university of groningen / faculty of science and engineering / mathematics and applied mathematics

Fruit puzzle and 2-isogeny descent

Naná Giadresco

July 2024

Bachelor's Project Mathematics

July 2024

Student: Naná Giadresco

First supervisor: J. Steffen Müller

Second supervisor: Pınar Kılıçer

Abstract

In 2014, Andrew Bremner and Allan Macleod published a paper regarding a cubic representation problem. The problem is about finding positive integer solutions a, b, c to the equation

$$\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} = N \quad (\star)$$

where N is a positive integer. This equation has a rational solution $(1, -1, 0)$, which allows us to transform it into an elliptic curve over the rationals, and therefore the problem can be translated to finding rational points on an elliptic curve corresponding to positive solutions to $(\star)$.

Elliptic curves play an important role in both pure and applied mathematics, and this thesis explores the rich theory of elliptic curves that revolves around solving the cubic representation problem, providing more insightful details to the paper by Bremner and Macleod. We explain the transformation from the projective curve defined by $(\star)$ to an elliptic curve in Weierstrass form. This is done through a change of coordinates that maps the rational point $(1 : -1 : 0)$ to the point at infinity on the elliptic curve. We compute the torsion subgroup of the elliptic curve and show that the points on the torsion subgroup do not give nonzero solutions to the original problem so points of infinite order are needed. This leads to discussing the method of '2-isogeny descent' used to compute the rank of the elliptic curve. We provide some examples of computing the rank and give some lesser known results about finding solutions to a quartic modulo a prime powers, useful to successfully compute the rank of the elliptic curve.

Acknowledgments

I would like to thank my supervisor J. Steffen Müller for the idea of this very nice project and for his support, as I never felt lost on what I had to do or felt dumb for asking questions. I would like to thank Pınar Kılıçer for being my second supervisor and for sparking my interest in some of the mathematics topics discussed in this thesis as she introduced them to me in the courses she taught me. I would also like to thank Krzysztof Pudowski and Jerzy Olszewski for the feedback and help they gave me, together with the patience they had for listening to me when I was stuck on something in the past months.

Contents

1 Introduction

The study of elliptic curves dates back to the Greeks studying Diophantine equations [Mar06] and they are still widely used and studied now, as in the famous proof of Fermat's Last Theorem by Andrew Wiles. Elliptic curves are both interesting from a purely mathematical perspective as well as having applications in the growing field of cryptography. This paper uses elliptic curves to solve a seemingly very simple fruit puzzle that requires a lot of theory to be able to find its solutions. The fruit puzzle became an internet meme, even though the authors Bremner and Macleod of [BM14], where the solution is discussed, were not involved. Its solutions (and different methods to reach them) were discusses on websites such as [Ami19] and [Ale16]. In this paper we discuss the method of descent by $2-$isogeny to compute the rank of the elliptic curve, as a positive rank allows us to then find a point whose multiple will correspond to a solution to the puzzle. From a theoretical point of view the method of descent by 2-isogeny is used in the proof of Mordell's Theorem in [ST15] for the case where the elliptic curve has a rational two torsion point, and in general, methods of p-descent are studied by many mathematicians [Cre97] [SS03]. Elliptic curves are used in cryptography and specifically, there is an area of cryptography that uses isogenies between elliptic curves to create more secure systems [Shu09].

This thesis is based on the paper 'An Unusual Cubic Representation Problem' written by Bremner and Macleod [BM14] in 2014, and the aim is to provide details to their work. We start by transforming the fruit puzzle into the curve Bremner and Macleod work on, which is a projective curve that depends on a parameter N, and then transform it into an elliptic curve in Weierstrass form. We explain the method of descent by 2-isogeny to compute the rank and provide some examples of how to do so for different values of N, presenting the solutions to the fruit puzzle for the case where the rank is positive. In doing so we also describe some of the results provided in the paper 'Counterexamples to the Hasse Principle' by Aitken and Lemmermeyer [AL11], which illustrate the use of prime powers to show some quartic equations have no solution. This is very useful to a part of the descent by 2-isogeny method which encounters the problem of finding (or showing the lack of) a primitive solution to some equations. We also provide some more remarks on the existence and size of the solutions to the fruit puzzle.

1.1 Outline

We begin the paper with some background information in Section 2, necessary to understand the further sections. If the reader is familiar with elliptic curves and a bit familiar with projective geometry then they can skip the first section. Throughout the rest of the paper each section follows from the previous section. Section 3 describes the fruit puzzle, and how to transform it into an elliptic curve. In Section 4 we show the structure of the elliptic curve and in Section 5, we explain the method of descent by 2-isogeny to compute the rank and provide some examples. We end with some results in Section 6 related to the conditions necessary to ensure solutions to the fruit puzzle and the size of these solutions.

2 Background Information

In order to understand the paper, we need some background information on elliptic curves. The following section is based on [Sil06] and [ST15, Section 1.4]. Throughout this paper we will work in both the affine and projective plane over the field $\mathbb{Q}$, therefore let us define these concepts over $\mathbb{Q}$ before we dive into the theory of elliptic curves.

Definition 2.1 (Projective plane)**.** *The set of $\mathbb{Q}-$rational points on projective plane over $\mathbb{Q}$, denoted as $\mathbb{P}^2(\mathbb{Q})$, is defined as*

$$\mathbb{P}^2(\mathbb{Q}) := \{(x, y, z) \mid x, y, z \in \mathbb{Q} \textit{ not all zero } \}/\sim$$

under the equivalence relation $\sim$ where $(x, y, z) \sim (x', y', z')$ if $(x', y', z') = (\lambda x, \lambda y, \lambda z)$ for some $\lambda \in \mathbb{Q}^*$.

We write the equivalence class as $(x : y : z)$. These are also called *homogeneous coordinates.* In a similar fashion we can define the affine plane over $\mathbb{Q}$ as follows.

Definition 2.2 (Affine plane)**.** *The set of $\mathbb{Q}-$rational points on the affine plane over $\mathbb{Q}$, denoted as $\mathbb{A}^2(\mathbb{Q})$, is defined as*

$$\mathbb{A}^2(\mathbb{Q}) := \{(x, y) \mid x, y \in \mathbb{Q}\}.$$

When we choose to map a point $(x, y, z) \in \mathbb{P}^2(\mathbb{Q})$ with $z \neq 0$ to $(x', y') \in \mathbb{A}^2(\mathbb{Q})$, we do so by diving by the $z-$coordinate so that (x, y, z) becomes $(\frac{x}{z}, \frac{y}{z}, 1)$ and $x' = \frac{x}{z}$ and $y' = \frac{y}{z}$.

Remark 2.3. *We could also map a projective point to an affine one by diving by a different coordinate (such as x or y) as long as they are nonzero, however the mapping is mostly done using z.*

To allow such a transformation to happen, we define all the points where the coordinate that we divide by, in this case the $z-$coordinate, is 0 to be the points at infinity. We say the line $z = 0$ is the *line at infinity.* In the projective plane, parallel lines intersect at infinity. The idea behind this comes from perspective drawing, where there is a focal point in the horizon where all parallel lines meet.

Recall that two points in the projective plane are equivalent if one is the constant multiple of the other. This creates an extra condition on how we define polynomials in the projective plane, as we need the requirement that if a polynomial $F \in \mathbb{Q}[x, y, z]$ satisfies $F(x, y, z) = 0$ then also $F(\lambda x, \lambda y, \lambda z)$ must be equal to 0. This gives rise to the definition of *homogeneous polynomials.*

Definition 2.4 (Total degree)**.** *The total degree of a monomial $x^n y^m z^l$ where $m, n, l \in \mathbb{Z}_{\geq 0}$ is $d = n + m + l$.*

Definition 2.5 (Homogeneous polynomial)**.** *A polynomial $F \in \mathbb{Q}[x, y, z]$ is said to be homogeneous if each monomial has the same total degree.*

Definition 2.6 (Affine curve)**.** *An affine curve C is defined by a polynomial $f \in \mathbb{Q}[X, Y]$. Its set of $\mathbb{Q}-$rational points is*

$$C(\mathbb{Q}) = \{(x, y) \in \mathbb{A}^2(\mathbb{Q}) : f(x, y) = 0\}$$

A projective curve is defined similarly.

Definition 2.7 (Projective curve)**.** *Let $F \in \mathbb{Q}[X, Y, Z]$ be a homogeneous polynomial of degree more than 1. Then F defines a projective curve C'. Its set of $\mathbb{Q}-$rational points is*

$$C'(\mathbb{Q}) = \{(x : y : z) \in \mathbb{P}^2(\mathbb{Q}) : F(x, y, z) = 0\}.$$

There are multiple definitions of elliptic curves, however since in this paper we always work with elliptic curves over $\mathbb{Q}$, we will define them for the case where the field is $\mathbb{Q}$. Note however that we can define elliptic curves more generally, but for the sake of this paper it is enough to define them for the $\mathbb{Q}$ case.

Definition 2.8 (Elliptic curve in Weierstrass form)**.** *An elliptic curve $E/\mathbb{Q}$ is defined by a Weierstrass equation*

$$y^2z = x^3 + Ax^2z + Bxz^2 + Cz^3 \tag{1}$$

where $A, B, C \in \mathbb{Q}$ and the discriminant $\Delta = -4A^3C + A^2B^2 + 18ABC - 4B^3 - 27C^2 \neq 0$. Its set of $\mathbb{Q}-$rational points is

$$E(\mathbb{Q}) = \{(x : y : z) \in \mathbb{P}^2(\mathbb{Q}) : y^2z = x^3 + Ax^2z + Bxz^2 + Cz^3\}.$$

Elliptic curves have a unique point at infinity, the point $(0 : 1 : 0)$. This specific form of an elliptic curve is called *Weierstrass form*, which is the form that will be used in this paper. More specifically, we will work with the affine version of the elliptic curve. The definition is similar to the projective one, but this time the point at infinity is considered a special point in the affine plane, denoted by $\mathcal{O}$. For simplicity, we work with $E : y^2 = x^3 + Ax^2 + Bx + C$. If we identify $\mathbb{A}^2(\mathbb{Q})$ with its image in $\mathbb{P}^2(\mathbb{Q})$ under the association of (x, y) with $(x : y : 1)$. Then,

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{A}^2(\mathbb{Q}) : y^2 = x^3 + Ax^2 + Bx + C\} \cup \{\mathcal{O}\}$$

where the discriminant is nonzero.

In general, for an elliptic curve defined over $\mathbb{Q}$, the nonzero discriminant ensures that $x^3 + Ax^2 + Bx + C$ has three distinct roots in the algebraic closure of $\mathbb{Q}$.

Remark 2.9. *Throughout this paper we will always work with the case where the constant coefficient C is equal to 0.*

A special property of elliptic curves is that the points on the curve form a group under the addition law. The group consists of the affine points on the curve, together with the point at infinity $\mathcal{O}$ which is the group's identity element.

The group law is defined as follows. Take $P_1, P_2 \in E(\mathbb{Q})$. We have the following cases:

- For all $P \in E(\mathbb{Q})$, $P + \mathcal{O} = P$.
- Let $P = (x, y) \in E(\mathbb{Q})$, then $-P = -(x, y) = (-x, y)$.
- Let $P_1 \neq \pm P_2$. Then for $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ we have that $P_1 + P_2 = (x_3, y_3) = (\lambda^2 - a - x_1 - x_2, x_3\lambda + v)$. Here
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } v = y_1 - x_1\lambda = y_2 - x_2\lambda.$$
- Let $P_1 = P_2 = (x, y)$. Then $P_1 + P_2 = (x_3, y_3) = (\lambda^2 - A - 2x, x\lambda + v)$. Here we have that for $y^2 = f(x)$ being our elliptic curve, $\lambda = \frac{f'(x)}{2y}$ and $v = y - x\lambda$.
- Let $P_1 \neq P_2$ such that $P_1 = -P_2$. Then $P_1 + P_2 = \mathcal{O}$.
- For $\mathcal{O}$ the identity element, $\mathcal{O} + \mathcal{O} + \ldots \mathcal{O} = \mathcal{O}$.

Although these formulas seem to come out of nowhere, there is a geometric intuition behind them. The reader can find this geometric understanding of the addition of points on an elliptic curve on [ST15, Section 1.4]. Another useful formula for addition of points on E is the duplication formula, which is a shortcut to find the point $2P$ given a point P.

Lemma 2.10 (Duplication formula)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and $x(P)$ be the x-coordinate of a point $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$, then*

$$x(2P) = \frac{x^4 - 2Bx^2 + B^2 - 8Cx - 4AC}{4(x^3 + Ax^2 + Bx + C)}.$$

Proof. This follows by using the addition formulas for $P_1 = P_2$ and substituting x^3+Ax^2+Bx+C for y^2 in the denominator of the $x-$coordinate. □

Theorem 2.11. *[Sil06, page 20] The group law makes the group $E(\mathbb{Q})$ a commutative group.*

3 Cubic Representation and Transformation

Imagine we are given a fruit puzzle as in Figure 1, where we want to know the amount of apples, bananas and cherries so that the amount of apples/(bananas + cherries) + bananas/(apples + cherries) + cherries/(apples + bananas) = 4.

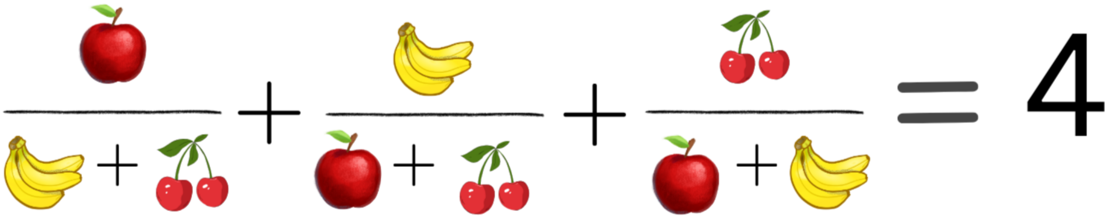

Figure 1: Fruit puzzle for $N = 4$

We can generalize the fruit puzzle for any integer N, not only for the number 4. Writing the puzzle this way implies that N is a positive integer, and so are a = apples, b = bananas and c = cherries, since we want 'full fruits'. This apparently simple fruit puzzle translates into a cubic representation problem. Throughout this paper we will show the following theorem.

Theorem 3.1 (Solution to the fruit puzzle)**.** *The smallest $N > 0$ for which there is a solution to the fruit puzzle is $N = 4$.*

This is already shown in [BM14] but without details and relying on computer algebra to compute ranks of elliptic curves, while in this paper we illustrate the method to do it (mostly) by hand. Suppose we want to represent the integer N using an equation in three variables. This is equivalent to finding positive integer solutions (a, b, c) to the equation

$$\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} = N. \tag{2}$$

This is the equation of a curve C_N in three variables in the projective 2-dimensional space $\mathbb{P}^2_{\mathbb{Q}}$ over the rationals. Note that the curve is symmetric for a, b, c and has the same total degree in each term hence it is already homogenized. This is easier to see once we put all the terms to one side. More formally, the homogenized version is the curve

$$C_N : N(a+b)(b+c)(a+c) = a(a+b)(a+c) + b(b+a)(b+c) + c(c+a)(c+b). \tag{3}$$

Definition 3.2 (Trivial point). *A point $(a, b, c) \in C_N$ is trivial if $a + b = 0$ or $b + c = 0$ or $a + c = 0$. In that case there is no solution to the fruit puzzle. We say a point is nontrivial otherwise.*

The curve C_N (3) has a rational point, namely the point $(1 : -1 : 0)$. Therefore, we can show there exists a bijective transformation

$$\varphi_N : C_N \to E_N$$

where E_N is an elliptic curve in Weierstrass form with an affine equation, $\varphi_N(C_N(\mathbb{Q})) = E_N(\mathbb{Q})$ and $\varphi_N((1 : -1 : 0)) = (0 : 1 : 0)$.

This is done through a series of transformations which allow us to choose the axis in such a way so that we can transform C_N to the elliptic curve E_N. This way we can map the rational point $(1 : -1 : 0)$ on (3) to $\mathcal{O}$. Therefore we make a linear change of coordinates so that the rational point becomes the point at infinity, $(0 : 1 : 0) = \mathcal{O}$. The idea is that the map φ_N maps $(a : b : c)$ to $(x : y : z)$, so that we define x, y, z in terms of a, b, c and then we divide by the $z-$coordinate to get the affine version of the elliptic curve.

Note that the point $(0 : 1 : 0)$ is a point of inflexion on an elliptic curve. The tangent to (3) at the point $(1 : -1 : 0)$ does not intersect the curve C_N again, so $(1 : -1 : 0)$ is a point of inflexion. Thus, the transformation can be done through a simple change of coordinates [Cas91, Chapter 8]. This is done by taking the tangent to $(1 : -1 : 0)$ and letting it be the line $Z = 0$. We then take another line not passing through $(1 : -1 : 0)$ and let it be the line $X = 0$. Finally we let the $Y-$axis be a third line that passes through the point $(1 : -1 : 0)$ which we do as in [ST15, Section 1.3] and in the proof of Proposition 5.7 in [Wut18].

The equation of the tangent line to a curve $F(x, y, z) = 0$ at a point $P = (x_1 : y_1 : z_1)$ is given by the formula

$$x \cdot \frac{\partial F}{\partial x}\bigg|_{x_1} + y \cdot \frac{\partial F}{\partial y}\bigg|_{y_1} + z \cdot \frac{\partial F}{\partial z}\bigg|_{z_1} = 0. \tag{4}$$

Computing the tangent of C_N at $(1 : -1 : 0)$ gives the line

$$(N+2)a + (N+2)b - c = 0$$

and hence we move this line to be equal to Z. We want to let $X = 0$ be another line that passes through the point $(1 : -1 : 0)$ so that it maps this point to $(0 : 1 : 0)$. We do this by letting $X = a + b + 2c$. We can then take Y to be a different line not going through that point such that it maps the rational point $(1 : -1 : 0)$ to $\mathcal{O}$. Taking $Y = a - b$ works. In summary, we have

$$\begin{aligned} \text{X} =& a + b + 2c \\ \text{Y} =& a - b \\ \text{Z} =& (N+2)(a+b) - c. \end{aligned} \tag{5}$$

If we substitute $(1, -1, 0)$ into (X, Y, Z) we get the point $(0 : 2 : 0) = (0 : 1 : 0)$ as desired. We have X, Y, Z in terms of a, b, c but in order to substitute it into (3) to continue the transformation we need to have a, b, c in terms of X, Y, Z. Solving for a, b, c gives us

$$a = \frac{X + (2N+5)Y + 2Z}{2(2N+5)}, \quad b = \frac{X - (2N+5)Y + 2Z}{2(2N+5)}, \quad c = \frac{(N+2)X - Z}{(2N+5)}. \tag{6}$$

Substituting a, b, c into C_N (3) yields

$$\begin{aligned}
&X^2Z\left(2N^3+11N+\frac{27N}{2}-\frac{15}{4}\right)+Y^2Z\left(-2N^3-15N-\frac{75N}{2}-\frac{125}{4}\right)\\
&\quad+XZ^2(-2N-10)+X^3(-2N^2-11N-14)\\
&=\frac{X^2Z(2N+5)(4N^2+12N-3)}{4}-\frac{Y^2Z(2N+5)^3}{4}\\
&\quad-2XZ^2(2N+5)-X^3(2N+5)(N+3)\\
&=0.
\end{aligned}$$

To solve for a, b, c and substitute them into C_N we used SageMath [The21] and the code can be found in Appendix A. We need to transform this projective curve into an affine one. This is done mapping $(X, Y, Z) \mapsto \left(\frac{X}{Z}, \frac{Y}{Z}, 1\right)$. In our case we do this by dividing both sides of the equation by Z^3 which results in

$$\frac{Y^2(2N+35)^3}{4Z^2}=\frac{-X^3(2N+5)(N+3)}{Z^3}+\frac{X^2(2N+5)(4N^2+12N-3)}{4}-2X(2N+5).$$

Letting the new coordinates be $(x_1, y_1) = \left(\frac{X}{Z}, \frac{Y}{Z}\right)$ and multiplying both sides by $\frac{4}{(2N+5)}$ yields

$$y_1^2(2N+5)^2=-4(N+3)x_1^3+(4N^2+12N-3)x_1^2-8x_1.$$

The elliptic curve in Weierstrass form requires the right hand side to be monic. We can get rid of the $-4(N+3)$ in front of the cubic term by letting $x = -4(N+3)x_1$, so $x_1 = \frac{x}{-4(N+3)}$. Substituting x_1 in and clearing denominators gives

$$(y_14(2N+5)(N+3))^2=x^3+(4N^2+12N-3)x^2+32(N+3)x.$$

We are almost there: we want the coefficient of the y_1 term to be 1. Note that the coefficient on the left hand side is a square, and therefore we can do the final change of coordinates by letting $y = 4(2N+5)(N+3)y_1$. This gives us the final result, which is the equation we will work with throughout this paper:

$$E_N : y^2=x^3+(4N^2+12N-3)x^2+32(N+3)x \tag{7}$$

with discriminant $\Delta(E_N) = 2^{14}(N+3)^2(2N-3)(2N+5)^3$.

Tracing back our steps, we can write x, y in terms of a, b and c

$$x=\frac{-4(a+b+2c)(N+3)}{(2+N)(a+b)-c} \quad\text{and}\quad y=\frac{4(a-b)(N+3)(2N+5)}{(2+N)(a+b)-c} \tag{8}$$

The transformation that maps (a, b, c) to (x, y) allows us to also define the following inverse transformation. We used SageMath [The21] using the code found in Appendix A to solve for a, b, c using the two equations we have for x, y. Letting $s = a + b + c$, we get

$$a=-\frac{8\,Ns-sx+sy+24\,s}{2\left((N+3)x-4\,N-12\right)},\quad b=-\frac{8\,Ns-sx-sy+24\,s}{2\left((N+3)x-4\,N-12\right)},\quad c=\frac{4\,Ns+(Ns+2\,s)x+12\,s}{(N+3)x-4\,N-12}.$$

We can further divide by s and rearrange the equations to get

$$\frac{a}{s}=\frac{8(N+3)-x+y}{2(4-x)(N+3)},\qquad \frac{b}{s}=\frac{8(N+3)-x-y}{2(4-x)(N+3)},\qquad \frac{c}{s}=\frac{-4(N+3)-(N+2)x}{(4-x)(N+3)}. \tag{9}$$

In [BM14, page 30] they provide the elliptic curve E_N together with the maps (8) and (9), but they do not explain the steps of how to transform C_N into E_N.

To solve the original fruit puzzle (1) we want to find the rational points $(x, y) \in E_N(\mathbb{Q})$ of (7) which give us positive integer solutions to the projective equation. The following sections describe the theory needed to be able to effectively solve this simple looking fruit puzzle.

4 Mordell's Theorem and the Torsion Subgroup

Since we want to find rational points $(x, y) \in E_N(\mathbb{Q})$ which then correspond to rational points $(a : b : c)$ in the projective plane, it is useful to know what $E_N(\mathbb{Q})$ looks like.

As we already know, the rational points on the elliptic curve form a group, and this group has a specific form, which is described by Mordell's Theorem.

Theorem 4.1 (Mordell's Theorem)**.** *[ST15, page 95] Let E be an elliptic curve in Weierstrass form*

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

where $a, b, c \in \mathbb{Q}$. Then $E(\mathbb{Q})$ is a finitely generated abelian group.

The proof of this theorem is quite lengthy and out of scope for this paper, but if interested the reader can find the proof for $c = 0$ in [ST15, Chapter 3].

In other words,

$$E(\mathbb{Q}) \cong \underbrace{\mathbb{Z} \oplus ... \oplus \mathbb{Z}}_{r\text{-copies}} \oplus \mathbb{Z}/p_1^{t_1}\mathbb{Z} \oplus ... \oplus \mathbb{Z}/p_s^{t_s}\mathbb{Z}$$

where $t_i \in \mathbb{Z}_{>0}$ and p_i is a prime for $i = 1, \ldots, s$.

Here 'r' is called the rank of the elliptic curve. The finite order part is called the *torsion.* This means $E(\mathbb{Q})$ is generated by finitely many points, and hence one can all rational points just by taking intersection of points and tangents to points.

Definition 4.2 (Torsion)**.** *The torsion subgroup of an elliptic curve, denoted $E(\mathbb{Q})_{tors}$ is the set of rational points of finite order on E. It is denoted by*

$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/p_1^{t_1}\mathbb{Z} \oplus ... \oplus \mathbb{Z}/p_s^{t_s}\mathbb{Z}.$$

In the case of our specific curve E_N defined in (7), the torsion subgroup is as follows.

Lemma 4.3. *[BM14, Lemma 2.1] The torsion subgroup of* (7) *is isomorphic to $\mathbb{Z}/6\mathbb{Z}$ if $N \neq 2$, and it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ if $N = 2$.*

Therefore the rational points of our elliptic curve are isomorphic to the group $\mathbb{Z}^r \oplus \mathbb{Z}/6\mathbb{Z}$ where the value of the rank depends on N. Before we begin with the proof of this lemma, we need to introduce a theorem called 'Mazur's Theorem'.

Theorem 4.4 (Mazur's Theorem)**.** *[Maz77, Theorem 8] Suppose E is an elliptic curve and that $E(\mathbb{Q})$ contains a rational point. Then the torsion subgroup of $E/\mathbb{Q}$ is isomorphic to one of the following groups:*

i) $\mathbb{Z}/n\mathbb{Z}$ *for* $n \in \{1, \ldots, 10\}$ *or* $n = 12$

ii) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ *for* $n \in \{1, 2, 3, 4\}$.

This was previously known as *Ogg's Conjecture* and gives us some restrictions on which points to compute to find what the torsion subgroup looks like. For example, if we have a point of order 7, we know we do not need to compute higher orders, as there cannot be such a point by Mazur's Theorem. Using this result, let us come back to the proof of Lemma 4.3.

Proof of Lemma 4.3. A point $P \in E_N(\mathbb{Q})$, $P \neq \mathcal{O}$ has order 2 when $2P = \mathcal{O}$ which is equivalent to saying $P = -P$. Since E_N is in Weierstrass form and the axis of symmetry is the $x-$axis, the points satisfying this are the points with $y-$coordinate 0 and since our curve has no constant term, the point $(0, 0)$ is a point of order 2. The $x-$coordinates of other points of order two are the rational roots of $x^2 + (4N^2 + 12N - 3)x + 32(N + 3)$. The discriminant of the quadratic equation is $(2N - 3)(2N - 5)^3$, which is a square when $(2N - 3)(2N + 5) = (2N + 1)^2 - 16 = \square$.

Claim: $(2N - 3)(2N + 5)$ is a square if and only if $N = 2$.

Proof of Claim. ($\Leftarrow$) Suppose $N = 2$. Then $(2N+1)^2 - 16 = 25 - 16 = 9$ which is a square. ($\Rightarrow$) Note that $2N-3$ and $2N+5$ are both odd. Moreover

$$2N + 5 = 1 \cdot (2N - 3) + 8$$

hence

$$8 = 1 \cdot (2N + 5) - 1 \cdot (2N - 3)$$

and by Bezóut's Theorem [Con, Theorem 3.5], $\gcd(2N+5, 2N-3) \mid 8$. The divisors of 8 are $\{1, 2, 4, 8\}$ but since $(2N-3)$ and $(2N+5)$ are odd, then $\gcd(2N+5, 2N-3) = 1$. Since they are relatively prime, the only way $(2N-3)(2N+5) = \square$ is when both terms are squares. The difference between them is 8, hence we want two squares whose difference is 8. The difference between two consecutive squares is

$$(n+1)^2 - n^2 = 2n + 1$$

which increases as n increases so the difference between squares always grows larger. Thus, there are no two more squares whose difference is 8 and the only time two squares have a difference of 8 is when one square is equal to 1 and the other is equal to 9. Suppose $2N+5 = 1$ then $2N = -4$ and $2N-3 = -7 \neq 9$. Hence $2N-3 = 1$ and $2N+5 = 9$ which implies $N = 2$.

■

Likewise a point has order 3 if and only if $2P = -P$. Recall that $-(x, y) = (x, -y)$ so the $x-$coordinate remains unchanged and we can apply the duplication formula in Lemma (2.10) to $x(2P) = x$ to get

$$\frac{x^4 - 2 \cdot 32(N+3)x + (32(N+3))^2}{4(x^3 + (4N^2 + 12N - 3)x^2 + 32(N+3)x)} = x.$$

If we re-arrange it, we have the following equation

$$3x^4 + 4(4N^2 + 12N - 3)x^3 + 6 \cdot 32(N+3)x^2 - (32(N+2))^2 = 0. \tag{10}$$

Solving (10) for x we have that for any N, the only rational solution to (10) is $x = 4$. We have found that 4 is the only rational solution by checking all the solutions to (10) and noticing that all the others are not rational for any N. We did this using SageMath (see Appendix A). Substituting $x = 4$ into (7) yields

$$4^3 + 4^2(4N^2 + 12N - 3) + 4 \cdot 32(N+3) = 16(2N+5) = y^2$$

hence $y = \pm 4(2N+5)$ which gives the points $(4, \pm 4(2N+5))$.

Since we have points of order 2 and 3, by Lagrange's Theorem, there must be a point of order 6.

Let $P \in E_N(\mathbb{Q})$ be a point of order 6. Then we have that $6P = \mathcal{O}$ which is equivalent to saying there is a point $P = (x, y) \in E_N(\mathbb{Q})$ such that $6P = 3 \cdot 2P = \mathcal{O}$. This means that to find a point of order 6 we can take a general point (x, y) on the curve so that when you double it, the $x-$coordinate corresponds to the $x-$coordinate of a point of order 3. We know that the only possible $x-$coordinate of a point of order 3 is 4, and we can use the duplication formula to find such a point of order 6. In other words,

$$\frac{(x^2 - 32(N+3))^2}{4(x^3 + (4N^2 + 12N - 3)x^2 + 32(N+3))x} = 4$$

which implies

$$x^4 - 16x^3 - 2(32(N+3) + 8(4N^2 + 12N - 3))x^2 - 12 \cdot 32(N+3)x + (32(N+3))^2 = 0.$$

Solving for x being an integer we get that the only such point has $x-$coordinate $x = 8(N+3)$ (see the SageMath code in Appendix A). Therefore

$$\begin{aligned} y^2 &= 8^3(N+3)^3 + 64(4N^2+12N-3)(N+3)^2 + 8\cdot 32(N+3)^2 \\ &= 8^2(N+3)^2(8(N+3)+4N^2+12N-3+4) \\ &= 8^2(N+3)^2(2N+5)^2 \end{aligned}$$

so $y = \pm 8(N+3)(2N+5)$, giving us the points $(8(N+3), \pm 8(N+3)(2N+5))$. By Mazur's Theorem 4.4 we know there are at most two points of order six, so since $8(N+3)$ is a solution to $E_N(\mathbb{Q})$ which gives us two points of order 6, we know there cannot be other rational solutions. Since there is a point of order 6, we need to check whether there is also a point of order 12. We do not need to check other multiples of 6 as $3\cdot 6 = 18$ and Mazur's Theorem 4.4 tells us that there is no such point.

If there were to be a point P of order 12, then such point would satisfy $12P = \mathcal{O}$ so $x(2P) = 8(N+3)$. By the duplication formula we have

$$\begin{aligned} 8(N+3) &= \frac{(x^2-(32(N+3))^2}{4(x^3+(4N^2+12N-3)x^2+32(N+3)x} \\ &= \frac{(x^2-(32(N+3))^2}{4y^2} \end{aligned}$$

implying $8(N+3) = \square$. Hence $4\cdot 2(N+3) = \square$ which means $N+3 = \square/2 \in \mathbb{Z}$ so $N+3 = 2K^2 \iff N = 2K^2-3$ for some integer K. Expanding the duplication formula leads to

$$(x^2-32(N+3))^2 = 32(N+3)(x^3+(4N^2+12N-3)x^2+32(N+3)x)$$

where by substituting $N = 2K^2-3$ we get

$$\begin{aligned} &= x^4 - 64K^2x^3 + (64K^2(-1+24K^2-16K^4))x^2 - 4096K^4x - 1024K^4 \\ &= (x^2+8K(1-4K-4K^2)x+64K^2)(x^2+8K(-1-4K+4K^2)x+64K^2) \\ &= 0. \end{aligned}$$

Solving for x means solving $x^2+8K(1-4K-4K^2)x+64K^2 = 0$. If x were to be rational it would imply the discriminant $4K(2K+1)\sqrt{(2K-1)(2K+3)}$ is rational. But one can check $(2K-1)(2K+3)$ is not a square modulo 8, and hence not a rational square. This is because there is no value of K that satisfies $(2K-1)(2K+3) \equiv \square \bmod 8$ where $\square \in \{0,1,4\}$ which are the squares modulo 8. Therefore x can only be rational when the discriminant is zero, implying $(2K-1)(2K+3)K = 0$. Similarly for $x^2+8K(-1-4K+4K^2)x+64K^2$ we get that x is rational when $K(2K-3)(2K+1) = 0$. Substituting these values of K into $N = 2K^2-3$ lead to the discriminant of E_N being 0 which is not allowed. Hence, we cannot have a point of order 12.

□

Remark 4.5. *We define $E_N(\mathbb{R})$ just as $E_N(\mathbb{Q})$. Then $E_N/\mathbb{R}$ (7) has two components as shown in figure (2) for $N = 4$. One is the 'egg', where $x < 0$ and the other is the unbounded component, with $x \geq 0$. Note that given that all the rational torsion points have positive $x-$coordinate then all the rational torsion points lie on the unbounded component of the curve.*

The points in the torsion subgroup do not lead us to desired solutions of (3). These points do not help us solve our cubic representation problem as they are just rational points on E_N corresponding to trivial points on C_N.

Lemma 4.6. *An integer solution (a,b,c) to the equation C_N is non trivial if and only if the corresponding point $(x,y) \in E_N(\mathbb{Q})$ is of infinite order.*

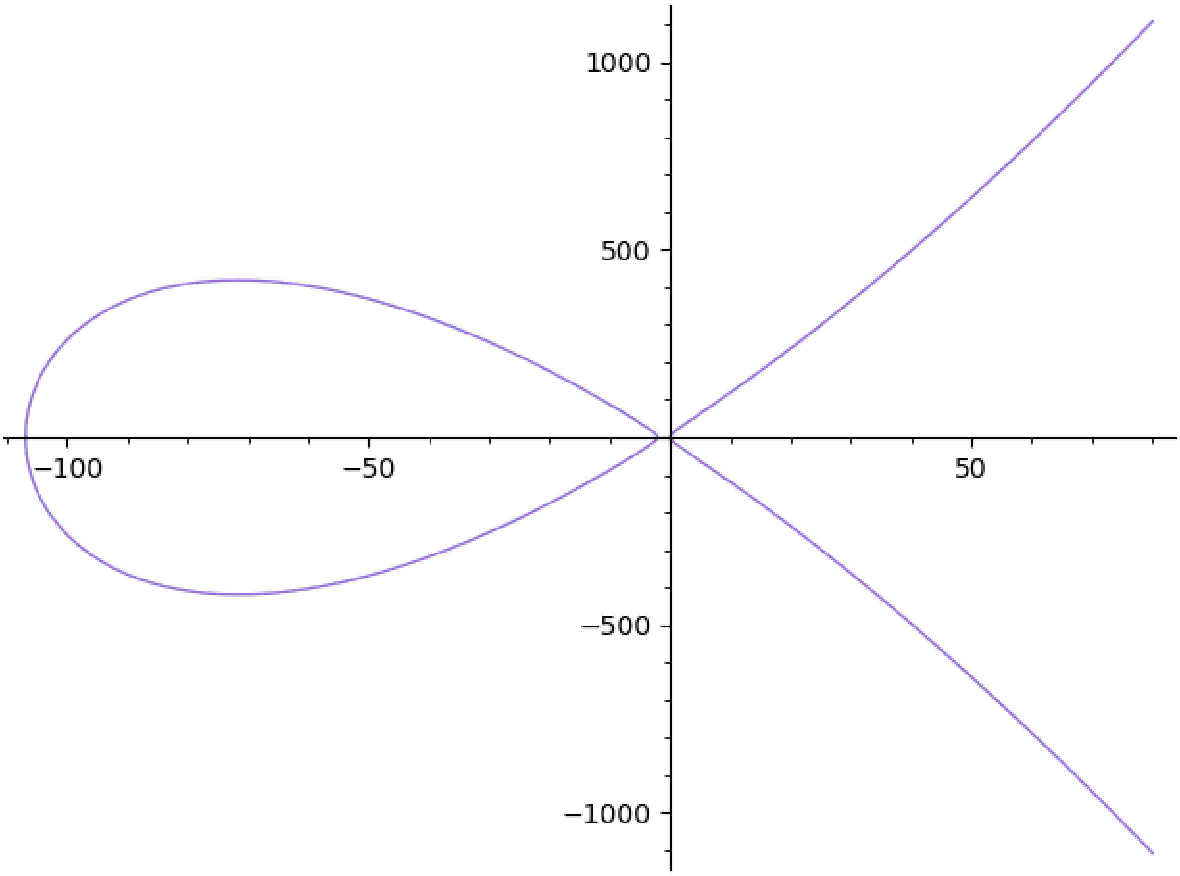

Figure 2: Plot of the elliptic curve E_4.

Proof. We can prove this lemma by proving the contrapositive statement instead: a point (a, b, c) on C_N is trivial if and only if it corresponds to a point $(x, y) \in E_N(\mathbb{Q})$ of finite order. Hence, we need to show that all the points in the torsion subgroup of $E_N(\mathbb{Q})$ correspond to trivial solutions and that all trivial solutions yield points in the torsion subgroup. To solve for both a, b, c in terms of x and y and vice versa, we used the SageMath (see Appendix A).

The point $(0, 0)$ of order two corresponds to $(1 : 1 : -1) \in \mathbb{P}^2(\mathbb{Q})$ which gives division by zero in (3). Similarly, for $N = 2$, the other two points of order two are $(-5, 0)$ and $(-32, 0)$. Solving for a, b, c in (9) gives again $a = b = -c$. The point of order three, $(4, \pm 4(2N + 5))$ gives division by zero when solving for a, b, c and thus gives no point on C_N. Similarly as the points of order two, the point of order six, $(8(N + 3), \pm 8(N + 3)(2N + 5))$ yields to a point where $a = b = -c$ and hence gives division by zero.

The rational points on (3) that we need to consider such that they give division by zero are the following. The tuples $(a : a : -a)$ and $(a : -a : 0)$ correspond to $(x, y) = (0, 0)$ which is a point of finite order. The cases where we have points of the form $(a : 0 : -a)$ and $(0 : a : -a)$ result in $x = 4$ and hence $y = \pm(2N + 5)$ which is the torsion point of order three. Finally the last points we need to consider that give division by zero in (3) are the points of the form $(-a : a : a)$ and $(a : -a : a)$ which correspond to $x = 8(N + 3)$. Thus, a point of order six in the torsion subgroup.

□

Since the torsion points do not lead to desired solutions, we look at the other rational points on E_N. This means looking at points on the subgroup $E_N(\mathbb{Q})$ having positive rank for $N > 0$.

This brings us to the next section, where we describe methods to compute the rank of an elliptic curve.

5 Descent by 2-Isogeny

There are several methods to compute the rank of an elliptic curve. In this paper we focus specifically on the method of 'descent by 2-isogeny'. We will explain the method for a general elliptic curve $E/\mathbb{Q}$ and in the next section provide some examples with $E_N/\mathbb{Q}$. The fact that we are working with an elliptic curve with no constant term implies that there always exists the point $(0,0) \in E(\mathbb{Q})$. This allows us to make use of isogenies between elliptic curves to compute the rank.

Remark 5.1. *In this paper we explore the method of descent by 2-isogeny, making use of the fact that we always have a point of order* 2. *In [BM14, page 32] they show isogenies of degrees* 3 *and* 6, *which can be computed as the torsion subgroup of* E_N *has order* 6. *Since* $E_N(\mathbb{Q})$ *always has a torsion point of order* 3, *we could also compute the rank using the method of descent by 3-isogeny. In the thesis [Tim15] and then later in [Bee10] the authors describe the method of descent by 3-isogeny, and compute the rank using such method.*

The following section is based on [ST15, Chapter 3] and [Bri]. The following lemma introduces two maps, ϕ and ψ, which are crucial in the method of isogeny by 2-descent.

Lemma 5.2. *[ST15, page 83] Let* $a, b \in \mathbb{Q}$. *Define* $E/\mathbb{Q}, \bar{E}/\mathbb{Q}$ *to be two elliptic curves as follows*

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

and

$$\bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$$

where $\bar{a} = -2a, \bar{b} = a^2 - 4b$. *Let* $T = (0,0) \in E(\mathbb{Q})$. *Then*

(i) The map $\phi : E(\mathbb{Q}) \to \bar{E}(\mathbb{Q})$ *defined as*

$$\phi(x,y) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) & \text{if } (x,y) \neq \mathcal{O} \text{ or } (x,y) \neq T \\ \bar{\mathcal{O}} & \text{otherwise} \end{cases} \tag{11}$$

is a group homomorphism with kernel $\{\mathcal{O}, T\}$.

(ii) Let $\bar{\phi} : \bar{E}(\mathbb{Q}) \to \bar{\bar{E}}(\mathbb{Q})$ *where* $\bar{\phi}$ *is defined in the same way as* ϕ,

$$\bar{\bar{E}}(\mathbb{Q}) : y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x$$

and $\bar{\bar{a}} = -2\bar{a}, \bar{\bar{b}} = \bar{a}^2 - 4\bar{b}$. *Then* $\bar{\bar{E}}(\mathbb{Q}) \cong E(\mathbb{Q})$ *via the map* $(x,y) \mapsto (\frac{1}{4}x, \frac{1}{8}y)$.

(iii) Let $\bar{T} = (\bar{0}, \bar{0})$. *We define* $\psi : \bar{E}(\mathbb{Q}) \to E(\mathbb{Q})$ *as*

$$\psi(\bar{x},\bar{y}) = \begin{cases} \left(\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b})}{8\bar{x}^2}\right) & \text{if } (\bar{x},\bar{y}) \neq \bar{\mathcal{O}} \text{ or } (\bar{x},\bar{y}) \neq \bar{T} \\ \mathcal{O} & \text{otherwise.} \end{cases} \tag{12}$$

Then ψ *is a group homomorphism with kernel* $\{\bar{\mathcal{O}}, \bar{T}\}$.

(iv) The composition $\psi \circ \phi : E(\mathbb{Q}) \to E(\mathbb{Q})$ *is a group homomorphism that sends* $P \mapsto 2P$.

Proof. The proof can be found on [ST15, pages 85-88]. □

The two maps ϕ and ψ are called *isogenies.*

Definition 5.3. *Isogenies are rational maps that are group homomorphisms between elliptic curves.*

Isogenies are defined more generally as maps between other structures, not only elliptic curves but for the sake of this paper they will be defined between elliptic curves.

Remark 5.4. *Having a rational 2-torsion point is crucial in the method of descent by 2-isogeny. This is because the existence of the 2-torsion point $T = (0, 0)$ allows the construction of the map ϕ. This is used in the proof of Mordell's Theorem 4.1 as the doubling map $\psi \circ \phi$ helps prove that the index $(E(\mathbb{Q}) : 2E(\mathbb{Q}))$ is finite and so $E(\mathbb{Q})$ is finitely generated. This is done using heights (see [ST15, Sections 3.1-3.3]).*

$$\begin{tikzcd}
E(\mathbb{Q}) \arrow[r, "\phi"'] & \overline{E}(\mathbb{Q}) \arrow[l, bend right, "\psi"'] \arrow[d, "\bar{\phi}"] \\
& \overline{\overline{E}}(\mathbb{Q}) \arrow[ul, "\cong"]
\end{tikzcd}$$

Figure 3: Diagram of the maps in Lemma 5.2.

The isogenies carry the rational points of one elliptic curve to the other. We use them to compute the index $(E(\mathbb{Q}) : 2E(\mathbb{Q}))$ which allows us to derive a formula to compute the rank of an elliptic curve.

Let us start by finding $2E(\mathbb{Q})$, by counting the number of points of order 2. Let $R_1, \ldots, R_r$ and $Q_1, \ldots, Q_s$ be such that $E(\mathbb{Q}) \cong \mathbb{Z}R_1 \oplus \ldots \oplus \mathbb{Z}R_r \oplus \mathbb{Z}Q_1 \oplus \ldots \oplus \mathbb{Z}Q_s$. Here $R_1, \ldots R_r$ have infinite order and $Q_1, \cdots Q_s$ have finite order. Then we can write $P \in E(\mathbb{Q})$, as $P = e_1R_1 + ... + e_rR_r + m_1Q_1 + \ldots + m_sQ_s$. If P has order 2, then $2(e_1R_1 + ... + e_rR_r + m_1Q_1 + \ldots + m_sQ_s) = \mathcal{O}$ so all the e_i's are 0.

Moreover, we have that $2m_i \equiv 0 \bmod p_i^{t_i}$, so if p_i is odd, then $m_i \equiv 0 \bmod p_i^{t_i}$, while if p_i is even then $m_i \equiv 0 \bmod p_i^{t_i-1}$. Denote the subgroup of points on $E(\mathbb{Q})$ of order 2 by $E(\mathbb{Q})[2]$, then $\#E(\mathbb{Q})[2] = 2^{\#\{p_i=2\}}$. If we compute the points of order dividing 2 on $E(\mathbb{Q})$ we see that there are either two of them, namely the point $\mathcal{O}$ and $(0, 0)$, or if the discriminant of the quadratic equation $x^2 + ax + b$ is a rational square, then we get an extra two points which are given by solving the quadratic equation.

By Mordell's Theorem (4.1) we have that

$$2E(\mathbb{Q}) \cong 2\mathbb{Z}^r \oplus 2\mathbb{Z}/p_1^{t_1}\mathbb{Z} \oplus ... \oplus 2\mathbb{Z}/p_s^{t_s}\mathbb{Z}.$$

If we quotient $\mathbb{Z}$ by $2\mathbb{Z}$ we get $\mathbb{Z}/2\mathbb{Z}$ while if we quotient $\mathbb{Z}/p_i^{t_i}\mathbb{Z}$ by $2\mathbb{Z}/p_i^{t_i}\mathbb{Z}$ we get two cases. If $p = 2$, then it is $\mathbb{Z}/2\mathbb{Z}$. Otherwise $(\mathbb{Z}/p_i^{t_i}\mathbb{Z})/(2\mathbb{Z}/p_i^{t_i}2\mathbb{Z}) \cong \{0\}$.

Let $e = \#\{i : p_i = 2\}$, then we get that

$$(E(\mathbb{Q}) : 2E(\mathbb{Q})) = 2^{r+e} = 2^r \cdot \#E(\mathbb{Q})[2].$$

Remark 5.5. *Note that $\#E(\mathbb{Q})[2]$ is either 2 if the discriminant $a^2 - 4b$ is not a square (namely the points $\mathcal{O}$ and $(0, 0)$) or it is 4 if the discriminant is a square as you get the two extra points given by factoring x out of $x^3 + ax^2 + bx$ and solving the quadratic equation.*

Here is where the 2-isogeny plays a role. As we have seen in Lemma 5.2, the composition map is the multiplication by 2, so $\psi \circ \phi(E(\mathbb{Q})) = 2E(\mathbb{Q})$. We can rewrite $(E(\mathbb{Q}) : 2E(\mathbb{Q}))$ as $(E(\mathbb{Q}) : \psi \circ \phi(E(\mathbb{Q})))$ and since $2E(\mathbb{Q}) \subseteq \psi(\bar{E}(\mathbb{Q})) \subseteq E(\mathbb{Q})$, we get

$$(E(\mathbb{Q}) : 2E(\mathbb{Q})) = (E(\mathbb{Q}) : \psi(\bar{E}(\mathbb{Q})))(\psi(\bar{E}(\mathbb{Q}) : \psi \circ \phi(E(\mathbb{Q}))).$$

The following is stated in [ST15, page 97] without a proof.

Lemma 5.6. *We can further simplify this expression*

$$(\psi(\bar{E}(\mathbb{Q})) : \psi \circ \phi(E(\mathbb{Q}))) = \frac{(\bar{E}(\mathbb{Q}) : \phi(E(\mathbb{Q})))}{(\ker \psi : (\ker \psi \cap \phi(E(\mathbb{Q})))}.$$

Proof. Let ψ and ϕ be defined as in Proposition 5.2 and denote $A = \bar{E}(\mathbb{Q})$, $B = \phi(E(\mathbb{Q}))$. Note that B is a subgroup of A. Let $G := A/(B + \ker \psi)$. Define the following map

$$\begin{aligned} \xi : G &\to \psi(A)/\psi(B) \\ g &\mapsto \psi(g) \bmod \psi(B) \end{aligned}$$

where $g = a + B + \ker\psi$ for $a \in A$. We claim ξ is a group isomorphism.

Firstly note that ξ is well defined as

$$\begin{aligned}\xi(g) &= \xi(a + B + \ker\psi)\\ &\equiv \psi(a + B + \ker\psi)\\ &\equiv \psi(a) + \psi(B) + \psi(\ker\psi)\\ &\equiv \psi(a) \bmod \psi(B)\end{aligned}$$

where we used the fact that ψ is a group homomorphism. To show ξ is a group homomorphism, take $g_1, g_2 \in G$, then $\xi(g_1 + g_2) \equiv \psi(g_1 + g_2) \equiv \psi(g_1) + \psi(g_2) \bmod \psi(B) = \xi(g_1) + \xi(g_2)$. For surjectivity, let $m \in \psi(A)/\psi(B)$ be a representative of $m' \in \psi(A)$. Then there exists an $a' \in A$ such that $\psi(a') = m'$. Thus, $m = \psi(a') + \psi(B) = \psi(a') + \psi(B) + \psi(\ker\psi) = \psi(a' + B + \ker\psi)$. Hence $\xi(a' + B + \ker\psi) \equiv m \bmod \psi(B)$. Thus, for each $m \in \psi(A)/\psi(B)$ we can construct some $g' \in G$ such that $\xi(g') \equiv m \bmod \psi(B)$, so ξ is surjective.

For injectivity, let $x \in \ker\xi$ and g defined as above. Then $\xi(x) = 0$ where $x = a+B+\ker\psi$ for some $a \in A$, and so $\xi(x) = \xi(a+B+\ker\psi) \equiv 0 \bmod \psi(B)$ and since ψ is a group homomorphism, then $\psi(a)+\psi(B)+\psi(\ker\psi) \equiv \psi(a) \bmod \psi(B) \equiv 0 \bmod \psi(B)$. So either $a \in \ker\psi$ so $a \equiv 0 \in G$ or $a \in B$ so $a \equiv 0 \in G$.

Therefore we have

$$\psi(A)/\psi(B) \cong A/(B + \ker\psi) \cong (A/B)/((B + \ker\psi)/B)$$

and by the 'first isomorphism theorem' in [TM18] we have that

$$(B + \ker\psi)/B \cong \ker\psi/(\ker\psi \cap B).$$

Hence

$$\psi(A)/\psi(B) \cong (A/B)/(\ker\psi/(\ker\psi \cap B)).$$

If we rewrite it in terms of $\bar{E}(\mathbb{Q})$ and $\phi(E(\mathbb{Q}))$ we have

$$\psi(\bar{E}(\mathbb{Q}))/\psi(\phi(E(\mathbb{Q}))) \cong (\bar{E}(\mathbb{Q})/\phi(E(\mathbb{Q})))/(\ker\psi/(\ker\psi \cap \phi(E(\mathbb{Q}))))$$

as desired.

□

Note that $\ker\psi = \{\bar{\mathcal{O}}, \bar{T}\}$ and that $\bar{T} \in \phi(E(\mathbb{Q}))$ if and only if $\bar{b} = a^2 - 4b = \square$ ([ST15, page 89]), hence $(\ker(\psi) : (\ker(\psi) \cap \phi(E(\mathbb{Q})))) = \begin{cases} 2 & \text{if } \bar{b} = \square \\ 1 & \text{otherwise.}\end{cases}$

Rearranging (5), the formula for the rank becomes

$$\begin{aligned}2^r &= \frac{(E(\mathbb{Q}) : 2E(\mathbb{Q}))}{\#E(\mathbb{Q})[2]}\\ &= \frac{(E(\mathbb{Q}) : \psi(\bar{E}(\mathbb{Q}))(\bar{E}(\mathbb{Q}) : \phi(E(\mathbb{Q})))}{\#E(\mathbb{Q})[2] \cdot (ker(\psi) : (ker(\psi) \cap \phi(E(\mathbb{Q}))))}\\ &= \frac{(E(\mathbb{Q}) : \psi(\bar{E}(\mathbb{Q})))(\bar{E}(\mathbb{Q}) : \phi(E(\mathbb{Q})))}{4}\end{aligned}$$

as the denominator is either $2 \cdot 2$ if $\bar{b} \neq \square$ or $4 \cdot 1$ if $\bar{b} = \square$.

The only thing left to us is to compute the indices in the numerator. We can translate the problem of finding the indices by finding the image of a map α isomorphic to the quotient group. Let $\mathbb{Q}^*$ denote the units of $\mathbb{Q}$.

Definition 5.7. *The subgroup* $(\mathbb{Q}^*)^2 \subset \mathbb{Q}^*$ *is equal to the set of squares in* $\mathbb{Q}^*$.

Remark 5.8. *Then, in* $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ *we have that for* $x \in \mathbb{Q}^*$ *where* $x = x_1^2 x_2$*, then* $x \equiv x_2 \bmod {\mathbb{Q}^*}^2$.

In other words, all the squares are mapped to 1. Recall that $T = (0,0)$.

Definition 5.9. *Let* $E : y^2 = x^3 + ax^2 + bx$ *and* $P = (x,y) \in E(\mathbb{Q})$*. We define* $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/{\mathbb{Q}^*}^2$

$$\alpha(P) = \begin{cases} b \bmod ({\mathbb{Q}^*}^2) & \text{if } P = T \\ 1 & \text{if } P = \mathcal{O} \\ x \bmod ({\mathbb{Q}^*}^2) & \text{otherwise.} \end{cases}$$

Proposition 5.10. *The map* $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ *is a group homomorphism.*

Proof. The proof can be found on [ST15, page 92]. □

Remark 5.11. *We define* $\bar{\alpha} : \bar{E}(\mathbb{Q}) \to \mathbb{Q}^*/({\mathbb{Q}^*}^2)$ *analogously.*

Proposition 5.12. *The image of* α *is isomorphic to* $E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$.

The same proposition also holds for $\bar{\alpha}$, as is isomorphic to $\bar{E}(\mathbb{Q})/\phi(E(\mathbb{Q}))$.

Proof of Proposition 5.12. The kernel of the map α consists of all the points $P \in E(\mathbb{Q})$ such that $\alpha(P) \equiv 1 \bmod ({\mathbb{Q}^*}^2)$. Thus, $\ker\alpha = \{\mathcal{O}, (0,0), \{(x,y) \in E(\mathbb{Q}) : x = \square\}\}$. From [ST15, page 91] we know that $\mathcal{O}, (0,0) \in \psi(\bar{E}(\mathbb{Q}))$, in addition to all the points $(x,y) \in E(\mathbb{Q})$ such that x is a nonzero square. Hence we can see $\ker\alpha \cong \psi(\bar{E}(\mathbb{Q}))$. From the Homomorphism Theorem in [TM18, page 82] it follows that

$$\alpha(E(\mathbb{Q})) \cong E(\mathbb{Q})/\ker\alpha \cong E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q})).$$

□

Combining this information together, we can finally rewrite the formula for the rank as

$$2^r = \frac{\#\alpha(E(\mathbb{Q}))\#\bar{\alpha}(\bar{E}(\mathbb{Q}))}{4}. \tag{13}$$

All we are left to do is compute the images $\alpha(E(\mathbb{Q}))$ and $\bar{\alpha}(\bar{E}(\mathbb{Q}))$.

5.1 Computing the image of α

We can illustrate how to get the image of $\alpha(E(\mathbb{Q}))$ and of $\bar{\alpha}(\bar{E}(\mathbb{Q}))$ using the two curves $E/\mathbb{Q}$ defined as $E : y^2 = x^3 + ax^2 + bx$ and $\bar{E}/\mathbb{Q}$ defined as $\bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$.

Rational points on an elliptic curve can be written in the form

$$(x,y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$$

where $m, n \in \mathbb{Z}$, $e \in \mathbb{Z}_{>0}$ and $\gcd(m,e) = \gcd(e,n) = 1$ (see [ST15, section 3.2]). Substituting these points in the elliptic curve will lead to the equation

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

Denote $\gcd(m, (m^2 + ame^2 + be^4)) = \gcd(m,b) = b_1$ where the sign of $mb_1 > 0$. Note that we assume $m \neq 0$ because the case where $m = 0$ is already included in the image of α. This is because if $m = 0$ then $(x,y) = (0,0)$ and $\alpha((0,0)) \equiv b$ which we know will always be there, so we want to exclude that case. Then we can rewrite $m = b_1 m_1$ and if we substitute it in we get the condition that $b_1^2 \mid n^2$ and hence we can write $n = n_1 b_1$ which leads to

$$n_1^2 = m_1(b_1 m_1^2 + ab_1 m_1 e^2 + b_2 e^4)$$

where $b_2 = \frac{b}{b_1}$.

We know $\gcd(m, e) = 1$ so $\gcd(m_1, e) = 1$. Moreover $\gcd(m, b) = b_1$ so $\gcd(m_1, b_2) = 1$ and therefore $\gcd(m_1, b_1 m_1^2 + ab_1 m_1 e^2 + b_2 e^4) = 1$. This implies both terms are squares as multiplied together they are equal to n_1^2. Therefore $m_1 \mid n_1^2$ and $(b_1 m_1^2 + ab_1 m_1 e^2 + b_2 e^4) \mid n_1^2$ so we can write $n_1 = ML$ where $M^2 = m_1$ and $L^2 = b_1 m_1^2 + ab_1 m_1 e^2 + b_2 e^4$. Substituting back in and simplifying we get a solution (M, e, L) of the equation

$$L^2 = b_1 M^4 + ae^2 M^2 + b_2 e^4 \text{ with } a, b_1, b_2 \in \mathbb{Z} \tag{14}$$

satisfying the conditions $M \neq 0$ and

$$\gcd(M, b_2) = \gcd(e, b_1) = \gcd(L, e) = \gcd(M, e) = 1. \tag{15}$$

Note that $m = M^2 b_1$ and $n = LMb_1$ hence the point $(x, y) \in E(\mathbb{Q})$ becomes

$$\left(\frac{b_1 M^2}{e^2}, \frac{b_1 ML}{e^3}\right)$$

where both terms are a fraction in lowest terms. Therefore $\alpha(E(\mathbb{Q}))$ will consists of 1 and $b \bmod (\mathbb{Q}^*)^2$, together with all x for which (14) has integer solutions (M, e, L) with $M, e, L \neq 0$, for some $b_1 \mid b$. Note that $x \equiv b_1 \bmod (\mathbb{Q}^{*^2})$ hence the image of α will consist of all square free b_1 dividing b such that (14) has an integer solution satisfying $M \neq 0$ and (15) holds.

Therefore, we need to check whether (14) does or does not have a nonzero solution for each square free b_1. The exact same procedure holds for $\bar{\alpha}(\bar{E}(\mathbb{Q}))$, however (14) will have $\bar{a}, \bar{b}$ as coefficients instead of a, b. Before we get to examples of how to compute the rank of our elliptic curve E_N (7), we need to describe a way to check whether (14) does not have nonzero solutions.

5.2 Reducing modulo prime powers

Suppose $\beta \in \mathbb{Z}$ is a root of a polynomial $f \in \mathbb{Z}[X]$. Then modulo a prime p, we will also have $f(\beta) \equiv 0 \bmod p$ and similarly for prime powers. Hence if f has solutions in integers, then f has solutions modulo p^k, for all $k \in \mathbb{Z}$, which implies that if there are no solutions modulo p^k, then there are no solutions in integers. Note that this also holds for polynomials in more than one variable.

Remark 5.13. *A trivial solution to* (14) *is a solution where $M, L = 0$. We will always have this solution as $M, L = 0$ implies $e = 0$ and thus we will always have the solution* $(0, 0, 0)$.

We will always also have the solution $(0, 0, 0)$ modulo some prime power, thus we want to find solutions (M, e, L) such that they are not equal to $(0, 0, 0)$ and satisfy (15). Thus by nontrivial modulo a prime power we mean not all M, e, L zero satisfying (15).

To compute the rank of an elliptic curve, we need to know which equations (14) have or do not have a nontrivial solution. A good approach to discard some equations is to show (14) has no nontrivial solutions modulo a prime power. We also need to check that if we find some nontrivial solutions, they also satisfy condition (15).

Theorem 5.14. *[AL11, Theorem 5] Let $a_1, a_3, a_4 \in \mathbb{Z} \setminus \{0\}, a_2 \in \mathbb{Z}$ and $a_2^2 - 4a_1 a_3$ be nonzero. The equation*

$$a_1 X^4 + a_2 X^2 Y^2 + a_3 Y^4 = a_4 Z^2 \tag{16}$$

has solutions modulo p^k for every prime p such that $p \nmid 2a_1 a_3 a_4 ({a_2}^2 - 4a_1 a_3)$ and $k \in \mathbb{Z}_{>0}$.

This theorem tells us that to check (14) has no solutions modulo a prime power, it is enough to check it has no nontrivial solutions modulo powers of p where $p \mid 2b_1b_2(a^2-4b_1b_2) = 2b(a^2-4b)$. In order to prove it, we first need some other results.

Definition 5.15. *A tuple $(x,y,z) \in \mathbb{Z}^3$ is called primitive if $\gcd(x,y,z)=1$.*

Lemma 5.16. *[AL11, Lemma 12] Let p be a prime such that $p^2 \nmid a_4$ and let $k \in \mathbb{Z}_{>0}$. Then the system*

$$\begin{aligned} a_1U^2 + a_2V^2 + a_3W^2 &= a_4Z^2 \\ UW &= V^2 \end{aligned} \tag{17}$$

where $a_1, a_2, a_3, a_4 \in \mathbb{Z}$, has a primitive solution modulo p^k if and only if (16) has a primitive solution modulo p^k.

Lemma 5.17. *[AL11, Lemma 13] Let p be a prime. The system (17), where $a_i \in \mathbb{F}_p$ for $i=1,2,3,4$ has a nontrivial $\mathbb{F}_p$ solution for any prime $p \nmid 2a_1a_3a_4({a_2}^2-4a_1a_3)$.*

The proof of the two lemmas can be found in [AL11], pages 15 and 17. The idea of the proof of Lemma 5.16 is that if one has a solution modulo p^k for (17) then one can produce a solution modulo p^k for (16) and vice versa. We will prove Lemma 5.17 but before we present the proof we need to introduce some other results.

In [AL11, Section 3] it is explained how to parametrize the unit circle to find Pythagorean triples. The following lemma extends this parametrization to conics of the form

$$ax^2 + by^2 = 1 \text{ where } a, b \in \mathbb{Z}_{>0}. \tag{18}$$

This will later allow us to construct a solution in the proof of Lemma 5.17. We will briefly explain the procedure of parametrizing (18) for a specific point, which then can be generalized to a point (x_0, y_0) on (18).

Suppose we have a conic as in (18) over $\mathbb{R}$. This is defined by

$$\{(x,y) \in \mathbb{R}^2 : ax^2 + by^2 = 1 \text{ for } a, b \in \mathbb{R}_{>0}\}.$$

with a point on the conic being $P = \left(\frac{-1}{\sqrt{a}}, 0\right)$, as shown in Figure 4.

We can then draw a line with slope t that goes through P, namely the line $y = t(x + 1/\sqrt{a})$. The line intersects the conic once more, at the point $Q = \left(\frac{a-bt^2}{\sqrt{a}(a+bt^2)}, \frac{2at}{\sqrt{a}(a+bt^2)}\right)$. This is shown in Figure 5. Since Q is on the conic, we get the following identity in $\mathbb{R}[t]$

$$a(a-bt^2)^2 + b(2at)^2 = a(a+bt^2)^2.$$

We can do this more generally for a starting point (x_0, y_0) and a more general base field, which leads to the polynomials defined in Lemma 5.19.

Definition 5.18 (Associate polynomials)**.** *[AL11, page 6] Let K be a field. Two polynomials in $K[t]$ are called associates if one is a constant multiple of the other.*

Lemma 5.19. *[AL11, Lemma 1] Let K be a field and $a, b \in K \setminus \{0\}$. Suppose there exist $x_0, y_0 \in K$ such that $ax_0 + by_0 = 1$. Then in $K[T]$*

$$aq_1^2 + bq_2^2 = q_3^2$$

where $q_1 = bx_0T^2 - 2by_0T - ax_0 \quad q_2 = -by_0T^2 - 2x_0T + ay_0$ and $q_3 = bT^2 + a$. Furthermore, at least two of q_1, q_2, q_3 have degree exactly 2, and if $\mathrm{char}(K) \neq 2$, then each q_1, q_2, q_3 is nonzero and no two are associates.

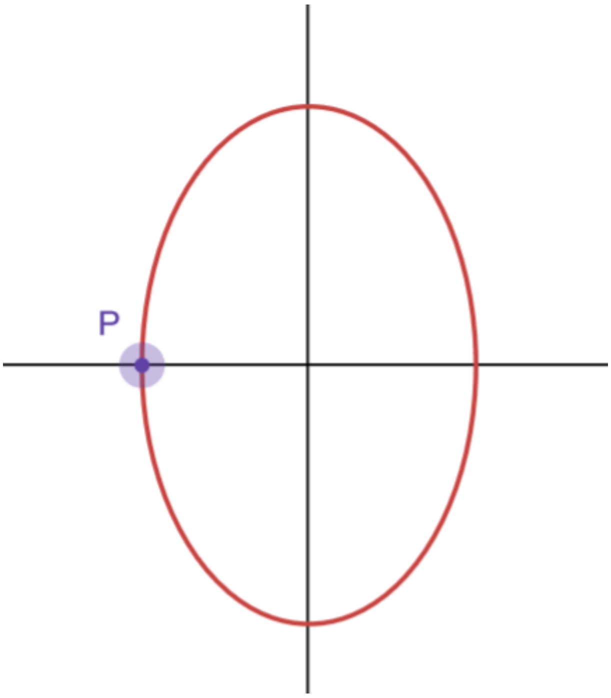

Figure 4: $ax^2 + by^2 = 1$

□

The following definition and theorem are useful tools that we will also use further in our paper. Let p be a prime. For $p \nmid a$ we call $a \in \mathbb{Z}$ a *quadratic residue* if a is a square modulo p, and a *quadratic nonresidue* otherwise.

Definition 5.20 (Legendre symbol)**.** *For a prime p and $a \in \mathbb{Z}$, the Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a quadratic residue} \\ -1 \text{ if } a \text{ is a quadratic nonresidue} \\ 0 \text{ if } a \text{ is } 0 \text{ modulo } p. \end{cases}$$

Theorem 5.21 (Euler's criterion)**.** *For a prime p and $a \in \mathbb{Z}$ such that $a \not\equiv 0 \bmod p$ then the Legendre symbol is as follows*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Proof. The proof can be found on [Ros11, page 418]. □

Theorem 5.22. *Let p be an odd prime. Then*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. The proof can be found on [Ros11, page 419]. □

The last lemma we need before we begin the proof of Lemma 5.17 is the following.

Lemma 5.23. *[AL11, page 8] Let p be prime and $f, g \in \mathbb{F}_p[X]$ be non zero polynomials of degree at most two. If $\left(\frac{f(t)}{p}\right) = \left(\frac{g(t)}{p}\right)$ or $\left(\frac{f(t)}{p}\right) = -\left(\frac{g(t)}{p}\right)$ for all $t \in \mathbb{F}_p$ then f and g are associates.*

The proof is based on the proof by [AL11].

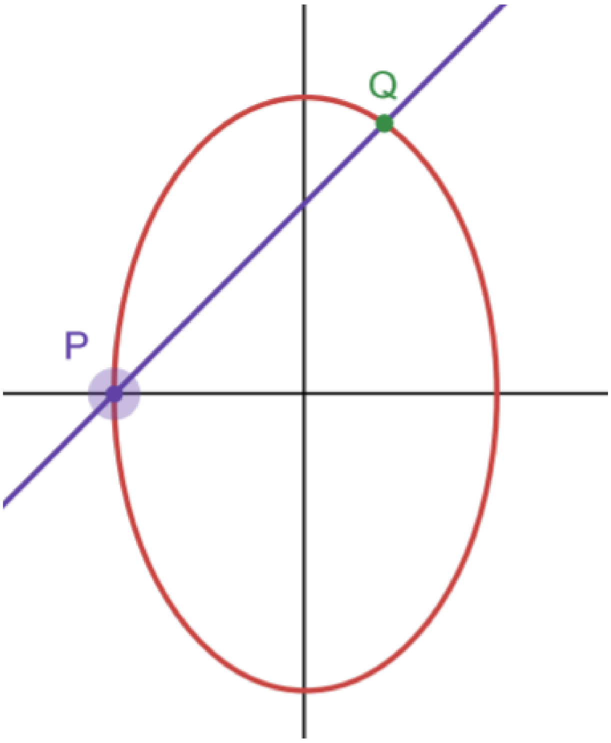

Figure 5: $ax^2 + by^2 = 1$

Proof. Let p be a prime and $f, g \in \mathbb{F}_p[X]$. Suppose there exists a $t \in \mathbb{F}_p$ such that $\left(\frac{f(t)}{p}\right) = \left(\frac{g(t)}{p}\right)$. Then $\left(\frac{f(t)}{p}\right) - \left(\frac{g(t)}{p}\right) = 0$ and by Euler's criterion

$$f(t)^{\frac{p-1}{2}} - g(t)^{\frac{p-1}{2}} \equiv 0 \bmod p. \qquad (\star)$$

Both f and g are of degree at most two so the left hand side of $(\star)$ is of degree at most $p-1$. However, every $t \in \mathbb{F}_p$ is a root of the left hand side $(\star)$ so the degree of $(\star)$ must be p. This implies left hand side of $(\star)$ is the zero polynomial. Therefore, $f(t)^{\frac{p-1}{2}}, g(t)^{\frac{p-1}{2}}$ are associates. If we factorize them into irreducible elements then they will have the same irreducible factors up to multiplication by constants. Hence, so will f and g and therefore f and g are associates.

Assume that $\left(\frac{f(t)}{p}\right) = -\left(\frac{g(t)}{p}\right)$. Let $a \in \mathbb{F}_p$ be a quadratic nonresidue. Then $\left(\frac{a}{p}\right) = -1$ so $\left(\frac{f(t)}{p}\right) = \left(\frac{ag(t)}{p}\right)$. By the same argument as above, we conclude that f and ag are associates and hence f and g are associates. □

The following proof is based on [AL11, Lemma 13].

Proof of Lemma 5.17. Let p be a prime and $p \nmid 2a_1a_3a_4(a_2^2 - 4a_1a_3)$. Since we are working over $\mathbb{F}_p$ and a_4 is nonzero, we can always multiply the whole equation by a_4^{-1} and work with the case where we have a system of equations of the form

$$\begin{aligned} a_1U^2 + a_2V^2 + a_3W^2 &= Z^2 \\ UW &= V^2. \end{aligned}$$

Consider the equation $f(X, Y) = a_1X^2 + a_2XY + a_3Y^2$. Since $p \nmid a_1$ and $p \nmid (a_2^2 - 4a_1a_3)$ then also $a_3 - \frac{a_2^2}{4a_1} \not\equiv 0 \bmod p$ and thus we can apply Lemma 5.19. Consider the polynomials q_1, q_2, q_3 found in Lemma 5.19 applied to

$$a_1X^2 + (a_3 - \frac{a_2^2}{4a_1})Y^2 = Z^2$$

so that we have

$$a_1q_1^2 + (a_3 - \frac{a_2^2}{4a_1})q_2^2 = q_3^2.$$

In this case

$$\begin{aligned} a_1X^2 + (a_3 - \frac{a_2^2}{4a_1})Y^2 = Z^2 \iff \\ a_1\frac{X^2}{Z^2} + (a_3 - \frac{a_2^2}{4a_1})\frac{Y^2}{Z^2} = 1. \end{aligned}$$

Note that in this case we have that x_0 and y_0 as in Lemma 5.19 correspond to $\frac{X}{Z}$ and $\frac{Y}{Z}$ respectively.

Let $q_1' = q_1 - \frac{a_2}{4a_1}q_2$, then

$$\begin{aligned} f(q_1', q_2) &= a_1(q_1 - \frac{a_2}{2a_1}q_2)^2 + a_2(q_1 - \frac{a_2}{2a_1})q_2 + a_3q_2^2 \\ &= aq_1^2 - a_2q_1q_2 + \frac{a_2^2}{4a_1}q_2^2 + a_2q_1q_2 - \frac{a_2^2}{2a_2}q_2^2 + a_3q_2^2 \\ &= aq_1^2 + (a_3 - \frac{a_2^2}{4a_1})q_2^2 \\ &= q_3^2. \end{aligned}$$

By Lemma 5.19 we know q_1, q_2 are not associates and since q_1' is nonzero then q_1', q_2 are not associates. By Lemma 5.23 there exists a $t \in \mathbb{F}_p$ such that

$$\left(\frac{q_1'(t)}{p}\right) \neq -\left(\frac{q_2(t)}{p}\right)$$

so that means $q_1'(t)q_2(t) = s^2$ for some $s \in \mathbb{F}_p[t]$. Hence, $(U, V, W, Z) = (q_1'(t), s, q_2(t), q_3(t))$ is a nontrivial solution to (17).

□

We can also double check that the solution $(q_1'(t), s, q_2(t), q_3(t))$ works by direct substitution. From Lemma 5.19 we know the polynomials q_i for $i = 1, 2, 3$ are given by

$$\begin{aligned} q_1(t) &= bx_0t^2 - 2by_0t - a_1x_0 \\ q_2(t) &= -by_0t^2 - 2a_1x_0t + a_1y_0 \\ q_3(t) &= bt^2 + a_1 \end{aligned}$$

where $b = \left(a_3 + \frac{a_2^2}{4a_1}\right)$ and $a_1x_0 + by_0 = 1$. We only need to check whether $a_1q_1^2 + bq_2^2 = q_3^2$ as we already know from the proof that substituting $q_1'(t)$ and $q_2(t)$ in the left hand side of (17) gives us $a_1q_1^2 + bq_2^2$. Thus

$$\begin{aligned} a_1q_1^2 + bq_2^2 &= (a_1b^2x_0^2 + b^3y_0^2)t^4 + 3(a_1^2bx_0^2 + a_1by_0^2)t^2 + a_1^3x_0^2 + a_1^2b_1y_0^2 \\ &= b^2(a_1x_0^2 + by_0^2)t^2 + 2a_1b(a_1x_0^2 + by_0^2)t^2 + a_1^2(a_1x_0^2 + by_0^2) \\ &= b^2t^4 + 2a_1bt^2 + a_1^2 \\ &= q_3^2 \end{aligned}$$

exactly as we wanted.

Lemma 5.17 tells us that (17) has a nontrivial $\mathbb{F}_p$ solution for primes $p \nmid 2a_1a_3a_4(a_2^2 - 4a_1a_3)$, and by Lemma 5.16 this then implies that (16) has a nontrivial $\mathbb{F}_p$ solution.

The following lemma tells us that if we have a solution modulo a prime p, then we can 'lift' the solution modulo p^k for all $k \in \mathbb{Z}_{>0}$. Hence, this helps us prove we have solutions modulo p^k in Theorem 5.14.

Lemma 5.24 (Hensel's Lemma)**.** *Let $f \in \mathbb{Z}[X]$, $k \in \mathbb{Z}_{>1}$ and p a prime. Suppose there is an $s \in \mathbb{Z}$ such that $f(s) \equiv 0 \mod p^{k-1}$ and $f'(s) \not\equiv 0 \mod p$. Then, there exists a unique $r \in \mathbb{Z}$, $0 \leq r < p$, given by $r = -(f'(s))^{-1}\frac{f(s)}{p^{k-1}} \mod p$ such that* [1]

$$f(s + rp^{k-1}) \equiv 0 \mod p^k.$$

A more precise version of this lemma together with its proof can be found in [Ros11, Chapter 4.4]. Having introduced these tools, we can proceed to prove Theorem 5.14.

Proof of Theorem 5.14. Let p be prime and $p \nmid 2a_1a_3a_4({a_2}^2 - 4a_1a_3)$. By Lemma 5.17, the system (17) has a nontrivial $\mathbb{F}_p$ solution and hence by Lemma 5.16, also (16) has a nontrivial $\mathbb{F}_p$ solution. Let $(x_0, y_0, z_0) \in \mathbb{Z}^3$ be such a solution. Without loss of generality the solution is primitive, as we can always factor out the common term. If $p \mid x_0$ and $p \mid y_0$ then $p \mid z_0$, so at least one of x_0, y_0 has to be coprime to p. Since they are symmetric, suppose $\gcd(p, y_0) = 1$. Then $y_0 \in \mathbb{F}_p^*$, and multiplying by its inverse we get that $(x_0{y_0}^{-1}, 1, z_0{y_0}^{-1})$ is also a solution to (16) (modulo p). Denote $x = x_0{y_0}^{-1}, z = z_0{y_0}^{-1}$, then substituting it in (16) we have $a_1x^4 + a_2x^2 + a_3 = a_4z^2$. Then we can have two cases.

Case I: $z \equiv 0 \mod p$. Then x is a root of $f(T) = a_1T^4 + a_2T^2 + a_3 \in \mathbb{F}_p[T]$. Suppose $f'(x) = 4a_1x^3 + 2a_2x \equiv 0 \mod p$. Note $x \not\equiv 0 \mod p$ as otherwise $f(x) \equiv a_3 \equiv 0 \mod p$ which is a contradiction as we assumed $p \nmid a_3$. Hence $4a_1x^3 \equiv -2a_2x^2 \mod p$ so $a_2 \equiv -2a_1x^2 \mod p$. Therefore

$$\begin{aligned} 0 &\equiv f(x) \\ &\equiv (-4a_1)a_1x^4 + (-4a_1)a_2x^2 + (-4a_1)a_x \\ &\equiv -4a_1^2x^4 + 2(-2a_1x^2)a_2 - 4a_1a_3 \\ &\equiv -a_2^2 + 2a_2^2 - 4a_1a_3 \\ &\equiv a_2^2 - 4a_1a_3 \mod p \end{aligned}$$

which is a contradiction since we assumed $p \nmid (a_2^2 - 4a_1a_3)$. Therefore $f'(x) \not\equiv 0 \mod p$. By Hensel's Lemma 5.24 there exists a unique $r \in \mathbb{Z}$, $0 \leq r < p$, such that $f(r) \equiv 0 \mod p^2$. Therefore $(r, 1, 0)$ is a solution to $a_1X^4 + a_2X^2Y^2 + a_3Y^4 - a_4Z^2 \equiv 0 \mod p^2$. We can repeat this procedure to get solutions modulo p^k for all $k \in \mathbb{Z}_{>1}$.

Case II: $z \not\equiv 0 \mod p$. Then z is a root of $f(T) = a_4T^2 - (a_1x^4 + a_2x^2 + a_3) \in \mathbb{F}_p[T]$. Note that $f'(z) = 2a_4z \not\equiv 0 \mod p$ since $p \nmid 2a_4$. Thus by Hensel's Lemma there exists a unique $r \in \mathbb{Z}$, $0 \leq r < p$, such that $f(r) \equiv 0 \mod p^2$. Therefore $(x, 1, r)$ is a solution modulo p^2. We can repeat the process to get solutions modulo p^k for all $k \in \mathbb{Z}_{>1}$.

□

In this subsection we worked with the idea that if there are solutions to some polynomial over the integers, then there is a solution to that polynomial modulo some prime power, and we showed which primes to consider for the case of the quartic (16). However, having solutions to a polynomial modulo some prime power, or even over the real numbers, does not imply that the same polynomial will have solutions in the integers. Hasse's Theorem [AL11, Theorem 2] tells us some information on the case where we work with a homogeneous polynomial of degree 2, but for higher degrees we cannot deduce much about integer solutions from real solutions or solutions modulo p^k for p prime and $k \in \mathbb{Z}_{>0}$.

One of the issues of the 2-isogeny descent method is if we encounter such a situation while computing the rank of the curve. The best we can do is apply some smart tricks. In the method of descent by 2-isogeny, we know that $\#\alpha(E(\mathbb{Q}))\#\bar{\alpha}(\bar{E}(\mathbb{Q})$ is a power of 2. Suppose for example, that for $E(\mathbb{Q})$ we get four equations of the form (14) and also that b is not a square. If we find

[1] Note that $(f'(s))^{-1}$ refers to the inverse of $f'(s)$ modulo p.

the first two have a solution but the third one does not, then we know the fourth one will not either as we cannot have 5 elements in the image of α.

Having acquired all the necessary tools to compute the rank we proceed to illustrate how it works with a couple of examples.

5.3 Examples of rank of E_N

Recall that we want to compute the rank of (7) since the points in the torsion subgroup do not lead to desired solutions. Consider the following examples, where we compute the rank for $N = 1$ and $N = 4$. Recall that the isogeny maps the rational points on E_N to the rational points on $\bar{E}_N$ defined as

$$\bar{E}_N : y^2 = x^3 + \bar{a}x^2 + \bar{b}x \text{ where } \bar{a} = -2a \text{ and } \bar{b} = a^2 - 4b. \tag{19}$$

More specifically we have an isogeny between elliptic curves

$$\begin{aligned} \phi : E_N &\to \bar{E}_N \\ (x, y) &\mapsto \left(\frac{y^2}{x^2}, \frac{(x^2 - 32(N+3))y}{x^2} \right) \end{aligned}$$

where $\bar{E}_N : y^2 = x^3 - 2(4N^3 + 12N - 3)x^2 + (2N - 3)(2N + 5)^3 x$ [BM14, page 32].

Example 5.25 ($N = 1$)**.** When $N = 1$, our elliptic curve E_N (7) becomes

$$E_1 : y^2 = x^3 + 13x^2 + 128$$

and the curve given by the isogeny is

$$\bar{E}_1 : y^2 = x^3 - 26x^2 - 343.$$

Let us compute first the image of $\alpha(E_1(\mathbb{Q}))$. Here $a = 13$ and $b = 128$. We can factorize b as $b = b_1 b_2 = \pm 1 \cdot \pm 128 = \pm 2 \cdot \pm 64$, which are the only square free options for b_1. Note that $\alpha(128) \equiv 2 \bmod {\mathbb{Q}^*}^2$, so we already know $1, 2 \in \alpha(E_1(\mathbb{Q}))$. This leaves us to check whether $-1, -2$ are in the image, which gives rise to the following equations

I. $L^2 = -M^4 + 13e^2M^2 - 128e^4$

II. $L^2 = -2M^4 + 13M^2e^2 - 64e^4$.

We compute $2b(a^2 - 4b) = 2 \cdot 128(13^2 - 4 \cdot 128) = -87808 = -2^8 \cdot 7^3$, so we can use Theorem 5.14 to check whether I and II have solutions modulo $p \mid 2b(a^2 - 4b)$, as those are the primes (and their powers) that might give us no solutions according to Theorem 5.14. To check for solutions modulo a prime power p^k we used SageMath [The21] (see Appendix A). Both equations have no nontrivial solutions modulo 7, and hence no rational solutions. Therefore $-1, -2 \notin \alpha(E_1(\mathbb{Q}))$, so $\#\alpha(E_1(\mathbb{Q})) = 2$, namely $\alpha(E_1(\mathbb{Q})) = \{1, 2\}$.

For $\bar{\alpha}(\bar{E}_1(\mathbb{Q}))$, we get have $a = -26$ and $b = -343 \equiv -7 \bmod {\mathbb{Q}^*}^2$, so we know that $1, -7 \in \bar{\alpha}(\bar{E}_1(\mathbb{Q}))$ and thus we only need to check $b_1 = -1, 7$. Hence we get

I. $L^2 = -M^4 - 26e^2M^2 + 343e^4$

II. $L^2 = 7M^4 - 26M^2e^2 - 49e^4$.

We compute $2b(a^2 - 4b) = -1404928 = -2^{12} \cdot 7^3$. Both equations have nontrivial solutions modulo 2^4, but none of these solutions satisfying being not all zero and (15). Therefore $-1, 7 \notin \bar{\alpha}(\bar{E}_1(\mathbb{Q}))$ and hence $\bar{\alpha}(\bar{E}_1(\mathbb{Q})) = \{1, -7\}$.

Substituting into the rank formula we get

$$2^r = \frac{2 \cdot 2}{4} = 1$$

so $r = 0$.

The example did not lead to desired solutions to the fruit puzzle, as the rank is 0. Another example which leads to a desired solution is for $N = 4$.

Example 5.26 ($N = 4$)**.** Substituting $N = 4$ we get the equations

$$E_4 : y^2 = x^3 + 109x^2 + 224x$$

and

$$\bar{E}_4 : y^2 = x^3 - 218x^2 + 10985x.$$

For E_4 we have $a = 109$ and $b = 224 \equiv 14 \bmod {\mathbb{Q}^*}^2$ so we know that $1, 14 \in \alpha(E_4(\mathbb{Q}))$. We can factorize b in the following ways to get $b_1 \neq 1, 14$ squarefree: $b = \pm 2 \cdot \pm 112 = \pm 7 \cdot \pm 32 = -14(-16)$. This leads to the following equations

I. $L^2 = 2M^4 + 109e^2M^2 + 112e^4$

II. $L^2 = -2M^4 + 109e^2M^2 - 112e^4$

III. $L^2 = 7M^4 + 109e^2M^2 + 32e^4$

IV. $L^2 = -7M^4 + 109e^2M^2 - 32e^4$

V. $L^2 = -14M^4 + 109e^2M^2 - 16e^4$

VI. $L^2 = -M^4 + 109e^2M^2 - 224e^4$.

Here we have that $2b(a^2 - 4b) = 2 \cdot 224(109^2 - 4 \cdot 224) = 2^6 \cdot 5 \cdot 7 \cdot 13^3$. Again we use Theorem 5.14 to check for powers of primes $p \mid 2b(a^2 - 4b)$, so the primes $2, 5, 7, 13$ and their powers. To check for solutions modulo these primes we used SageMath (again, see Appendix A).

For I, note that $\gcd(M, 112) = 1$ so $M \equiv 1 \bmod 2$. Therefore $M \equiv 1 \bmod 4$ or $M \equiv 3 \bmod 4$, and since $3^4 \equiv 3^2 \equiv 1 \bmod 4$, we get that reducing modulo 4, I becomes $N^2 \equiv 2 + e^2 \bmod 4$ which has no solutions. We get that II also has no solutions modulo 4, and III no solutions modulo 5 and IV has no solutions modulo 13. Equations V and VI both have the same solution, namely $(M, e, L) = (2, 1, 14)$. Note that because in Equation (14) both M, e are squared, then $(-2, 1, 14), (2, -1, 14), (-2, -1, 14)$ are also solutions. Therefore we get that $\alpha(E_4(\mathbb{Q})) = \{\pm 1, \pm 14\}$.

The curve $\bar{E}_4$ has $a = -218$ and $b = 10985 \equiv 65 \bmod (\mathbb{Q}^*)^2$, so $1, 65 \in \bar{\alpha}(\bar{E}_4(\mathbb{Q}))$. Since $a < 0$ and $b > 0$, factorizing b to get $b_1, b_2 < 0$ will lead to $L^2 < 0$ and since we want integer solutions that does not work. Hence, factorizing b to get square free, positive b_1's (excluding $1, 65$) we have

I. $L^2 = 5M^4 - 218e^2M62 + 2197e^4$

II. $L^2 = 13M^4 - 218e^2M62 + 845e^4$.

Here $2b(a^2 - 4b) = 78740480 = 2^{10} \cdot 5 \cdot 7 \cdot 13^3$. Reducing I and II modulo 7 we get that they both do not have nontrivial solutions, so $\bar{\alpha}(\bar{E}(\mathbb{Q})) = \{1, 65\}$. Hence, the rank formula gives us

$$2^r = \frac{2 \cdot 4}{4} = 2$$

ans thus $r = 1$. Therefore we have that

$$E_4(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Since the rank is one, Lemma 4.6 tells us that we get nontrivial solutions for (a, b, c) in the projective plane. Looking back at our elliptic curve for $N = 4$,

$$E_4 : y^2 = x^3 + 109x^2 + 224x$$

we got the following results from equations V and VI:

We have that for V, the solutions $(2, 1, 14)$ and $(-2, -1, 14)$ give us $(x, y) = (-4, -28)$. This point only gives us the trivial solution $(a, b, c) = (0, 0, 0)$. However, the points $(-2, 1, 14)$ and

$(2, -1, 14)$ give the point $(x, y) = (-4, 28)$ which corresponds to $(a, b, c) = (11, 2, -1)$ in the projective plane.

For VI we have the opposite. The points $(-2, 1, 14)$ and $(2, -1, 14)$ give us $(x, y) = (-56, 392)$ which leads to the trivial solution, while the other two points lead to nontrivial solutions, namely $(x, y) = (-56, -392)$ corresponding to $(a, b, c) = (-5, 9, 11)$.

Let $P = (-4, 28)$. The point P is of infinite order and it can be written as $P = (-56, -392) + (0, 0)$ where $(-56, -392)$ is a point of infinite order and $(0, 0)$ is a point of order 2. However, there is no point $S \in E_4(\mathbb{Q})$ such that a multiple of S is equal to P. A generator for $E_4(\mathbb{Q})$ given by SageMath is the point $(-100, 260)$, which is equal to $P + Q_3$ where Q_3 is a point of order 3 or equivalently, is equal to $(-56, -392) + Q_6$ where $Q_6 \in \mathbb{Z}/6\mathbb{Z}$ is a point of order 6. Recall that $E_4(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ and therefore we can also generate it by letting P be a generator for the infinite part while the torsion subgroup is cyclic and is generated by a point of order 6 (see [BM14, Remark 2.2]). Thus, every rational point in $E_4(\mathbb{Q})$ can be written as $nP + mQ$ where $n \in \mathbb{Z}$, Q is a torsion point of order 6 and $m \in \{0, 1, 2, 3, 4, 5\}$.

We can compute multiples of the point P until we reach a point on $E_4(\mathbb{Q})$ which corresponds to $a, b, c > 0$. We do this using SageMath, in the code that can be found in the Appendix A. As also stated in [BM14], we find that the smallest integer n, for which $a, b, c > 0$, is $n = 9$. The point of $9P$ and the corresponding point $(a : b : c)$ are as follows:

$$9P = \left(\frac{-66202368404229585264842409883878874707453676645038225}{13514400292716288512070907945002943352692578000406921}, \right.$$
$$\left. \frac{5880083515730808330737675172734718133008567285029673035187174871330798870061121 0}{157106866859797843455636470729189626883808694543003132219675439042028040734646 9} \right)$$

with corresponding values

$$\begin{aligned}(a : b : c) = (&154476802108746166441951315019919837485664325669565431700026634898253202035277999 : \\ &368751317941299998271978115652254748254929799689719709962831374716372246340555 79 : \\ &437361267792869725786125260237139015281653755816161361862143799337842346777203 6).\end{aligned}$$

In fact P is the generator of $E(\mathbb{Q})$ modulo the torsion subgroup, for which the smallest multiple corresponds to a positive solution to the fruit puzzle. If we define a new point $P' = P + T$ where T is in the torsion subgroup of $E_4(\mathbb{Q})$, we can see that indeed there is no $m \in \mathbb{Z}$ such that mP' corresponds to all $a, b, c > 0$ for $m < 9$. In some cases, for example for Q being a point of order 3 we see that $9P'$ corresponds to $a, b, c > 0$. The values of mP' and the corresponding points $(a : b : c)$ are not written in this paper, but one can find them using the SageMath code we used, found in Appendix A. We will elaborate more on the size of these solutions in a later section. In the table below we summarized the first multiple of P', denoted by n, for all the different torsion points, for which there are positive solutions to the fruit puzzle.

P'	**n**	**# digits of a**	**# digits of b**	**# digits of c**
$P + (0, 0)$	13	168	167	167
$P + (4, 52)$	9	81	80	79
$P + (4, -52)$	9	81	80	79
$P + (46, 728)$	13	167	194	167
$P + (46, -728)$	13	167	167	168

Table 1: Smallest n for which nP' corresponds to $a, b, c > 0$.

However, if we compute higher multiples of P', although the number of digits of a, b, c increases (see the last subsection of Section 6) a, b, c can be negative again. This is because in order to get positive a, b, c we need the $x-$coordinate of the point P' to be within certain bounds which depend on N and as P' grows it can happen that x is not within those bounds anymore. We will elaborate more on this in later sections.

A later result tells us that the rank of $E_N(\mathbb{Q})$ will be 0 for all odd N. Thus, if we want to know which smallest positive N yields rank 1, we only need to check the rank of the elliptic curve $E_N(\mathbb{Q})$ for the case where $N = 2$.

Example 5.27 (N=2)**.** Let $N = 2$. Then

$$E_2(\mathbb{Q}) : y^2 = x^3 + 37x^2 + 160x \quad \text{and}$$
$$\bar{E}_2(\mathbb{Q}) : y^2 = x^3 - 74x^2 + 729x.$$

For E_2, we have $b = 160 \equiv 10 \bmod (\mathbb{Q}^*)^2$, thus $1, 10 \in \alpha(E_2(\mathbb{Q}))$. We can factorize b as follows

$$b = b_1 b_2 = -1(-160), \pm 2 \cdot \pm 80, \pm 5 \cdot \pm 32$$

where we excluded the case of $\pm 1 \pm 160$ as we already know it is contained in the image of α. Using Theorem 5.14, we find that the primes whose powers we need to check to exclude some equations of the form

$$L^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4$$

are $2, 3$ and 5. The equations corresponding to $b_1 = -1, 2, 5$ have no solution modulo 3 (or some power of 3). For $b_1 = -2$ we have the solution $(M, e, L) = (2, 1, 36)$. For $b_1 = -5$ we find the same solution, $(2, 1, 36)$. For all the remaining values of b_1 we find the equations have no solution modulo 2^2. Thus, $\alpha(E_2(\mathbb{Q})) = \{1, 10, -2, -5\}$. For the isogenous curve we see that $b = 3^6 \equiv 1 \bmod (\mathbb{Q}^*)^2$, and that we can only factor it as $b_1 b_2 = (\pm 3)(\pm 243)$. For the case where $b_1 = -3$ and $b_2 = -243$ we see that it yields the equation

$$L^2 = -3M^4 - 74e^2 M^2 - 243e^4$$

which cannot have any solutions as we have that the right hand side is always negative and we cannot have a negative square. If $b_1 = 3$ we see instead that $L^2 = 3M^4 - 74e^2 M^2 + 243e^4$ has no solution modulo 2^4 for which $\gcd(M, e), \gcd(L, e) = 1$. Therefore $\#\bar{\alpha}(\bar{E}_2(\mathbb{Q})) = 1$.

Thus,

$$\begin{aligned} 2^r &= \frac{\#\alpha(E_2(\mathbb{Q}))\#\bar{\alpha}(\bar{E}_2(\mathbb{Q})}{2} \\ &= \frac{4 \cdot 1}{4} \\ &= 1 \end{aligned}$$

so the rank is 0 and thus $E_2(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

This proves Theorem 3.1, as we know that the rank can only be positive if N is even. Since $N = 2$ gives 0 rank, then the smallest positive rank for $E_N(\mathbb{Q})$ occurs when $N = 4$.

6 Positive Solutions to the Fruit Puzzle

The example with $N = 4$ gave us positive rank and thus a solution (a, b, c) to C_N (3). However, if we want to solve the fruit puzzle, we cannot have negative fruits. This focuses our attention on finding $(x, y) \in E_N(\mathbb{Q})$ such that they give positive (a, b, c) on C_N. For the case where $N > 0$ the following theorem gives some conditions on x that give the desired positive solution.

Theorem 6.1 ([BM14]). *Let $(x, y) \in E_N(\mathbb{Q})$ with corresponding $(a, b, c) \in C_N(\mathbb{Q})$. Then $a, b, c > 0$ if and only if*

$$\frac{1}{2}\left(3 - 12N - 4N^2 - (2N+5)\sqrt{(2N+5)(2N-3)}\right) < x < -2(N+3)(N + \sqrt{N^2-4}) \tag{20}$$

or

$$-2(N+3)(N - \sqrt{N^2-4}) < x < -4\left(\frac{N+3}{N+2}\right). \tag{21}$$

The following proof is based on the proof of Theorem 4.1 in [BM14].

Proof. ($\implies$) Suppose $a, b, c > 0$. Then $s = a+b+c$ is also positive. Then we have that $\frac{a}{s}, \frac{b}{s} > 0$ and in particular substituting (9)

$$\frac{ab}{s^2} = \frac{(8(N+3) - x + y)(8(N+3) - x - y)}{s^2} > 0.$$

This happens if and only if

$$\begin{aligned}
0 &< (8(N+3) - x + y)(8(N+3) - x - y) \\
&= -16(N+3)x + 64(N+3)^2 + x^2 - y^2 \\
&= -16(N+3)x + 64(N+3)^2 + x^2 - x^3 - (4N^2 + 12N - 3)x^2 - 32(N+3)x \\
&= 64(N+3)^2 - x^3 - 4N(N+3)x^2 + 4x^2 - 48(N+3) \\
&= (4-x)(x^2 + 4N(N+3)x + 16(N+3)^2).
\end{aligned}$$

Either both terms are negative or both positive. Suppose they are both negative, so $x > 4$, then $x^2 + 4N(N+3)x + 16(N+3)^2 < 0$ which can only happen when x is negative, contradicting the fact that $x > 4$. Therefore both terms are positive, so $x < 4$ and $x^2 + 4N(N+3)x + 16(N+3)^2 > 0$. Using the quadratic formula we find that this happens when either

$$x > -2(N+3)(N - \sqrt{N^2-4})$$

or

$$x < -2(N+3)(N + \sqrt{N^2-4}).$$

Similarly

$$\frac{c}{s} = \frac{-4(N+3) - (N+2)x}{(4-x)(N+3)} > 0 \iff x < -4\left(\frac{N+3}{N+3}\right).$$

The inequality $y^2 > 0$ gives one last bound for x. Note that

$$y^2 = x^3 + (4N^2 + 12N - 3)x^2 + 32(N+3)x > 0$$

when $x > \frac{1}{2}(3 - 4N(N+3) - (2N+5)\sqrt{(2N+5)(2N-3)})$.

Thus we have

$$\begin{aligned}
\frac{1}{2}(3 - 4N(N+3) - (2N+5)\sqrt{(2N+5)(2N-3)}) &< -2(N+3)(N + \sqrt{N^2-4}), \\
\text{and } \; -2(N+3)(N + \sqrt{N^2-4}) &< -2(N+3)(N - \sqrt{N^2-4}), \\
\text{and } \; -2(N+3)(N - \sqrt{N^2-4}) &< -4\left(\frac{N+3}{N+2}\right).
\end{aligned}$$

The first inequality follows from assuming $\frac{1}{2}(3 - 4N(N+3) - (2N+5)\sqrt{(2N+5)(2N-3)}) > -2(N+3)(N + \sqrt{N^2-4})$ which leads to a contradiction as it implies $N < 0$. The second inequality follows from the fact that $-2(N+3)\sqrt{N^2-4} < 2(N+3)\sqrt{N^2-4}$. The last inequality follows from assuming $-2(N+3)(N-\sqrt{N^2-4}) > -4\left(\frac{N+3}{N+2}\right)$ which leads again to N being negative. This leads to the desired bounds for x

$$\frac{1}{2}\left(3-12N-4N^2-(2N+5)\sqrt{(2N+5)(2N-3)}\right) < x < -2(N+3)(N+\sqrt{N^2-4})$$

or

$$-2(N+3)(N-\sqrt{N^2-4}) < x < -4\left(\frac{N+3}{N+2}\right).$$

($\Longleftarrow$) Suppose $(x,y) \in E_N(\mathbb{Q})$ such that x satisfies (20) and (21). Substituting x as in (8) into one of the bounds gives

$$\begin{aligned} \frac{-4(a+b+2c)(N+3)}{(N+2)(a+b)-c} &< -4\left(\frac{N+3}{N+2}\right) \\ \Longleftrightarrow\ a+b+2c &> a+b-\frac{c}{N+2} \\ \Longleftrightarrow\ (2(N+2)+1)c &> 0. \end{aligned}$$

Since $N > 0$ then $2(N+2)+1 > 0$ which implies $c > 0$. Likewise

$$\begin{aligned} \frac{-4(a+b+2c)(N+3)}{(N+2)(a+b)-c} &> -2(N+3)(N-\sqrt{N^2-4} \\ \Longleftrightarrow\ 2(a+b+2c) &< (N-\sqrt{N^2-4})((N+2)(a+b)-c) \\ \Longleftrightarrow\ (a+b)((N+2)(N-\sqrt{N^2-4})-2) &> c(N+4-\sqrt{N^2-4}). \end{aligned}$$

We want to check whether the right hand side is negative. We have that $N+4-\sqrt{N^2-4} < 0$ if and only if $16N+20 < 0$ and since $N > 0$, that is impossible. Since $c > 0$ then the right hand side is positive. Next we need to know what the sign of $a+b$ is, so we need to check whether $((N+2)(N-\sqrt{N^2-4})-2) < 0$ (as it could happen that both expressions on the right hand side are negative thus being positive once multiplied together). If we assume $((N+2)(N-\sqrt{N^2-4})-2) < 0$ it leads to $N < 0$. Therefore $((N+2)(N-\sqrt{N^2-4})-2) > 0$ and hence $a+b > 0$. Thus, the last thing we need to check is if one of a or b is negative. Suppose that is the case. Then, $ab < 0$ and hence

$$\frac{ab}{s^2} < 0.$$

But we know from the first part of the proof that this would imply $x < -2(N+3)(N-\sqrt{N^2-4})$ or $x > -2(N+3)(N+\sqrt{N^2-4})$ and it contradicts our assumption of x satisfying (20) and (21), therefore both $a, b > 0$. □

This theorem tells us that the rational points $(x,y) \in E_N(\mathbb{Q})$ that correspond to the points $(a,b,c) \in C_N$ that are solutions to the fruit puzzle live on the 'egg' component of the elliptic curve. Therefore we have some restriction on x, so the next question to ask is whether we have restriction on N.

Remark 6.2. *In [BM14, Section 6] it is explained if there is a rational point on the egg component of E_N, there there will be a point that satisfies the inequalities of Theorem 6.1 and thus leads to desired solutions of the fruit puzzle. This is because the rational points are dense on both the egg and the unbounded component of E_N. Therefore, there will always be a solution to the fruit puzzle.*

6.1 Odd N and parametrization of N

The following theorem tells us that for odd N there are no rational points on the egg component, thus no positive solutions to the fruit puzzle.

Theorem 6.3. *[BM14, Theorem 5.1] Suppose $N \equiv 1 \bmod 2$. Then all rational points $(x, y) \in E_N(\mathbb{Q})$ satisfy $x \geq 0$.*

The proof is based on the proof of Theorem 5.1 in [BM14]. Throughout the proof we will repeatedly use the Jacobi symbol, which is defined as follows.

Definition 6.4 (Jacobi symbol)**.** *Let $n \in \mathbb{Z}$ odd with prime factorization $n = p_1^{t_1}...p_s^{t_s}$, $t_i \in \mathbb{Z}$, where $p_i \neq p_j$ for all $i \neq j$, $i, j = 1, \dots, s$. For $\gcd(a, n) = 1$ the Jacobi symbol is*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{t_1} \cdots \left(\frac{a}{p_s}\right)^{t_s}$$

where each $\left(\frac{a}{p_i}\right)$ is the Legendre symbol for the prime p_i and $i \in \{1, ..., s\}$.

The Jacobi symbol behaves similarly as the Legendre symbol, as described in the Theorem below.

Theorem 6.5 ([Ros11] page 444)**.** *Let $n \in \mathbb{Z}$ be odd and $a, b \in \mathbb{Z}$ be relatively prime to n. Then*

i. if $a \equiv b \bmod n$ then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$;

ii. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$;

iii. $\left(\frac{-1}{n}\right) = (-1)^{\left(\frac{n-1}{2}\right)}$;

iv. $\left(\frac{2}{n}\right) = (-1)^{\left(\frac{n^2-1}{8}\right)}$.

Theorem 6.6 (The reciprocity law for Jacobi symbols)**.** *[Ros11, page 446] For $n, m \in \mathbb{Z}_{>1}$ odd and relatively prime, then*

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}}.$$

The proof of both theorems can be found on [Ros11, pages 444-447]. Using these tools we go back to the proof of Theorem 6.3.

Proof of Theorem 6.3. Suppose $N \equiv 1 \bmod 2$. Then $N + 3$ is even and hence we can write it as $N + 3 = 2M$, so that it simplifies the equation of the elliptic curve E_N. Substituing M into (7) yields

$$\begin{aligned} y^2 &= x^3 + 4N(N+3)x^2 - 3x^2 + 32(N+3)x \\ &= x^3 + 4(2M-3)(2M)x^2 - 3x^2 + 64Mx \\ &= x^3 + (16M^2 - 24M - 3)x^2 + 64Mx. \end{aligned}$$

Note that if $(x, y) \in E_N(\mathbb{Q})$ then the $x-$coordinate is of the form $x = \frac{dr^2}{s^2}$ where $d, r, s \in \mathbb{Z}$, d is square free and $\gcd(r, s) = 1$ Substituting this in we get

$$\begin{aligned} y^2 &= \frac{dr^2}{s^2}\left(\frac{d^2r^4}{s^4} + (16M^2 - 24M - 3)\frac{r^2}{s^2} + 64M\right) \\ \iff \left(\frac{ys}{r}\right)^2 &= \frac{d^3r^2}{s^2} + (16M^2 - 24M - 3)\frac{d^2rr}{s^2} + 64Md \\ \iff \left(\frac{ys^3}{rd}\right)^2 &= dr^4 + (16M^2 - 24M - 3)r^2s^2 + \frac{64M}{d} \qquad (\star) \end{aligned}$$

and since the square on the left hand side is an integer that implies $d \mid 64M$. Letting $\left(\frac{ys^3}{rd}\right)^2 = \square$, multiplying by $4d$ and completing the square gives

$$\begin{aligned}4d\square &= 4d^2r^4 + 4d(16M^2 - 24M - 3)r^2s^2 + 4\cdot 64Ms^4\\ &= (2dr^2 + (16M^2 - 24M - 3)s^2)^2 - (16M^2 - 24M - 3)^2s^4 + 4\cdot 64Ms^4\\ &= (2dr^2 + (16M^2 - 24M - 3)s^2)^2 - (4M - 1)^3(4M - 9)s^4 \qquad (\star\star)\end{aligned}$$

and in particular since $d \mid 64M$ and is square free, $d \mid 2M$.

The idea is to show that there can be no solutions $r, s \in \mathbb{Z}$ to $(\star)$ when $d < 0$. We do this by considering different cases for d.

Case I. $d < 0$ and odd. Let $d = -u$ where $u > 0$ and odd. Since $d \mid M$, let $M = um$. Then $(\star)$ becomes

$$\begin{aligned}\square &= -ur^4 + (16M^2 - 24M - 3)r^2s^2 + \frac{64um}{-u}s^4\\ &= -ur^4 + (16M^2 - 24M - 3)r^2s^2 - 64ms^4.\end{aligned}$$

Note that $\gcd(-u, um - 1) = 1$ so the Jacobi symbol

$$\left(\frac{-u}{4M-1}\right) = \left(\frac{-1}{4M-1}\right)\left(\frac{u}{4M-1}\right).$$

Then $\left(\frac{-1}{4M-1}\right) = (-1)^{\frac{4M-1-1}{2}} = (-1)^{2M-1} = -1$ which follows from applying Theorem 6.5. Note that $\left(\frac{4M-1}{u}\right)$ is its own inverse, as $\left(\frac{4M-1}{u}\right)^2 = 1$ so together with applying Theorem 6.6 we have

$$\left(\frac{u}{4M-1}\right) = (-1)^{\frac{u-1}{2}}\left(\frac{4M-1}{u}\right)$$

Here

$$\left(\frac{4M-1}{u}\right) = \left(\frac{4um-1}{u}\right) = \left(\frac{-1}{u}\right)$$

as $4um - 1 \equiv -1 \bmod u$. Putting it back together gives

$$\begin{aligned}\left(\frac{-u}{4M-1}\right) &= -(-1)^{\frac{u-1}{2}}\left(\frac{-1}{u}\right)\\ &= -(-1)^{\frac{u-1}{2}}(-1)^{\frac{u-1}{2}}\\ &= -1.\end{aligned}$$

Therefore there exists a prime $p \mid (4M-1)$ such that $\left(\frac{-u}{p}\right) = -1$. This is because if for all primes p dividing $4M-1$ we had $\left(\frac{-u}{p}\right) = 1$ then $\left(\frac{-u}{4M-1}\right) = 1$. Therefore modulo that prime $(\star\star)$ becomes

$$(-2ur^2 + (16M^2024M - 3)s^2)^2 \equiv -4u\square \bmod p$$

which can only happen if $(-2ur^2 + (16M^2024M - 3)s^2)^2 \equiv 0 \bmod p$ since $-u$ is not a square modulo p. Since $4M - 1 \equiv 0 \bmod p$, then $4M \equiv 1 \bmod p$ so

$$\begin{aligned}-2ur^2 + (16M^2 + 24M - 3)s^2 &\equiv 0 \bmod p\\ \Rightarrow -2ur^2(1 - 6 - 3)s^2 &\equiv 0 \bmod p\\ \Rightarrow -2ur^2 - 8s^2 &\equiv 0 \bmod p\\ \Rightarrow 4s^2 &\equiv -ur^2 \bmod p.\end{aligned}$$

Since u is not a square this implies $s \equiv r \equiv 0 \bmod p$ which contradicts the fact that $gcd(r,s) = 1$. **Case II.** $d < 0$ and even. Set $d = -2u, u > 0$ odd and $M = um$ as before. Then $(\star\star)$ becomes

$$(-4ur^2(16M^2 - 24M - 3)s^2)^2 - (4M-1)^3(4M-9)s^4 = -8u\square.$$

We apply the same method as in case I, but first we need to subdivide into two subcases. **Subcase I.** M even. Then, by Theorem 6.5

$$\left(\frac{-2u}{4M-1}\right) = \left(\frac{-2}{4M-1}\right)\left(\frac{u}{4M-1}\right),$$

where

$$\left(\frac{-2}{4M-1}\right) = \left(\frac{-1}{4M-1}\right)\left(\frac{2}{4M-1}\right).$$

Evaluating those Jacobi symbols we have

$$\left(\frac{-1}{4M-1}\right) = (-1)^{2M-1} = -1 \text{ and } \left(\frac{-1}{4M-1}\right) = (-1)^{2M^2-M} = (-1)^{M(2M-1)} = 1,$$

since M is even. By Theorem 6.6

$$\left(\frac{u}{4M-1}\right) = (-1)^{\frac{u-1}{2}}\left(\frac{4M-1}{u}\right) = (-1)^{\frac{u-1}{2}}\left(\frac{-1}{u}\right).$$

Hence

$$\begin{aligned}\left(\frac{-2}{4M-1}\right)\left(\frac{u}{4M-1}\right) &= -(-1)^{\frac{u-1}{2}}\left(\frac{-1}{u}\right)\\ &= -(-1)^{\frac{u-1}{2}}(-1)^{\frac{u-1}{2}}\\ &= -1.\end{aligned}$$

Therefore there exists a prime $p \mid (4M-1)$ such that $\left(\frac{-2u}{p}\right) = -1$. Then $(\star\star)$ becomes

$$(-4ur^2(16M^2 - 24M - 3)s^2)^2 \equiv -8u\square \bmod p$$

and since $-8u\square = -2u \cdot 4\square$ and we know $-2u$ is not square, this can only happen if

$$\begin{aligned}-4ur^2(16M^2 - 24M - 3)s^2 &\equiv 0 \bmod p\\ \Rightarrow -4ur^2 + (1-6-3)s^2 &\equiv 0 \bmod p\\ \Rightarrow 4s^2 &\equiv -2ur^2 \bmod p\end{aligned}$$

and again, since $-2u$ is not a quadratic residue modulo p, then this can only happen when $r \equiv s \equiv 0 \bmod p$ which again contradicts the fact that r and s are relatively prime.

Subcase II. M odd. Write $M = um$ with both u, m odd and $d = -2u$ as before. Then $(\star)$ becomes

$$\begin{aligned}\square &= -2ur^4 + (16M^2 - 24M - 3)s^2r^2 + \frac{64um}{-2u}s^4\\ &= -2ur^4 + (16M^2 - 24M - 3)s^2r^2 - 32ms^4.\end{aligned}$$

Modulo 4, it becomes

$$r^2(2ur^2 + s^2) \equiv \square \bmod 4.$$

The squares modulo 4 are 0 and 1. Suppose s is even, then we can write it as $s = 2k$ for some $k \in \mathbb{Z}$ and hence $s^4 \equiv 0 \bmod 4$. Since r and s are relatively prime, then r can either be 1 or 3 modulo 4. Note that u is odd and $r^4 \equiv 1 \bmod 4$ for both $r \equiv 1, 3 \bmod 4$. Therefore we have the following

$$r^2(2ur^2 + s^2) \equiv 2ur^4 = 2u = \begin{cases} 2 \cdot 1 \equiv 2 & \text{if } u \equiv 1 \bmod 4 \\ 2 \cdot 3 \equiv 2 & \text{if } u \equiv 3 \bmod 4 \end{cases}$$

and since 2 is not a square modulo 4, then s must be odd. We know r and s are relatively prime, so r is even. We can write $r = 2k$ so

$$\begin{aligned} 2ur^4 + (16M^2 - 24M - 3)s^2r^2 - 32ms^4 &\equiv \square \bmod 8 \\ \iff -3r^2s^2 &\equiv \square \bmod 8 \\ \iff -3(r/2)^2 &\equiv \square/4s^2 \bmod 8 \end{aligned}$$

since r is divisible by 2. Therefore $(r/2) \equiv 0 \bmod 8$ so it is even. Write $\frac{r}{s} = 2t$ for some $t \in \mathbb{Z}$ so $r = 4t$. Therefore

$$\begin{aligned} \square &= -2ur^4 + (16M^2 - 24M - 3)s^2r^2 - 32ms^4 \\ &= -2u4^4t^4 + ((16M^2 - 24M - 3)s^2 16t^2 - 32ms^4. \end{aligned}$$

Dividing everything by 16 yields

$$-32ut^4 + (16M^2 - 24M - 3)t^2s^2 - 2ms^4 = \square$$

and modulo 4 it becomes

$$-3(r/4)^2s^2 - 2ms^4 \equiv \square \bmod 4.$$

Note that s is odd and hence $s \equiv 1 \bmod 4$ or $s \equiv 3 \bmod 4$ so $s^2 \equiv 1 \bmod 4$. Therefore we have $-3\left(\frac{r}{4}\right)^2 - 2m \equiv \square \bmod 4$ and since m is odd we have that $2m \equiv 2 \cdot 1 \equiv 2 \bmod 4$ if $m \equiv 1 \bmod 4$ or $2m \equiv 2 \cdot 3 \equiv 2 \bmod 4$ if $m \equiv 3 \bmod 4$ and thus

$$-3\left(\frac{r}{4}\right)^2 - 2 \equiv \square \bmod 4.$$

Here

$$-3\left(\frac{r}{4}\right)^2 - 2 \equiv \begin{cases} 2 & \text{if } (r/4)^2 \equiv 0 \bmod 4 \\ 3 & \text{if } (r/4)^2 \equiv 1 \bmod 4 \end{cases}$$

which are both not a square modulo 4 so this is also impossible.

□

This result narrows down the options we have for N to get positive solutions to the fruit puzzle. Together with Theorem 6.1 we know that not only we need even N, but we also need x to be negative (in fact, less than -4) to be able to get positive solutions at all. The next questions we can ask ourselves is whether there are infinitely many even positive integers N which result in positive solutions to C_N.

Theorem 6.7. *[BM14, Theorem 5.3] There exist infinitely many positive even integers N such that (3) has positive solutions.*

Proof. We want infinitely many positive values of N, so we try to write N as a polynomial $N(t)$, and we want $N(t)$ to be always even. Let $N \in \mathbb{Z}[t]$ such that $N = t^2+t+4$, then $N(t) \equiv t^2+t \equiv 0 \bmod 2$ for all t, thus $N(t)$ is always even. Moreover, $N(t)$ is always positive as $t^2 + t > 0$ for all $t \in \mathbb{Z}$. Let $x = -4(t^2+t+1)^2$. Substituting $x = -4(t^2+t+1)^2$ and $N = t^2+t+4$ into the right hand side of (7) leads to the right hand side being equal to $(4(2t+1)(t^2+t+1)(3t^2+3t+7))^2$ and hence $y = 4(2t+1)(t^2+t+1)(3t^2+3t+7)$. One can check that $x = -4(t^2+t+1)^2$ satisfies the inequalities given in Theorem 6.1 and thus ensures positive a, b, c. □

Remark 6.8. *There could be different parametrizations of N for which (3) has positive solutions. Such a parametrization needs to satisfy the requirements of being a polynomial in $\mathbb{Z}[t]$ such that it is always even and positive. For that polynomial one needs to be able to find x satisfying Theorem 6.1 and for which the right hand side of (7) is a square.*

The points a, b, c corresponding to such a parametrization [BM14, Remark 5.4] are given by

$$a = (t^2+1)(3t^3+8t^2+14t+11) \quad b = -(t^2+2t+2)(3t^3+t^2+7t-2)$$
$$c = t^6+3t^5+11t^4+17t^3+20t^2+12t-1.$$

Therefore a multiple of the point $(x, y) = (-4(t^2+t+1)^2, 4(2t+1)(t^2+t+1)(3t^2+3t+7))$ would be necessary in order to get positive a, b, c.

6.2 Height of the points

We can make a few comments on the size of solutions we found in Example 5.3, and how these relate to nP. Before we do this we need to introduce the notion of height.

Definition 6.9 (Height)**.** *[ST15, Section 3.1] Let $x \in \mathbb{Q}$ so that $x = \frac{m}{n}$ for $m, n \in \mathbb{Z}$, written in lowest terms. The height function $H(\cdot)$ is defined by*

$$H(x) \coloneqq \max\{|m|, |n|\}.$$

Definition 6.10 (Height of a point)**.** *The height of a rational point $P = (x, y)$ is defined to be the height of the $x-$coordinate of P. We write $H(P) = H(x)$.*

The height tells us how ‘complicated’ a point is. If m and n are ‘close’, then x will be close to 1, but the absolute values of m and n could still be very large.

Definition 6.11. *The logarithmic height $h(P)$ of a point $P = (x, y)$ is defined by*

$$h(P) \coloneqq \log H(P).$$

The height function has the following properties.

Lemma 6.12. *[ST15, Lemma 3.1] Let $K \in \mathbb{R}_{>0}$. Then the set*

$$\{P \in E(\mathbb{Q}) : h(P) \leq K\}$$

is finite.

Lemma 6.13. *[ST15, Lemma 3.3] Let $P \in E(\mathbb{Q})$, then there exists a constant κ that depends on the coefficients of $E(\mathbb{Q})$ such that*

$$h(2P) \geq 4h(P) - \kappa.$$

Lemma 6.12 is stated in [ST15] without proof, while the proof of Lemma (6.13) can be found in [ST15, Section 3.3].

There is a generalization of Lemma 6.13 that replaces the 2 in $h(2P)$ for $n \in \mathbb{Z}$, thus being the logarithmic height of nP. Hence we double a point, Lemma 6.13 tells us that the we expect the height to increase. Thus, for a point $P \in E(\mathbb{Q})$ we expect the height of nP to increase as n increases. In Example 5.3 we can see this happening, as the height of nP increases as n goes from 1 to 9. Moreover, in (9) we see that a, b and c are defined in terms of x and y and hence as the height of nP increases, we expect the size of the corresponding a, b, c to increase too. We showed the case when this happens corresponding to Example 5.3, where $P = (-4, 28)$ and for $n = 9$ all a, b, c are positive integers.

Remark 6.14. *As future work, some more rigorous theory could be developed about the height of a point on $E_N(\mathbb{Q})$ whose multiples correspond to positive solutions to the fruit puzzle and relation to the number of digits of each a, b and c.*

n	$h(nP)$	**# digits of a**	**# digits of b**	**# digits of c**
1	~ 1.39	2	1	1
2	~ 6.52	4	4	4
3	~ 13.5	9	9	9
4	~ 23.0	16	16	16
5	~ 39.1	25	25	25
6	~ 53.9	36	36	36
7	~ 74.2	49	49	48
8	~ 98.6	64	64	63
9	~ 122.0	81	80	79

Table 2: Height of P versus size of a, b, c

A Appendix

Code used to perform the calculations needed in the transformation from C_N to E_N.

```
# Importing SageMath
from sage.all import var, solve, show

# Define the variables
var('a b c x y z N')

# Define the system of equations
eq1 = x == (a + b + 2*c)
eq2 = y == (a - b)
eq3 = z == (N + 2)*(a + b) - c

# Solve the system for a, b, and c
solutions = solve([eq1, eq2, eq3], a, b, c)

# Display the solutions
show(solutions)

abc = solutions[0]

a1= abc[0].rhs()
a2= abc[1].rhs()
a3= abc[2].rhs()

def proj_eq(a,b,c):
    return N*(a + b)*(a + c)*(b + c) - a*(a + b)*(a + c) - b*(a + b)*(b + c) - c*(a + c)*(b

proj_eq_in_xyz = expand(proj_eq(a1, b1, c1))

show(proj_eq_in_xyz)
```

To check for integer solutions to (10) we used the following SageMath code.

```
#name the variables and set N to be an integer
var('x')
N = var('N', domain='integer')
```

```
    #define what a and b are in our elliptic curve
    a = 4*N^2+12*N-3
    b=32*(N+3)
    #equation satifying duplication formula for a point of order 3
    eq_order_3 = 3*x^4 + 4*a*x^3 +6*b*x^2 -b^2==0
    #equation satifying duplication formula for a point of order 3
    eq_order_6 = x^4 -16*x^3 - 2*(b+8*a)*x^2 - 16*b*x +b^2

    #function that takes as input the equation we want to
    #solve and returns the integer solutions
    def int_sol_finder(f):
        solutions = solve(f, x, solution_dict=True)

        integer_solutions = []
        for sol in solutions:
            if sol[x].is_integer():
                integer_solutions.append(sol[x])

        return integer_solutions
```

SageMath code used to solve the system of equations in (9).

```
var('N, a, b, c')

#put values of (x,y) to solve for a, b and c
x= 0
y= 0

#a/s, b/s, c/s expressions
f_a=(8*(N+3)-x+y)/(2*(4-x)*(N+3))
f_b=(8*(N+3)-x-y)/(2*(4-x)*(N+3))
f_c=(-4*(N+3)-(N+2)*x)/((4-x)*(N+3))

s= a+b+c

#solve the expressions for a, b and c
solve([a/s == f_a, b/s==f_b, c/s==f_c], a, b, c)
```

SageMath code used to substitute values of a, b, c into the equations of x and y (8).

```
var('N')

#write values of a, b and c to find (x,y)
a = -1
b = 1
c = 1

#expressions of x,y in terms of a,b,c
x = (-4*(a+b+2*c*(N+3)))/((2+N)*(a+b)-c)
y = (4*(a-b)*(N+3)*(2*N+5))/((2+N)*(a+b)-c)


print('(', x, ',', y, ')')
```

```
var('a b c N x y s')

# Define the equations
eq1 = x == (-4*(a+b+2*c)*(N+3)) / ((N+2)*(a+b) - c)
eq2 = y == (4*(a-b)*(N+3)*(2*N+5)) / ((N+2)*(a+b) - c)
eq3 = s == a + b + c

# Solve the system for a, b, c
solution = solve([eq1, eq2, eq3], a, b, c)

solution
```

This is the SageMath code used in the examples 5.3.

```
# Define function f that takes the values b1,b2,a of our equation and p being
#the prime we want to check, r the prime power
def f(b1, b2, a, p, r):
    # Define variables
    var('M, e, N')

    # Check solutions for all M, e, N satisfying the equation
    #N^2 = b1*M^4 + ae^2M^2 + b2e^4
    solutions = solve_mod(N^2 == b1*M^4 + a*e^2*M^2 + b2*e^4, p^r)

    # Function to check if gcd of all variables in a solution is 1
    def is_valid_solution(sol):
        gcd_M_e = gcd(sol[0], sol[1])
        gcd_M_N = gcd(sol[0], sol[2])
        gcd_e_N = gcd(sol[1], sol[2])
        return (gcd_M_e == gcd_M_N == gcd_e_N == 1)

    # Filter solutions based on gcd conditions
    valid_solutions = [sol for sol in solutions if is_valid_solution(sol)]

    return valid_solutions

# Call function f with given parameters
```

Code used to find multiples of the point $(-4, 28) \in E_4(\mathbb{Q})$ and to compute the corresponding values of a, b, c.

```
#compute multiples of the elliptic curve

N=4

a2 = 4*N^2+12*N-3
a4 = 32*(N+3)

E = EllipticCurve([0,a2,0,a4,0])
P = E([-4,28]); #P

n=9
```

```
n*P
Q = n*P

#solve for a b c

var('a b c')

#x and y coordinates of the point nP
x = Q.x()
y = Q.y()

s = a+b+c

a_expr = a == s*((8*(N+3)-x+y))/(2*(4-x)*(N+3))
b_expr = b == s*((8*(N+3)-x-y))/(2*(4-x)*(N+3))
c_expr = c == s*(-4*(N+3)-(N+2)*x)/((4-x)*(N+3))

solve([a_expr,b_expr, c_expr],a,b,c)
```

Code used to find the multiples of P' together with the corresponding values of $(a : b : c)$. The code provided is for the case where $P' = P + Q$ where $P = (-4, 28)$ and Q is a point of order 2.

```
P = E([-4,28])
N=4

#torsion points given by

#point of order 2
Q_2 = E([0,0])

#points of order 3
Q_3_1 = E([4, 4*(2*N+5)])
Q_3_2 = E([4, -4*(2*N+5)])

#points of order 6
Q_6_1 = E([8*(N+3), 8*(N+3)*(2*N+5)])
Q_6_2 = E([8*(N+3), -8*(N+3)*(2*N+5)])

#a,b,c equations
def equations(x, y):
    a, b, c = var('a b c')

    s = a+b+c
    eq1 = a == s*((8*(N+3)-x+y))/(2*(4-x)*(N+3))
    eq2 = b == s*((8*(N+3)-x-y))/(2*(4-x)*(N+3))
    eq3 = c == s*(-4*(N+3)-(N+2)*x)/((4-x)*(N+3))

    return [eq1, eq2, eq3]

#define the torsion point, in this case the one of order 2
P_2 = P + Q_2
```

```python
# Compute nP for n in range 1 to 9 and solve the system of equations
solutions = []
for n in range(1, 10):
    nP_2 = n * P_2
    x, y = nP_2.xy()
    eqs = equations(x, y)
    sol = solve(eqs, a, b, c)
    solutions.append(sol)

# Print the solutions
for i, sol in enumerate(solutions, 1):
    print(f"Solution for {i}P_2:")
    print(sol)
    print()
```

References

[AL11] Wayne Aitken and Franz Lemmermeyer. "Counterexamples to the Hasse Principle". In: *American Mathematical Monthly* 118 (2011), pp. 610–628. DOI: 10.4169/amer.math.monthly.118.07.610.

[Ale16] Alex Alexeq. *Math Overflow*. Accessed on July 22nd, 2024. 2016. URL: https://mathoverflow.net/questions/227713/estimating-the-size-of-solutions-of-a-diophantine-equation/227722#227722.

[Ami19] Alon Amit. *Quora*. Accessed on July 22nd, 2024. 2019. URL: https://www.quora.com/How-do-you-find-the-positive-integer-solutions-to-frac-x-y+z-+-frac-y-z+x-+-frac-z-x+y-4/answer/Alon-Amit.

[Bee10] Monique van Beek. *The rank of elliptic curves of the form $E_{A,B} : y^2 = x^3 + A(x - B)^2$*. Master's thesis. 2010. URL: https://fse.studenttheses.ub.rug.nl/9259/1/Monique_van_Beek_MW_2010.pdf.

[BM14] A. Bremner and A. Macleod. "An unusual cubic representation problem". In: *Annales Mathematicae et Informaticae* 43 (2014), pp. 29–41.

[Bri] Martin Bright. *Descent by 2-isogeny (following Cassels)*. Lecture notes. URL: http://www.boojum.org.uk/maths/descent.pdf.

[Cas91] J. W. S. Cassels. *LMSST: 24 Lectures on Elliptic Curves*. London Mathematical Society Student Texts. Cambridge University Press, 1991.

[Con] Keith Conrad. *Divisibility and Greatest Common Divisors*. URL: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/divgcd.pdf.

[Cre97] John Cremona. *Higher Descents on Elliptic Curves*. Lecture notes. 1997. URL: https://johncremona.github.io/papers/d2.pdf.

[Mar06] Andreas Mars. *Elliptic Curves*. Lecture notes. 2006. URL: https://www.maths.tcd.ie/pub/Maths/Courseware/499/2006/Mars/ellcurves.pdf.

[Maz77] Barry Mazur. "Modular curves and the Eisenstein ideal". In: *Publications Mathématiques de l'IHÉS* 47 (1977), pp. 33–186. URL: http://www.numdam.org/item/PMIHES_1977__47__33_0/.

[Ros11] K.H. Rosen. *Elementary Number Theory and Its Applications*. Addison-Wesley, 2011. ISBN: 9780321500311. URL: https://books.google.nl/books?id=tI7tPAAACAAJ.

[Shu09] Daniel Shumow. *Isogenies of Elliptic Curves: A Computational Approach*. 2009. arXiv: 0910.5370. URL: https://arxiv.org/abs/0910.5370.

[Sil06] Joseph H Silverman. *An introduction to the theory of elliptic curves*. Lecture notes. 2006. URL: %5Chref%7Bhttps://www.math.brown.edu/johsilve/Presentations/WyomingEllipticCurve.pdf%7D.

[SS03] Edward F. Schaefer and Michael Stoll. "How to do a p-descent on an elliptic curve". In: *Transactions of the American Mathematical Society* 356 (2003), pp. 1209–1231. URL: https://api.semanticscholar.org/CorpusID:1252613.

[ST15] Joseph H Silverman and John T Tate. *Rational points on elliptic curves*. en. 2nd ed. Undergraduate texts in mathematics. Cham, Switzerland: Springer International Publishing, 2015.

[The21] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.3)*. https://www.sagemath.org. 2021.

[Tim15] Lianne van Timmeren. *On Elliptic Curves of the Form $y^2 = x^3 + A(x - B)^2$*. Master's thesis. 2015. URL: https://fse.studenttheses.ub.rug.nl/13007/1/Main.pdf.

[TM18] Jaap Top and J.Steffen Müller. *Group Theory*. Lecture notes. 2018. URL: https://www.rug.nl/staff/steffen.muller/lecture_notes_group_theory.pdf.

[Wut18] Chris Wuthrich. *Elliptic curves*. Lecture notes. 2018. URL: https://www.maths.nottingham.ac.uk/plp/pmzcw/.