TORSION POINTS OF ELLIPTIC CURVES

MICHAEL GALPERIN

Abstract. Elliptic curves as an area of mathematical study are initially simple to understand, but reveal startling complexity when considered over different fields. This paper discusses the general properties and characteristics of projective space, elliptic curves, and the group structure that arises with certain binary operations on the curve. We discuss elliptic curves over $\mathbb{Q}$, including the topic of the discriminant and a proof of the Nagell-Lutz theorem. Finally, we discuss the properties of elliptic curves over finite fields, including a proof of the Reduction Modulo p Theorem.

Contents

Date: August 30, 2013.

1. Introduction

Elliptic curves are an interesting field of study that is easily accessible, but yields often startling results with significant parallels to geometry, algebra, and number theory. This paper will focus primarily upon the number theoretic implications of the theory of elliptic curves. Such curves are characterized by a number of properties that allow organization of the set of points on the curve into an abelian group. This paper will attempt to establish this group structure, and explore a number of implications of such a structure's existence.

2. Cubics in Projective Space

In order to correctly address the topic of elliptic curves, we must first describe the notions of space from which they arise. Elliptic curves in the affine plane, $\mathbb{A}^2$, are projections of cubic curves in the projective plane, $\mathbb{P}^2$. The following section seeks to describe the projective plane, and the method by which cubics in $\mathbb{P}^2$ are transformed into elliptic curves in $\mathbb{A}^2$.

2.1. **The Projective Plane.** The projective plane is defined as the set of all triples (a, b, c), such that a, b, and c are not all 0, and where (a, b, c) is considered to be the same point as $(a', b'c')$ if $(a', b'c') = (ta, tb, tc)$ for some nonzero t. In other words, the projective plane is defined in terms of an equivalence relation $\sim$ on all triples of homogenous coordinates (a, b, c), such that $(a, b, c) \sim (a', b', c')$ if and only if $a' = ta, b' = tb, c' = tc$ for some nonzero t. This equivalence relation allows for the following simplified definition of $\mathbb{P}^2$:

$$\mathbb{P}^2 = \frac{\{(a, b, c) \mid a, b, c \text{ are not all } 0\}}{\sim} \tag{2.1}$$

This definition lends itself to a somewhat more intuitive definition of the projective plane. If a triple (a,b,c) is to be thought of as a vector in $\mathbb{R}^3$, then the vector (a, b, c) is considered equivalent to all scalar multiples of the vector itself. Thus, for any given triple (a, b, c), the set of all triples considered equivalent to (a, b, c) is the line passing through the origin and (a, b, c). Because all points in a given direction from the origin are equivalent in projective space, the projective plane can simply be thought of as including the set of all *directions* in $\mathbb{R}^3$.

An interesting implication is the notion of points at infinity. Because any two parallel lines in $\mathbb{A}^2$ must by definition have the same direction, in projective space the lines must have the point defining their direction in common. This intersection is the basis for the notion of a "point at infinity" – it is the point at which two parallel lines travelling in a given direction must intersect in projective space. In order to maintain the property that two lines may only intersect at one point, there must be a point at infinity for every given direction in $\mathbb{A}^2$. Thus, projective space can also be defined as:

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \{\text{The set of directions in } \mathbb{A}^2\}. \tag{2.2}$$

It is important to remember that both projective space and affine space are defined over a field. Convention dictates that when working with elliptic curves in either of these spaces, one must mention the field over which the curve is defined. The associated field can be crucial in defining establishing properties of the mathematical objects within them. This paper explores the differences that arise when

mathematical objects defined by the same equation are positioned in spaces over *different* fields.

2.2. **Projective Cubics.** A cubic curve in projective space is defined as the set of solutions of a polynomial function $F(X, Y, Z)$:

$$E\colon F(X, Y, Z) = 0$$

More specifically, because such curves exist in projective space, the polynomial $F(X, Y, Z)$ must be homogenous of degree d. This means that it must satisfy the property:

$$F(tX, tY, tZ) = t^d F(X, Y, Z),$$

where d is the degree of the polynomial F.

2.3. **Homogenization.** The question still remains of how curves in $\mathbb{P}^2$ might be transformed into curves in $\mathbb{A}^2$. Such transformations are typically carried out through a process known as *homogenization*. Homogenization maps a curve E in $\mathbb{P}^2$ to a curve in $\mathbb{A}^2$ by transforming the function by which E is defined, $F(X, Y, Z)$, into a function $f(x, y)$. The process for such transformations is rather straightforward. We define f by the following relation:

$$f(x, y) = F(X, Y, 1).$$

In such a transformation, every homogenous triple (a, b, c) that solves the polynomial F is scaled by the reciprocal of an element of the triple. For example, if the function F is to be homogenized with respect to Z, the solutions to F are scaled in the following way:

$$(a, b, c) \mapsto \left(\frac{a}{c}, \frac{b}{c}, 1\right)$$

Note that, in projective space, the original triple and the triple to which it is mapped are equivalent because $\frac{1}{c}$ is a nonzero scalar applied to each element of the triple.

3. Elliptic Curves and Group Structure

An **Elliptic Curve** is a function with the the general formula:

$$y^2 = f(x) = x^3 + ax^2 + bx + c \tag{3.1}$$

Such curves are also expressed in the less generalized **Weierstrass Normal Form** (often referred to simply as the normal form), expressed by:

$$y^2 = f(x) = 4x^3 - ax - c. \tag{3.2}$$

An example of an elliptic curve is shown in Figure 1.

Elliptic curves in $\mathbb{A}^2$ are the result of homogenization of cubic curves in projective space. A relevant question, then, is how curves drawn in $\mathbb{A}^2$ take into account the existence of the point at infinity. Our discussion of the group structure of elliptic curves will make the importance and positioning of the point at infinity more intuitively clear.

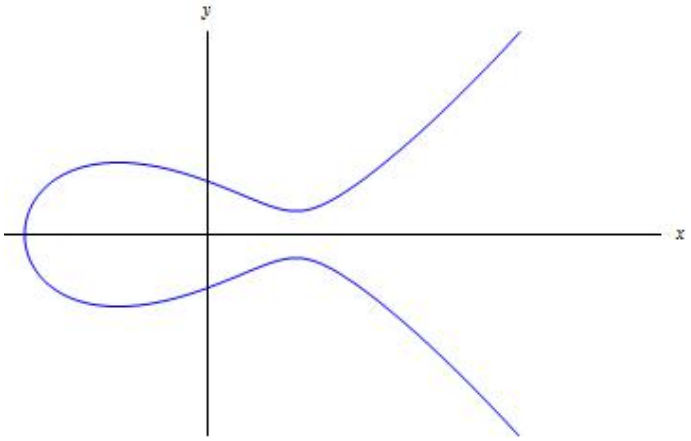

FIGURE 1. The elliptic curve $y^2 = x^3 - 6x + 7$

3.1. **Elliptic Curves over Fields.** In analyzing elliptic curves, it is important to consider the **field** over which such curves are defined. For a given elliptic curve E, the properties of the curve may change depending on the field over which it is defined.

The coordinates of the points of elliptic curves can belong to a number of fields, such as $\mathbb{C}, \mathbb{R}, \mathbb{Q}$, and so on. By considering an elliptic curve defined over a certain field, we mean to say that we are analyzing only the points of the elliptic curve in which both coordinates are elements of that field. We denote an elliptic curve E defined over a field F as $E(F)$. An intuitive consequence of this idea is that if a field is a subset of another field, then the same containment will apply to the elliptic curves defined over these two fields. Thus, for any elliptic curve E, we have:

$$E(\mathbb{N}) \subset E(\mathbb{Z}) \subset E(\mathbb{Q}) \subset E(\mathbb{R}) \subset E(\mathbb{C}),$$

and so on. Note that, of course, $\mathbb{N}$ and $\mathbb{Z}$ are not fields, but we may still analyze $E(\mathbb{Z})$ or $E(\mathbb{N})$ by considering only the points on elliptic curves with coordinates in $\mathbb{Z}$ or $\mathbb{N}$.

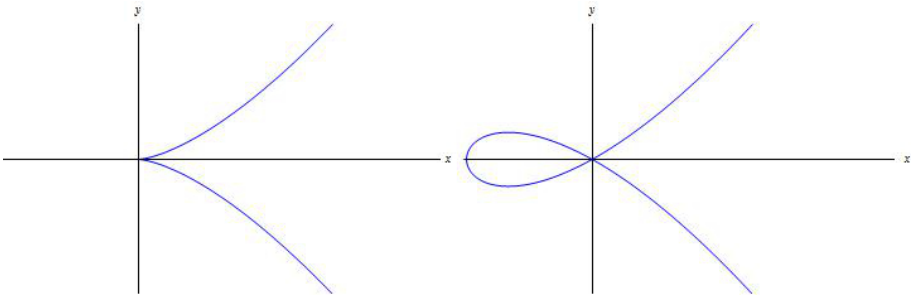

FIGURE 2. Two examples of singular elliptic curves.

3.2. **Singularity.** Elliptic curves with distinct roots are called **nonsingular**. In all analyses of elliptic curves performed in this paper, we will assume that the curves

studied are nonsingular. Singular elliptic curves are characterized graphically by cusps or nodes, which makes meaningful analysis in terms of our group structure difficult because the property does not necessarily hold that a line through two points on the curve must pass through a third. Figure 2 shows two examples of singular elliptic curves.

3.3. **Binary Relations.** By a particular design of a binary relation between distinct points on an elliptic curve, the points on such a curve form an abelian group. This section aims to describe this particular relation, and prove that this relation transforms the set of points on an elliptic curve into an abelian group.

Let P and Q be two distinct points on an elliptic curve. The line through P and Q must intersect the cubic at a third point. We define the point $P * Q$ as this third point of intersection. This relationship is demonstrated in Figure 3. Additionally, we define $P * P$ to be the second point of intersection between the line tangent to the elliptic curve at the point P and the elliptic curve itself.

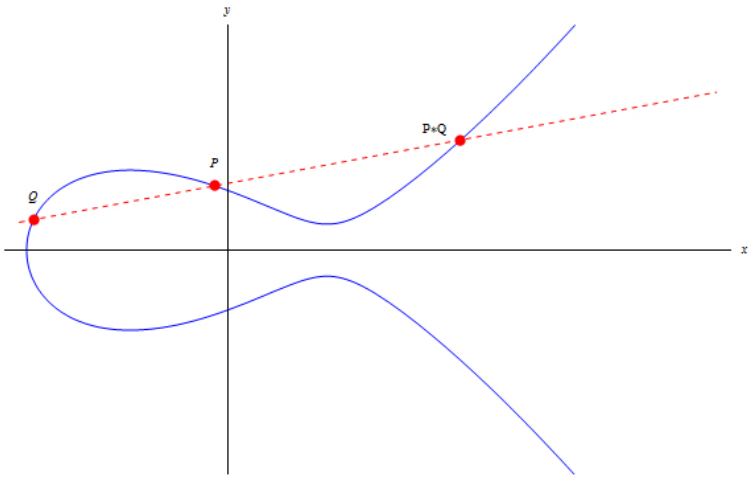

FIGURE 3. The binary relation $*$ applied to points P and Q.

Note that the relation $*$ is commutative; a line through P and Q is the same as a line through Q and P, and will result in the same third point $P * Q = Q * P$. Thus, we will see that if we succeed in proving that the points of an elliptic curve form a group, the group must be abelian.

Furthermore, we define the binary relation $+$ in terms of $*$, where $P + Q = \mathcal{O} * (P * Q)$, and $\mathcal{O}$ is the point at infinity. In the affine plane, drawing a line through $\mathcal{O}$ and $P * Q$ is equivalent to drawing a vertical line through the point $P * Q$ and defining the line's second point of intersection with the elliptic curve as $P + Q$. Because elliptic curves are symmetric about the x-axis, this is functionally equivalent to reflecting the point $P * Q$ about the x-axis and defining the reflected point as $P + Q$. This method of defining $P + Q$ is demonstrated graphically in Figure 4.

3.4. **The Duplication Formula.** It is relatively simple, given two points P_1 and P_2, to graphically find the point $P_1 + P_2$ through the process outlined above. However, we may also algebraically determine the coordinates of $P_1 + P_2$. We start with

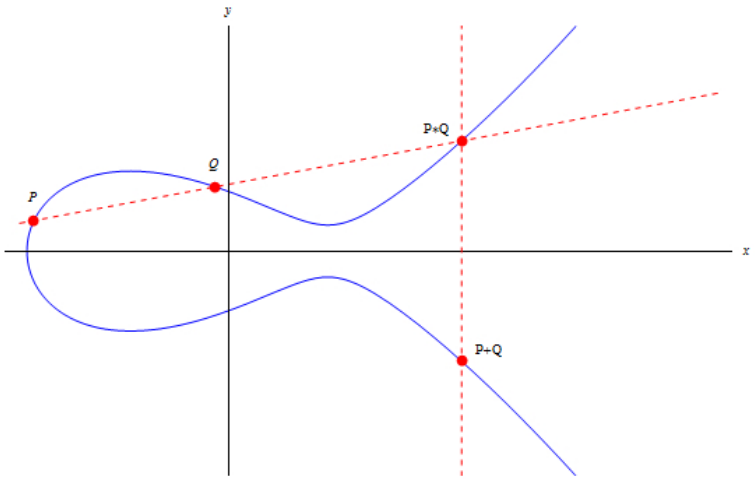

FIGURE 4. Defining the point $P + Q$.

our equation for the elliptic curve E:

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

Let $P_1 = (x_1, x_2)$ and $P_2 = (x_2, y_2)$. We may define $P_1 * P_2 = P_3$, where $P_3 = (x_3, y_3)$. From this construction, it follows that $P_1 + P_2 = (x_3, -y_3)$. We define the line connecting P_1, P_2, and P_3 as:

$$y = \lambda x + v, \quad \text{where} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad v = y_1 - \lambda x_1 = y_2 - \lambda x_2$$

We can substitute the equation for this line into the equation for E, so we have $(\lambda x + v)^2 = x^3 + ax^2 + bx + c$. Moving everything to one side and expanding, we get:

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

After some factoring, this yields:

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

The roots of this equation are x_1, x_2, and x_3, so we can rewrite the left side:

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

Finally, expanding gives us our final equation:

$$x^3 - (x_1 + x_2 + x_3)x^2 + (1 + x_3)x_1x_2x - x_1x_2x_3 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda v)x + (c - v^2).$$

From the coefficients for x^2 on both sides, we therefore have that $\lambda^2 - a = x_1 + x_2 + x_3$. We can use this to find formulas for x_3 and y_3:

$$x_3 = \lambda^2 - a - x_1 - x_2, \qquad y_3 = \lambda x_3 + v$$

This equation is called the **duplication formula**. This is a useful result because it allows us to find the coordinates of $P_1 * P_2$ given distinct points P_1 and P_2 on an elliptic curve. To find $P_1 + P_2$, all we have to do is use the duplication formula to find the coordinates of P_3, and then reflect over the x-axis by taking the opposite of y_3.

3.5. **The Group Structure.** It still remains to show that the set of points on an elliptic curve, combined with the binary relation + on the curve, forms a group. The field over which binary operations are done on the curve is important to consider here, as it is possible to establish a group structure on a curve E only when the set S over which the curve is defined satisfies the condition that $E(S)$, the set of points in E with coordinates in S, is closed under the binary operations defined above. We will prove each condition for the group structure independently.

The Identity Element.

The identity element for the binary operation + is the point at infinity, $\mathcal{O}$. This property is rather clear intuitively. Recall that for all points P and Q on the elliptic curve, $P + Q = \mathcal{O} * (P * Q)$. Thus, for any point P on the elliptic curve, $\mathcal{O} + P = \mathcal{O} * (\mathcal{O} * P)$. The right side of this equation reflects the point P over the x-axis twice, resulting in the point P. Thus, $\mathcal{O} + P = P$, and there is an identity element for the group.

Inverses.

The property that every point P on the elliptic curve must have an inverse is also rather clear to prove intuitively. For any point P on the elliptic curve, we define $P^{-1} = -P$ to be the point on the elliptic curve obtained by reflecting P over the x-axis. Thus, $P * (-P)$ must be the point at infinity, implying that $P + (-P) = \mathcal{O}$ and, therefore, that the inverse property holds.

Associativity.

The most significant challenge in proving the group structure of rational points on elliptic curves is proving associativity. This paper will use Bezout's theorem to demonstrate this result, particularly in showing that for any three rational points on an elliptic curve, denoted P, Q, and R, we have that $(P+Q)+R = P+(Q+R)$.

We shall assert Bezout's theorem, and use this result to prove a more specific theorem about cubics. It is then rather simple to prove that associativity holds for the group structure on an elliptic curve.

Theorem 3.3 (Bezout's Theorem)**.** *For any two polynomials C_1 and C_2 that do not have a component in common, where C_1 has degree n and C_2 has degree m, C_1 and C_2 intersect at nm distinct points.*

The implication of this theorem for our purposes is that two cubics must intersect at 9 distinct points. It is important to recognize, in this case, that the point at infinity can be considered to be one of these points. Additionally, multiplicity factors into these calculations – for this reason, it is possible for a single point to be counted "twice" in evaluating how many points of intersection there are between two curves. We can use Bezout's theorem to prove an important lemma about points on cubic curves:

Lemma 3.4. *For any three cubic curves C_1, C_2, C_3 in projective space, where C_1 and C_2 do not have a component in common, if C_3 passes through eight of the nine intersection points of C_1 and C_2, then C_3 also passes through the ninth intersection point.*

Proof. Let C_1 and C_2 be two cubic curves. Bezout's theorem gives us that C_1 and C_2 intersect at 9 distinct points. Assume that C_3 passes through 8 of the 9 intersection points of C_1 and C_2.

Because C_1 and C_2 are defined in projective space, they are associated with two functions F_1 and F_2 such that $C_1 \colon F_1(X, Y, Z) = 0$ and $C_2 \colon F_2(X, Y, Z) = 0$.

It is therefore possible to create a linear combination of F_1 and F_2, defined by $\lambda_1 F_1 + \lambda_2 F_2$ for some values of λ_1 and λ_2. Because such a linear combination is defined in projective space, it forms a one-dimensional family. Because C_3 is pinned down by 8 points through which it must travel, it is part of a one-dimensional family.

Thus, for some values of λ_1 and λ_2, we have $F_3 = \lambda_1 F_1 + \lambda_2 F_2$ for $C_3 \colon F_3(X, Y, Z)$.

If we are to evaluate this relationship at the ninth intersection point of C_1 and C_2, we have $F_1 = F_2 = 0$ by definition. Thus, $F_3 = 0$ at this point, and therefore, C_3 passes through the ninth point of intersection. □

We can now use Bezout's theorem to prove the associativity property for the group operation + on the points on an elliptic curve. To show that $P + (Q + R) = (P + Q) + R$, it suffices to show that $P * (Q + R) = (P + Q) * R$, because this point will simply be reflected over the x-axis to obtain the desired result.

Theorem 3.5. *For any three points P, Q, R on an elliptic curve C, $P * (Q + R) = (P + Q) * R$.*

Proof.
Let P, Q, R be points on an elliptic curve C. We will now give names to the lines used in defining the relevant points on C:
Let L_1 be the line passing through P, Q, and $P * Q$.
Let L_1' be the line passing through Q, R, and $Q * R$.
Let L_2 be the vertical line passing through $\mathcal{O}, Q * R$, and $Q + R$.
Let L_2' be the vertical line passing through $\mathcal{O}, P * Q$, and $P + Q$.
Let L_3 be the line passing through $P + Q$ and R.
Let L_3' be the line passing through P and $Q + R$.
Because C is a projective curve, the lines L_3 and L_3' must intersect at a single point, denoted A. Furthermore, because both L_3 and L_3' are lines through two points on C, they must intersect C at a third point. Thus, if A lies on the elliptic curve, then $A = P * (Q + R) = (P + Q) * R$ and the associative property holds.

Let D be the set consisting of P, Q, R, the compositions $P * Q$ and $Q * R$, the additions $P + Q$ and $Q + R$, and the point A. By construction, every point $p \in D$ has both a line L_i and a line L_i' passing through it. We may define $C_1 = L_1 \cdot L_2 \cdot L_3$ and let $C_2 = L_1' \cdot L_2' \cdot L_3'$, so C_1 and C_2 both pass through all of the nine points $p \in D$.

By definition, the elliptic curve C passes through the eight points $p \in (D \setminus A)$, so C passes through A by Lemma 3.4, and the associative property holds. □

Figure 5 gives a graphical demonstration of this proof.

3.6. **Subgroups over Fields.** An interesting result of the construction of the group law on an elliptic curve is that elliptic curves will always be groups when defined over certain fields, but will not form groups over certain other fields. We will state it as fact here that for an elliptic curve E, the sets $E(\mathbb{Q}), E(\mathbb{R})$, and $E(\mathbb{C})$ are groups. That is to say, if one is to add two points in any of these sets according to the definition of addition outlined above, the resulting third point will also be an element of that set. As a general rule, for a field $\mathbb{F}$, $E(\mathbb{F})$ will be a group if and only if $E(\mathbb{F})$ is closed under addition on the curve. The same does not necessarily hold for sets such as $\mathbb{Z}$ without imposing stricter conditions. Therefore, the statement $E(\mathbb{Q}) \subset E(\mathbb{R}) \subset E(\mathbb{C})$ is a relation between *subgroups*.

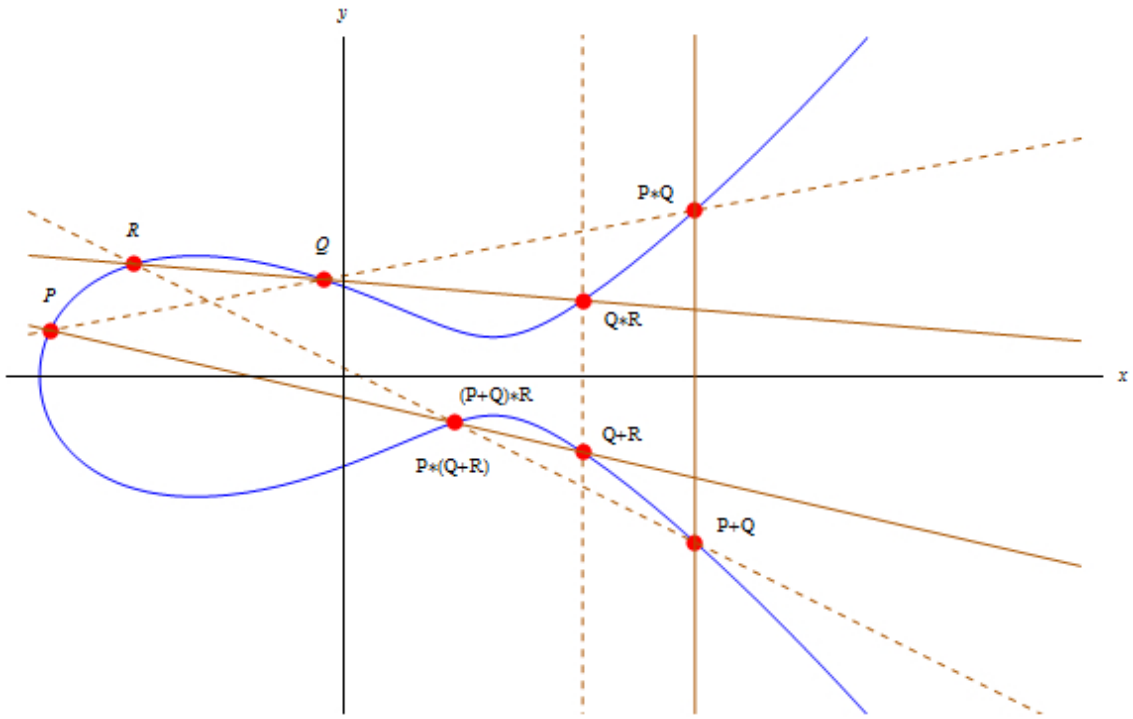

FIGURE 5. A graphical demonstration of the associativity property.

4. Rational Points, the Discriminant, and the Nagell-Lutz Theorem

The **discriminant**, we will see, is a particularly relevant mathematical value that provides useful insight into the properties of elliptic curves. Let us define our elliptic curve E, for which we assume that the coefficients satisfy $a, b, c \in \mathbb{Q}$.

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

If we define variables $X = d^2x$ and $Y = d^3y$ for some $d \in \mathbb{Z}$, then our relation becomes:

$$Y^2 = d^6(x^3 + ax^2 + bx + c)$$
$$\Rightarrow Y^2 = X^3 + d^2aX^2 + d^4bX + d^6c$$

Because a, b, and c are rational numbers multiplied by an integer d of arbitrary size, there must be a sufficiently large $d \in \mathbb{Z}$ such that it would cancel with the denominators of a, b, and c, and so we may assume that $a, b, c \in \mathbb{Z}$. Subsequent calculations will be done with this assumption in mind. We are now ready to define the discriminant.

Definition 4.1. The **discriminant** D of a cubic polynomial E is defined by:

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

Additionally, we may the cubic polynomial associated with E over the complex numbers, obtaining three complex roots:

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

This allows us to rewrite the discriminant in the following way:

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

This reformulation should make it intuitively clear that the cubic polynomial will be nonsingular (that is, will have distinct roots) if and only if $D \neq 0$. Additionally, the discriminant of a cubic function gives us valuable information concerning the nature of the roots themselves. If $D > 0$, then all roots are real. If $D < 0$, then the polynomial has one real root and two complex conjugate roots.

Warning 4.2. It is important to recognize that while this paper will make exclusive use of the above definition, it is only a special case of a more generalized formula for n-degree polynomials. This paper will not examine more generalized forms of the discriminant, but the reader should not assume that all formulas for the discriminant of a polynomial follow a similar structure.

Remark 4.3. If the cubic curve is defined by $E\colon y^2 = f(x) = x^3 + ax^2 + bx + c$, then the discriminant can be written as:

$$\left[(18b - 6a^2)x - (4a^3 - 15ab + 27c)\right] f(x) +$$
$$\left[(2a^2 - gb)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2)\right] f'(x)$$

In general, what is relevant about this result is that the discriminant can be written as the sum of the product of a polynomial $r(x)$ with $f(x)$, and another polynomial $s(x)$ with $f'(x)$, where $r(x)$ and $s(x)$ both have integer coefficients:

$$D = r(x)f(x) + s(x)f'(x)$$

Theorem 4.4 (Nagell-Lutz)**.** *The rational points (x, y) of finite order on a given elliptic curve satisfy:*

(1) x and y are integers.
(2) Either $y = 0$ or $y \mid D$
(3) There is a finite number of such points.

Warning 4.5. This is not an "if and only if" statement. That is, it is entirely possible for a point on an elliptic curve to have integer coordinates and satisfy $y \mid D$, but have infinite order. However, if a point P satisfies $y = 0$, then the point must have order 2, because $P + P = \mathcal{O}$.

The Nagell-Lutz theorem is especially significant in that it yields a method for finding the points of finite order on an elliptic curve. Given the equation $f(x)$, one can simply calculate the discriminant, consider all $y \in \mathbb{Z}$ that satisfy $y = 0$ or $y \mid D$, and plug all such y into $y^2 = f(x)$ to verify if the corresponding x is also an integer. This makes the Nagell-Lutz theorem an extremely useful tool in analyzing an elliptic curve over $\mathbb{Q}$.

This paper will aim to prove the Nagell-Lutz theorem. First, a preliminary lemma:

Lemma 4.6. *If $P = (x, y)$ is a point on an elliptic curve E such that P and $2P$ both have integer coordinates, then $y = 0$ or $y \mid D$.*

Proof. We will assume that $y \neq 0$, and demonstrate that this implies that $y \mid D$. If $y \neq 0$, then $2P \neq \mathcal{O}$, by the definition of a point of order 2. Thus, $2P = (X, Y)$ for some $X, Y \in \mathbb{Z}$. The duplication formula gives us the following result:

$$2x + X = \lambda^2 - a, \text{ where } \lambda = \frac{f'(x)}{2y}.$$

Because x, X, and a are all integers, we know that λ is an integer, and therefore that $f'(x)$ and $2y$ are integers. By the construction of λ, we have that $2y \mid f'(x)$, and therefore that $y \mid f'(x)$. From the construction of E, we also have that $y^2 = f(x)$, and thus we have that $y \mid f(x)$. Because $D = r(x)f(x) + s(x)f'(x)$ by Remark 4.3, and because $y \mid f(x)$ and $y \mid f'(x)$, we therefore have that $y \mid D$. □

Next, we will attempt to show that all torsion points on an elliptic curve defined over $\mathbb{Q}$ must have integer coordinates. Because a number is equal to 1 if and only if it is not evenly divisible by any prime numbers, and because integers have a denominator of one, this is equivalent to proving that the denominators of all points of finite order are non-divisible by all prime numbers. Another useful observation for our proof is that any rational number can be expressed by the following formula:

$$\frac{m}{n}p^v,$$

where the prime number p does not divide either m or n, where $n > 0$, and where v is some integer. We define the **order** of a rational number to be the integer v:

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

The order of a rational number provides useful insight concerning whether p divides the numerator and/or denominator of the rational number in question. It is intuitively clear to see that p divides the numerator (resp. denominator) if and only if the order is positive (resp. negative). Also, p will not divide the numerator or the denominator of the rational number if and only if the order is equal to 0.

We will use the concept of orders of rational numbers in order to prove the Nagell-Lutz theorem. This will be done by fixing a prime p, and considering points of E with coordinates divisible by certain powers of p, a construction that we will prove is a subgroup of $E(\mathbb{Q})$. Then, by showing that no point of finite order is contained in such a subgroup, we will see that points of finite order have coordinates that cannot be evenly divided by primes - and thus, that they have integer coordinates.

Lemma 4.7. *Fix a prime p. For any point $(x, y) \in E(\mathbb{Q})$, if p divides the denominator of x, then p divides the denominator of y.*

Proof. Consider a point $(x, y) \in E(\mathbb{Q})$, where there exists a prime p dividing the denominator of x. Because x and y are rational numbers, we can express them as follows:

$$x = \frac{m}{np^\mu}, \qquad\qquad y = \frac{u}{wp^\sigma}$$

Because p divides the denominator of x, we have that $\mu > 0$. This proof, then, aims to show that $\sigma > 0$. By construction, we also know that $p \nmid m, n, u, w$. By substituting our equations for x and y into the equation $y^2 = x^3 + ax^2 + bx + c$, we get:

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

Finding a common denominator, this becomes:

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

We can now examine the orders of both sides of this equation. Because $p \nmid u^2$ and $p \nmid w^2$, we have:

$$\text{ord}\left(\frac{u^2}{w^2 p^{2\sigma}}\right) = \text{ord}\left(\frac{u^2}{w^2} p^{-2\sigma}\right) = -2\sigma.$$

For the right side of the equation, we know that $p \nmid n$ and thus that $p \nmid n^3$. We also know that $p \nmid m$, so it is true that $p \nmid (m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu})$. Thus, we have:

$$\text{ord}\left(\frac{m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}\right) = -3\mu.$$

Because both sides of our equation must have the same order, these two results give us that $2\sigma = 3\mu$. Because σ is greater than 0 by assumption, this proves that $\mu > 0$, and thus that p divides the denominator of y. □

Another important implication of the arguments in the proof above is that, because $2 \mid \mu$ and $3 \mid \sigma$, we have that $\mu = 2v$ and $\sigma = 3v$ for some $v \in \mathbb{Z}$. So, if v divides either x or y, then it divides both, and the converse of the above proof is also true. The following definition becomes important in finishing our proof:

Definition 4.8. For an elliptic curve E over $\mathbb{Q}$, we define the set $E(p^v)$ by:

$$E(p^v) = \{(x, y) \in E(\mathbb{Q}) \mid \text{ord}(x) \leq -2v \quad \text{and} \quad \text{ord}(y) \leq -3v\}.$$

Intuitively, $E(p^v)$ is the set of all points of $E(\mathbb{Q})$ in which the denominators of the coordinates of x and y are divisible by powers of p greater than $2v$ and $3v$, respectively. By convention, we also include the point at infinity, $\mathcal{O}$, in all sets $E(p^v)$. Additionally, it is intuitively clear that $E(\mathbb{Q}) \supset E(p) \supset E(p^2) \supset E(p^3) \supset \cdots$, from the definition of the sets $E(p^v)$.

We aim to prove that for all primes p, the denominators of the coordinates x and y of all torsion points are not divisible by p. Therefore, it is sufficient to show that for all points P of finite order, $P \notin E(p^v)$ for all v. First, we will show that $E(p^v)$ is a subgroup of $E(\mathbb{Q})$.

Lemma 4.9. *$E(p^v)$ is a subgroup of $E(\mathbb{Q})$ for all v.*

Proof. We will define two new variables t and s by:

$$t = \frac{x}{y} \qquad s = \frac{1}{y}.$$

Substituting in t and s, our equation for the elliptic curve ($y^2 = x^3 + ax^2 + bx + c$) becomes:

$$s = t^3 + at^2s + bts^2 + cs^3 \tag{4.10}$$

Effectively, what this reformulation does is establish a one-to-one mapping between two different "forms" or "views" of the elliptic curve's graph. That is, every point (x, y) on E has a unique corresponding point on the graph defined by Equation 4.10. Notably, this is with the exception of points of order 2 on E, because these points have $y = 0$ and therefore make s undefined. However, the point at infinity $\mathcal{O}$ **is** expressed by a point on the graph of Equation 4.10 - namely, the point $(0, 0)$. Figure 6 shows both graphs in this mapping.

Similarly, lines passing through E in the (x, y) plane have corresponding lines in the (t, s) plane. If the equation for a line in the (x, y) plane is $y = \lambda x + v$, then

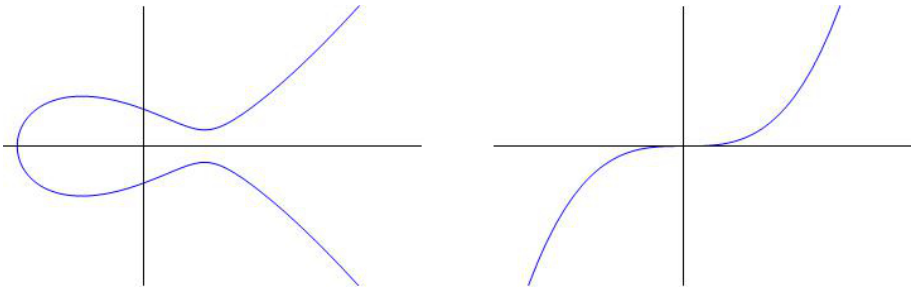

FIGURE 6. The elliptic curve E, and the corresponding equation in terms of s and t.

dividing the equation by vy gives us an equation for the corresponding line in the (t, s) plane:

$$\frac{1}{v} = \frac{\lambda}{v}\frac{x}{y} + \frac{1}{y} \Rightarrow s = -\frac{\lambda}{v}t + \frac{1}{v}$$

Adding points on the mapping of E in the (t, s) plane works in the same general way as adding points on E. Just like on an ellitic curve, we connect two points P_1 and P_2 on the curve with a line, and find the third point of intersection (t_3, s_3). Recall that on a regular elliptic curve, P_3 is found by drawing a line between $P_1 * P_2$ and $\mathcal{O}$, and then finding the third point of intersection of this line with the elliptic curve. In our relation, $\mathcal{O}$ is mapped to $(0, 0)$, so all we have to do is draw a line through (t_3, s_3) and the origin, and find the third point of intersection. Because Equation 4.10 is an odd function, this just means that $P_3 = (-t_3, -s_3)$. We can find a general formula for this addition. Then, by considering only points in $E(p^v)$, we can show that this way of defining addition makes $E(p^v)$ a group.

We will define the ring R_p as the set of all rational numbers such that p does not divide the denominator. Notationally, this means that for all $x \in R_p$, we have that $\text{ord}(x) \geq 0$. The invertible elements of R_p (that is, all elements u that have an inverse v under multiplication in R_p) are called the **units** of R_p, and are in this case those elements with order equal to 0, or those in which both the numerator and denominator are coprime to p.

Let (x, y) be a point with rational coordinates in $E(p^v)$. By definition, we have that $\text{ord}(x) \leq -2v$ and $\text{ord}(y) \leq -3v$, so we can express x and y by the following equations:

$$x = \frac{m}{np^{2(v+i)}} \qquad y = \frac{u}{wp^{3(v+i)}}$$

for some $i \geq 0$. Using our equations for t and s, this yields:

$$t = \frac{x}{y} = \frac{mw}{nu}p^{v+i} \qquad s = \frac{1}{y} = \frac{w}{u}p^{3(v+i)}$$

Thus, for a point to satisfy $(x, y) \in E(p^v)$, p^v must divide the numerator of t, and p^{3v} must divide the numerator of s, for the associated pair (t, s). This is equivalent to saying that (t, s) must satisfy $t \in p^v R_p$ and $s \in p^{3v} R_p$. So, to show that $E(p^v)$ is a subgroup, then we can simply show that if an arbitrary power of p divides the t coordinate of two points P_1 and P_2, then the same power of p will divide the t coordinate of their sum.

Let $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$ be distinct points on the curve. There are two possible cases to consider:

(1) $t_1 = t_2$
If $t_1 = t_2$, then $P_1 = -P_2$ by the addition law, so $P_1 + P_2$ must be an element of $E(p^v)$, because they add to the point $(0, 0)$.

(2) $t_1 \neq t_2$
Let $s = \alpha t + \beta$ be the line passing through P_1 and P_2. The slope of the line, α, is given by $\alpha = \frac{s_2 - s_1}{t_2 - t_1}$. We also know that (t_1, s_1) and (t_2, s_2) satisfy the equation $s = t^3 + at^2 s + bts^2 + cs^3$. So, we can attempt to express the slope as a function of the coordinates of P_1 and P_2, as well as the coefficients a, b, and c. We may subtract the equation for P_1 from the equation for P_2:

$$s_2 - s_1 = t_2^3 - t_1^3 + a(t_2^2 s_2 - t_1^2 s_1) + b(t_2 s_2^2 - t_1 s_1^2) + c(s_2^3 - s_1^3)$$

This can be reformulated to include factors in the form of $(t_2 - t_1)$ and $(s_2 - s_1)$:

$$s_2 - s_1 = t_2^3 - t_1^3 + a(t_2^2 - t_1^2)s_2 + at_1^2(s_2 - s_1) + b(t_2 - t_1)s_2^2 + bt_1(s_2^2 - s_1^2) + c(s_2^3 - s_1^3)$$

So, factoring out the quantity $(t_2 - t_1)$, we can find an equation for $(t_2 - t_1)$:

$$t_2 - t_1 = \frac{-s_1 + t_1^3 - t_2^3 + at_1^2 s_1 + cs_1^3}{bs_2^2} + \frac{1 - a(t_2^2 - t_1^2) - at_1}{bs_2} + \frac{t_1 s_1^2}{s_2^2} - \frac{cs_2}{b} - t_1$$

Now, we can express the ratio $\alpha = \frac{s_2 - s_1}{t_2 - t_1}$ using the two equations above. After some algebra, the result is:

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)} \tag{4.11}$$

We will put this result aside for now. Next, we will look at addition on the cubic curve. Let $P_3 = (t_3, s_3)$ be the third point of intersection of the line $s = \alpha t + \beta$, which is drawn through P_1 and P_2, and the cubic curve $s = t^3 + at^2 s + bts^2 + cs^3$ on which P_1 and P_2 lie. The equation with t_1, t_2, and t_3 as roots can be found by substituting the equation of the line $s = \alpha t + \beta$:

$$\alpha t + \beta = t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3$$

Expanding, multiplying, and factoring out powers of t gives us:

$$0 = (1 + a\alpha + \alpha^2 b + c\alpha^3)t^3 + (a\beta + 2\alpha b\beta + 3c\alpha^2\beta)t^2 + (b\beta^2 + 3c\alpha\beta^2 - \alpha)t + c\beta^3 - \beta$$

It is generally true that the sum of the roots of a cubic equation of the form $0 = ax^3 + bx^2 + cx + d$ is equal to $-\frac{b}{a}$. This convenient fact gives us an equation for the sum $t_1 + t_2 + t_3$, based solely upon the coefficients of t^3 and t^2 in the above equation.

$$t_1 + t_2 + t_3 = -\frac{a\beta + 2\alpha b\beta + 3c\alpha^2\beta}{1 + a\alpha + \alpha^2 b + c\alpha^3}. \tag{4.12}$$

This is a powerful result that gives us a way to calculate t_3 given only t_1 and t_2, and therefore allows us to find $P_1 + P_2$ for any P_1, P_2 on the curve.

We can finally begin to analyze all of the above preliminary results. First, we will look at our extended formula for α, given by Equation 4.11. By definition, we know that t_1, t_2, s_1, s_2 are all elements of $p^v R_p$. The

formula for the numerator, $\left[t_2^2 + t_1 t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2\right]$, when expanded out, satisfies the condition that every term includes two of the elements t_1, t_2, s_1, s_2 multiplied together. Thus, p^{2v} divides the numerator of α, and it is therefore an element of $p^{2v}R_p$. The denominator of α is $\left[1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)\right]$, in which all terms except for 1 are divisible by p^{2v} by a similar argument. Because of the value 1, the denominator is coprime to p, and is therefore a unit in R_p. So, looking at α in its entirety, we have that p^{2v} divides the numerator and not the denominator, giving us the result that $\alpha \in p^{2v}R_p$.

From our equation for the line through P_1 and P_2, we know that $s_1 = \alpha t_1 + \beta$. Because $s_1 \in p^v R_p$, we know that $s_1 \in p^{3v}R_p$. And, because $\alpha \in p^{2v}R_p$ and $t_1 \in p^v R_p$, we have that $\alpha t_1 \in p^{3v}R_p$. Therefore, the equation for the line gives us that $\beta \in p^{3v}R_p$.

Finally, we can analyze Equation 4.12 through a process similar to our analysis of α. Similarly to the denominator of α, the denominator of the equation for $t_1 + t_2 + t_3$ is a unit in R_p. The term $a\beta$ in the numerator of Equation 4.12 gives us that $t_1 + t_2 + t_3 \in p^{3v}R_p$. But we know by assumption that t_1 and t_2 are elements of $p^v R_p$, so t_3 must be an element of $p^v R_p$ as well, implying that $-t_3 \in p^v R_p$.

Thus, if the t-coordinates of P_1 and P_2 are in $p^v R_p$, then the t-coordinate of $P_1 + P_2$ is also in $p^v R_p$. Also, because the curve is symmetric about the origin, we know that if the t-coordinate of P is in $p^v R_p$, then the t-coordinate of $-P$ is also in $p^v R_p$. This shows that $E(p^v)$ is closed under both addition and negatives, making it a subgroup of $E(\mathbb{Q})$.

□

In proving that $E(p^v)$ is a subgroup of $E(\mathbb{Q})$, we also proved a stronger result: that $t_1 + t_2 + t_3 \in p^{3v}R_p$. So we know that, for any $P_1, P_2 \in E(p^v)$,

$$t(P_1) + t(P_2) - t(P_1 + P_2) \in p^{3v}R_p,$$

where $t(P_1)$ denotes the t-coordinate of the (t, s) pair associated with P. So, the numerator of the sum of t_1, t_2, and $-t_3$ must be divisible by p^{3v}. This lends itself to a useful reformulation:

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \mod p^{3v}R_p \tag{4.13}$$

We can use this fact to finally prove that points of finite order on $E(\mathbb{Q})$ have integer coordinates.

Lemma 4.14. *Given an elliptic curve E, for all prime numbers p, the group $E(p)$ contains no points of finite order (other than $\mathcal{O}$).*

Proof by contradiction. Let P be a point of finite order m. Let p be some prime number. Because $P \neq \mathcal{O}$, we know that $m > 1$. We will assume that $P \in E(p)$ and establish a contradiction. It is possible that P is contained in some subgroup $E(p^v)$ of $E(p)$. However, P cannot be contained in all such subgroups, because it is impossible for the denominator of P to be divisible by all artibtrarily large powers of P. Thus, there must be some v such that $P \in E(p^v)$, but $P \notin E(p^{v+1})$. Pick this p. There are two possible cases to consider:

(1) $p \nmid m$

From Equation 4.13, we have that $t(P_1 + P_2) \equiv t(P_1) + t(P_2) \mod p^{3v}R_p$.

Because P is a point of order m, we are adding it to itself m times. So, our congruence becomes:

$$t(mP) \equiv mt(P) \mod p^{3v}R_p$$

Because $mP = \mathcal{O}$, and because $t(\mathcal{O}) = 0$, this becomes $0 \equiv mt(P) \mod p^{3v}R_p$. We also know that m is coprime to p, making it a unit in R_p. So, we end up with:

$$0 \equiv t(P) \mod p^{3v}R_p,$$

which implies that $P \in E(p^{3v}R_p)$, contradicting the above assumption that $P \notin E(p^{v+1})$.

(2) $p \mid m$
Because p divides m, we have that $m = pn$ for some $n \in \mathbb{Z}$. If we let $P' = nP$, then P' has order p, and is an element of $E(p)$ because $P \in E(p)$ by assumption. Similarly to the first case, this yields that $0 \equiv pt(P') \mod p^{3v}R_p$. Dividing out p, we get this ultimate result:

$$0 \equiv t(P') \mod p^{3v-1}R_p$$

This gives us that $P' \in E(p^{3v-1})$, which contradicts the assumption that $P' \notin E(p^{v+1})$ because $3v - 1 > v + 1$.

Therefore, for all primes p, the group $E(p)$ contains no points of finite order greater than 1. □

Completing the Nagell-Lutz theorem becomes easy:

Corollary 4.15. *All points of finite order on $E(\mathbb{Q})$ have integer coordinates.*

Proof. Let $P = (x, y)$ be a point of finite order on $E(\mathbb{Q})$. We know that $P \notin E(p)$ for all primes p, so the denominator of the coordinates of P are not evenly divided by any primes. By definition, a number that cannot be evenly divided by any prime numbers has to be equal to 1, so the denominators of the coordinates of P are 1, and the coordinates must be integers. □

5. Elliptic Curves over Finite Fields

We define a finite field $\mathbb{F}_p$ as the integers modulo some integer p:

$$\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$$

An elliptic curve E is defined over a finite field $\mathbb{F}_p$ if the coefficients of the function $f(x)$ satisfy $a, b, c \in \mathbb{F}_p$. In analyzing E, we will look for solutions $(x, y) \in \mathbb{F}_p$. There are a few relevant considerations.

5.1. **Singularity.** There are two conditions that must be satisfied for E to be nonsingular:

(1) $p \geq 3$
If p is 2 or less, then it is impossible to have three distinct numbers in $\mathbb{F}_p$, and thus three distinct roots. This makes the elliptic curve necessariliy singular.

(2) $D \neq 0$
This is the usual condition for nonsingularity. In $\mathbb{F}_p$, this implies that $p \nmid D$ is a condition for nonsingularity, because otherwise D would be reduced to 0.

5.2. **Addition on the Elliptic Curve.** Addition on the elliptic curve defined over $\mathbb{F}_p$ uses a special case of the duplication formula. The sum P_3 of two points P_1 and P_2 is found by connecting P_1 and P_2 with a line, and reflecting the third point of intersection with the elliptic curve over the x-axis. Our elliptic curve E is defined in the usual way. Let $P_1 = (x_1, y_1)$, and let $P_2 = (x_2, y_2)$. We define the line connecting P_1 and P_2 in the following way:

$$y = \lambda x + v, \text{ where } \lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if} \quad x_1 \neq x_2 \\ \dfrac{3x_1^2 + 2ax_1 + b}{2y_1} & \text{if} \quad P_1 = P_2 \end{cases}, \quad v = y_1 - \lambda x_1 = y_2 - \lambda x_2$$

By substitution, this yields the following formulas for the coordinates of $P_3 = (x_3, y_3)$, which we define in the usual way by finding the third point of intersection of the line $y = \lambda x + v$ with the elliptic curve E and reflecting over the x-axis:

$$x_3 = \lambda^2 - a - x_1 - x_2 \qquad\qquad y_3 = -\lambda x_3 - v$$

Note that these formulas hold only if the coordinates of P_1 and P_2 and coefficients of E are all contained in $\mathbb{F}_p$.

Example 5.1.
For the elliptic curve $E\colon y^2 = x^3 + x + 1$, we have:
$E(\mathbb{F}_5) = \{\mathcal{O}, (0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2)\}$

Note that because $\mathbb{F}_p$ is a finite set by definition, $E(\mathbb{F}_p)$ must always be a finite group.

6. The Reduction Modulo p Theorem

An interesting application of the theory of elliptic curves defined over $\mathbb{F}_p$ is the idea that, given an elliptic curve $E\colon y^2 = f(x) = x^3 + ax^2 + bx + c$, with $a, b, c \in \mathbb{Z}$, we can establish a mapping between the points of E and the points of $E(\mathbb{F}_p)$. Our goal, then, is to define a function $\mathbb{Z} \longrightarrow \frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p$, where $z \mapsto \overline{z}$. Thus, we have $E \mapsto \overline{E}(\mathbb{F}_p)\colon y^2 = x^3 + \overline{a}x^2 + \overline{b}x + \overline{c}$, where $\overline{a}, \overline{b}, \overline{c} \in \mathbb{F}_p$.

6.1. **Singularity.** Again, there are two conditions to ensure that the reduced elliptic curve $\overline{E}(\mathbb{F}_p)$ is nonsingular. First, p must be greater than 2, because this is a necessary condition for having three distinct roots. The second condition is more interesting.
Recall that the discriminant is defined by $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$, in which all coefficients are integers. For this reason, the discriminant can also be reduced modulo p to $\overline{D} = -4\overline{a}^3\overline{c} + \overline{a}^2\overline{b}^2 + 18\overline{a}\overline{b}\overline{c} - 4\overline{b}^3 - 27\overline{c}^2$. Therefore, for $\overline{E}(\mathbb{F}_p)$ to be nonsingular, p cannot divide the discriminant, or else $\overline{D}$ would be equal to 0 and the reduced curve would be singular.

6.2. **Points of Finite Order.** If p is a prime number, and if a point $(x, y) \in E$ satisfies $x, y \in \mathbb{Z}$, then (x, y) can be reduced modulo p to a point $(\overline{x}, \overline{y})$ that lies on the reduced curve $\overline{E}$. Thus, for all $(x, y) \in E$ with $x, y \in \mathbb{Z}$, we have:

$$(x, y) \mapsto (\overline{x}, \overline{y}) \in \overline{E}(\mathbb{F}_p)$$

Recall from the Nagell-Lutz theorem that for any elliptic curve with rational coefficients, the points of finite order must have integer coordinates. Thus, the result

above gives us a correspondence between the points of finite order on the curves $E(\mathbb{Q})$, and a subgroup of $\overline{E}(\mathbb{F}_p)$ generated by these points.

Definition 6.1. We define the group Φ by:

$$\Phi = \{P = (x, y) \in E(\mathbb{Q}) \mid P \text{ has finite order}\}$$

Thus, we define the **reduction modulo p map** described above as:

$$\Phi \longrightarrow \overline{E}(\mathbb{F}_p), \quad \text{where} \quad P \mapsto \overline{P} = \begin{cases} (\overline{x}, \overline{y}) & \text{if} \quad P = (x, y) \\ \overline{\mathcal{O}} & \text{if} \quad P = \mathcal{O} \end{cases}$$

We will show below that this map between groups is a homomorphism, and under certain conditions, an isomorphism.

Theorem 6.2. *The reduction modulo p map $\Phi \longrightarrow \overline{E}(\mathbb{F}_p)$ is a homomorphism.*

Proof. As a preliminary step, we may show that negativity is preserved under the mapping. We have:

$$\overline{-P} = \overline{(x, -y)} = (\overline{x}, \overline{-y}) = -\overline{P} \Rightarrow \overline{-P} = -\overline{P}$$

Thus, negatives are mapped to negatives. We now consider what is necessary to show to demonstrate that the map is a homomorphism. We want to show:

$$\overline{P_1 + P_2 + P_3} = \overline{P_1} + \overline{P_2} + \overline{P_3}$$

To demonstrate this, it suffices to show that $P_1 + P_2 + P_3 = \mathcal{O}$ implies that $\overline{P_1} + \overline{P_2} + \overline{P_3} = \overline{\mathcal{O}}$. there are a number of cases to consider:

(1) If at least one of the points P_1, P_2, or P_3 is equal to $\mathcal{O}$:
Without loss of generality, assume that $P_1 = \mathcal{O}$. By the definition of our mapping, $\overline{P_1} = \overline{\mathcal{O}}$. Therefore, $\mathcal{O} + P_2 + P_3 = \mathcal{O}$. Because this implies $P_2 = -P_3$, we have that $\overline{P_2} = -\overline{P_3}$, and so, $\overline{P_1} + \overline{P_2} + \overline{P_3} = \overline{\mathcal{O}}$ ✓

(2) If P_1, P_2, and P_3 are all not equal to $\mathcal{O}$:
Assume that $P_1 + P_2 + P_3 = \mathcal{O}$. This implies that P_1, P_2, and P_3 are on a line, $y = \lambda x + v$. From the results obtained above, we have that $x_3 = \lambda^2 - a - x_1 - x_2$ and $y_3 = -\lambda x_3 - v$. Because y_3, x_3, x_1, x_2, and a are all integers, we have $\lambda, v \in \mathbb{Z}$, and thus that λ and v can be reduced modulo p. Setting y equal to $\lambda x + v$ in the equation for E, we have $x^3 + ax^2 + bx + c - (\lambda x + v)^2 = 0$. Because x_1, x_2, x_3 are roots of $f(x)$, this yields $x^3 + ax^2 + bx + c - (\lambda x + v)^2 = (x - x_1)(x - x_2)(x - x_3)$. Because all coefficients in this expression are integers, this yields:

$$x^3 + \overline{a}x^2 + \overline{b}x + \overline{c} - (\overline{\lambda}x + \overline{v})^2 = (x - \overline{x_1})(x - \overline{x_2})(x - \overline{x_3})$$

and, $\overline{y_i} = \overline{\lambda}\overline{x_i} + \overline{v}$ for $i = 1, 2, 3$. So, the line $y = \overline{\lambda}x + \overline{v}$ intersects $\overline{E}(\mathbb{F}_p)$ at the points $\overline{P_1}, \overline{P_2}$, and $\overline{P_3}$, yielding the result that $\overline{P_1} + \overline{P_2} + \overline{P_3} = \overline{\mathcal{O}}$. ✓

Thus, all cases end in the result that $P_1 + P_2 + P_3 = \mathcal{O}$ implies that $\overline{P_1} + \overline{P_2} + \overline{P_3} = \overline{\mathcal{O}}$, proving that the map between groups is a homomorphism. □

As an additional result, if $p \nmid 2D$, then the mapping is an *isomorphism* from Φ onto a subgroup of $\overline{E}(\mathbb{F}_p)$. This is because every nonzero $(x, y) \in \Phi$ is sent to some $(\overline{x}, \overline{y})$ in $\overline{E}(\mathbb{F}_p)$, and not to $\overline{\mathcal{O}}$, so $\mathcal{O}$ is the sole element of the kernel of the reduction modulo p map, making the relation between groups necessarily one-to-one.

6.3. **Finding Torsion Points – Two Examples.** We conclude with two examples that allow us, using the Nagell-Lutz theorem and the Reduction Modulo p Theorem, to find the number of torsion points on an elliptic curve over $\mathbb{Q}$.

Example 6.3. Let E be the elliptic curve defined by the equation $y^2 = x^3 + 5$. We will use the Nagell-Lutz theorem and some basic properties to find the torsion points of E. For this equation, we have that $D = -675 = -1 \cdot 3^3 \cdot 5^2$, so this gives us the set of y coordinates we must consider:

$$\{\pm 1, \pm 3, \pm 9, \pm 15, \pm 25, \pm 27, \pm 45, \pm 75, \pm 225, \pm 675\}$$

While it's possible to check all of these by hand, there is an easier way to check. All possible values of y are divisible either by 3 or 5, or by both. If we consider the y-values divisible by 5, we know that if $5 \mid y$, then the equation $y^2 = x^3 + 5$ implies that x is divisible by 5. However, this means that the equation $5 = y^2 - x^3$ implies that 5 is divisible by 25, because the right side of this equation contains only terms that are divisible by 5, and squared. Obviously this is a contradiction, so none of our points with integer coordinates and y divisible by 5 lie on E. Additionally, it is obvious from the equation $y^2 = x^3 + 5$ that points with $y = \pm 1$ cannot lie on E and have integer coordinates. This leaves us with:

$$\{\pm 3, \pm 9, \pm 27\}$$

This is substantially easier to check by hand. If we are to do this, we see that none of these points satisfy our equation. Thus, the elliptic curve E has no points of finite order other than $\mathcal{O}$, and $\#E = 1$.

Example 6.4. Let E be the elliptic curve defined by the equation $y^2 = x^3 + 3$. We will use the Nagell-Lutz Theorem and the Reduction Modulo p Theorem to find the rational torsion points on E.

For this curve, we have that $D = -243 = -3^5$. So, from the Reduction Modulo p theorem, we know that there is an injective homomorphic correspondence between the torsion points of E and the points in the reductions $\overline{E}(\mathbb{F}_5)$ and $\overline{E}(\mathbb{F}_7)$. Lagrange's Theorem, a concept in group theory, requires that $\#E \mid \#E(\mathbb{F}_5)$ and $\#E \mid \#E(\mathbb{F}_7)$. Thus, because $\overline{E}(\mathbb{F}_5)$ and $\overline{E}(\mathbb{F}_7)$ are coprime, we must have that $\#E = 1$, a result that implies that $\mathcal{O}$ is the sole torsion point in $E(\mathbb{Q})$.

Resources

All graphics in this paper were created using Wolfram Mathematica. The Mathematica files are available publicly at http://bit.ly/1fmpKLU.

Acknowledgements

First and foremost, I would like to thank my advisor, Chang Mou Lim, for his invaluable guidance, suggestions, and advice throughout the process of writing this paper. Chang Mou provided me with the direction to delve headfirst into a topic (and really, an entire branch of mathematics) with which I had absolutely no prior experience, and did so with a sense of patience and understanding for which I am very grateful. I could not have done this without him. I'd like to thank the professors and organizers of the 2013 UChicago Math REU, for teaching me more about mathematics than I've ever learned before, and in such a short time. I'd also like to thank my parents and family for their support of my endeavors, academic or otherwise - I am truly lucky to have such a strong and lasting source

of support and confidence. Thank you to Eddie Herman, whose help during the school year was truly instrumental in making my participation in the REU possible. Finally, thank you to all of the students in the REU who made the program such a positive experience, especially Freddy Boulton and Kira Ghandhi. It was a pleasure spending a summer with you all.

References

[1] Joseph H. Silverman and John Tate. Rational Points on Elliptic Curves. Springer. 2010.
[2] Joseph H. Silverman. The Arithmetic of Elliptic Curves. Springer. 2009.
[3] David S. Dummit, and Richard M. Foote. Abstract Algebra. Wiley. 2013.