S. Moerman

Sizes of solutions

Bachelor thesis

June 22, 2018

Thesis supervisor: dr. R.M.M. Griffon

Leiden University
Mathematical Institute

This page is left intentionally blank.

Contents

Introduction

In this thesis, we study the positive rational solutions (x, y) of the equation $x^3 + y^3 = n$ for any integer $n \geq 1$. Our goal is to find the "smallest" solution if there even is one. Here a solution is called the smallest if the nominators and denominators of x and y are as small as possible.

This search is based on two of the *Canterbury Puzzles* of Henry E. Dudeney [1].

Example 1 (The Silver Cubes)**.** A merchant has some silver, which he always keeps under the form of two cubes. One day, he has 16 cm^3 of silver in two cubes of side-length 2 cm. After a transaction, he earns one more cube centimetre of silver. How can he divide 17 cm^3 of silver in two cubes with rational side-length? In other words, the problem is to find $x, y \in \mathbb{Q}_{>0}$ such that $x^3 + y^3 = 17$.

Example 2 (Doctor of Physics)**.** A doctor has two spherical bottles containing a drug: one sphere has diameter 1 cm^3 and the other has diameter 2 cm^3. One day, she wants to transfer the contents of these bottles into two other spherical bottles with other diameters. What can the diameters of these new bottles be such that together they contain the same volume of drug? In other words, the problem is to find $x, y \in \mathbb{Q}_{>0}$ such that $x^3 + y^3 = 1^3 + 2^3 = 9$ with x and y different from 1 and 2.

In the end of the book, Dudeney gives the solutions to the puzzles. For Example 1 and Example 2 he gives respectively the solutions:

$$(x_1, y_1) = \left(\frac{104940}{40831}, \frac{11663}{40831}\right) \quad \text{and} \quad (x_2, y_2) = \left(\frac{415280564497}{348671682660}, \frac{676702467503}{348671682660}\right).$$

Unfortunately, he does not give a clue how he found these solutions, but it is really unlikely that he found them by trial-and-error.

In this thesis we always assume that $n \in \mathbb{Z}_{\geq 1}$ is a cube-free integer. This assumption is not really restrictive, because a solution (x, y) for $n = c^3 m$ produces a solution $(x/c, y/c)$ for m. Furthermore, we often assume that n is greater or equal to 3. The cases $n = 1$ and $n = 2$ are special, because they have the special solutions $(1, 0)$ and $(1, 1)$ respectively and with that we already found their smallest solutions. However, some of the obtained theory is still applicable in these cases.

We will consider the equation $x^3 + y^3 = n$ as a curve E_n°. Notice that the line $x + y = 0$ is an asymptote of E_n° so there is some point $\mathcal{O}$ 'at infinity'. To include this point we consider the projective version of E_n°: the curve E_n given by $X^3 + Y^3 = nZ^3$ for $(X : Y : Z) \in \mathbb{P}^2$. Then we have $\mathcal{O} = (1 : -1 : 0)$ and a solution (x, y) of $x^3 + y^3 = n$ corresponds to $(x : y : 1)$. We denote by $E_n^\circ(\mathbb{Q})$ and $E_n(\mathbb{Q})$ the rational points on E_n° and E_n respectively. So we have $E_n(\mathbb{Q}) \cong E_n^\circ(\mathbb{Q}) \cup \{\mathcal{O}\}$. Note that we also include the rational points with negative coordinates. We define $E_n^+(\mathbb{Q}) \subset E_n^\circ(\mathbb{Q})$ as the set of rational solutions with positive coordinates.

In Chapter 1, we will equip $E_n(\mathbb{Q})$ with an abelian group law $\oplus$ and we give explicit formulas for this operation. Then we will focus on constructing a measure of the elements of $E_n(\mathbb{Q})$ in Chapter 2. This gives us the Néron-Tate Height $\hat{h}$ which is a quadratic form on $E_n(\mathbb{Q})$ In Chapter 3, we will show for $n \geq 3$ that if $E_n^\circ(\mathbb{Q})$ is non-empty, $E_n^\circ(\mathbb{Q})$ has infinitely many elements and therefore $E_n^+(\mathbb{Q})$ has infinitely many elements. In the end, we will discuss the Mordell-Weil Theorem, which states that $E_n(\mathbb{Q})$ is finitely generated as an abelian group with group law $\oplus$.

With these results, we can try to find a solution such that its Néron-Tate Height is a small as possible. Therefore, we have to find the generators of $E_n(\mathbb{Q})$, but we don't know how many generators $E_n(\mathbb{Q})$ has. When we found one, we search for the smallest multiple of a generator in $E_n^+(\mathbb{Q})$.

In Example 1, we can easily find the point $P = (18 : -1 : 7) \in E_{17}(\mathbb{Q})$. Then we have $2P = (11663 : 104940 : 40831) \in E_{17}^+(\mathbb{Q})$, which gives the same solution as the solution Dudeney found.

For Example 2, we already have $Q = (2 : 1 : 1) \in E_9^+(\mathbb{Q})$ from the solution $(2, 1)$, but want to find another one. We will find that $2P, \ldots, 5P \notin E_9^+(\mathbb{Q})$, but

$$6P = (415280564497 : 676702467503 : 348671682660).$$

This gives also the same solution as the solution Dudeney found.

1 Chapter 1

We study the rational solutions of the equation $x^3+y^3=n$. Therefore, we look at the curve $E_n^\circ : x^3+y^3=n$ and its projective version $E_n \subset \mathbb{P}^2$ given by $X^3+Y^3=nZ^3$ for $(X:Y:Z)\in\mathbb{P}^2$. Notice that $\mathcal{O}=(1:-1:0)$ and some point (x,y) on E_n° corresponds to $(x:y:1)$ on E_n. Since $F=X^3+Y^3-nZ^3$ is an irreducible polynomial in $\mathbb{R}[X,Y,Z]$, E_n is an irreducible curve. Moreover, E_n is a smooth curve since

$$\left(\frac{\partial F}{\partial X},\frac{\partial F}{\partial Y},\frac{\partial F}{\partial Z}\right)\neq 0$$

and hence every point has a tangent line.

To talk about rational and real points on a curve, we define for any field extension $K\subset\mathbb{R}$ of $\mathbb{Q}$ the sets:

$$\begin{aligned} E_n^\circ(K) &:= \{(x,y)\in K^2 | x^3+y^3=n\},\\ E_n(K) &:= \{(X:Y:Z)\in\mathbb{P}^2(K)|X^3+Y^3=nZ^3\}. \end{aligned}$$

Note that $E_n(K)=E_n^\circ(K)\cup\{\mathcal{O}\}$.

In this chapter, we will construct a group law $\oplus$ on $E_n(K)$ and give explicit formulas for this operation. This is based on §5.1 (p. $169-174$) from [2].

1.1 Introduction to projective geometry

Here we give a brief overview of some definitions from projective geometry. For some field extension $K\subset\mathbb{R}$ of $\mathbb{Q}$, some degree $d\geq 1$ and any distinct points $P_1,\dots,P_m\in\mathbb{P}^2(K)$ with $m\geq 1$, we consider following vector spaces of polynomials:

$$\begin{aligned} W_d &:= \{F\in K[X,Y,Z] | F \text{ is homogeneous of degree } d\}\\ &= \left\{ F(X,Y,Z)=\sum_{\substack{0\leq i,j\leq d\\ i+j\leq d}} a_{ij}X^iY^jZ^{d-i-j} \,\middle|\, a_{ij}\in K\right\},\\ W_d(P_1,\dots,P_m) &:= \{F\in W_d | F(P_1)=\cdots=F(P_m)=0\}. \end{aligned}$$

When we want to emphasize the field K we denote $W_d(K)$ and $W_d(K)(P_1,\dots,P_m)$ respectively. Note that $\dim(W_d)=\frac{1}{2}(d+1)(d+2)$ and hence $\dim(W_d(P_1,\dots,P_m))\geq\frac{1}{2}(d+1)(d+2)-m$, because vanishing in a point is a linear condition.

We call a set $C\subset\mathbb{P}^2(K)$ a line, a conic or a cubic if C is given by an equation $F(X,Y,Z)=0$ for some polynomial F in respectively W_1, W_2 or W_3. In particular, $E_n\subset\mathbb{P}^2(K)$ is a cubic for any field extension K of $\mathbb{Q}$.

Notice that for any two distinct points $P_1,P_2\in\mathbb{P}^2(K)$, there is exactly one line through P_1 and P_2. So $\dim(W_1(P_1,P_2))=1$. Moreover, for any five points $P_1,\dots,P_5\in\mathbb{P}^2(K)$ such that no 4 of them are on the same line (they are not colinear), there is exactly one conic through $P_1,\dots,P_5$. So $\dim(W_2(P_1,\dots,P_5))=1$.

Usuallly we identify a curve of degree d by a polynomial $F\in W_d$ such that this curve is given by $F=0$. Notice that this polynomial is not unique: for all $\lambda\in K^*$ and $F\in W_d$ the equations $F=0$ and $\lambda F=0$ give the same curve.

For the vector spaces of polynomials in an m-dimensional projective space, we introduce:

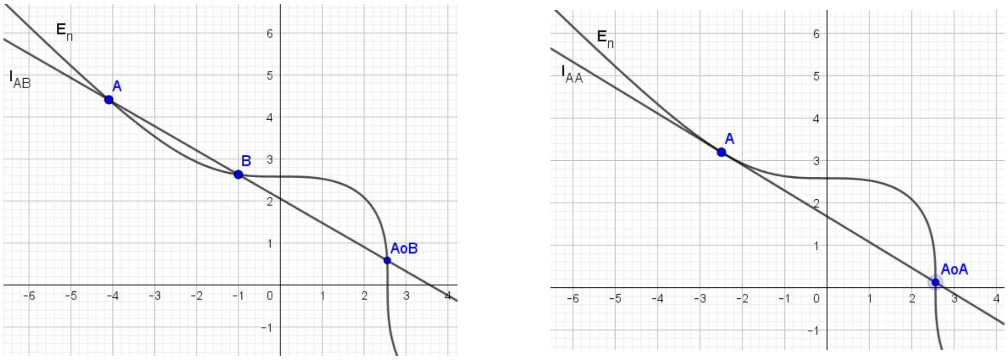
$$W_{d,m}:=\{F\in\mathbb{Q}[X_0,\dots,X_m]|F \text{ is homogeneous of degree } d\}.$$

1.2 The points on the curve as an abelian group

We have a closer look at the set $E_n(K)$ for some field extension $K\subset\mathbb{R}$ over $\mathbb{Q}$. We want to describe a group law $\oplus$ on $E_n(K)$. Let $A,B\in E_n(K)$. First we define l_{AB} as the line through A and B. If $A=B$, then l_{AB} is the tangent line of E_n in $A=B$. Since A and B have K-rational coordinates, we have that $l_{AB}\in W_1(K)(A,B)$, so the coefficients of l_{AB} are as well K-rational.

Since E_n is a conic with K-rational coefficients, the intersection of E_n with l_{AB} consists of three points counting multiplicity. Finding these points amounts to solving a cubic equation with coefficients in K and in one variable. Two solutions are known: A and B. Then we define $A \circ B$ as the third intersection point. Since A and B have K-rational coordinates, $A \circ B$ has K-rational coordinates as well and therefore we have $A \circ B \in E_n(K)$. Note that this third intersection point can be A or B if l_{AB} is the tangent line of E_n in A or B. Finally we define $A \oplus B := (A \circ B) \circ \mathcal{O}$.

In Figure 1 one can find two examples of the construction of $A \circ B$. In Figure 1a A and B are different so l_{AB} is the line joining them and in Figure 1b we have $A = B$ so l_{AA} is the tangent line of E_n in A.



(a) Construction of $A \circ B$ with $A \neq B$

(b) Construction of $A \circ A$

Figure 1: Some examples of the construction of $A \circ B$.

Theorem 1.1. *For any field extension $K \subset \mathbb{R}$ of $\mathbb{Q}$, the operation $\oplus$ defines a abelian group law on $E_n(K)$.*

Proof. Notice that we have $A \oplus \mathcal{O} = A = \mathcal{O} \oplus A$ for any $A \in E_n(K)$. Therefore, $\mathcal{O}$ is indeed the neutral element with respect to the operation $\oplus$.

Furthermore we have $A \oplus (A \circ \mathcal{O}) = \mathcal{O}$, since A, $A \circ \mathcal{O}$ and $\mathcal{O}$ lie on one line for all $A \in E_n(K)$. Hence $A \circ \mathcal{O}$ is the inverse of A, because $\oplus$ is clearly commutative. Since we write the group additively, we denote the inverse by: $-A = A \circ \mathcal{O}$.

The associativity will be proved in Theorem 1.5. □

Remark 1.2. For $A \oplus -B$, we denote $A \ominus B$.

1.2.1 Associativity of $\oplus$

The last thing we need to verify that $\oplus$ is a group law, is its associativity. Although it may seem easy to verify, it is really hard to prove it by writing out the explicit formulas we will introduce in Theorem 1.6. Therefore, we use projective geometry to prove the associativity. First we need two lemmas from the projective geometry.

Lemma 1.3. *Let $P_1, \ldots, P_8$ be eight distinct points in $\mathbb{P}^2$ such that no subset of four points is colinear and no subset of seven points lie on the same conic. Then the vector space of homogeneous polynomials of degree 3 which vanish at $P_1, \ldots, P_8$ has dimension 2.*

Proof. Note that $\dim(W_3) = 10$ and $\dim(W_3(P_1, \ldots, P_8) \geq 2$ by the discussion in §1.1. Now we distinguish 3 cases.

Suppose that there are three colinear points, say P_1, P_2 and P_3 are on the same line $L = 0$ with $L \in W_1(P_1, P_2, P_3)$. Then we choose P_9 on this line L. Hence, for any $F \in W_3(P_1, \ldots, P_9)$, we have $F = LQ$, with $Q \in W_2(P_4, \ldots, P_8)$. Since no 4 of these points are colinear, we have $\dim(W_2(P_4, \ldots, P_8)) = 1$. So there is only one conic Q_0 vanishing in $P_4, \ldots, P_8$ up to scaling. Hence $\dim(W_3(P_1, \ldots, P_9)) = 1$ and thus $\dim(W_3(P_1, \ldots, P_8)) \leq \dim(W_3(P_1, \ldots, P_9)) + 1 = 2$.

Suppose that there are six points on the same conic, say $P_1, \ldots, P_6$ are on the same conic $Q = 0$ with $Q \in W_2(P_1, \ldots, P_6)$. Then we choose P_9 on this conic Q. Hence, for any $F \in W_3(P_1, \ldots, P_9)$, we have

$F = LQ$, with $L \in W_1(P_7, P_8)$. Note that there is only one line between P_7 and P_8, so $\dim(W_1(P_7, P_8)) = 1$. Hence $\dim(W_3(P_1, \dots, P_9)) = 1$ and thus $\dim(W_3(P_1, \dots, P_8)) \leq \dim(W_3(P_1, \dots, P_9)) + 1 = 2$.

Suppose that there are no three colinear points and no six points all lie on the same conic. Then we choose P_9 and P_{10} on the line (P_1, P_2) given by $L = 0$ with $L \in W_1(P_1, P_2)$. Suppose that $\dim(W_3(P_1, \dots, P_8)) \geq 3$, then $\dim(W_3(P_1, \dots, P_{10})) \geq 1$. Thus there is a non-trivial $F \in W_3(P_1, \dots, P_{10})$. Then we can write $F = LQ$ with some non-trivial conic $Q \in W_2(P_3, \dots, P_8)$. However, we assumed that there is no conic passing through any subset of six points of $P_1, \dots, P_8$. Therefore, we have $\dim(W_3(P_1, \dots, P_8)) \leq 2$.

Thus we have $\dim(W_3(P_1, \dots, P_8)) = 2$. □

Lemma 1.4. *Let C_1 and C_2 be two cubics and C_1 is irreducible. Assume that a cubic C passes through 8 distinct points $P_1, \dots, P_8$ of the 9 intersection points $P_1, \dots, P_9$ of C_1 and C_2. Then C also passes through the ninth intersection point P_9.*

Proof. Suppose that there are 4 distinct points $A_1, \dots, A_4$ on C_1 on the same line $L \in W_1(A_1, \dots, A_4)$. Note that a cubic and a line can only intersect in 3 points or the whole line. Therefore, every point on the line L also lies on C_1. Therefore C_1 can be written as $C_1 = LQ$ for some conic Q. However C_1 is irreducible, so this is not possible. Thus there are no 4 colinear points on C_1.

Suppose that there are 7 distinct points $A_1, \dots, A_7$ on C_1 on the same conic $Q \in W_2(A_1, \dots, A_7)$. Note that a cubic and a conic can only intersect in 6 points or the whole conic. Therefore, every point on the conic Q also lies on C_1. Therefore C_1 can be written as $C_1 = QL$ for some line L. However C_1 is irreducible, so this is not possible. Thus there are no 7 points on C_1 on the same conic.

Hence we can apply Lemma 1.3 and thus $\dim(W_3(P_1, \dots, P_8))$ is of dimension 2 and therefore generated by C_1 and C_2. So we can write C as a linear combination of C_1 and C_2 and hence $C(P_9) = 0$. Thus C also passes through P_9. □

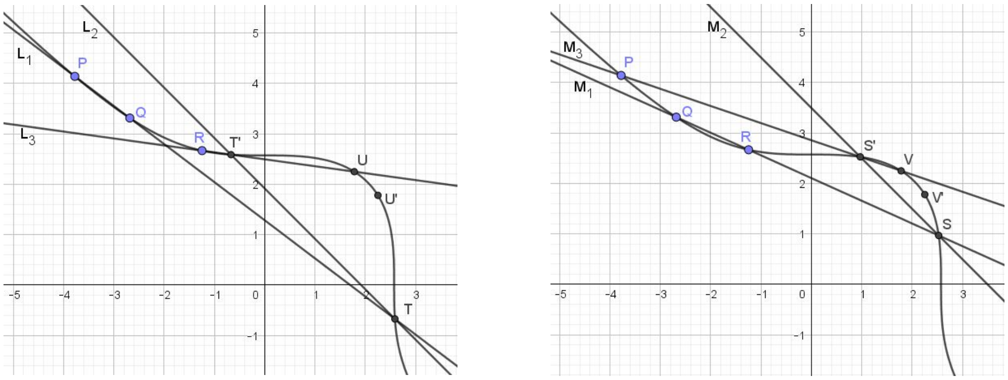
Now we can prove the associativity by applying Lemma 1.4.

Theorem 1.5. *The operation $\oplus$ is associative.*

Proof. To show the associativity, we take some $P, Q, R \in E_n(K)$ distinct to each other, each other's inverses and sums and $\mathcal{O}$. We will consider the special cases later.

First we construct $(P \oplus Q) \oplus R$. Therefore, we draw the line L_1 through P and Q and call the third intersection point $T := P \circ Q$. Then we take its inverse $T' := T \circ \mathcal{O} = P \oplus Q$ by drawing the line L_2 through T and $\mathcal{O}$. To add R, we draw the line L_3 through T' and R, whose third intersection point we call $U := T' \circ R = (P \oplus Q) \circ R$. Taking its inverse, we construct $U' := U \circ \mathcal{O} = (P \oplus Q) \oplus R$ by drawing the line L_4 through U and $\mathcal{O}$. In Figure 2a you can find an example of this construction.

Then we also construct $P \oplus (Q \oplus R)$. Therefore, we draw the line M_1 through Q and R and call the third intersection point $S := Q \circ R$. Then we take its inverse $S' := S \circ \mathcal{O} = Q \oplus R$ by drawing the line M_2 through S and $\mathcal{O}$. To add P, we draw the line M_3 through P and S', whose third intersection point we call $V := P \circ S' = P \circ (Q \oplus R)$. Taking its inverse, we construct $V' := V \circ \mathcal{O} = P \oplus (Q \oplus R)$ by drawing the line M_4 through V and $\mathcal{O}$. In Figure 2b you can find an example of this construction.



(a) Construction of $(P \oplus Q) \oplus R$

(b) Construction of $P \oplus (Q \oplus R)$

Figure 2: An example of the associativity of $\oplus$ on $E_{17}(\mathbb{R})$.

Next, we observe the cubics $C_1 = L_1 \cdot M_2 \cdot L_3$ and $C_2 = M_1 \cdot L_2 \cdot M_3$. Hence we have:

$$E_n(K) \cap C_1 = \{P, Q, T, S, \mathcal{O}, S', T', R, U\},$$
$$E_n(K) \cap C_2 = \{Q, R, S, T, \mathcal{O}, T', P, S', V\}.$$

Since E_n is an irreducible conic, C_1 has to pass through V and C_2 has to pass through U by Lemma 1.4. Therefore U and V have to be the same and hence $U' = V'$. Thus $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

In conclusion, $\oplus$ is in general associative but for some special cases where $E_n(K) \cap C_1$ and $E_n(K) \cap C_2$ does not contain 8 distinct points and U respectively V.

Let $P, Q, R \in E_n(\mathbb{R})$ be a special case. Then we can write P, Q and R as the limits of some sequences $\{P_k\}_{k=0}^{\infty}$, $\{Q_k\}_{k=0}^{\infty}$ and $\{R_k\}_{k=0}^{\infty}$ respectively where P_k, Q_k, R_k is a nonspecial case for all $k \in \mathbb{Z}_{\geq 0}$. Then we have $(P_k \oplus Q_k) \oplus R_k = P_k \oplus (Q_k \oplus R_k)$ for all $k \in \mathbb{Z}_{\geq 0}$. Taking limits we get $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ by the continuity of $\oplus$. The continuity of $\oplus$ will be proved in Corollary 1.7 from the explicit formulas for $\oplus$. Therefore we use for $E_n(\mathbb{R})$ the induced topology from $\mathbb{P}^2(\mathbb{R})$. Hence $\oplus$ is associative in $E_n(\mathbb{R})$. Therefore, $\oplus$ is also associative for fields contained in $\mathbb{R}$.

Thus $\oplus$ is associative and defines a group law on $E_n(K)$ for any field extension $K \subset \mathbb{R}$ of $\mathbb{Q}$. □

1.3 The explicit group law

For our curves E_n° we can write the group law explicitly. To avoid fractions and special cases, we will again use projective geometry and write out the group law for the curve E_n.

Theorem 1.6. *Let $P = (x : y : z), P_1 = (x_1 : y_1 : z_1), P_2 = (x_2 : y_2 : z_2) \in E_n(K)$ with $P_1 \neq P_2$. Then we have:*

$$\begin{aligned} -P &= (y : x : z), \\ P_1 \oplus P_2 &= (x_1x_2(x_1y_2 - x_2y_1) + nz_1z_2(y_1z_2 - y_2z_1) : \\ &\qquad y_1y_2(y_1x_2 - y_2x_1) + nz_1z_2(x_1z_2 - x_2z_1) : \\ &\qquad x_1x_2(x_1z_2 - x_2z_1) + y_1y_2(y_1z_2 - y_2z_1)), \\ 2P &= (-y(2x^3 + y^3) : x(x^3 + 2y^3) : z(x^3 - y^3)). \end{aligned}$$

Proof. We parametrize the line through P_1 and P_2:

$$(\lambda x_1 + \mu x_2 : \lambda y_1 + \mu y_2 : \lambda z_1 + \mu z_2) \text{ with } (\lambda : \mu) \in \mathbb{P}^1(\mathbb{Q}).$$

To find the third intersection point of this line with E_n, we fill in this parametrization in our homegeneous equation for the curve E_n:

$$(\lambda x_1 + \mu x_2)^3 + (\lambda y_1 + \mu y_2)^3 = n(\lambda z_1 + \mu z_2)^3.$$

Writing out gives us:

$$\lambda^3x_1^3 + 3\lambda^2\mu x_1^2x_2 + 3\lambda\mu^2x_1x_2^2 + \mu^3x_2^3 + \lambda^3y_1^3 + 3\lambda^2\mu y_1^2y_2 + 3\lambda\mu^2y_1y_2^2 + \mu^3y_2^3 = \\ n\lambda^3z_1^3 + 3n\lambda^2\mu z_1^2z_2 + 3n\lambda\mu^2z_1z_2^2 + \mu^3z_2^3.$$

Since P_1 and P_2 are on E_n, we have:

$$3\lambda^2\mu x_1^2x_2 + 3\lambda\mu^2x_1x_2^2 + 3\lambda^2\mu y_1^2y_2 + 3\lambda\mu^2y_1y_2^2 = 3n\lambda^2\mu z_1^2z_2 + 3n\lambda\mu^2z_1z_2^2.$$

Note that $\lambda = 0$ and $\mu = 0$ gives us respectively P_1 and P_2. Since we search for the third intersection point of the line with the curve, we can assume $\lambda, \mu \neq 0$. Hence we have:

$$\begin{aligned} \lambda x_1^2x_2 + \mu x_1x_2^2 + \lambda y_1^2y_2 + \mu y_1y_2^2 &= n\lambda z_1^2z_2 + n\mu z_1z_2^2 \\ \lambda(x_1^2x_2 + y_1^2y_2 - nz_1^2z_2) &= \mu(-x_1x_2^2 - y_1y_2^2 + nz_1z_2^2). \end{aligned}$$

Thus we have:

$$(\lambda : \mu) = (-x_1x_2^2 - y_1y_2^2 + nz_1z_2^2 : x_1^2x_2 + y_1^2y_2 - nz_1^2z_2).$$

This gives us the point:

$$\begin{aligned}
P_1 \circ P_2 = ((&-x_1x_2^2 - y_1y_2^2 + nz_1z_2^2)x_1 + (x_1^2x_2 + y_1^2y_2 - nz_1^2z_2)x_2 : \\
&(-x_1x_2^2 - y_1y_2^2 + nz_1z_2^2)y_1 + (x_1^2x_2 + y_1^2y_2 - nz_1^2z_2)y_2 : \\
&(-x_1x_2^2 - y_1y_2^2 + nz_1z_2^2)z_1 + (x_1^2x_2 + y_1^2y_2 - nz_1^2z_2)z_2) \\
= (&- x_1^2x_2^2 - x_1y_1y_2^2 + nx_1z_1z_2^2 + x_1^2x_2^2 + x_2y_1^2y_2 - nx_2z_1^2z_2 : \\
&- x_1x_2^2y_1 - y_1^2y_2^2 + ny_1z_1z_2^2 + x_1^2x_2y_2 + y_1^2y_2^2 - ny_2z_1^2z_2 : \\
&- x_1x_2^2z_1 - y_1y_2^2z_1 + nz_1^2z_2^2 + x_1^2x_2z_2 + y_1^2y_2z_2 - nz_1^2z_2^2) \\
= (&- x_1y_1y_2^2 + nx_1z_1z_2^2 + x_2y_1^2y_2 - nx_2z_1^2z_2 : \\
&- x_1x_2^2y_1 + ny_1z_1z_2^2 + x_1^2x_2y_2 - ny_2z_1^2z_2 : \\
&- x_1x_2^2z_1 - y_1y_2^2z_1 + x_1^2x_2z_2 + y_1^2y_2z_2) \\
= (&y_1y_2(y_1x_2 - y_2x_1) + nz_1z_2(x_1z_2 - x_2z_1) : \\
&x_1x_2(x_1y_2 - x_2y_1) + nz_1z_2(y_1z_2 - y_2z_1) : \\
&x_1x_2(x_1z_2 - x_2z_1) + y_1y_2(y_1z_2 - y_2z_1)).
\end{aligned}$$

Notice that for any point $P = (x : y : z) \in E_n^\circ(K)$, we hence have (recall that $\mathcal{O} = (1 : -1 : 0)$):

$$-P = P \circ \mathcal{O} = (- y(y + x) : -x(x + y) : -z(x + y)) = (y : x : z).$$

From this we have:

$$\begin{aligned}
P_1 \oplus P_2 &= (P_1 \circ P_2) \circ \mathcal{O} \\
&= (x_1x_2(x_1y_2 - x_2y_1) + nz_1z_2(y_1z_2 - y_2z_1) : \\
&\quad y_1y_2(y_1x_2 - y_2x_1) + nz_1z_2(x_1z_2 - x_2z_1) : \\
&\quad x_1x_2(x_1z_2 - x_2z_1) + y_1y_2(y_1z_2 - y_2z_1)).
\end{aligned}$$

Since E_n is given by $F(X, Y, Z) = 0$ for $F(X, Y, Z) = X^3 + Y^3 - nZ^3 \in W_3$, the tangent line through P is given by:

$$\begin{aligned}
\partial_X F(P)(X - x) + \partial_Y F(P)(Y - y) + \partial_Z F(P)(Z - z) &= 0, \\
(3X^2)(P)(X - x) + (3Y^2)(P)(Y - y) + (-3nZ^2)(P)(Z - z) &= 0, \\
3x^2X - 3x^3 + 3y^2Y - 3y^3 &= 3nz^2Z - 3nz^3.
\end{aligned}$$

Since P is on E_n, we have $x^3 + y^3 = nz^3$, so:

$$T_PE_n : x^2X + y^2Y = nz^2Z.$$

Now we want the other intersection point $P \circ P = (a : b : c)$ of T_PE_n with E_n besides P. Therefore we can combine these equations and we get:

$$\begin{aligned}
y^6X^3 + (nz^2Z - x^2X)^3 &= ny^6Z^3 \\
(y^6 - x^6)X^3 + (3nz^2x^4)X^2Z + (-3n^2z^4x^2)XZ^2 + (n^3z^6 - ny^6)Z^3 &= 0.
\end{aligned}$$

Since $(x : z)$ is a double root is this equation and the other intersection point is $(a : c)$, this equation can be rewritten as:

$$\begin{aligned}
(zX - xZ)^2(cX - aZ) &= 0 \\
z^2cX^3 + (-z^2a - 2xzc)X^2Z + (2xza + x^2c)XZ^2 - x^2aZ^3 &= 0.
\end{aligned}$$

This gives us:

$$\begin{aligned}(-z^2a - 2xzc)(y^6 - x^6) &= (z^2c)(3nz^2x^4)\\ (-za - 2xc)z(x^3 + y^3)(y^3 - x^3) &= 3x^4z(x^3 + y^3)c.\end{aligned}$$

If $P \neq \mathcal{O}$, then this gives us:

$$\begin{aligned}(-za - 2xc)(y^3 - x^3) &= 3x^4c\\ z(x^3 - y^3)a &= (2xy^3 - 2x^4 + 3x^4)c = x(x^3 + 2y^3)c.\end{aligned}$$

Thus:

$$(a : c) = (x(x^3 + 2y^3) : z(x^3 - y^3)).$$

Similarly we get:

$$(b : c) = (y(2x^3 + y^3) : z(y^3 - x^3)) = (-y(2x^3 + y^3) : z(x^3 - y^3)).$$

Thus we have:

$$P \circ P = (a : b : c) = (x(x^3 + 2y^3) : -y(2x^3 + y^3) : z(x^3 - y^3)).$$

Hence we have:

$$2P = (-y(2x^3 + y^3) : x(x^3 + 2y^3) : z(x^3 - y^3)).$$

Note that for $P = \mathcal{O}$ we have $2P = \mathcal{O}$ and this also satisfies the formulas. □

Using the explicit formulas we can prove the continuity of $\oplus$ on $E_n(\mathbb{R})$ supplied with the induced topology of $\mathbb{P}^2(\mathbb{R})$.

Corollary 1.7. *The operation $\oplus$ is continuous on $E_n(\mathbb{R})$.*

Proof. We need to show that for all $P \in E_n(\mathbb{R})$ the map $Q \mapsto P \oplus Q$ is continuous. From the explicit group law we have that this map is continuous in Q for all $Q \in E_n(\mathbb{R})$ except for $Q = P$. Thus we need to show that:

$$\lim_{Q \to P} (P \oplus Q) = 2P.$$

This holds true if and only if $\lim_{Q \to P} P \circ Q = P \circ P$. Note that this is true for $P = \mathcal{O}$. So if we can show for all $P \in E_n^\circ(\mathbb{R})$ that $\lim_{Q \to P} l_{PQ} = l_{PP}$, we are done.

Since $P \in E_n^\circ(\mathbb{R})$, we can write $P = (x_P : y_P : 1)$ and for all $Q \in E_n^\circ(\mathbb{R})$ we can write $Q = (x_Q : y_Q : 1)$. Then lines l_{PQ} and $l_{PP} = T_P E_n$ in $\mathbb{P}^2(\mathbb{R})$ are given by:

$$\begin{aligned}&l_{PQ} : (y_P - y_Q)(X - x_P Z) - (x_P - x_Q)(Y - y_P Z) = 0,\\ &l_{PP} : x_P^2(X - x_P Z) + y_P(Y - y_P Z) = 0.\end{aligned}$$

To show that $l_{PQ} \to l_{PP}$ as $Q \to P$, we want to show that

$$\frac{-(x_P - x_Q)x_P^2}{(y_P - y_Q)y_P^2} = \frac{x_P^2 x_Q - x_P^3}{y_P^3 - y_P^2 y_Q} \to 1 \text{ as } Q \to P.$$

Now we write $x_Q = x_P + \delta$ such that $\delta \to 0$ as $Q \to P$. Since $P, Q \in E_n^\circ(\mathbb{R})$, we can write $y_P = \sqrt[3]{n - x_P^3}$

and $y_Q = \sqrt[3]{n - x_Q^3}$. This gives us $x_P^2 x_Q - x_P^3 = \delta x_P^2$ and by Taylor expansion we have:

$$\begin{aligned} y_P^3 - y_P^2 y_Q &= n - x_P^3 - \sqrt[3]{(n - x_P^3)^2(n - (x_P + \delta)^3)} \\ &= n - x_P^3 - \sqrt[3]{(n - x_P^3)^3 - \delta(3x_P^2 + 3\delta x_P + \delta^2)(n - x_P^3)^2} \\ &= n - x_P^3 - \left(\sqrt[3]{(n - x_P^3)^3} - \frac{1}{3}\delta(3x_P^2 + 3\delta x_P + \delta^2)(n - x_P^3)^2 \cdot (n - x_P^3)^{-2} + \mathcal{O}(\delta^2) \right) \\ &= \delta \left(x_P^2 + \delta x_P + \frac{1}{3}\delta^2 \right) + \mathcal{O}(\delta^2) \\ &= \delta x_P^2 + \mathcal{O}(\delta^2). \end{aligned}$$

Hence we have:

$$\lim_{Q \to P} \frac{-(x_P - x_Q)x_P^2}{(y_P - y_Q)y_P^2} = \lim_{\delta \to 0} \frac{\delta x_P^2}{\delta x_P^2 + \mathcal{O}(\delta^2)} = 1.$$

Thus $\oplus$ is a continuous operation on $E_n(\mathbb{R})$ for all $n \in \mathbb{Z}_{\geq 1}$. □

Since the explicit formulas are derived without using the associativity of $\oplus$, we can use the continuity to prove the associativity.

Remark 1.8. If there were some $P = (x : y : z) \in E_n(\mathbb{Q})$ such that $2P = \mathcal{O}$, then we have by Theorem 1.6 that $z = 0$ or $x^3 = y^3$ and hence $x = y$, because $x, y \in \mathbb{Q}$. If $z = 0$ then we have $P = \mathcal{O}$. If $x = y$, then we have $2x^3 = nz^3$. This is not possible if $n \geq 3$ is cube-free. Thus if $n \neq 2$ is cube-free then for all $P \in E_n(\mathbb{Q})$ we have $2P = \mathcal{O}$ if and only if $P = \mathcal{O}$.

Notice that for $n = 2$, $2x^3 = nz^3$ gives us $x = z$ since $x, z \in \mathbb{Q}$. Then we have the point $(1 : 1 : 1) \in E_2(\mathbb{Q})$ with $2(1 : 1 : 1) = \mathcal{O}$.

2 Chapter 2

In this section our goal is to measure the sizes of rational solutions on the curve $E_n^\circ : x^3 + y^3 = n$. Thereafter we look for relations between this size and the group law on $E_n(\mathbb{Q})$. Since we also want to include $\mathcal{O}$, we work in the rational projective plane $\mathbb{P}^2(\mathbb{Q})$. This is based on §5.2 (p. $174 - 184$) from [2].

2.1 The Weil Height

We have a look at the Weil Height on rational projective spaces $\mathbb{P}^m(\mathbb{Q})$ and prove some nice properties.

To define the Weil Height, we need the p-adic absolute values for primes p on $\mathbb{Q}$. Let $x \in \mathbb{Q}^*$ be given, then for any prime p we can write $x = p^{-e_p} \cdot \frac{a}{b}$ with unique $a, b, e_p \in \mathbb{Z}$ and $\gcd(a, b) = \gcd(a, p) = \gcd(b, p) = 1$. Then we put:

$$|x|_p := p^{-e_p}, \qquad |0|_p := 0.$$

One can verify that the p-adic absolute values satisfy the following properties:

$$|xy|_p = |x|_p |y|_p, \qquad |x + y|_p \leq \max\{|x|_p, |y|_p\}.$$

We take $|\cdot|_\infty$ as the usual absolute value on $\mathbb{Q}$. Defining $M_\mathbb{Q}$ as the set of all primes and infinity, we have a set of absolute values $|\cdot|_v$ for $v \in M_\mathbb{Q}$. For more details, one may be referred to §5.2.1 (p. 174-175) from [2].

Proposition 2.1 (Product Formula)**.** *For all $x \in \mathbb{Q}^*$, we have:*

$$\prod_{v \in M_\mathbb{Q}} |x|_v = 1.$$

Proof. Again we can write $x = \pm \prod_{i=1}^k p_i^{e_i}$ with primes p_i and $e_i \in \mathbb{Z}$. Then we have:

$$\prod_{v \in M_\mathbb{Q}} |x|_v = |x|_\infty \cdot \prod_{\text{primes } p} |x|_p = \prod_{i=1}^k p_i^{e_i} \cdot \prod_{i=1}^k p_i^{-e_i} = 1.$$

□

Definition 2.2. For $P = (x_0 : \cdots : x_m) \in \mathbb{P}^m(\mathbb{Q})$, the Weil Height of P is defined to be

$$h(P) := \sum_{v \in M_\mathbb{Q}} \log\left(\max_{i=0}^{n}\{|x_i|_v\}\right).$$

We need to check that the Weil Height is well-defined: that is that the formula above is independent of the choice of the homogeneous coordinates. Let $x \in \mathbb{Q}^*$ be given, then we can write $P = (x_0 : \cdots : x_m) = (xx_0 : \cdots : xx_m)$ and hence we have using Proposition 2.1:

$$h(P) = \sum_{v \in M_\mathbb{Q}} \log\left(\max_{i=0}^{n}\{|x|_v \cdot |x_i|_v\}\right) = \sum_{v \in M_\mathbb{Q}} \log(|x|_v) + \log\left(\max_{i=0}^{n}\{|x_i|_v\}\right) = \sum_{v \in M_\mathbb{Q}} \log\left(\max_{i=0}^{n}\{|x_i|_v\}\right).$$

Remark 2.3. Notice that for any $P \in \mathbb{P}^m(\mathbb{Q})$, we can write $P = (z_0 : \cdots : z_m)$ with coprime integers $z_0, \ldots, z_m$. Then for any prime $p \in M_\mathbb{Q}$ we have:

$$\max_{i=0}^{m}\{|z_i|_p\} = 1.$$

since $|z_i|_p \leq 1$ for all i, and at least one z_i is coprime with p and hence $|z_i|_p = 1$ for this z_i. Therefore we have:

$$h(P) = \log\left(\max_{i=0}^{m}\{|z_i|_\infty\}\right).$$

2.2 The Weil Height and polynomial maps

In this subsection we study the behaviour of the Weil Height with polynomial maps between projective spaces. Therefore these polynomials require a special property.

Definition 2.4. Let $F_0, \ldots, F_m \in W_{d,m}(\mathbb{Q})$ be homogeneous polynomials of degree $d \geq 1$. Then we call this set of m polynomials good if there is an $M \in \mathbb{Z}_{\geq 1}$ and there are polynomials $A_{ij} \in W_{M-d,m}(\mathbb{Q})$ for $0 \leq i, j \leq m$ such that for all $i \in \{0, \ldots, m\}$:

$$\sum_{j=0}^{m} A_{ij} F_j = X_i^M.$$

Theorem 2.5. *Let $F_0, \ldots, F_m \in W_{d,m}(\mathbb{Q})$ be a good set of homogeneous polynomials of degree d in $(X_0, \ldots, X_m)$. Let $Z \subset \mathbb{P}^m(\mathbb{Q})$ be the set of common zeros of $F_0, \ldots, F_m$ and define:*

$$\Phi : \mathbb{P}^m(\mathbb{Q}) \setminus Z \to \mathbb{P}^m(\mathbb{Q}) : \Phi(X_0 : \cdots : X_m) = (F_0(X_0, \ldots, X_m) : \cdots : F_m(X_0, \ldots, X_m)).$$

Then there are constants $C_1 > 0$ and $C_2 > 0$ only depending on Φ such that for all $P \in \mathbb{P}^m(\mathbb{Q}) \setminus Z$ we have:

$$dh(P) - C_2 \overset{(2)}{\leq} h(\Phi(P)) \overset{(1)}{\leq} dh(P) + C_1.$$

In other words, there exists a constant $C = \max\{C_1, C_2\} > 0$ depending only on Φ such that for all $P \in \mathbb{P}^m(\mathbb{Q}) \setminus Z$ we have:

$$|h(\Phi(P)) - dh(P)| \leq C.$$

Remark 2.6. Note that inequality (1) is true for any set of homogeneous polynomials $F_1, \ldots, F_m \in W_{d,m}(\mathbb{Q})$. From the proof it will be clear that we don't use the assumption that they are good.

Proof. (1) Note that $W_{d,m}$ is generated by the monomials:

$$\left\{ \prod_{j=0}^{m} X_j^{n_j} \,\middle|\, \vec{n} \in N_{d,m} \right\} \quad \text{with} \quad N_{d,m} := \left\{ \vec{n} = (n_0, \ldots, n_m) \in \mathbb{N}^{m+1} \,\middle|\, \sum_{j=0}^{m} n_j = d \right\}.$$

Hence, we have for $i = 0, \ldots, m$ and any $\vec{x} = (x_0, \ldots, x_m) \in \mathbb{Q}^{m+1}$

$$F_i(\vec{x}) = \sum_{\vec{n} \in N_{d,m}} \lambda_{i,\vec{n}} \vec{x}^{\vec{n}} \quad \text{with} \quad \lambda_{i,\vec{n}} \in \mathbb{Q} \quad \text{and} \quad \vec{x}^{\vec{n}} := \prod_{j=0}^{m} x_j^{n_j}.$$

This gives us for any prime p:

$$|F_i(\vec{x})|_p = \left| \sum_{\vec{n} \in N_{d,m}} \lambda_{i,\vec{n}} \vec{x}^{\vec{n}} \right|_p \leq \max_{\vec{n} \in N_{d,m}} \left\{ |\lambda_{i,\vec{n}}|_p \prod_{j=0}^{m} |x_j|_p^{n_j} \right\} \leq \max_{\vec{n} \in N_{d,m}} \{|\lambda_{i,\vec{n}}|_p\} \cdot \max_{j=0}^{m} \{|x_j|_p\}^d.$$

Note that $\#N_{d,m} = \dim(W_{d,m}) = \binom{d+m}{d}$. Thus for the usual absolute value we have:

$$\begin{aligned} |F_i(x_0, \ldots, x_m)|_\infty = \left| \sum_{\vec{n} \in N_{d,m}} \lambda_{i,\vec{n}} \vec{x}^{\vec{n}} \right|_\infty &\leq \binom{d+m}{d} \max_{\vec{n} \in N_{d,m}} \left\{ |\lambda_{i,\vec{n}}|_\infty \prod_{j=0}^{m} |x_j|_\infty^{n_j} \right\} \\ &\leq \binom{d+m}{d} \max_{\vec{n} \in N_{d,m}} \{|\lambda_{i,\vec{n}}|_\infty\} \cdot \max_{j=0}^{m} \{|x_j|_\infty\}^d. \end{aligned}$$

Hence we have for all $P = (x_0 : \cdots : x_m) \in \mathbb{P}^m(\mathbb{Q})$:

$$\begin{aligned}
h(\Phi(P)) &= \sum_{v\in M_{\mathbb{Q}}} \log\left(\max_{i=0}^{m}\{|F_i(\vec{x})|_v\}\right) \\
&= \log\left(\max_{i=0}^{m}\{|F_i(\vec{x})|_\infty\}\right) + \sum_{\text{primes } p} \log\left(\max_{i=0}^{m}\{|F_i(\vec{x})|_p\}\right) \\
&\le \log\left(\binom{d+m}{d}\right) + \log\left(\max_{i=0}^{m}\left\{\max_{\vec{n}\in N_{d,m}}\{|\lambda_{i,\vec{n}}|_\infty\}\right\}\right) + d\log\left(\max_{j=0}^{m}\{|x_j|_\infty\}\right) \\
&\quad + \sum_{\text{primes } p}\left\{\log\left(\max_{i=0}^{m}\left\{\max_{\vec{n}\in N_{d,m}}\{|\lambda_{i,\vec{n}}|_p\}\right\}\right) + d\log\left(\max_{j=0}^{m}\{|x_j|_p\}\right)\right\} \\
&\le dh(P) + \log\left(\binom{d+m}{d}\right) + \sum_{v\in M_{\mathbb{Q}}} \log\left(\max_{i=0}^{m}\left\{\max_{\vec{n}\in N_{d,m}}(|\lambda_{i,\vec{n}}|_v)\right\}\right).
\end{aligned}$$

Thus we have for all $P \in \mathbb{P}^m(\mathbb{Q})$:

$$h(\Phi(P)) \le dh(P) + C_1.$$

with

$$C_1 = \log\left(\binom{d+m}{d}\right) + \sum_{v\in M_{\mathbb{Q}}} \log\left(\max_{i=0}^{m}\left\{\max_{\vec{n}\in N_{d,m}}\{|\lambda_{i,\vec{n}}|_v\}\right\}\right).$$

(2) Since $F_0, \ldots, F_m$ is a good set of polynomials, there is an $M \in \mathbb{Z}_{\ge 1}$ and polynomials A_{ik} for $0 \le i, k \le m$ such that for all $i = 0, \ldots, m$:

$$X_i^M = \sum_{k=1}^{m} A_{ik} F_k.$$

Then we have for $P = (x_0 : \cdots : x_m) \in \mathbb{P}^m(\mathbb{Q}) \setminus Z$:

$$x_i^M = \sum_{k=1}^{m} A_{ik}(\vec{x}) P_k(\vec{x}).$$

Note that $A_{ik} \in W_{M-d,m}(\mathbb{Q})$, so we can write:

$$A_{ik}(\vec{x}) = \sum_{\vec{n}\in N_{M-d,m}} a_{ik,\vec{n}}\vec{x}^{\vec{n}} \quad \text{with} \quad a_{ik,\vec{n}} \in \mathbb{Q}$$

and hence

$$\begin{aligned}
|A_{ik}(\vec{x})|_p &\le \max_{\vec{n}\in N_{M-d,m}}\{|a_{ik,\vec{n}}|_p\} \cdot \max_{j=0}^{m}\{|x_j|_p\}^{M-d}, \\
|A_{ik}(\vec{x})|_\infty &\le \binom{M-d+m}{M-d} \max_{\vec{n}\in N_{M-d,m}}\{|a_{ik,\vec{n}}|_\infty\} \cdot \max_{j=0}^{m}\{|x_j|_\infty\}^{M-d}.
\end{aligned}$$

So we have:

$$\begin{aligned}
|x_i|_p^M &\le \max_{k=1}^{m}\{|A_{ik}(\vec{x})|_p\} \max_{k=1}^{m}\{(|F_k(\vec{x})|_p\} \\
&\le \max_{k=1}^{m}\left\{\max_{\vec{n}\in N_{M-d,m}}\{|a_{ik,\vec{n}}|_p\}\right\} \cdot \max_{j=0}^{m}\{|x_j|_p\}^{M-d} \cdot \max_{k=1}^{m}\{|F_k(\vec{x})|_p\}, \\
|x_i|_\infty^M &\le m \max_{k=1}^{m}\{|A_{ik}(\vec{x})|_\infty\} \max_{k=1}^{m}\{|F_k(\vec{x})|_\infty\} \\
&\le m\binom{M-d+m}{M-d} \max_{k=1}^{m}\left\{\max_{\vec{n}\in N_{M-d,m}}\{|a_{ik,\vec{n}}|_\infty\}\right\} \cdot \max_{j=0}^{m}\{|x_j|_\infty\}^{M-d} \cdot \max_{k=1}^{m}\{|F_k(\vec{x})|_\infty\}.
\end{aligned}$$

Hence we have:

$$\begin{aligned}
\max_{i=0}^{m}\{|x_i|_p\}^M &\leq \max_{i=1}^{m}\max_{k=1}^{m}\left\{\max_{\vec{n}\in N_{M-d,m}}\{|a_{ik,\vec{n}}|_p\}\right\}\cdot\max_{j=0}^{m}\{|x_j|_p\}^{M-d}\cdot\max_{k=1}^{m}\{|F_k(\vec{x})|_p\},\\
\max_{i=0}^{m}\{|x_i|_\infty\}^M &\leq m\binom{M-d+m}{M-d}\max_{i=1}^{m}\max_{k=1}^{m}\left\{\max_{\vec{n}\in N_{M-d,m}}\{|a_{ik,\vec{n}}|_\infty\}\right\}\cdot\max_{j=0}^{m}\{|x_j|_\infty\}^{M-d}\cdot\max_{k=1}^{m}\{|F_k(\vec{x})|_\infty\}.
\end{aligned}$$

Thus:

$$\begin{aligned}
\max_{i=0}^{m}\{|x_i|_p\}^d &\leq \max_{i=1}^{m}\max_{k=1}^{m}\left\{\max_{\vec{n}\in N_{M-d,m}}\{|a_{ik,\vec{n}}|_p\}\right\}\cdot\max_{k=1}^{m}\{|F_k(\vec{x})|_p\},\\
\max_{i=0}^{m}\{|x_i|_\infty\}^d &\leq m\binom{M-d+m}{M-d}\max_{i=1}^{m}\max_{k=1}^{m}\left\{\max_{\vec{n}\in N_{M-d,m}}\{|a_{ik,\vec{n}}|_\infty\}\right\}\cdot\max_{k=1}^{m}\{|F_k(\vec{x})|_\infty\}.
\end{aligned}$$

Hence we have:

$$\begin{aligned}
h(\Phi(P)) &= \sum_{v\in M_{\mathbb{Q}}}\log\left(\max_{i=0}^{m}\{|F_i(\vec{x})|_v\}\right)\\
&\geq \sum_{v\in M_{\mathbb{Q}}}\left\{d\log\left(\max_{i=0}^{m}\{|x_i|_v\}\right)-\log\left(\max_{i=1}^{m}\max_{k=1}^{n}\left\{\max_{\vec{n}\in N_{M-d,m}}\{|a_{ik,\vec{n}}|_v\}\right\}\right)\right\}\\
&\quad -\log(m)-\log\left(\binom{M-d+m}{M-d}\right)\\
&\geq dh(P)-\left(\log(m)+\log\left(\binom{M-d+m}{M-d}\right)+\sum_{v\in M_{\mathbb{Q}}}\log\left(\max_{i=1}^{m}\max_{k=1}^{n}\left\{\max_{\vec{n}\in N_{M-d,m}}\{|a_{ik,\vec{n}}|_v\}\right\}\right)\right).
\end{aligned}$$

Thus we have for all $P\in\mathbb{P}^m(\mathbb{Q})\setminus Z$:

$$h(\Phi(P))\geq dh(P)-C_2$$

with

$$C_2=\log(m)+\log\left(\binom{M-d+m}{M-d}\right)+\sum_{v\in M_{\mathbb{Q}}}\log\left(\max_{i=1}^{m}\max_{k=1}^{m}\left\{\max_{\vec{n}\in N_{M-d,m}}\{|a_{ik,\vec{n}}|_v\}\right\}\right).$$

□

Lemma 2.7. *For all $x, y\in\mathbb{Q}$, we have:*

$$|h(1:x+y:xy)-h(x:1)-h(y:1)|\leq\log(2).$$

Proof. First we show that for all $v\in M_{\mathbb{Q}}$, there are constants C_v and D_v such that for all $x, y\in\mathbb{Q}$, we have:

$$C_v\leq\frac{\max\{|1|_v,|x+y|_v,|xy|_v\}}{\max\{|1|_v,|x|_v\}\max\{|1|_v,|y|_v\}}\leq D_v.$$

For any prime p we have:

$$\begin{aligned}
|x+y|_p&\leq\max\{|x|_p,|y|_p\}\leq\max\{|1|_p,|x|_p,|y|_p,|xy|_p\}=\max\{|1|_p,|x|_p\}\max\{|1|_p,|y|_p\},\\
|x+y|_\infty&\leq|x|_\infty+|y|_\infty\leq2\max\{|x|_\infty,|y|_\infty\}\leq2\max\{|1|_\infty,|x|_\infty\}\max\{|1|_\infty,|y|_\infty\}.
\end{aligned}$$

So $D_p=1$ and $D_\infty=2$ are suitable constants.

Let p be a prime, then we can assume $|x|_p\leq|y|_p$ without loss of generality. If $|x|_p\leq|y|_p\leq1$, then we also have $|x+y|_p\leq1$ and $|xy|_p\leq1$. If $|x|_p\leq1\leq|y|_p$, then we have $|xy|_p\leq|y|_p\leq|x+y|_p$. If $1\leq|x|_p\leq|y|_p$, then we have $|y|_p\leq|xy|_p$. So $C_p=1$ is a suitable constant.

Note that $(x-y)^2 \geq 0$, so $x^2+2xy+y^2 \geq 4xy$. Hence $4xy \leq (x+y)^2$ and thus $2\sqrt{|xy|_\infty} \leq |x+y|_\infty$. So $C_\infty = \frac{1}{2}$ is a suitable constant.

By summing over all $v \in M_{\mathbb{Q}}$, we have:

$$|h(1 : x+y : xy) - h(x:1) - h(y:1)| \leq \log(2)$$

for all $x, y \in \mathbb{Q}$. □

Remark 2.8. In the proof above, we have discovered the remarkable result that for any prime p and $x, y \in \mathbb{Q}$, we have:

$$\max\{1, |x+y|_p, |xy|_p\} = \max\{1, |x|_p\} \max\{1, |y|_p\}.$$

2.3 Sizes of solutions

To define the size of a solution of $E_n : X^3+Y^3 = nZ^3$, we could use directly the Weil Height, but to acquire some nice properties, we use the map:

$$\Omega : E_n^\circ(\mathbb{Q}) \to \mathbb{Q} : \Omega(x,y) = \frac{1}{x+y}.$$

This is well-defined, because the only point in $E_n(\mathbb{Q})$ with $x+y=0$ is $\mathcal{O}$.

Definition 2.9. For any solution $P \in E_n(\mathbb{Q})$ of the equation $X^3+Y^3 = nZ^3$, we define its height by:

$$\bar{h}(P) := h(\Omega(P) : 1) \text{ for } P \in E_n^\circ(Q) \text{ and } \bar{h}(\mathcal{O}) := 0$$

with h the Weil Height on $\mathbb{P}^1(\mathbb{Q})$.

We also call $\bar{h}(P)$ the size of a solution $P \in E_n(\mathbb{Q})$. In addition, $h(P)$ is proportional to the number of digits of $P = (z_0 : \cdots : z_m)$ where $z_0, \ldots, z_m$ are coprime integers.

Remark 2.10. Notice that for any $P = (x,y) \in E_n^\circ(\mathbb{Q})$, we have $-P = (y,x)$ and hence $\Omega(-P) = \Omega(P)$. Thus we also have $\bar{h}(-P) = \bar{h}(P)$.

Remark 2.11. For any point $R = (x_R, y_R) \in E_n^\circ(\mathbb{Q})$, we have:

$$n = x_R^3 + y_R^3 = (x_R+y_R)^3 - 3x_Ry_R(x_R+y_R) = \frac{1}{\Omega(R)^3} - x_Ry_R\frac{3}{\Omega(R)}.$$

So:

$$x_Ry_R = \frac{1-n\Omega(R)^3}{3\Omega(R)^2}.$$

By similar calculations we have:

$$x_R^2 + y_R^2 = \frac{1+2n\Omega(R)^3}{3\Omega(R)^2}, \qquad x_R^4 + x_R^4 = \frac{-1+8n\Omega(R)^3+2n^2\Omega(R)^6}{9\Omega(R)^4}.$$

For any $P = (x_P, y_P), Q = (x_Q, y_Q) \in E_n^\circ(\mathbb{Q})$ with $P \oplus Q, P \ominus Q, 2P \neq \mathcal{O}$ we have by Theorem 1.6:

$$P \oplus Q = \left(\frac{x_Px_Q(x_Py_Q - x_Qy_P) + n(y_P - y_Q)}{x_Px_Q(x_P-x_Q) + y_Py_Q(y_P-y_Q)}, \frac{y_Py_Q(y_Px_Q - y_Qx_P) + n(x_P-x_Q)}{x_Px_Q(x_P-x_Q) + y_Py_Q(y_P-y_Q)}\right),$$

$$P \ominus Q = \left(\frac{x_Py_Q(x_Px_Q - y_Qy_P) + n(y_P - x_Q)}{x_Py_Q(x_P-y_Q) + y_Px_Q(y_P-x_Q)}, \frac{y_Px_Q(y_Py_Q - x_Qx_P) + n(x_P-y_Q)}{x_Py_Q(x_P-y_Q) + y_Px_Q(y_P-x_Q)}\right),$$

$$2P = \left(\frac{-y_P(2x_P^3+y_P^3)}{x_P^3-y_P^3}, \frac{x_P(x_P^3+2y_P^3)}{x_P^3-y_P^3}\right).$$

Hence we have:

$$\begin{aligned}
\Omega(P \oplus Q) &= \frac{(x_P x_Q(x_P - x_Q) + y_P y_Q(y_P - y_Q))}{(x_P y_Q - y_P x_Q)(x_P x_Q - y_P y_Q) + n((x_P + y_P) - (x_Q + y_Q))},\\
\Omega(P \ominus Q) &= \frac{(x_P y_Q(x_P - y_Q) + y_P x_Q(y_P - x_Q))}{(x_P y_Q - y_P x_Q)(x_P x_Q - y_P y_Q) + n((x_P + y_P) - (x_Q + y_Q))},\\
\Omega(2P) &= \frac{x_P^3 - y_P^3}{x_P^4 - 2x_P^3 y_P + 2x_P y_P^3 - y_P^4} = \frac{(x_P - y_P)(x_P^2 + x_P y_P + y_P^2)}{(x_P - y_P)(x_P^3 + x_P^2 y_P + x_P y_P^2 + y_P^3) - 2x_P y_P(x_P - y_P)(x_P + y_P)}\\
&= \frac{x_P^2 + x_P y_P + y_P^2}{x_P^3 + x_P^2 y_P + x_P y_P^2 + y_P^3 - 2x_P^2 y_P - 2x_P y_P^2} = \frac{x_P^2 + x_P y_P + y_P^2}{x_P^3 - x_P^2 y_P - x_P y_P^2 + y_P^3}.
\end{aligned}$$

Lemma 2.12. *The height $\bar{h}$ is almost quadratic: there is a constant $C > 0$ such that for all $P \in E_n(\mathbb{Q})$, we have:*

$$\left|\bar{h}(2P) - 4\bar{h}(P)\right| \leq C.$$

Proof. The case that $P = \mathcal{O}$ is trivial. If $n \neq 2$, we have $2P \neq \mathcal{O}$ for $P \in E_n^\circ(\mathbb{Q})$ by Remark 1.8. Recall that for $n = 2$, we have the point $(1 : 1 : 1)$ such that $2(1 : 1 : 1) = \mathcal{O}$, but for all $P \in E_2^\circ(\mathbb{Q}) \setminus \{(1 : 1 : 1)\}$, we have $2P \neq \mathcal{O}$.

By Remark 2.11 we have for all $P = (x_P, y_P) \in E_n^\circ(\mathbb{Q})$ with $2P \neq \mathcal{O}$:

$$\Omega(2P) = \frac{x_P^2 + x_P y_P + y_P^2}{x_P^3 - x_P^2 y_P - x_P y_P^2 + y_P^3} = \frac{n\Omega(P)^4 + 2\Omega(P)}{4n\Omega(P)^3 - 1}.$$

Now we introduce the maps:

$$\begin{array}{rcccrcc}
\phi: & \mathbb{P}^1(\mathbb{Q}) & \to & \mathbb{P}^1(\mathbb{Q}): & \phi(T:U) & = & (4nTU^3 - T^4 : nU^4 + 2T^3U),\\
\psi: & E_n^\circ(\mathbb{Q}) & \to & \mathbb{P}^1(\mathbb{Q}): & \psi(P) & = & (1 : \Omega(P)),\\
\theta: & E_n^\circ(\mathbb{Q}) & \to & E_n^\circ(\mathbb{Q}): & \theta(P) & = & 2P.
\end{array}$$

Notice that we have:

$$\begin{array}{rccccccc}
\phi \circ \psi: & E_n^\circ(\mathbb{Q}) & \to & \mathbb{P}^1(\mathbb{Q}): & P & \mapsto & (1 : \Omega(P)) & \mapsto \quad (4n\Omega(P)^3 - 1 : n\Omega(P)^4 + 2\Omega(P)) = (1 : \Omega(2P)),\\
\psi \circ \theta: & E_n^\circ(\mathbb{Q}) & \to & \mathbb{P}^1(\mathbb{Q}): & P & \mapsto & 2P & \mapsto \quad (1 : \Omega(2P)).
\end{array}$$

So $\phi \circ \psi = \psi \circ \theta$ on $E_n^\circ(\mathbb{Q})$.

Now we want to apply Theorem 2.5 to ϕ. Therefore, we need to show that the polynomials $P_0(T : U) = 4nTU^3 - T^4$ and $P_1(T : U) = nU^4 + 2T^3U$ are good and we need to identify the set Z_ϕ of common zeros of P_0 and P_1 in $\mathbb{P}^1(\mathbb{Q})$.

Suppose $(T : U)$ is a common zero. If $T = 0$, then we also have $U = 0$, so this is not possible. Therefore we have $T \neq 0$ and hence we can assume that $T = 1$. This gives us the following two equations.

$$\begin{cases} 4nU^2 & = & 1 \quad (1)\\ nU^4 + 2U & = & 0 \quad (2) \end{cases}$$

From (2), we can derive that $U = 0$ or $nU^3 = -2$. By (1) we know that $U \neq 0$, so $U^3 = -\frac{2}{n}$ and $U^2 = \frac{1}{4n}$. Hence $U = \frac{-8n}{n} = -8$. However $(-8)^2 = 64 > 1 > \frac{1}{4n}$, since $n \in \mathbb{Z}_{\geq 1}$. So $U \neq -8$ and this gives a contradiction. Thus $Z_\phi = \emptyset$.

We introduce the following polynomials $A_{ij} \in W_{3,2}$:

$$\begin{array}{rclrcl}
A_{00}(T:U) & = & -\frac{1}{9}(4nU^3 + 9T^3), & A_{01}(T:U) & = & \frac{16}{9}nTU^2,\\
A_{10}(T:U) & = & -\frac{4}{9n^2}T^2U, & A_{11}(T:U) & = & \frac{1}{9n^2}(9nU^3 - 2T^3).
\end{array}$$

Then one can check by a direct computation that:

$$A_{00}P_0 + A_{01}P_1 = T^7, \qquad A_{10}P_0 + A_{11}P_1 = U^7.$$

So $P_0, P_1 \in W_{4,2}$ are good.

Therefore we can apply Theorem 2.5 to ϕ. So there is a constant $C > 0$ such that for all $(x : y) \in \mathbb{P}^1(\mathbb{Q})$ we have:

$$|h(\phi(x : y)) - 4h(x : y)| \leq C.$$

Hence we have for all $P \in E_n^\circ(\mathbb{Q})$ with $2P \neq \mathcal{O}$:

$$\begin{aligned}
|\bar{h}(2P) - 4\bar{h}(P)| &= |h(\Omega(2P) : 1) - 4h(\Omega(P) : 1)| \\
&= |h(\psi(2P)) - 4h(\psi(P))| \\
&= |h(\psi(\theta(P))) - 4h(\psi(P))| \\
&= |h(\phi(\psi(P))) - 4h(\psi(P))| \leq C.
\end{aligned}$$

Thus there is a constant $C > 0$ such that for all $P \in E_n(\mathbb{Q})$ we have $\left|\bar{h}(2P) - 4\bar{h}(P)\right| \leq C$. Note that for $n = 2$, we have to take a new constant $c = \max\{C, \bar{h}(1 : 1 : 1)\} = \max\{C, \log(2)\}$. □

Remark 2.13. Note that C depends only on n and therefore we can express C in n. Recall that we have $d = 4$, $m = 1$ and $M = 7$. From Theorem 2.5 we have for the upper bound:

$$\begin{aligned}
C_1 &= \log\left(\binom{d+m}{d}\right) + \sum_{v \in M_{\mathbb{Q}}} \log\left(\max_{i=0}^{m}\left\{\max_{\vec{n} \in N_{d,m}}\{|\lambda_{i,\vec{n}}|_v\}\right\}\right) \\
&= \log(5) + \log(4n) = \log(20n).
\end{aligned}$$

From Theorem 2.5 we have for the lower bound:

$$\begin{aligned}
C_2 &= \log(m) + \log\left(\binom{M-d+m}{M-d}\right) + \sum_{v \in M_{\mathbb{Q}}} \log\left(\max_{i=1}^{m}\max_{k=1}^{m}\left\{\max_{\vec{n} \in N_{M-d,m}}\{|a_{ik,\vec{n}}|_v\}\right\}\right) \\
&= \log(4) + \log\left(\max\left\{|n|_2, \frac{1}{2}\right\}\right) + \log(16n^3) \leq \log(64n^3).
\end{aligned}$$

Note that $\log(20n) \leq \log(64n^3) = 3\log(4n)$. Thus for all $P \in E_n(\mathbb{Q})$ we have:

$$\left|\bar{h}(2P) - 4\bar{h}(P)\right| \leq 3\log(4n).$$

For $n = 2$ we have $3\log(4n) > \log(2)$, thus then this estimation still holds.

Lemma 2.14. *The height $\bar{h}$ almost satisfies the parallelogram law: there is a constant $C > 0$ such that for all $P, Q \in E_n(\mathbb{Q})$, we have:*

$$\left|\bar{h}(P \oplus Q) + \bar{h}(P \ominus Q) - 2\bar{h}(P) - 2\bar{h}(Q)\right| \leq C.$$

Proof. If $P = \mathcal{O}$ or $Q = \mathcal{O}$, then we have $\bar{h}(P \oplus Q) + \bar{h}(P \ominus Q) = 2\bar{h}(P) + 2\bar{h}(Q)$ by Remark 2.10. Moreover, if $P = Q$ or $P = -Q$ we can see the statement is obviously true by Lemma 2.12.

Let $P = (x_P, y_P), Q = (x_Q, y_Q) \in E_n^\circ(\mathbb{Q})$ with $P \oplus Q, P \ominus Q \neq \mathcal{O}$, then we have by Remark 2.11 with $U := \Omega(P) + \Omega(Q)$ and $V := \Omega(P)\Omega(Q)$:

$$\begin{aligned}
\Omega(P \oplus Q) + \Omega(P \ominus Q) &= \frac{12n((x_P^2 + y_P^2)(x_Q + y_Q) - (x_P + y_P)(x_Q^2 + y_Q^2))}{(x_P^2 + y_P^2)(x_Q y_Q) - (x_P y_P)(x_Q^2 + y_Q^2) + n((x_P + y_P) - (x_Q + y_Q))} \\
&= \frac{2n\Omega(P)\Omega(Q)(\Omega(P) + \Omega(Q)) - 1}{n(\Omega(P) - \Omega(Q))^2} = \frac{2nUV - 1}{nU^2 - 4nV}, \\
\Omega(P \oplus Q) \cdot \Omega(P \ominus Q) &= \frac{n\Omega(P)^2\Omega(Q)^2 + (\Omega(P) + \Omega(Q))}{n(\Omega(P) - \Omega(Q))^2} = \frac{nV^2 + U}{nU^2 - 4nV}.
\end{aligned}$$

Now we introduce the maps:

$$\begin{array}{lcccccc}
\Phi : & \mathbb{P}^2(\mathbb{Q}) & \to & \mathbb{P}^2(\mathbb{Q}) : & \Phi(T : U : V) & = & (nU^2 - 4nTV : 2nUV - T^2 : nV^2 + TU), \\
\Psi : & E_n^\circ(\mathbb{Q})^2 & \to & \mathbb{P}^2(\mathbb{Q}) : & \Psi(P, Q) & = & (1 : \Omega(P) + \Omega(Q) : \Omega(P)\Omega(Q)), \\
\Theta : & E_n^\circ(\mathbb{Q})^2 & \to & E_n^\circ(\mathbb{Q})^2 : & \Theta(P, Q) & = & (P \oplus Q, P \ominus Q).
\end{array}$$

Notice that we have:

$$\begin{array}{rcccl} \Phi\circ\Psi: & E_n^\circ(\mathbb{Q})^2 & \to & \mathbb{P}^2(\mathbb{Q}): & (P,Q) & \mapsto & (1:\Omega(P)+\Omega(Q):\Omega(P)\Omega(Q)) \\ & & & & & \mapsto & (1:\Omega(P\oplus Q)+\Omega(P\ominus Q):\Omega(P\oplus Q)\Omega(P\ominus Q)), \\ \Psi\circ\Theta: & E_n^\circ(\mathbb{Q})^2 & \to & \mathbb{P}^2(\mathbb{Q}): & (P,Q) & \mapsto & (P\oplus Q, P\ominus Q) \\ & & & & & \mapsto & (1:\Omega(P\oplus Q)+\Omega(P\ominus Q):\Omega(P\oplus Q)\Omega(P\ominus Q)). \end{array}$$

So $\Psi\circ\Theta = \Phi\circ\Psi$ on $E_n^\circ(\mathbb{Q})^2$.

Now we want to apply Theorem 2.5 to Φ. Therefore, we need to show that the polynomials $P_0(T:U:V) = nU^2 - 4nTV$, $P_1(T:U:V) = 2nUV - T^2$ and $P_2(T:U:V) = nV^2 + TU$ are good and we need to identify the set Z_Φ of common zeros of $P_0, P_1, P_2 \in W_{2,3}$ in $\mathbb{P}^2(\mathbb{Q})$.

Suppose $(T:U:V)$ is a common rational zero. If $T=0$, then we have $nU^2 = 2nUV = nV^2 = 0$ and hence $U=V=0$, so this is not possible. Therefore we have $T\neq 0$ and hence we can assume that $T=1$. This gives us the following three equations.

$$\begin{cases} U^2 & = & 4V & (1) \\ 2nUV & = & 1 & (2) \\ nV^2 & = & -U & (3) \end{cases}$$

Combining (1) and (3) gives us $n^2V^4 = 4V$, so $V(n^2V^3-4)=0$. Thus $V=0$ or $n^2V^3 = 4$. Note that we have $V\neq 0$ by (2), so we have $V^3 = \frac{4}{n^2}$. Thus $V = \frac{1}{n}\sqrt[3]{4n}$. Since V is a rational number and n is a positive cube-free integer, n has to be 2. This gives us $V=1$. From (2) we can derive $U=\frac{1}{4}$, but from (3) we have $U=-2$. Hence we have a contradiction. Thus $Z_\Phi = \emptyset$.

We introduce the polynomials $A_{ij}\in W_{2,3}$:

$$\begin{array}{lcclcclcc} A_{00}(T:U:V) & = & 4nV^2, & A_{01}(T:U:V) & = & -2nUV-9T^2, & A_{02}(T:U:V) & = & 16nTV, \\ A_{10}(T:U:V) & = & \frac{1}{n}(4TU+9U^2), & A_{11}(T:U:V) & = & -16V^2, & A_{12}(T:U:V) & = & 32UV, \\ A_{20}(T:U:V) & = & \frac{T^2}{n^3}, & A_{21}(T:U:V) & = & -\frac{4TV}{n^2}, & A_{22}(T:U:V) & = & \frac{9nV^2-TU}{n^2}. \end{array}$$

Then one can check by direct computation that:

$$A_{00}P_0 + A_{01}P_1 + A_{02}P_2 = 9T^4, \qquad A_{10}P_0 + A_{11}P_1 + A_{12}P_2 = 9U^4, \qquad A_{20}P_0 + A_{21}P_1 + A_{22}P_2 = 9V^4.$$

So $P_0, P_1, P_2 \in W_{2,3}$ are good.

Now we can apply Theorem 2.5 to Φ. So there is a constant $C'>0$ such that for all $(x:y:z)\in\mathbb{P}^2(\mathbb{Q})$ we have:

$$|h(\Phi(x:y:z)) - 2h(x:y:z)| \leq C'.$$

By Lemma 2.7, we also have for all $P,Q\in E_n^\circ(\mathbb{Q})$ with $P\oplus Q, P\ominus Q \neq \mathcal{O}$:

$$\begin{aligned} & |h(\Psi(P,Q)) - h(\Omega(P):1) - h(\Omega(Q):1)| \\ = {} & |h(1:\Omega(P)+\Omega(Q),\Omega(P)\Omega(Q)) - h(\Omega(P):1) - h(\Omega(Q):1)| \leq \log(2). \end{aligned}$$

From this we can derive that for all $P,Q\in E_n^\circ(\mathbb{Q})$ with $P\oplus Q, P\ominus Q\neq\mathcal{O}$ we have:

$$\begin{aligned} & |\bar{h}(P\oplus Q) + \bar{h}(P\ominus Q) - 2\bar{h}(P) - 2\bar{h}(Q)| \\ = {} & |h(\Omega(P\oplus Q):1) + h(\Omega(P\ominus Q):1) - 2h(\Omega(P):1) - 2h(\Omega(Q):1)| \\ \leq {} & |h(\Psi(P\oplus Q, P\ominus Q)) - 2h(\Psi(P,Q))| + 3\log(2) \\ = {} & |h(\Psi(\Theta(P,Q))) - 2h(\Psi(P,Q))| + 3\log(2) \\ = {} & |h(\Phi(\Psi(P,Q))) - 2h(\Psi(P,Q))| + 3\log(2) \\ \leq {} & C' + 3\log(2). \end{aligned}$$

Since the other cases are trivial or treated in the previous Lemma 2.12, there is a constant $C>0$ such that for all $P,Q\in E_n(\mathbb{Q})$, we have

$$\left|\bar{h}(P\oplus Q) + \bar{h}(P\ominus Q) - 2\bar{h}(P) - 2\bar{h}(Q)\right| \leq C.$$

□

2.4 The Néron-Tate Height

In the previous subsection, we constructed the height $\bar{h}$ for solutions $(X : Y : Z) \in \mathbb{P}^2(\mathbb{Q})$ of the equation $E_n : X^3 + Y^3 = nZ^3$ and in Lemma 2.12 and Lemma 2.14 we proved that $\bar{h}$ is almost quadratic and almost satisfies the parallelogram rule. Using this height, we construct the Néron-Tate Height. This new height will be quadratic and satisfy the parallelogram rule.

Lemma 2.15. *Let S be a set, $d > 1$ a constant and $h : S \to \mathbb{R}$ and $f : S \to S$ two maps such that there is some $C > 0$ such that for all $x \in S$ we have $|(h \circ f)(x) - dh(x)| \leq C$. Then for all $x \in S$ the sequence $\left\{d^{-k}h\left(f^k(x)\right)\right\}_{k=0}^{\infty}$ converges and we define $\hat{h}_f(x) := \lim_{k\to\infty} d^{-k}h\left(f^k(x)\right)$ which satisfies for all $x \in S$:*

$$\left|h(x) - \hat{h}_f(x)\right| \leq \frac{C}{d-1}, \qquad \hat{h}_f(f(x)) = d\hat{h}_f(x).$$

Proof. Let $m < k \in \mathbb{Z}_{\geq 0}$. Then we have:

$$\begin{aligned}\left|d^{-m}h\left(f^m(x)\right) - d^{-k}h\left(f^k(x)\right)\right| &\leq \sum_{i=1}^{k-m}\left|d^{-m+1-i}h\left(f^{m+1-i}(x)\right) - d^{-m-i}h\left(f^{m-i}(x)\right)\right| \\ &\leq \sum_{i=1}^{k-m} d^{-m-i}C = \frac{C}{d-1}\left(d^{-m} - d^{-k}\right) \leq \frac{C}{d^m(d-1)},\end{aligned}$$

since $d > 1$ and $m < k$. Therefore, for all $\varepsilon > 0$ there exists an $m \in \mathbb{Z}_{\geq 0}$ such that $\frac{C}{d^m(d-1)} < \varepsilon$. Thus $\left\{d^{-k}h\left(f^k(x)\right)\right\}_{k=0}^{\infty}$ is a Cauchy sequence and hence it converges.

For all $k \in \mathbb{Z}_{\geq 0}$, we have $\left|h(x) - d^{-k}h\left(f^k(x)\right)\right| \leq \frac{C}{d-1}$, so:

$$|\hat{h}_f(x) - h(x)| = \lim_{n\to\infty}\left|h(x) - d^{-k}h\left(f^k(x)\right)\right| \leq \frac{C}{d-1}.$$

Moreover, we also have for all $x \in S$:

$$\hat{h}_f(f(x)) = \lim_{k\to\infty} d^{-k}h\left(f^{k+1}(x)\right) = d\lim_{k\to\infty} d^{-k-1}h\left(f^{k+1}(x)\right) = d\hat{h}_f(x).$$

□

Theorem 2.16. *For all $P \in E_n(\mathbb{Q})$ we define the Néron-Tate Height by:*

$$\hat{h}(P) := \lim_{n\to\infty} \frac{\bar{h}(2^n P)}{4^n} \geq 0.$$

This is well-defined and $\hat{h}$ satisfies the parallelogram rule: for all $P, Q \in E_n(\mathbb{Q})$ we have:

$$\hat{h}(P \oplus Q) + \hat{h}(P \ominus Q) = 2\hat{h}(P) + 2\hat{h}(Q).$$

Moreover, for all $P \in E_n(\mathbb{Q})$ and $m \in \mathbb{Z}_{\geq 1}$, we have $\hat{h}(mP) = m^2\hat{h}(P)$. So $\hat{h}$ is a quadratic form.

Proof. By Lemma 2.12, we can apply Lemma 2.15 to $E_n(\mathbb{Q})$, $d = 4$, the height $\bar{h}$ and the duplication map $P \mapsto 2P$. Therefore, the Néron-Tate Height $\hat{h}$ is well-defined. Since $\bar{h}(P) \geq 0$ for all $P \in E_n(\mathbb{Q})$, we also have $\hat{h}(P) \geq 0$ for all $P \in E_n(\mathbb{Q})$.

From Lemma 2.14, there is some $C > 0$ such that for all $P, Q \in E_n(\mathbb{Q})$ and $k \in \mathbb{Z}_{\geq 0}$ we have:

$$\left|\bar{h}((2^k P) \oplus (2^k Q)) + \bar{h}((2^k P) \ominus (2^k Q)) - 2\bar{h}(2^k P) - 2\bar{h}(2^k Q))\right| \leq C.$$

Dividing by 4^k we have:

$$\lim_{k\to\infty}\left|\frac{\bar{h}(2^k(P \oplus Q))}{4^k} + \frac{\bar{h}(2^k(P \ominus Q))}{4^k} - 2\frac{\bar{h}(2^k P)}{4^k} - 2\frac{\bar{h}(2^k Q))}{4^k}\right| = 0.$$

Thus we have for all $P, Q \in E_n(\mathbb{Q})$:

$$\hat{h}(P \oplus Q) + \hat{h}(P \oplus -Q) = 2\hat{h}(P) + 2\hat{h}(Q).$$

Assuming that $\hat{h}(mP) = m^2\hat{h}(P)$ for any $P \in E_n(\mathbb{Q})$ and $1 \leq m < M$, we have:

$$\hat{h}(MP) = 2\hat{h}((M-1)P) + 2\hat{h}(P) - \hat{h}((M-2)P) = (2(M-1)^2 + 2 - (M-2)^2)\hat{h}(P) = M^2\hat{h}(P).$$

Thus for all $P \in E_n(\mathbb{Q})$ and $m \in \mathbb{Z}_{\geq 1}$, we have $\hat{h}(mP) = m^2\hat{h}(P)$, since $\hat{h}(P) = \hat{h}(P)$. □

Remark 2.17. Notice that Lemma 2.15 gives with Remark 2.13 the following remarkable result. For all $n \geq 3$ and $P \in E_n(\mathbb{Q})$ we have:

$$\left|\bar{h}(P) - \hat{h}(P)\right| \leq \frac{C}{3} \leq \log(4n).$$

3 Chapter 3

In this section, we will investigate how many rational solutions our equation $E_n^\circ : x^3 + y^3 = n$ has: how many elements has $E_n^\circ(\mathbb{Q})$? Since we are interested in the solutions with positive coordinates we also wonder how many elements $E_n^+(\mathbb{Q}) := \{(x, y) \in E_n^\circ(\mathbb{Q}) | x, y > 0\}$ has. Thereafter we will investigate how $E_n(\mathbb{Q})$ is generated.

3.1 The number of solutions

We don't know if $E_n^\circ(\mathbb{Q})$ has any elements at all, but if we assume that it contains at least one point, we can derive some really nice results. The following theorem can be found in §17.9 (p. 287-288) from [3].

Theorem 3.1. *If $E_n^\circ(\mathbb{Q})$ is non-empty for some $n \geq 3$, it has infinitely many elements.*

Proof. Since $E_n^\circ(\mathbb{Q})$ is non-empty, there is some $P = (x_0 : y_0 : z_0) \in E_n^\circ(\mathbb{Q})$ with coprime integers x_0, y_0, z_0 with $z_0 \neq 0$ and $x_0 + y_0 \neq 0$, because $P \neq \mathcal{O}$. Note that x_0, y_0, z_0 are even pairwise coprime since $x_0^3 + y_0^3 = nz_0^3$ and n is cubefree. Furthermore, we also know that $x_0 \neq y_0$ and $x_0, y_0 \neq 0$, since $n \geq 3$ is cubefree. Thus $x_0, y_0, z_0 \neq 0$ and $x_0 \neq \pm y_0$. By Theorem 1.6 we have coprime integers x_1, y_1, z_1 such that:

$$2P = (x_1 : y_1 : z_1) = (-y_0(2x_0^3 + y_0^3) : x_0(x_0^3 + 2y_0^3) : z_0(x_0^3 - y_0^3)).$$

Then we have:

$$Ax_1 = -y_0(2x_0^3 + y_0^3), \tag{1}$$
$$Ay_1 = x_0(x_0^3 + 2y_0^3), \tag{2}$$
$$Az_1 = z_0(x_0^3 - y_0^3), \tag{3}$$

with $A := \gcd(-y_0(2x_0^3 + y_0^3), x_0(x_0^3 + 2y_0^3), z_0(x_0^3 - y_0^3))$. Since $x_1^3 + y_1^3 = nz_1^3$, x_1, y_1, z_1 are even pairwise coprime.

Let $p \in \mathbb{Z}_{>1}$ be a prime divisor of A. If $p | x_0$, then also $p | y_0$ by equation (1), but x_0 and y_0 are coprime, so this is not possible. So $p \nmid x_0$. Similarly $p \nmid y_0$ by equation (2). If $p | z_0$, then we have $p^3 | x_0^3 + y_0^3$ thus $p | x_0^3 + y_0^3$. Since $p \nmid y_0$, we have $p | 2x_0^3 + y_0^3$ by equation (1). So $p | x_0^3$. However, we already showed that $p \nmid x_0$. Thus $p \nmid z_0$. So $p \nmid x_0 y_0 z_0$.

Suppose that $p^n \mid A$, but $p^{n+1} \nmid A$. Then we have: $p^n | 2x_0^3 + y_0^3$ and $p^n | x_0^3 - y_0^3$ by equations (1) and (3). So $p^n | 3x_0^3$. Since $p^n \nmid x_0$, we have $p^n | 3$, so $p = 3$ and $n = 0$ or $n = 1$. Therefore $A = 1$ or $A = 3$.

To show that there are infinitely many solutions, we want to show that $|z_1| > |z_0|$. Then we can create a sequence by duplication with infinitely distinct elements in $E_n^\circ(\mathbb{Q})$.

Since $x_0, y_0 \neq 0$ and $x_0 \neq \pm y_0$:

$$|z_1| = \frac{|z_0|}{A}|x_0^3 - y_0^3| = \frac{|z_0|}{A}|x_0 - y_0||x_0^2 + x_0y_0 + y_0^2| = |z_0|\frac{|x_0 - y_0|}{4A}|(2x_0 + y_0)^2 + 3y_0^2| > |z_0|\frac{|x_0 - y_0|}{A}.$$

If $A = 1$, we have $|z_1| > |z_0|$ since $|x_0 - y_0| \geq 1$. If $A = 3$, we have $3 | x_0^3 - y_0^3$ so $x_0^3 \equiv y_0^3 \mod 3$. This gives us $x_0 \equiv y_0 \mod 3$ by Fermat, so $|x_0 - y_0| \geq 3$. Hence we have $|z_1| > |z_0|$.

Consider the sequence $\{P_i\}_{i=0}^\infty = \{2^i P\}_{i=0}^\infty \subset E_n(\mathbb{Q})$ with $P_i = (x_i : y_i : z_i)$ in pairwise coprime integers. Then does not contain some point twice, since $|z_i| < |z_j|$ for any $i < j$. Therefore, $E_n(\mathbb{Q})$ contains infinitely many elements and thus $E_n^\circ(\mathbb{Q})$ does too. □

Corollary 3.2. *$E_n(\mathbb{Q})$ is torsion-free for $n \geq 3$: for all $P \in E_n^\circ(\mathbb{Q})$ and all $m \in \mathbb{Z}_{\geq 0}$ we have $mP \neq \mathcal{O}$. Moreover, for $P \in E_n^\circ(\mathbb{Q})$ we have $\hat{h}(P) = 0$ if and only if $P = \mathcal{O}$.*

Proof. Let $P \in E_n^\circ(\mathbb{Q})$ be given. Suppose that $kP = \mathcal{O}$ for some $k \in \mathbb{Z}_{\geq 2}$ but $mP \neq \mathcal{O}$ for all $1 \leq m < k$. Let p be a prime dividing k such that $k = p \cdot a$ for some $a \in \mathbb{Z}$. Let $Q = aP$, so $pQ = \mathcal{O}$ and $Q \neq \mathcal{O}$. Then we have $mQ = (m \mod p)Q$ for all $m \in \mathbb{Z}$. Note that $2^p \equiv 2 \mod p$ by Fermat. Hence we have $2^p Q = 2Q$. However the proof of Theorem 3.1 showed us that for any $Q \in E_n^\circ(\mathbb{Q})$ and any $m \in \mathbb{Z}$ we have $2^m Q \neq 2Q$. So we have contradiction. Thus for all $P \in E_n^\circ(\mathbb{Q})$ and all $k \in \mathbb{Z}_{\geq 2}$ we have $kP \neq \mathcal{O}$ and therefore $E_n(\mathbb{Q})$ is torsion-free.

Let $P_0 = (x_0 : y_0 : z_0) \in E_n^\circ(\mathbb{Q})$ with coprime integers x_0, y_0, z_0. Suppose that $\hat{h}(P_0) = 0$. Defining $P_k = (x_k : y_k : z_k) := 2^k P_0$ for $k \in \mathbb{Z}_{\geq 1}$ with coprime integers x_k, y_k, z_k, we have $\hat{h}(P_k) = 0$ for all $k \in \mathbb{Z}_{\geq 1}$ by Theorem 2.16. By Remark 2.17, we know that $\bar{h}(P_k) \leq \log(4n)$ and hence $\log(|z_k|_\infty) \leq \log(4n)$ for all $k \in \mathbb{Z}_{\geq 1}$. From the proof of Theorem 3.1 we have a strictly increasing sequence $0 < |z_0| < |z_1| < |z_2| < \dots$ in integers. This contradicts the fact that $\log(|z_k|_\infty) \leq \log(4n)$ for all $k \in \mathbb{Z}_{\geq 1}$. Thus $\hat{h}(P_0) \neq 0$. □

Remark 3.3. From the proof of Theorem 3.1 we know that for any integer solution $(x : y : 1) \in E_n(\mathbb{Q})$ with $n \geq 3$ there is no point $P \in E_n(\mathbb{Q})$ such that $2P = (x : y : 1)$.

Theorem 3.4. *If $E_n^\circ(\mathbb{Q})$ has infinitely many elements, then $E_n^+(\mathbb{Q})$ has also infinitely many elements.*

Proof. Assume that $E_n^+(\mathbb{Q})$ has only a finite number of elements. We consider for any field $K \subset \mathbb{R}$ over $\mathbb{Q}$ the set $F_n(K) := \{(x, y) \in E_n^\circ(K) | x < 0\}$. By the symmetry of $E_n^\circ(\mathbb{Q})$ in $x = y$, $F_n(\mathbb{Q})$ has infinitely many elements.

We define the duplication map on $F_n(\mathbb{R})$ by $\psi_n : F_n(\mathbb{R}) \to E_n^\circ(\mathbb{R}) : P \mapsto 2P$. Note that ψ_n is continuous. Let $P = (x, y) \in F_n(\mathbb{R})$. Then we have $\psi_n(P) = 2P = (-y\frac{2x^3+y^3}{x^3-y^3}, x\frac{x^3+2y^3}{x^3-y^3})$ from Theorem 1.6. Note that $x + y > 0$, so $x^3 + 2y^3 > y^3 > 0$, thus $x(x^3 + 2y^3) < 0$. Moreover, $x^3 - y^3 < 0$, so $x\frac{x^3+2y^3}{x^3-y^3} > 0$. Therefore, for all $P = (x, y) \in F_n(\mathbb{R})$, we have $\psi_n(P) = (x', y')$ with $y' > 0$.

Let $P = (x_P, y_P), Q = (x_Q, y_Q) \in F_n(\mathbb{R})$ be given with $x_Q \leq x_P < 0$ and suppose that $\psi_n(P) = \psi_n(Q)$ but $P \neq Q$. Consider the tangent lines $T_P E_n^\circ : y = a_P x + b_P$ and $T_Q E_n^\circ : y = a_Q x + b_Q$. Note that $F_n(\mathbb{R})$ is convex, so $a_Q \leq a_P$. On the other hand, we know that the tangent lines $T_P E_n^\circ$ and $T_Q E_n^\circ$ intersect in a point $(x, y) \in E_n^\circ(\mathbb{R})$. Note that $x > 0$ and $y < y_P \leq y_Q$. Since $F_n(\mathbb{R})$ is convex, we have $a_P \leq a_Q$. Therefore $a_P = a_Q$ and hence $P = Q$. This gives us a contradiction. Thus ψ_n is injective.

By the convexity of $F_n(\mathbb{R})$, we know that for any $P = (x_P, y_P), Q = (x_Q, y_Q) \in F_n(\mathbb{R})$ with $x_Q < x_P$ we have $\psi_n(P) = (x'_P, y'_P)$ and $\psi_n(Q) = (x'_P, y'_P)$ with $x'_Q < x'_P$.

Consider $S_0 = (0, \sqrt[3]{n}) \in E_n^\circ(\mathbb{R})$ and $S_1 = (x_1, y_1) \in F_n(\mathbb{R})$ such that $\psi_n(S_1) = S_0$. Note that S_1 is well-defined since ψ_n is injective. Now we consider $F_n^0(K) := \{(x, y) \in E_n^\circ(K) | x_1 < x \leq 0\}$.

We want to show that $F_n^0(\mathbb{Q})$ cannot be the empty set. Therefore we construct the sequence $\{S_i\}_{i=0}^\infty \subset F_n(\mathbb{R})$ with $S_i = (x_i, y_i)$ such that for all $i \in \mathbb{Z}_{\geq 1}$ we have $\psi_n(S_i) = 2S_i = S_{i-1}$. Hence $x_i > x_j$ for $i < j$, so the sequence is monotone and therefore $\{x_i\}_{i=0}^\infty$ converges in $\mathbb{R} \cup \{\pm\infty\}$. Let S_∞ be the convergence point. Then we have $2S_\infty = S_\infty$. Thus $S_\infty = \mathcal{O}$.

Defining $F_n^i(K) := \{(x, y) \in E_n^\circ(K) | x_{i+1} < x \leq x_i\}$, we have $F_n(K) = \bigcup_{i=0}^\infty F_n^i(K)$. Moreover we have that for any $P = (x, y) \in F_n^i(K)$ with $2P = (x', y')$ that $x_i < x' < x_{i-1}$. So we have $\psi_n(F_n^i(K)) \subset F_n^{i-1}(K)$ for all $i \geq 1$. Suppose that $F_n^0(\mathbb{Q}) = \emptyset$. Then we have $F_n^i(\mathbb{Q}) = \emptyset$ for all $i \geq 0$. Hence $F_n(\mathbb{Q}) = \emptyset$. However, $F_n(\mathbb{Q})$ contains infinitely many elements, so this gives contradiction. Thus $F_n^0(\mathbb{Q}) \neq \emptyset$.

Suppose that $F_n^0(\mathbb{Q})$ contains infinitely many elements. Note that $\psi_n(F_n^0(\mathbb{Q})) \subset E_n^+(\mathbb{Q})$. Thus $E_n^+(\mathbb{Q})$ contains infinitely many elements, since ψ_n is injective. This is contradiction with our assumption.

Thus $F_n^0(\mathbb{Q})$ contains only finitely many elements. Then there is a point $T = (x_T, y_T) \in F_n^0(\mathbb{Q})$ such that for all $(x, y) \in F_n(\mathbb{Q})$ we have $x \leq x_T < 0$. Since $T \in F_n^0(\mathbb{Q})$, we have $T \oplus T = 2T \in E_n^+(\mathbb{Q})$.

Consider the map $\phi_n : F_n(K) \to E_n^\circ(K) : P \mapsto P \oplus T$. Suppose that there are $P \neq Q \in F_n(\mathbb{R})$ such that $\phi_n(P) = \phi_n(Q)$. Then $P \oplus T = Q \oplus T$, so $P \circ T = Q \circ T$ and thus P, Q, T and $P \circ T$ are collinear. Therefore $P = Q$. Thus ϕ_n is injective.

By the convexity of $F_n(\mathbb{R})$, we know that for any $P = (x_P, y_P), Q = (x_Q, y_Q) \in F_n(\mathbb{R})$ with $x_Q < x_P$ we have the lines $L_{PT} : y = a_P x + b_P$ and $L_{QT} : y = a_Q x + b_Q$ through respectively P and T and Q and T with $a_Q < a_P$. Therefore, we have $\phi_n(P) = (x'_P, y'_P)$ and $\phi_n(Q) = (x'_Q, y'_Q)$ with $x'_Q < x'_P$ and $y'_Q > y'_P$. Thus for any $P = (x, y) \in F_n(\mathbb{Q})$, we have $\phi_n(P) = (x', y')$ with $y' > 0$ and $x' > x_T$. So $x' > 0$. Hence $\phi_n(P) \in E_n^+(\mathbb{Q})$. Thus $E_n^+(\mathbb{Q})$ contains infinitely many elements. This is in contradiction with our assumption. Thus $E_n^+(\mathbb{Q})$ contains infinitely many solutions. □

Remark 3.5. In fact we can prove a much stronger statement if $E_n^\circ(\mathbb{Q})$ is not empty for some $n \geq 3$. Then $E_n(\mathbb{Q})$ with the topology induced from $\mathbb{P}^2(\mathbb{R})$ is dense in $E_n(\mathbb{R})$ as a topological space. To prove this we need some more advanced tools.

First we note that $E_n(\mathbb{R})$ is a 1-dimensional Lie group: a smooth real 1-dimensional manifold where the map $\oplus : E_n(\mathbb{R}) \times E_n(\mathbb{R}) \to E_n(\mathbb{R})$ and the inversion map $E_n(\mathbb{R}) \to E_n(\mathbb{R}) : P \mapsto -P$ are smooth. Moreover, $E_n(\mathbb{R})$ is also connected, abelian and compact, since $\mathbb{P}^2(\mathbb{R})$ is compact. Then we can apply the following theorem.

Theorem 3.6. *A Lie group G which is compact, connected, abelian and of dimension 1 is isomorphic to $\mathbb{S}^1$.*

This is a well-known classification theorem, but for more details one may be referred to chapter 5 from [4]. Note that $\mathbb{S}^1$ is a compact, connected, abelian Lie group of dimension 1. In this theorem G and $\mathbb{S}^1$ are isomorphic as Lie groups. That holds that there is a diffeomorphism $\phi : G \to \mathbb{S}^1$: a smooth group isomorphism such that ϕ^{-1} is smooth too.

So $E_n(\mathbb{R})$ is isomorphic to the unit circle $\mathbb{S}^1$. By Theorem 3.1 we hence know that the subgroup $E_n(\mathbb{Q}) \subset E_n(\mathbb{R})$ is isomorphic to an infinite subgroup $S \subset \mathbb{S}^1$. Note that a subgroup of $\mathbb{S}^1$ is either the group μ_k of k-th roots of unity or dense in $\mathbb{S}^1$. Since $\#\mu_k < \infty$, S is dense in $\mathbb{S}^1$. Therefore, $E_n(\mathbb{Q})$ is also dense in $E_n(\mathbb{R})$.

3.2 Generators of $E_n(\mathbb{Q})$

Now we will look how $E_n(\mathbb{Q})$ is generated. We can prove the following theorem:

Theorem 3.7 (Mordell-Weil Theorem)**.** *The group $E_n(\mathbb{Q})$ is finitely generated.*

We will prove this except for the Weak Mordell-Weil Theorem, which we will assume in the proof. In this proof we will use both the group structure of $\oplus$ and the Néron-Tate Height $\hat{h}$ defined in Theorem 2.16.

Theorem 3.8 (Weak Mordell-Weil Theorem)**.** *The quotient $E_n(\mathbb{Q})/2E_n(\mathbb{Q})$ is a finite group.*

The Weak Mordell-Weil Theorem will not be proved here, but the proof can be found in §VIII.1 (p. $208-214$) from [5]. Before we can prove the Mordell-Weil Theorem, we need to prove a lemma about the sets $H(c) = \left\{P \in E_n(\mathbb{Q}) \middle| \hat{h}(P) < c\right\}$ for $c \in \mathbb{R}$.

Lemma 3.9. *For all $c \in \mathbb{R}$, $H(c)$ is finite.*

Proof. Note that $H(c) = \emptyset$ for $c < 0$ and $H(0) = \{\mathcal{O}\}$, because $E_n(\mathbb{Q})$ is torsion-free by Corollary 3.2 and $\hat{h}$ is quadratic by Theorem 2.16.

By Remark 2.17 we know that for all $c \in \mathbb{R}$ we have

$$H(c) = \left\{P \in E_n(\mathbb{Q}) \middle| \hat{h}(P) < c\right\} \subset \left\{P \in E_n(\mathbb{Q}) \middle| \bar{h}(P) < c + \log(4n)\right\}.$$

So $H(c)$ is finite for all $c \in \mathbb{R}_{>0}$ if $H'(c) := \left\{P \in E_n(\mathbb{Q}) \middle| \bar{h}(P) < c\right\}$ is finite for all $c \in \mathbb{R}_{>0}$.

Notice that $\bar{h}(\mathcal{O}) = 0$, so $\mathcal{O} \in H'(c)$ for all $c \in \mathbb{R}_{>0}$. Recall from Definition 2.9 that for all $P = (x, y) \in E_n^\circ(\mathbb{Q})$ we have $\bar{h}(P) := h(\Omega(P) : 1) = h(1 : x + y)$. Consider for all $u \in \mathbb{R}$ the sets

$$l_u := \{(x, y) \in \mathbb{Q}^2 | \Omega(x, y) = x + y = u\} \subset \{(x : y : z) \in \mathbb{P}^2(\mathbb{Q}) | x + y = uz\} =: L_u.$$

Then we have:

$$O(u) := \{P \in E_n^\circ(\mathbb{Q}) | \Omega(P) = u\} = E_n^\circ(\mathbb{Q}) \cap l_u \subset E_n(\mathbb{Q}) \cap L_u.$$

Since $E_n(\mathbb{Q})$ is a cubic and L_u is a line and $L_u \not\subset E_n(\mathbb{Q})$, because $E_n(\mathbb{Q})$ is an irreducible cubic, this intersection can contain at most 3 distinct elements. Therefore we have $\#O(u) < \infty$ for all $u \in \mathbb{Q}$. Note that for $u \in \mathbb{R} \setminus \mathbb{Q}$ we have $O(u) = \emptyset$.

Now we need to show that $\{P \in \mathbb{P}^1(\mathbb{Q}) | h(P) < c\}$ is finite for all $c \in \mathbb{R}_{>0}$. From Remark 2.3, we can write any $P \in \mathbb{P}^1(\mathbb{Q})$ as $P = (x : y)$ with x, y coprime integers. Moreover, we have $h(P) = \log(\max(|x|_\infty, |y|_\infty))$. So if $h(P) < c$, this gives us $\max(|x|_\infty, |y|_\infty) < e^c$ and hence $-e^c < x, y < e^c$. Hence $\#\{P \in \mathbb{P}^1(\mathbb{Q}) | h(P) < c\} \leq (2e^c + 1)^2 < \infty$.

Therefore $\#H'(c) < \infty$ for all $c \in \mathbb{R}_{>0}$. Thus $H(c)$ is finite for all $c \in \mathbb{R}$. □

Proof. (Theorem 3.8 implies Theorem 3.7) We define for all $P \in E_n(\mathbb{Q})$ the euclidean norm $|P| := \sqrt{\hat{h}(P)}$ and we have inner product $\langle P, Q\rangle := \frac{1}{2}(\hat{h}(P \oplus Q) - \hat{h}(P) - \hat{h}(Q))$ since $\hat{h}$ is a quadratic form by Theorem 2.16. Then the Cauchy-Schwarz Inequality $|\langle P, Q\rangle| \le \sqrt{\langle P, P\rangle\langle Q, Q\rangle}$ gives us $|\hat{h}(P \oplus Q) - \hat{h}(P) - \hat{h}(Q)| \le 2\sqrt{\hat{h}(P)\hat{h}(Q)}$. Hence we have $|P \oplus Q| \le |P| + |Q|$ for all $P, Q \in E_n(\mathbb{Q})$. We also have $|mP| = m|P|$ for all $P \in E_n(\mathbb{Q})$ and $m \in \mathbb{Z}_{\ge 1}$.

Since we assume the Weak Mordell-Weil Theorem 3.8, we have a finite set $S \subset E_n(\mathbb{Q})$ of representations of $E_n(\mathbb{Q})$ modulo $2E_n(\mathbb{Q})$. Then we take $C := \max_{P \in S} \hat{h}(P)$ and consider $H(C)$.

Let $P_0 \in E_n(\mathbb{Q})$ be such that $P_0 \notin H(C)$. Then we can write $P_0 = Q_1 \oplus 2P_1$ for some $Q_0 \in S$ and $P_1 \in E_n(\mathbb{Q}) \setminus S$. Iterating this process gives a sequence $\{P_k\}$ and $Q_k \in S$ with $P_k = Q_{k+1} \oplus 2P_{k+1}$. Notice that for any $k \in \mathbb{Z}_{\ge 1}$ we have:

$$|P_k| = \frac{|P_{k-1} - Q_k|}{2} \le \frac{|P_{k-1}| + |Q_k|}{2} \le \frac{|P_{k-1}| + \sqrt{C}}{2} < |P_{k-1}|.$$

Furthermore, $P_k \in H(\hat{h}(P))$. Since $H(\hat{h}(P))$ is finite by Lemma 3.9, there is some $m \in \mathbb{Z}_{\ge 1}$ such that $P_m \in H(C)$. Therefore we have $P_0 = \bigoplus_{k=1}^{m} Q_k \oplus 2^m P_m$. Hence $H(C)$ generates $E_n(\mathbb{Q})$. Thus $E_n(\mathbb{Q})$ is finitely generated since $H(C)$ is finite by Lemma 3.9. □

3.3 Applying the theory to the problem

Now we apply the acquired knowledge to the original problem. From the Mordell-Weil Theorem 3.7 we know that $E_n(\mathbb{Q})$ is finitely generated. So if we are looking for the solution $(x, y) \in E_n^\circ(\mathbb{Q})$ with the smallest height $\hat{h}$, this has to be a generator because $\hat{h}$ is quadratic by Theorem 2.16. However we also require that this solution has positive coordinates: i.e. $(x, y) \in E_n^+(\mathbb{Q})$. Then we look for a multiple of a generator in $E_n^+(\mathbb{Q})$. Although this may seem easy, the number of generators is still unknown.

In Example 1, we have $n = 17$. By trial-and-error, we can find the point $P = (18 : -1 : 7) \in E_{17}(\mathbb{Q})$, which is the element in $E_{17}(\mathbb{Q})$ with the smallest positive z-coordinate. Therefore it has to be a generator. Then we have $2P = (11663 : 104940 : 40831) \in E_{17}^+(\mathbb{Q})$. This gives us the same solution as Dudeney:

$$Q_{17} := \left(\frac{11663}{40831}, \frac{104940}{40831}\right).$$

In Example 2 we have $n = 9$ and the initial solutions $(2, 1)$ and $(1, 2)$ or in homogeneous coordinates $(2 : 1 : 1)$ and $(1 : 2 : 1)$. Therefore, one of them has to be a generator of $E_9(\mathbb{Q})$ by Remark 3.3. To find another solution in $E_n^+(\mathbb{Q})$, we list the multiples of $P = (2 : 1 : 1)$.

$$\begin{array}{rcl@{\qquad}rcl}
P &=& (2:1:1) & 4P &=& (-36520 : 188479 : 90391) \\
2P &=& (-17:20:7) & 5P &=& (169748279 : -152542262 : 53023559) \\
3P &=& (919:-271:438) & 6P &=& (415280564497 : 676702467503 : 348671682660)
\end{array}$$

This gives us the same solution as Dudeney:

$$Q_9 := \left(\frac{415280564497}{348671682660}, \frac{676702467503}{348671682660}\right).$$

Notice that we can verify that some solution $Q_n \in E_n^+(\mathbb{Q})$ has the smallest Néron-Tate Height (except for some initial solutions) by checking that

$$\{P \in E_n^+(\mathbb{Q}) | \hat{h}(P) < \hat{h}(Q_n)\} \subset \{P \in E_n^+(\mathbb{Q}) | \bar{h}(P) < \bar{h}(Q_n) + 2\log(4n)\}$$

are empty or contained in the set of initial solutions.

In fact, $n = 9$ and $n = 17$ are both cases where $E_n(\mathbb{Q})$ is generated by one element. However, there are also a lot of cases where $E_n(\mathbb{Q})$ is the trivial group $\{\mathcal{O}\}$, for example $n = 3$, $n = 4$ and $n = 5$. The cases where $E_n(\mathbb{Q})$ is generated by two or more elements are rarer. For example $E_{19}(\mathbb{Q})$ has generators $(3 : -2 : 1)$ and $(5 : 3 : 2)$.

References

[1] Dudeney, H.E. (1907). *The Canterbury Puzzles And Other Curious Puzzles.* Thomas Nelson Ans Sons, London, Edinburgh and New York

[2] Hindry, M. (2008). *Arithmetics.* Calvage et Mounet, France.

[3] Ireland, K., Rosen, M. (1990). *A Classical Introduction to Modern Number Theory.* Springer-Verlag New York, Inc.

[4] Sepanski, M.R. (2007). *Compact Lie Groups.* Springer Science+Business Media, New York.

[5] Silverman, J.H. (1986). *The Arithmetic of Elliptic Curves.* Springer Science+Business Media, New York.