accomplish this by showing that no prime greater than 3 divides $\#E(\mathbb{Q})_{\text{tors}}$, and that the smallest powers of 2 and 3 ($2^2 = 4$ and $3^3 = 9$) do not divide $\#E(\mathbb{Q})_{\text{tors}}$. Thus, we will conclude 2 divides $\#E(\mathbb{Q})_{\text{tors}}$ and 3 divides $\#E(\mathbb{Q})_{\text{tors}}$, which implies $\#E(\mathbb{Q})_{\text{tors}}$ divides 6.

We start by noting that by Thm. 2.2.1, for all sufficiently large primes of good reduction ℓ, $\#E(\mathbb{Q})_{\text{tors}}$ divides $\#\widetilde{E}(\mathbb{F}_\ell)$. Also, by Prop. 3.2.1, $\#E(\mathbb{Q})_{\text{tors}}$ divides $\ell + 1$ for all sufficiently large primes ℓ with $\ell \equiv 2 \mod 3$.

Next, we will show that 4 does not divide $\#E(\mathbb{Q})_{\text{tors}}$. By Dirichlet's theorem, we can choose a prime ℓ as previously described with $\ell \equiv 5 \mod 12$. Then, $\ell \equiv 2 \mod 3$. If 4 divides $\#E(\mathbb{Q})_{\text{tors}}$, then $4 \,\big|\, (\ell + 1)$. But, $\ell \equiv 1 \mod 4$ means that $\ell + 1 \equiv 2 \mod 4$. So, $4 \nmid (\ell + 1)$, and we have a contradiction.

We will now show that 9 does not divide $\#E(\mathbb{Q})_{\text{tors}}$. By Dirichlet's theorem again, we can choose ℓ large enough with $\ell \equiv 2 \mod 9$. Then, $\ell \equiv 2 \mod 3$. Thus, $9 \,\big|\, \#E(\mathbb{Q})_{\text{tors}}$ implies $9 \,\big|\, (\ell + 1)$. However, $\ell + 1 \equiv 3 \mod 9$ implies that $9 \nmid (\ell + 1)$, and we have a contradiction.

Finally, let us show that no prime $q > 3$ divides $\#E(\mathbb{Q})_{\text{tors}}$. By Dirichlet's theorem, we can choose ℓ large with $\ell \equiv 2 \mod 3q$. Then, $\ell \equiv 2 \mod 3$. Thus $q \,\big|\, \#E(\mathbb{Q})_{\text{tors}}$ implies $q \,\big|\, (\ell + 1)$. But, $\ell + 1 \equiv 3 \mod 3q$ implies $\ell + 1 \equiv 3 \mod q$. So, $q \nmid (\ell + 1)$, and we have a contradiction.

Thus, we have shown that $\#E(\mathbb{Q})_{\text{tors}}$ divides 6. The torsion subgroup has an element of order 2 if and only if D is a cube, as previously shown. Therefore, we now only need to determine when the torsion subgroup has elements of order 3. For such a point $P = (X, Y)$, $2P = -P$. Furthermore, the X-value is what matters, since $2P = +P$ is impossible for $P \neq \mathcal{O}$. By the duplication

formula, the question is whether

$$\frac{X^4 - 8DX}{4(X^3 + D)} = X$$

has any rational solutions X. Clearing fractions, we have

$$4X^4 + 4DX = X^4 - 8DX$$

$$X^4 = -4DX.$$

One solution is $X = 0$, which gives $Y^2 = D$; so $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z}$ occurs if D is a square. The only other possibility is $X^3 = -4D$. By substitution, $Y^2 = -3D$. As in our analysis, this implies $D < 0$. Since D is sixth-power free, the only possible prime divisors of D are 2 and 3. We readily find $D = -2^4 3^3$. So, $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z}$ occurs if and only if either D is a square or $D = -2^4 3^3 = -432$. □

Returning to Question 1.5.2, we see that for Mordell curves, the possible torsion subgroups that pop out appear to be quite restricted. Naturally, we wonder if some set of restrictions govern the torsion subgroups for *all* elliptic curves defined over the rationals. As it turns out, a torsion subgroup generally for an elliptic curve defined over $\mathbb{Q}$ is in fact isomorphic to one of only 15 possible groups! This idea was conjectured by Andrew Ogg in 1973 [Ogg73] and proved by Barry Mazur in 1977.

Theorem 3.3.2 (Ogg's Conjecture; Mazur [Maz77])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/N\mathbb{Z} \quad \textit{with} \quad 1 \leq N \leq 10 \textit{ or } N = 12, \textit{ or}$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} \quad \textit{with} \quad 1 \leq M \leq 4.$$

This neat result—in both senses of the word—is remarkable! But, after its proof, mathematicians set their sights beyond $\mathbb{Q}$, asking what sort of torsion subgroups occur if we enlarge the field of definition from $\mathbb{Q}$ to some algebraic extension of $\mathbb{Q}$. This remains an open question and is a current area of research, specifically for those who love the curves that lay at the intersection of algebra, geometry, and number theory.

References

[Kna92] Anthony W. Knapp, Elliptic curves, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992. MR 1193029

[Lut37] Élisabeth Lutz, Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps $\mathfrak{p}$-adiques, J. Reine Angew. Math. **177** (1937), 238–247. MR 1581558

[Maz77] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978), With an appendix by Mazur and M. Rapoport. MR 488287

[Mor22] L. J. Mordell, Note on Certain Modular Relations Considered by Messrs. Ramanujan, Darling, and Rogers, Proc. London Math. Soc. (2) **20** (1922), no. 6, 408–416. MR 1577380

[Nag35] T. Nagell, Solution de quelque problemes dans la theorie arithmetique des cubiques planes du premier genre, Wid. Akad. Skrifter Oslo I (1935), no. 1.

[Ogg73] A. P. Ogg, Rational points on certain elliptic modular curves, Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972), 1973, pp. 221–231. MR 0337974

[Poi08] H. Poincaré, Sur l'uniformisation des fonctions analytiques, Acta Math. **31** (1908), no. 1, 1–63. MR 1555036

[Sil86] Joseph H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR 817210

[ST15] J.H. Silverman and J. Tate, Rational points on elliptic curves, second edition ed., Undergraduate Texts in Mathematics, Springer, 2015.

[Wei28] André Weil, L'arithmétique sur les courbes algébriques, Doctorat d'état, 1928. MR 3532958

[Wil95] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2) **141** (1995), no. 3, 443–551.