RATIONAL POINTS ON CURVES

BLANCA VIÑA PATIÑO

Contents

1. Introduction

Consider polynomial equations with integer coefficients where we look for rational solutions. Diophantus initiated the study of these equations around AD 200 which is why we refer to them as Diophantine equations. Mathematicians have been interested in them for hundreds of years, and as a consequence, the study has given rise to different mathematical subjects, results, and methods. Hilbert's 10th problem asked if there existed an algorithm for determining whether any Diophantine equation had a solution with integer values. In 1970, Yuri Matiyasevich, along with a few other mathematicians, proved that no such algorithm existed. However, studying specific types of Diophantine equations and describing their solution sets is still an interesting and difficult problem.

The paper "Invitation to Integral and Rational points on Curves and Surfaces" by P. Das and A. Turchet explores solution sets by examining geometric and arithmetic properties of curves. We will see that solving Diophantine equations often reduces to studying rational points on their respective curve representation. A point (x, y) is a rational point if the coordinates x, y are rational numbers. Additionally, if x, y satisfy $f(x, y) = 0$ for some f, we call x, y rational solutions to f. We will explore algebraic and geometric properties of curves. In particular, we will look at curves based on 'genus', an invariant, which we will define later. Then, we will consider specific examples for curves of different genus, namely the Pell Equation and Elliptic curves, to see how genus can correlate to the number of solutions an equation may have. Finally, we will cite important results, including Faltings' Theorem, the Uniformity Conjecture, and a few others as well as discuss their significance.

2. Algebraic Curves

We consider the solutions to Diophantine equations as curves to understand the relationship between genus and the number of rational points. First, we define some some technical terms from algebraic geometry that will be essential to our discussion.

Assuming the reader has a basic understanding of abstract algebra, we will move on to defining algebraic curves and their geometric properties. A *plane affine algebraic curve* $\mathbb{C}$ defined over a field K is the set of points $(x, y) \in K^2$ that satisfy $f(x, y) = 0$ where $f \in K[x, y]$. For simplicity, we will focus on affine plane curves over $\mathbb{Q}$.

To every affine algebraic curve we can associate a projective curve in the projective plane $\mathbb{P}^2$. The reason for working in projective space is so that there we can find as many solutions as possible to polynomial equations.

Definition 2.1. *The projective plane is set of equivalence classes of triples* $[a : b : c]$*, with* a, b, c *not all 0, such that two triples* $[a : b : c]$ *and* $[a' : b' : c']$ *are considered to be the same point if there is a nonzero* t *such that* $a = ta'$*,* $b = tb'$*, and* $c = tc'$*,* a, b, c *are said to be homogeneous coordinates for the point* $[a, b, c]$*.*

For instance, the point $(x, y) \in \mathbb{A}^2$, can be associated to $[x, y, 1] \in \mathbb{P}^2$. Now suppose you have $[a, b, c] \in \mathbb{P}^2$, then we associate $(a/c, b/c) \in \mathbb{A}^2$. The points where $c = 0$, are points not in $\mathbb{A}^2$, but are in $\mathbb{P}^2$. These points in $\mathbb{P}^2$ are known as 'points at infinity'. Thus, $\mathbb{P}^2$ is the set of all affine points adjoining the points at infinity, so we can see that $\mathbb{A} \subset \mathbb{P}^2$. In order to define curves in $\mathbb{P}^2$, we need polynomials in three variables because points in $\mathbb{P}^2$ are represented by homogeneous triples. However, we saw that each point in $\mathbb{P}^2$ can be represented by several different homogeneous triples. Hence we look only at polynomials with the property that if $f(a, b, c) = 0$, then $f(ta, tb, tc) = 0$ for all t. These are calledhomogeneous polynomials, and we use them to define curves in $\mathbb{P}^2$.

Definition 2.2. *A polynomial* $f(X, Y, Z)$ *is called a homogeneous polynomial of degree* d *if it satisfies the identity*

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

Now we have the tools to define projective curves.

Definition 2.3. *A projective curve* C *defined over* K *is the set of points* $[x : y : z] \in \mathbb{P}^2$ *that satisfy*

$$f(x, y, z) = 0$$

where $f \in K[x, y, z]$ *is a non-constant homogeneous polynomial.*

Note that a curve is *irreducible* if its defining polynomial cannot be factored into two non-constant polynomials. The *degree* of an irreducible curve is the degree of a defining polynomial for the curve. For example, a line given by $ax+by+c = 0$ is irreducible where $ax+by+c$ is the defining polynomial, and is a curve of degree 1. The reason for considering irreducible curves can be explained by a simple example. The equations $f(x) = x = 0$ and $f(x) = x^2 = 0$ define the same curve since they have the

same solution, $x = 0$. Notice that x^2 is not irreducible since it can be factored into $x \cdot x$. Hence we consider irreducible curves. In the following sections we will look at sets of solutions to both affine and projective curves. Prior to that, we must define genus as it is the invariant by which we hope to classify curves. Genus depends on the degree of a curve as well as the multiplicities of singular points. If C is a curve and $P = (a, b) \in C$ then P is called a *simple point* of C if either partial derivatives $C_x(P) \neq 0$ or $C_y(P) \neq 0$. In this case, the tangent line at P is well defined. A point that is not simple is called a *multiple* or *singular* point. A curve with only simple points is called a *non-singular*. We let $m_P(C)$ be the multiplicity of a singular point which represents the number of times P appears as a root of $C : f(x, y) = 0$. Furthermore, a singular point P on the curve is called an *ordinary multiple point* if it has $m_P(C)$ distinct tangents at P. For a more thorough discussion on local properties of plane curves, refer to [7].

Proposition 2.4. *Let C be a curve with at most ordinary multiple points. Then the genus of C is given by*

$$g = \frac{(d-1)(d-2)}{2} - \sum_{P_{sing}} \frac{m_P(C)(m_P(C)-1)}{2}$$

where d is the degree of C.

The degree-genus formula above is a way to compute the genus and we will use it as our definition of genus for this paper. In general, when given a curve, as long as the curve is not 'too' singular, the genus increases as the degree of the curve increases. If a curve is non-singular, the genus is solely given by the degree of the curve. In the next few sections will discuss the role of genus and other algebraic properties of curves that give us insight into their solution sets.

3. Genus 0

By our definition of genus, smooth curves of genus 0 are given by polynomial equations of degree 1 or 2, namely lines and conics. The general equation of a line is $g(x, y) = ax+by+c = 0$. Similarly, the general conic equation is given by

$$g(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0 \tag{3.1}$$

Since we are interested in Diophantine equations, we will consider lines and conics with rational coefficients. Furthermore, lines and conics are simple objects that most people are familiar with, so understanding their set of rational points is essential to understand those of curves with higher genus.

Definition 3.1. *We call $(x, y) \in C : g(x, y) = 0$ rational if $(x, y) \in \mathbb{Q}^2$.*

Equations of degree 1 with rational coefficients, or lines with rational coefficients, have infinite solutions. Next we want to see if the same holds for curves of genus 0, but of degree 2. One example of extensively studied smooth curves with genus 0 and degree 2 are those given by Pell equations. It is interesting to note that Pell equations represent hyperbolas in the plane. An application of Pell equations is in Diophantine approximation since they can be used to approximate quadratic irrationals.

Pell equations are of the form

$$x^2 - dy^2 = 1 \tag{3.2}$$

where $d \in \mathbb{N}$ and where d is not a perfect square. If d were a perfect square, i.e. $d = n^2$, the equation has only the trivial solutions $(-1, 0)$ and $(1, 0)$; when $(x, y) \in \mathbb{Z}^2$, we have $(x + ny)(xny) = 1$, so $x = \pm ny$ have both to divide 1 and thus must be equal to ± 1. Note that the trivial solutions are always solutions to the Pell equation, but we want to hopefully find all possible solutions. Additionally, if (x, y) is a solution, then so is $(-x, -y)$, so we can focus on positive solutions. We can do this by using the continued fraction expansion of $\sqrt{d}$.

Definition 3.2. *A continued fraction is an expression of the form*

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}}$$

and it is a theorem that irrational numbers can be written as infinite continued fractions. Typically, we express the infinite continued fraction as $[a_1, \ldots, a_n, \ldots]$.

Definition 3.3. *The n^{th} convergent of an irrational number $\alpha = [a_1, \ldots, a_n, \ldots]$ is defined as the rational number $\frac{p_n}{q_n}$ that satisfies:*

$$\frac{p_n}{q_n} = [a_1, a_2, \ldots, a_n]$$

The reader may refer to chapters 12 and 13 in [8] for more details about continued fractions and the Pell equation. The next example will show how the continued fraction expansion of $\sqrt{d}$ allows us to find solutions to the Pell equation.

Example 3.4. *Suppose you have the following Pell equation with $d = 2$:*

$$x^2 - 2y^2 = 1 \tag{3.3}$$

Then, the continued fraction expansion of $\sqrt{2}$ is

$$\begin{aligned} \sqrt{2} &= 1 + \frac{1}{1 + \sqrt{2}} \\ &= 1 + \frac{1}{1 + (1 + \frac{1}{1+\sqrt{2}})} \\ &= 1 + \frac{1}{2 + \frac{1}{1+\sqrt{2}}} \ldots \end{aligned}$$

The first convergent is $\frac{3}{2}$. Notice that setting $x = 3$ and $y = 2$ in (3.2) gives a solution. Furthermore, $(-3, 2), (3, -2)$, and $(-3, -2)$ are also solutions. Figure 1 is the curve of (3.2) with the trivial solutions as well as the solutions we found by continued fractions. The convergent that gives the smallest x is known as the fundamental solution. In this example, $(3, 2)$ is the fundamental solution, since one can prove that further convergents yield a larger numerator. So why are we interested in the fundamental solution? The significance of the fundamental solution to a Pell equation is established by the following theorem:

Theorem 3.5. *Let (x_1, y_1) be the fundamental solution of the Pell equation $x^2 - dy^2 = 1$ where d is a positive integer that is not a perfect square. Then all positive solutions (x_k, y_k) are given by*

$$x_k + \sqrt{d}y_k = (x_1 + \sqrt{d}y_1)^k$$

Since we can take k to be any power, the Pell equation has infinitely many integer solutions. Hence we have some evidence that non-singular genus 0 curves have might infinitely many rational solutions.

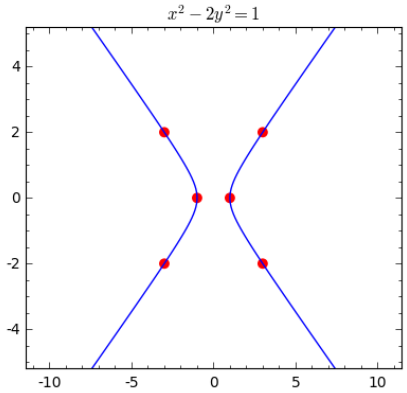

FIGURE 1. Plane curve of Pell equation with $d = 2$

However, consider the equation $x^2 + y^2 - 3 = 0$ representing the circle of radius $\sqrt{3}$. The curve is non-singular and of degree 2 so has genus 0.

Example 3.6. *Claim: $x^2 + y^2 - 3 = 0$ has no rational solutions. Suppose for contradiction that the equation has a rational solution. Then there exist $a, b, c \in \mathbb{Z}$, with $c \neq 0$, such that $x = \frac{a}{c}$ and $y = \frac{b}{c}$. Hence $a^2 + b^2 = 3c^2$ and a, b, c have no common factor greater than 1. Note that $a^2 + b^2$ is divisible by 3 since $3q^2$ is. It follows that a and b are divisible by 3 since if one or both of a and b is not divisible by 3, then*

$$a^2 + b^2 \equiv 1 (mod\ 3) \qquad or \qquad a^2 + b^2 \equiv 2 (mod\ 3)$$

It then follows that c is divisible by 3, contradicting our assumption that a, b, c have no common divisor greater than 1.

These examples provide some evidence that non-singular curves of genus 0 have either infinite or no rational points. In general, the following theorem states that the existence of one rational point on a conic implies that there are infinitely many rational points. The proof is fairly simple to understand as it takes an intuitive geometric approach. First we provide a useful theorem and then a simple example to motivate the geometric process of finding rational points on a conic where we know there exists one rational point.

Theorem 3.7 (Bézout's theorem)**.** *LetC_1 and C_2 be non-singular projective curves with only transversal intersections. Then,*

$$\#(C_1 \cap C_2) = (deg\ C_1)(deg\ C_2)$$

Example 3.8. *Consider the equation $x^2 + y^2 = 1$, the equation for the unit circle shown in Figure 2. Expressing this in the general form, we have $g(x, y) = x^2+y^2-1 = 0$. Then, we know there exists a rational point $(\frac{3}{5}, \frac{4}{5})$ which we will denote by $\mathcal{P}$. Then we can pick a line with rational slope going through $\mathcal{P}$ which will intersect at another point $\mathcal{Q}$ by Bézout's theorem. $\mathcal{Q}$ will also be rational since our line equation has rational coefficients and we are plugging in a rational point. For instance, if we take the line $y = \frac{1}{3}x + \frac{3}{5}$ through $\mathcal{P}$, we have another intersection at $\mathcal{Q} = (-\frac{24}{25}, \frac{7}{25})$.*

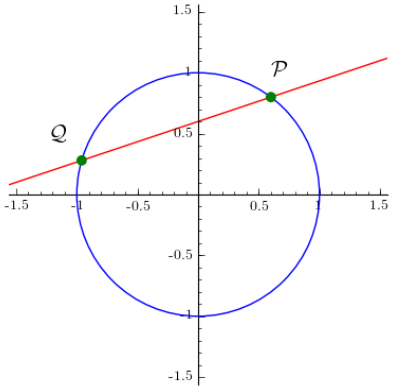

FIGURE 2. Unit circle with known rational point $\mathcal{P}$ and rational line intersecting at that point.

In the above example, we took one rational line, but we can take infinitely many rational lines through $\mathcal{P}$ and obtain infinitely many rational points on the conic. Now we are ready to consider the general case. For convention, we let $C(\mathbb{Q})$ denote the set of rational points on a curve C.

Proposition 3.9. *Given a smooth projective curve C defined over $\mathbb{Q}$ of genus 0, one of the following holds:*

(1) *If $C(\mathbb{Q}) \neq \emptyset$, then $C(\mathbb{Q})$ is infinite*
(2) *$C(\mathbb{Q}$ is empty*

Proof. In the case when $C(\mathbb{Q}) = \emptyset$ there is nothing to prove, so we prove (1). Suppose there exists a rational point $(\overline{x}, \overline{y})$ on $C : g(x, y) = 0$. Now take the line L parameterized by $x = \overline{x} + tu$ and $y = \overline{y} + t$ where $u \in \mathbb{Q}$. L will intersect the conic at another point by Bezout Theorem. We claim that the second point of intersection is also a rational point.

$$g(\overline{x} + tu, \overline{y} + t) = a(\overline{x} + tu)^2 + b(\overline{x} + tu)(\overline{y} + t) + \\ + c(\overline{y} + t)^2 + d(\overline{x} + tu) + e(\overline{y} + t) + f$$

Since the first point $(\overline{x}, \overline{y})$ corresponds to $t = 0$ in L and $g(\overline{x}, \overline{y}) = 0$, we can see that the constant term f vanishes. We continue to simplify and get

$$g(\overline{x}, \overline{y}) = t^2(au^2 + bu + c) + t(du + e + 2a\overline{x} + b\overline{x} + b\overline{y}u + 2c\overline{y})$$

Therefore, after rearranging, the second intersection point corresponds to

$$t_2 = \frac{du + e + 2au\overline{x} + b\overline{x} + b\overline{y}u + 2c\overline{y}}{au^2 + bu + c}$$

Since $u \in \mathbb{Q}$ can be chosen arbitrarily, we get infinitely many valued for t_2 and hence infinitely many rational points on the curve given by $(\overline{x} + t_2 u, \overline{y} + t_2)$. Thus, as long as we find one rational point, we can find infinitely many rational points on a conic, proving the result. □

Note that the above proposition only applies to smooth conics. However, one can prove that singular conics are unions of overlapping lines. Thus, the proposition can be extended to singular conics.

4. Genus 1

The genus equation we provided in section 2 tells us that smooth cubics are genus 1. A smooth projective curve of genus 1 over $\mathbb{Q}$ with a rational point is called an *elliptic curve* over $\mathbb{Q}$. Our main focus will be elliptic curves since they have been thoroughly studied in different areas of mathematics and their group structure makes them more approachable than other curves. First we will provide some definitions and then prove the Mordell-Weil theorem. Up to change of coordinates, any elliptic curve can be rewritten in *Weierstrass normal from* which is

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

Eaquations in Weierstrass normal form are symmetric about the x-axis. As well as affine solutions, we would like to include solutions in $\mathbb{P}^2$. Thus we can extend $E(x, y)$ to a function $E(x, y, z)$ by homogenizing. This means that we want $E(x, y, z)$ to be a homogeneouos polynomial and $E(x, y)$ to correspond to $E(x, y, 1)$. The method of homogenization is explained in [6]. With this in mind, we denote the set of rational points on an elliptic curve by $E(\mathbb{Q})$ and defined to be

$$E(\mathbb{Q}) = \{(x, y, z) \in \mathbb{P}^2 : E(x, y, z) = x^3y^2z + axz^2 + bz^3 = 0\} \tag{4.1}$$

Note that the only point in $E(\mathbb{Q})$ with $z = 0$ is the point $(0, 1, 0)$ which represents the point at infinity, $\mathcal{O}$.

When we discussed conics earlier, we saw that if a rational point is already known, we can find more by a geometric method. Similarly, in elliptic curves, given two rational points, $\mathcal{P}$ and $\mathcal{Q}$, we can take the line between these points, $\mathcal{PQ}$, and obtain a third intersection $\mathcal{P} * \mathcal{Q}$ by Bézout's theorem. $\mathcal{PQ}$ will have rational coefficients so $\mathcal{P} * \mathcal{Q}$ is also rational. Finally, we can reflect this $\mathcal{P} * \mathcal{Q}$ about the x-axis to obtain another rational point which we call $\mathcal{P} + \mathcal{Q}$. We claim that the binary operation $+$ makes the set $E(\mathbb{Q})$ into an abelian group. This operation will be refered to as 'adding points' on elliptic curves. Figure 3 provides a visual interpretation of adding points.

4.1. Group of $E(\mathbb{Q})$.

By the discussion on adding points above, we can define the following.

Definition 4.1. *Let E be a an elliptic curve and take the point at infinity on E to be $\mathcal{O}$. Then, for for arbitrary rational points $\mathcal{P}, \mathcal{Q} \in E$, define $\mathcal{P} + \mathcal{Q} = \mathcal{O} * (\mathcal{P} * \mathcal{Q})$.*

After establishing the binary operation of adding points on elliptic curves, we claim that the set of rational points forms an abelian group. The reader will notice that proving commutativity as well existence of an identity and inverses is rather simple. However, proving the associativity property for rational points on elliptic curves is tidious. Due to this, we will assume associativity is satisfied and prove the other properties.

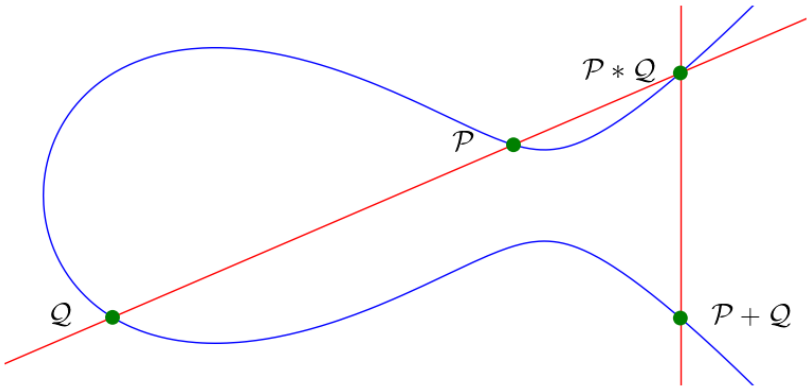

FIGURE 3. Adding points on elliptic curves

Theorem 4.2. *In the conditions of the definition above,* $(E(\mathbb{Q}), +)$ *is an abelian group.*

The following propositions, along with the associativity property (not proven in this paper), will prove the above theorem. For a proof and explanation of the associativity property refer to [6].

Proposition 4.3. *The operation* $+$ *on* $E(\mathbb{Q})$ *is commutative.*

Proof. Commutativity of $+$ is implied by the commutativity of $*$ which is obvious. □

Proposition 4.4. *The point at infinity,* $\mathcal{O}$*, is the identity on* $E(\mathbb{Q})$*.*

Proof. Suppose $\mathcal{Q} = \mathcal{O}$ and $\mathcal{P} \in E$. Then $\mathcal{P} + \mathcal{O} = \mathcal{O} * (\mathcal{P} * \mathcal{O})$. The line $\mathcal{P}\mathcal{O}$ intersects E at $\mathcal{P}, \mathcal{O}$, and $\mathcal{P} * \mathcal{O}$. This line is the same as the line $\mathcal{O}(\mathcal{O} * \mathcal{P})$ since it intersects E at the same points. Hence $\mathcal{O}(\mathcal{O} * \mathcal{P}) = P$ which implies $\mathcal{O}$ is the identity on $(E(\mathbb{Q}), +)$ □

Proposition 4.5. $E(\mathbb{Q})$ *has inverse elements.*

Proof. Let $\mathcal{P} \in E(\mathbb{Q})$, $\mathcal{S} = \mathcal{O} + \mathcal{O}$, and $\mathcal{P}' = \mathcal{P} * \mathcal{S}$. Then, $\mathcal{P} * \mathcal{P}' = \mathcal{S}$ and $\mathcal{P} + \mathcal{P}' = \mathcal{O} * \mathcal{S} = \mathcal{O}$. Hence $\mathcal{P}'$ is an inverse for $\mathcal{P}$ □

4.2. **Mordell-Weil Theorem.** Now that we have formally defined ellitic curves and their group law, we can prove the Mordell-Weil Theorem which states that the group $E(\mathbb{Q})$ is finitely generated. This theorem requires that $E(\mathbb{Q})/2\mathbb{Q}$ is finite, which is the statement of the Weak Mordell-Weil theorem. Here, we use $2E(\mathbb{Q})$ to denote the subgroup of $E(\mathbb{Q})$ consisting of points which are twice other points. In addition, we also need the existence of a height function with specific properties. Height functions and the Weak Mordell-Weil theorem will not be discussed in this paper, but more details can be found in [6]. Thus we will prove the Mordell-Weil theorem by assuming certain facts and applying some basic group theory.

First, we define the *height* of a rational point.

Definition 4.6. *Let* $P = (x, y)$ *be a rational point on* E *and let* $x = \frac{a}{b}$*. Then the height of* P *is given in terms of the* x *coordinate:*

$$H(P) = H(x) = H\left(\frac{a}{b}\right) = \max\{|a|, |b|\}$$

for convenience we will define 'small h' to be

$$h(P) = \log H(P)$$

Assuming the Weak Mordell-Weil theorem as well as three other properties of a height function, we are ready to prove the Mordell-Weil Theorem.

Theorem 4.7. *(Mordell-Weil) Let $E(\mathbb{Q})$ represent the abelian group of rational points on E. Suppose that there exists a function*

$$h : E(\mathbb{Q}) \to [0, \infty)$$

with the following properties:

(1) *For every real number M, the set $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ is finite.*
(2) *For every $P_0 \in E(\mathbb{Q})$, there is a constant k_0 so that*

$$h(P + P_0) \leq 2h(P) + k_0 \qquad \text{for all } P \in E(\mathbb{Q})$$

(3) *There is a constant k so that*

$$h(2P) \geq 4h(P) - k \qquad \text{for all } P \in E(\mathbb{Q})$$

(4) *The subgroup $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

Then $E(\mathbb{Q})$ is finitely generated.

Proof. We know that there are finitely many cosets of $2E(\mathbb{Q})$ so let $Q_1, Q_2, \ldots, Q_n$ be representatives for the cosets. Let i_1 denote indexing of cosets. Then for any $P \in E(\mathbb{Q})$,

$$P - Q_{i_1} \in 2E(\mathbb{Q})$$

since P has to be in a coset. Hence, we can rewrite

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

For some $P_1 \in E(\mathbb{Q})$. We apply the same method to P_1 and so on to obtain

$$\begin{aligned} P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\ldots \\ P_{m-1} - Q_{i_m} &= 2P_m \end{aligned}$$

where each Q_{i_j} are chosen coset representatives from our original list. Additionally, $P_j \in E(\mathbb{Q})$. With these equations, we can do some substitution rewrite P as

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \ldots + 2^{m-1}Q_{i_m} + 2^m P_m \tag{4.2}$$

This shows us that $P \in E(\mathbb{Q})$ is generated by the cosets as well as P_m. Note that by (1) the set of points with height less than some arbitrary bound M is finite. Hence it suffices to show we can pick m large enough so that the height of P_m will be less than a fixed bound. Then the finite set of points with height less than the height of P_m and the Q_is will generate $E(\mathbb{Q})$.

Pick P_j and apply (2) with $-Q_i = P_0$. Doing so we get

$$h(P_{j-1} - Q_i) = h(2P_j) \leq h(P_{j-1}) + k_j$$

By (3), we have

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

rearranging terms,

$$h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{k'+k}{4} =$$
$$= \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (k'+k))$$

So in the case when $h(P_j) \geq k' + k$, we have

$$h(P_j) \leq \frac{3}{4}h(P_{j-1})$$

The heights will approach 0 as $j \to \infty$ so we can find m so that $h(P_m) \leq k' + k$. Thus every element in $E(\mathbb{Q})$ can be written as

$$P = a_1Q_1 + a_2Q_2 + \ldots + a_nQ_n + 2^mR$$

for $a_i \in \mathbb{Z}$ and $R \in E(\mathbb{Q})$ that satisfies $h(R) \leq k' + k$. Hence the finite set of points with height less than $k' + k$ along with the Q_is will generate the group of rational points on E. □

In particular, the theorem implies that we can always find a finite extension of $\mathbb{Q}$ for which any given elliptic curve has infinitely many rational points. The proof requires more than the elementary group theory we have used to prove the theorem above, so for more details, refer to [6].

5. Genus ≥ 2

Describing the set of rational points of genus 1 curves, particularly elliptic curves, was more difficult than describing the set of rational points for genus 0 curves. These difficulties were due to the way lines intersect with cubics and the required group theory to prove that the set of rational points on an elliptic curve is a finite set. Describing the set of rational points for genus 2 curves is even more complicated. The Mordell Conjecture, one of the most famous problems in arithmetic geometry, hypothesized that curves of genus 2 or higher had a finite number of solutions. Gerd Faltings, a German mathematician, proved the result in 1983. The theorem states the following

Theorem 5.1. ***Faltings' Theorem (1983)*** *Let C be a smooth curve defined over $\mathbb{Q}$ of genus ≥ 2. Then, the number of rational points on C is finite.*

In other words, Faltings' theorem tells us that all curves which have genus 2 have a finite number rational points. Faltings' theorem can be applied to curves over finite extensions of $\mathbb{Q}$, which is much stronger. Additionally, the theorem provides an effective upper bound for the number of rational points on a given curve, but it depends on many different properties. The proof of the theorem is highly nontrivial and beyond the scope of this paper, but the reader may refer to [3] for the proof.

6. Uniformity of Rational Points

Faltings' theorem gives a result based on solely the genus of curves. Since the theorem was proven, mathematicians have wondered if the genus can tell us anything else about the number of rational points that a curve may have. Lucia Caporaso, Joe Harris and Barry Mazur raised a relevant question in their paper "Uniformity of Rational Points". The conjecture in their paper states the following

Conjecture 6.1. ***Uniformity Conjecture*** *Let $g \geq 2$ be an integer. There exists a number $B(g)$, depending only on g, such that for any smooth curve C with fixed genus g defined over $\mathbb{Q}$, the number of rational points on C is less than $B(g)$.*

Although this result is a conjecture, it suggests that genus essentially categorizes curves by the upper bound to number of solutions they may have. Another reason for its importance is that there exists a large amount of evidence supporting the conjecture. One example is the following theorem:

Theorem 6.2. ***Katz, Rabinoff, Zureick-Brown*** *(2016) Let C be any smooth curve of genus g and let $r = rank(J_C)$. Suppose that $0 \leq r \leq g-3$. Then,*

$$\#C(\mathbb{Q}) \leq 84g^2 - 98g + 28$$

Understanding the concepts required for this theorem, such as $rank(J_C)$, requires some knowledge of algebraic geometry. However, for our purposes, note that since r is non negative this theorem applies to curves of genus 3 or higher. Hence the theorem provides an upper bound on the number of rational points that is solely dependent on the genus, thus supporting the Uniformity Conjecture.

7. Conclusion

By Faltings' theorem, we know that for genus 0 the solution set is either infinite or empty. We proved this by drawing lines with rational slope through a known rational point and then seeing that the line intersected the curve at another rational point. Then for genus 1 curves, like Elliptic curves, there are an infinite number of solutions up to a finite extension of $\mathbb{Q}$. To show this we came up with a geometric procedure to find more points from known ones. Then by the Mordell-Weil theorem we saw that the set of rational points on an elliptic curve is a finitely generated set. From these results, we have some evidence that genus, and hence the degree of of a curve, gives us some idea what the set of rational points on a given curve might be. The next step towards uniformity was brought up by Caporaso, Harris, and Mazur who hoped to provide upper bounds on the set of rational points on curves solely dependent on genus [4]. Furthermore, Katz, Rabinoff, Zureick-Brown were also able to provide an upper bound, dependent on genus, for curves of genus 3 or higher. However, much is still unknown for curves of genus 2.

References

[1] SageMath. *CoCalc - Collaborative Computation Online* , 2016, `https://cocalc.com/`

[2] Pranabesh Das and Amos Turchet *Invitation to Integral and Rational Points on Curves and Surfaces*(Jul. 2014)

[3] G. Faltings. *Finiteness theorems for abelian varieties over number fields, Arithmetic geometry* (Storrs, Conn., 1984), Springer, New York, 1986, Translated from the German original.

[4] L. Caporaso, J. Harris and B. Mazur, *Uniformity of Rational Points.* Journal of the American Mathematical Society,Vol. 10, No. 1 (Jan., 1997), pp. 1-35.

[5] E. Katz, J. Rabinoff, and D. Zureick-Brown *Diophantine and Tropical Geometry, and Uniformity of Rational Points on Curves.* 30 Jun 2016.

[6] Joseph H. Silverman and John T. Tate *Rational Points on Elliptic Curves* Second Edition. Springer. 2015.

[7] William Fulton *Algebraic Curves*, An Introduction to Algebraic Geometry. 2008.

[8] Kenneth H. Rosen *Elementary Number Theory and its Applications* Fourth Edition. 1999.