The Prouhet-Tarry-Escott problem

by

Timothy Caley

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Pure Mathematics

Waterloo, Ontario, Canada, 2012

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Given natural numbers n and k, with $n > k$, the Prouhet-Tarry-Escott (PTE) problem asks for distinct subsets of $\mathbb{Z}$, say $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$, such that

$$x_1^i + \cdots + x_n^i = y_1^i + \cdots + y_n^i$$

for $i = 1, \ldots, k$. Many partial solutions to this problem were found in the late 19th century and early 20th century.

When $k = n - 1$, we call a solution $X =_{n-1} Y$ *ideal*. This is considered to be the most interesting case. Ideal solutions have been found using elementary methods, elliptic curves, and computational techniques.

This thesis focuses on the ideal case. We extend the framework of the problem to number fields, and prove generalizations of results from the literature. This information is used along with computational techniques to find ideal solutions to the PTE problem in the Gaussian integers.

We also extend a computation from the literature and find new lower bounds for the constant C_n associated to ideal PTE solutions. Further, we present a new algorithm that determines whether an ideal PTE solution with a particular constant exists. This algorithm improves the upper bounds for C_n and in fact, completely determines the value of C_6.

We also examine the connection between elliptic curves and ideal PTE solutions. We use quadratic twists of curves that appear in the literature to find ideal PTE solutions over number fields.

Acknowledgements

Many thanks to my supervisor Kevin G. Hare under whose guidance this thesis was written. His patience, kindness and support throughout this process was essential, and I deeply appreciate it.

As well as reading this thesis, Cameron L. Stewart also provided many helpful ideas for Chapter 4 and 5, for which, along with his encouragement, I am grateful.

I also wish to thank the other readers of this thesis, Yu-Ru Liu, Jeffrey Shallit and Michael Filaseta.

Thank you also to my mathematical "uncle", Michael Coons, for numerous conversations and especially for his advice with the preparation of [7], much of which is included in this thesis.

Further, I acknowledge the following people I have not met, but who assisted with the research in this thesis:

- Adam Hartfiel for his technical support for my work on Gamay.
- The technical support team from Sharcnet.

More generally, I wish to thank the Department of Pure Mathematics at the University of Waterloo. The time I have spent here has been a wonderful experience. The staff members of the department, Lis, Shonn, Nancy and Pavlina, deserve special recognition for their kindness and willingness to help.

To Chris Ramsey, with whom I have shared an office for the last five years – it has been a blast.

I have made many wonderful friends during my time at Waterloo, and I cherish the experiences we have had together.

Dedication

I dedicate this thesis to my parents, Rodney and Margaret Caley for their continuous love and support.

Table of Contents

List of Tables

Chapter 1

Introduction

The Prouhet-Tarry-Escott problem, or PTE problem for short, is a classical number-theoretic problem: given natural numbers n and k, with $k < n$, find two distinct subsets of $\mathbb{Z}$, say $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$, such that

$$\sum_{i=1}^{n} x_i^j = \sum_{i=1}^{n} y_i^j \quad \text{for } j = 1, 2, \ldots, k. \tag{1.1}$$

A solution is written $X =_k Y$, where n is its *size* and k is its *degree*. The maximal nontrivial case of the PTE problem occurs when $k = n - 1$. A solution in this case, say $X =_{n-1} Y$, is called *ideal*.

For example, $\{0, 3, 5, 11, 13, 16\} =_5 \{1, 1, 8, 8, 15, 15\}$ is an ideal PTE solution of size 6 and degree 5 since

$$\begin{aligned}
0 + 3 + 5 + 11 + 13 + 16 &= 48 = 1 + 1 + 8 + 8 + 15 + 15 \\
0^2 + 3^2 + 5^2 + 11^2 + 13^2 + 16^2 &= 580 = 1^2 + 1^2 + 8^2 + 8^2 + 15^2 + 15^2 \\
0^3 + 3^3 + 5^3 + 11^3 + 13^3 + 16^3 &= 7776 = 1^3 + 1^3 + 8^3 + 8^3 + 15^3 + 15^3 \\
0^4 + 3^4 + 5^4 + 11^4 + 13^4 + 16^4 &= 109444 = 1^4 + 1^4 + 8^4 + 8^4 + 15^4 + 15^4 \\
0^5 + 3^5 + 5^5 + 11^5 + 13^5 + 16^5 &= 1584288 = 1^5 + 1^5 + 8^5 + 8^5 + 15^5 + 15^5.
\end{aligned}$$

Similarly, for $a, b, c, d \in \mathbb{Z}$,

$$\{a + b + d, a + c + d, b + c + d, d\} =_2 \{a + d, b + d, c + d, a + b + c + d\},$$

is a family of PTE solutions of size 4 and degree 2 due to Goldbach. In fact, this example was also found by Euler for the case when $d = 0$. Many other elementary solutions can be found in [17] and an early history of the problem may be found in [18].

The PTE problem is interesting because it is an old problem with both algebraic and analytic aspects. It and also has many connections to other problems. Ideal solutions are especially interesting because of their connection to problems in theoretical computer science [2], combinatorics [21], a conjecture of Erdős and Szekeres [13,24], [3, Chapter 13], and as well to the "Easier" Waring problem, which we discuss below.

Given an integer k, the "Easier" Waring problem asks for the smallest n, denoted $v(k)$, such that for all integers m, there exist integers $x_1, \ldots, x_n$ such that

$$\pm x_1^k \pm \cdots \pm x_n^k = m,$$

for any choices of signs. This problem was posed by E. M. Wright as a weakening of the usual Waring problem, which allows only addition. Note that $v(k)$ is conjectured to be $O(k)$ [3, Chapter 12]. For arbitrary k, the best known bound is $v(k) \ll k \log(k)$ [3, Chapter 12], which is derived from the usual Waring problem. For small values of k, the best bounds for $v(k)$ are derived from ideal solutions of the PTE problem. In fact, these are much better than those which are derived from the usual Waring problem. See again [3, Chapter 12] for a full explanation of the connection between the two problems.

In 1935, Wright [39] conjectured that ideal solutions to the PTE problem should exist for all n. However, it does not appear that this conjecture is close to being resolved. For $n = 2, 3, 4, 5$, complete parametric ideal solutions are known. For $n = 6, 7, 8$, only incomplete parametric solutions are known. See [3, Chapter 11] and [4, 9, 10] for further details of these cases. For $n = 10$, infinite inequivalent families of solutions are known (albeit incomplete) [32].

For size 9, only two inequivalent solutions are known. These were found computationally by P. Borwein, Lisoněk and Percival [5]. Until 2008, there were also only two inequivalent solutions known for size $n = 12$. They were both found computationally, by Kuosa, Myrignac and Shuwen [29] and Broadhurst [6]. However, in 2008, Choudhry and Wróblewski [12] found some infinite inequivalent families of solutions for $n = 12$ (again incomplete). Both infinite families of solutions for sizes 10 and 12 arise from rational points on elliptic curves using a method of Letac from 1934, which appears in [20].

For $n = 11$ and $n \geq 13$, no ideal solutions are known.

Analytic methods are no closer to resolving Wright's conjecture. Along the same lines as the "Easier" Waring problem, define $N(k)$ to be the least n such that the PTE problem of degree k has a solution of size n. Much work has been done on obtaining upper bounds for $N(k)$, for example, see [22, 25, 39] and [3, Chapter 12]. The best upper bound is due to Melzak, which is $N(k) \leq \frac{1}{2}(k^2 - 3)$ when k is odd, and $N(k) \leq \frac{1}{2}(k^2 - 4)$ when k is even. Meanwhile, there is no lower bound on $N(k)$ that would rule out ideal solutions.

Although the PTE problem is traditionally looked at over $\mathbb{Z}$, it may be viewed over any ring. Alpers and Tijdeman [1] were the first to consider the PTE problem over a ring other than the integers. Their article discusses the PTE problem over the ring $\mathbb{Z} \times \mathbb{Z}$ and shows that ideal solutions of size n in this case come from a particular kind of convex $2n$-gons. Their article also gives an example of a solution to the PTE problem over the Gaussian integers, $\mathbb{Z}[i]$. It further notes that there does not appear to be any other mention in the literature of the PTE problem in this setting. Subsequently, Prugsapitak examined the degree 2 case of the problem over number fields in [26]. In [11], Choudhry examines the PTE problem over the ring of 2×2 integer matrices, $M_2(\mathbb{Z})$, and Černý [37] has extended Prouhet's solution to complex matrices.

In Chapter 2, we introduce some background results concerning the PTE problem, stating them over a ring of integers of a number field when possible. These are standard results from the literature and will be used in later chapters of this thesis. In many cases, their proofs appear in Appendix A.

In Chapter 3, we consider the case of PTE solutions in $\mathbb{Z}[i]$, and describe a generalization of the computational search done by Borwein, Lisoněk and Percival mentioned above. Much of the material in Chapters 2 and 3 first appeared in the author's article [7].

There is a fundamental constant C_n associated to ideal PTE solutions of size n. Investigating the divisibility properties of C_n is important.

In Chapter 4, we explain how divisibility result for C_n in the literature may be obtained through computation. We extend these computations further and present the new results. Additionally, we explain how the data yields new information about the problem.

In Chapter 5, we describe a new algorithm that given positive integers n and C, determines whether or not an ideal $\mathbb{Z}$-PTE solution of size n with constant C exists. Since we must have $C_n \mid C$, we use the divisilbity results of the previous chapter to optimize the search.

In Chapter 6, we further build upon the work of Letac, Smyth and Choudhry and Wróblewski and connect the PTE problem to finding rational points on elliptic curves.

Chapter 2

Background

2.1 Background

Solutions to the $\mathbb{Z}$-PTE problem satisfy many relations. Most of them generalize to a ring of integers of a number field, which we will denote by $\mathcal{O}$, in a completely trivial way, and can easily be proved using Newton's identities (see Appendix 2 for more details and proofs of all the following facts). We list a few of them. Suppose $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$ are subsets of $\mathcal{O}$, and $k \in \mathbb{N}$ with $k \leq n-1$. Then the following relations are equivalent (see Lemma A.2.1 for the proof):

$$\sum_{i=1}^{n} x_i^j = \sum_{i=1}^{n} y_i^j \quad \text{for } j = 1, 2, \ldots, k, \tag{2.1}$$

$$\deg\left(\prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i)\right) \leq n - k - 1, \tag{2.2}$$

$$(z-1)^{k+1} \Bigg| \sum_{i=1}^{n} z^{x_i} - \sum_{i=1}^{n} z^{y_i}. \tag{2.3}$$

Note that if $\mathcal{O} \not\subseteq \mathbb{R}$, then z^{x_i} may not be well defined. However, we see that for any $c \in \mathbb{C}$, we have $z^c = e^{c\ln(z)}$. Since

$$\frac{d}{dz}(z^c) = \frac{d}{dz}\left(e^{c\ln(z)}\right) = c\frac{1}{z}e^{c\ln(z)} = cz^{c-1},$$

and we merely need differentiation for the proof of (2.2) $\iff$ (2.3), we can use this fact formally. Similarly, since the terms in the sum $\sum_{i=1}^{n} z^{x_i} - \sum_{i=1}^{n} z^{y_i}$ are not, in general, polynomials, we consider the division in (2.3) to refer to the order of the zero at 1. These relations provide an alternative formulation for the PTE problem.

Note that in particular, the relation (2.1) $\iff$ (2.2) implies that when $X =_{n-1} Y$,

$$\prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i)$$

is a constant in $\mathcal{O}$. This constant plays a significant role in the study of the PTE problem, which we discuss later in Sections 3.1 and 3.2.

Given a solution to the $\mathcal{O}$-PTE problem, we can generate an infinite family of solutions. That is, if $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_n\}$ are subsets of $\mathcal{O}$ with $\{x_1, \ldots, x_n\} =_k \{y_1, \ldots, y_n\}$, then

$$\{Mx_1 + K, \ldots, Mx_n + K\} =_k \{My_1 + K, \ldots, My_n + K\}, \tag{2.4}$$

for any $M, K \in \mathcal{O}$. This fact leads us to give the following definition:

Definition 2.1.1. Let $\mathbb{Q}(\zeta)$ be a number field for some algebraic number ζ and $\mathcal{O}$ be its ring of integers. Suppose $X_1 =_k Y_1$ and $X_2 =_k Y_2$. If there exists an affine transformation $f(x) = Mx + K$ with M, K in $\mathbb{Q}(\zeta)$ such that $f(X_1) = X_2$ and $f(Y_1) = Y_2$, then we say that $X_1 =_k Y_1$ and $X_2 =_k Y_2$ are *equivalent*.

Another useful fact is due to M. Frolov [19]. Suppose $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_n\}$ are subsets of $\mathcal{O}$. If

$$\{x_1, \ldots, x_n\} =_k \{y_1, \ldots, y_n\}$$

then

$$\{x_1, \ldots, x_n, y_1 + M, \ldots, y_n + M\} =_{k+1} \{x_1 + M, \ldots, x_n + M, y_1, \ldots, y_n\},$$

for any $M \in \mathcal{O}$.

The following fact can be used as a criterion for PTE solutions to be equivalent. It will be useful later.

Proposition 2.1.2. *Suppose* $\{x_1, \ldots, x_n\} =_{n-1} \{y_1, \ldots, y_n\}$ *and*

$$\{x_1', \ldots, x_n'\} =_{n-1} \{y_1', \ldots, y_n'\}$$

are equivalent ideal PTE *solutions via the transformation* $f(x) = Mx + K$ *where* $M, K \in \mathbb{Q}(\zeta)$. *If* $\prod_{i=1}^{n}(x - x_i) - \prod_{i=1}^{n}(x - y_i) = C$ *and* $\prod_{i=1}^{n}(x - x_i') - \prod_{i=1}^{n}(x - y_i') = C'$, *then* $C' = CM^n$.

Proof. If these solutions are equivalent, without loss generality, we may assume $Mx_i+K = x'_i$ and $My_i + K = y'_i$ for $i = 1, \ldots, n$. Thus, we have

$$\prod_{i=1}^{n}(x - (Mx_i + K)) - \prod_{i=1}^{n}(x - (My_i + K)) = C',$$

and since this holds for all values of x, we may replace x by $x + K$ to obtain

$$\prod_{i=1}^{n}((x + K) - (Mx_i + K)) - \prod_{i=1}^{n}((x + K) - (My_i + K)) = C'.$$

Simplifying, dividing through by M^n and then replacing x/M by x, we obtain

$$\prod_{i=1}^{n}(x - x_i) - \prod_{i=1}^{n}(x - y_i) = \frac{C'}{M^n},$$

proving the result. □

Let $\overline{z}$ denote the complex conjugate of z. It is clear that if $\{x_1, \ldots, x_n\} =_k \{y_1, \ldots, y_n\}$, then $\{\overline{x}_1, \ldots, \overline{x}_n\} =_k \{\overline{y}_1, \ldots, \overline{y}_n\}$ also. This is true more generally for any Galois action.

One fact that only generalizes to real number fields is the following from [4]:

Theorem 2.1.3 (Interlacing Theorem)**.** *If $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$ are an ideal* PTE *solution with $x_1 \leq x_2 \leq \cdots \leq x_n$ and $y_1 \leq y_2 \leq \cdots \leq y_n$, then $x_1 \neq y_j$ for any j and*

$$x_1 < y_1 \leq y_2 < x_2 \leq x_3 \cdots < x_{n-1} \leq x_n < y_n, \; n \text{ odd},$$

$$x_1 < y_1 \leq y_2 < x_2 \leq x_3 \cdots < x_{n-2} \leq x_{n-1} < y_{n-1} \leq y_n < x_n, \; n \text{ even},$$

where without loss of generality, we assume that $x_1 < y_1$.

Proof. From the second form of the ideal solution, we have

$$\prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i) = C.$$

Thus, we view the polynomial $p(z) := \prod_{i=1}^{n}(z - x_i)$ as a shift of the polynomial $q(z) := \prod_{i=1}^{n}(z - y_i)$. Now consider the graph of $p(z)$ and the graph of $q(z) = p(z) - C$. The polynomials p and q have the same critical points, and these critical points separate the zeros of both p and q. Further, the polynomials never intersect. □

Remark 2.1.4. There are some immediate consequences of this Theorem for the PTE problem over $\mathbb{Z}$. First, no integer may appear more than twice among either the x_i or y_i. Secondly, we may not have three consecutive integers on one side of the solution, or two repeated integers and a consecutive integer. These facts will be important later in Chapter 4.

Chapter 3

The PTE problem over Gaussian integers and other number fields

3.1 A Computational Search for Ideal Solutions over $\mathbb{Z}[i]$

This chapter is based on [7]. Because $\mathbb{Z}[i]$ contains $\mathbb{Z}$, we might expect "smaller" (with respect to norm) ideal solutions to the PTE problem in this setting. Therefore, this chapter examines ideal solutions to the PTE problem over $\mathbb{Z}[i]$. In particular, we view ideal solutions over $\mathbb{Z}$ as special cases of solutions over $\mathbb{Z}[i]$. We also describe a computational search for ideal solutions of size n for $\mathbb{Z}[i]$ for $n \geq 8$. This search generalizes the methods of Borwein, Lisoněk and Percival in [5] (and abbreviated to BLP from now on). They performed a computer search for ideal solutions of size $n = 10$ and $n = 12$, which took advantage of an alternative formulation of the problem to reduce the number of variables. Their search was further optimized by using the arithmetic properties of ideal solutions.

All the results that are required for the method of BLP generalize sufficiently to $\mathbb{Z}[i]$. We proceed by discussing some further background from the existing literature in Section 2.1, and then explaining the computational method to be used Section 3.1. In Section 3.2, we will provide analogues of existing theorems in the literature for the PTE problem over the Gaussian integers, which allow the computational search to be optimized. Finally in Section 3.4, we describe the results of a computational search for ideal solutions for $n = 10$ and $n = 12$.

For convenience, we state some results in greater generality than $\mathbb{Z}[i]$. As a general

notation, we refer to the PTE problem over the ring R as the R-PTE problem. Throughout this chapter, let $\zeta \in \mathbb{C}$ be an algebraic integer, and let $\mathcal{O}$ denote the ring of integers of the number field $\mathbb{Q}(\zeta)$. Note that it is easy to find $\mathcal{O}$-PTE solutions, such as the example found by Goldbach given in Chapter 1. Hence, we proceed to discuss the PTE problem in this general setting.

We might naively search for ideal solutions to the PTE problem over $\mathbb{Z}$ in the following way. Suppose our search space is $x_i, y_i \in [0, S] \cap \mathbb{Z}$. We may assume $x_1 = 0$. Then select the remaining integers so that $0 \leq x_2 \leq x_3 \leq \cdots \leq x_n$ and $1 \leq y_1 \leq \cdots \leq y_{n-1}$, and take $y_n = x_1 + \cdots + x_n - (y_1 + \cdots + y_{n-1})$. Now check whether or not

$$x_1^k + \cdots + x_n^k = y_1^k + \cdots + y_n^k$$

for each $k = 2, \ldots, n-1$. This method requires searching in $2n-1$ variables.

However, BLP [5] improve on this significantly. Recall from (2.2) that if $\{x_1, \ldots, x_n\} =_{n-1} \{y_1, \ldots, y_n\}$ is an ideal PTE solution, then

$$(z - x_1)(z - x_2) \cdots (z - x_n) - (z - y_1)(z - y_2) \cdots (z - y_n) = C,$$

for some constant $C \in \mathbb{Z}$. Rearranging this equation and then substituting $z = y_j$ for $j = 1, \ldots, n$ we obtain

$$(y_j - x_1) \cdots (y_j - x_n) = C. \tag{3.1}$$

For any $k \in \{1, \ldots, n\}$, equation (3.1) can be rearranged to

$$\frac{1}{C}(y_j - x_{n-k+2}) \cdots (y_j - x_n) = \frac{1}{(y_j - x_1) \cdots (y_j - x_{n-k+1})}. \tag{3.2}$$

Now define

$$f(z) := \frac{1}{C}(z - x_{n-k+2}) \cdots (z - x_n).$$

From (3.2), we have $f(y_j) = \frac{1}{(y_j - x_1) \cdots (y_j - x_{n-k+1})}$ for $j = 1, \ldots, k$. So if the variables $x_1, \ldots, x_{n-k+1}$ and $y_1, \ldots, y_k$ are known, then we also have the ordered pairs $(y_j, f(y_j))$ for $j = 1, \ldots, k$. We may determine $f(z)$ uniquely by using Lagrange polynomials and the ordered pairs $(y_j, f(y_j))$ for $j = 1, \ldots, k$ (see, for example [38, Chapter 5]). Thus, $f(x)$ is a polynomial of degree $k-1$, and solving $f(z) = 0$ yields its roots, which are $x_{n-k+2}, \ldots, x_n$. Repeating this process gives the remaining $y_{k+1}, \ldots, y_n$. Alternatively, once $x_1, \ldots, x_n$ are determined, the values of $y_1, \ldots, y_n$ can be obtained from the roots of the polynomial

$$(z - y_1) \cdots (z - y_n) = (z - x_1) \cdots (z - x_n) - C.$$

The value of C is determined from the leading coefficient of $f(z)$ which has already been computed or by using (3.1) with $j = 1$.

The method of BLP requires searching through only $n+1$ variables, instead of $2n-1$. This method can clearly be generalized to any ring of integers $\mathcal{O}$, and this is what we have implemented for $\mathcal{O} = \mathbb{Z}[i]$.

3.1.1 Optimizing the Search

In order to explain how BLP further optimize the search over $\mathbb{Z}$, we need the following definition. In order to state it, we now restrict ourselves to any $\mathcal{O}$ that is also a unique factorization domain (UFD). We maintain this restriction for the remainder of this chapter.

Definition 3.1.1. Fix a positive integer n and a UFD $\mathcal{O}$. For each $\mathcal{O}$-PTE solution $X =_{n-1} Y$, let $C_{n,X,Y} = \prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i)$. Then let

$$C_n := \gcd\{C_{n,X,Y} | X =_{n-1} Y\}.$$

We say that C_n is the *constant associated* with the $\mathcal{O}$-PTE problem of size n.

Thus, C_n keeps track of all the common factors that appear among the constants that come from the second formulation of the PTE problem in (2.2). The requirement that $\mathcal{O}$ is a UFD is necessary for C_n to be well-defined.

We have the following Theorem, generalized from Proposition 3 in [5],

Theorem 3.1.2. *Let $\{x_1, \ldots, x_n\} =_{n-1} \{y_1, \ldots, y_n\}$ be subsets of $\mathcal{O}$ that are an ideal $\mathcal{O}$-PTE solution. Suppose that $q \in \mathcal{O}$ is a prime such that $q \mid C_n$. Then we can reorder the y_i such that*

$$x_i \equiv y_i \pmod{q} \qquad \text{for } i = 1, \ldots, n.$$

The proof of Theorem 3.1.2 follows that of Proposition 3 from [5], but we repeat it for completeness.

Proof. Assume $q \in \mathcal{O}$ is a prime dividing C_n. Since $\mathcal{O}$ is an integral domain and q is prime, $\langle q \rangle$ is a prime ideal. Since prime ideals of rings of integers of number fields are also maximal (see, for example [36]), the quotient $\mathcal{O}/\langle q \rangle$ is a field. Let $\mathbb{F}_q$ denote this field. It follows that $\prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i)$ equals a constant times q, and so is zero in $\mathbb{F}_q[z]$. Hence, $\prod_{i=1}^{n}(z - x_i) = \prod_{i=1}^{n}(z - y_i)$ in $\mathbb{F}_q[z]$. Since $\mathbb{F}_q$ is a field, the polynomial ring $\mathbb{F}_q[z]$ is a unique factorization domain. Since each of the factors $z - x_i$ and $z - y_i$ are irreducible, it follows that the sets $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_n\}$ are equal as subsets of $\mathbb{F}_q$. That is, they are equal modulo q, as desired. □

BLP [5] use Theorem 3.1.2 to optimize the search for ideal solutions over $\mathbb{Z}$. This can also be applied over $\mathcal{O}$. Suppose q_1 and q_2 are the two largest primes (in $\mathcal{O}$, ordered by absolute value of norm) dividing C_n. (If two such primes are not uniquely determined, we may pick any two, since we simply wish to reduce our search space by the largest factor possible.) Assume $x_1 = 0$, and pick the rest of the variables so that for $i = 1, \ldots, n$

$$x_i \equiv y_i \pmod{q_1}$$
$$(x_{i+1} - y_i) \cdot \sum_{j=1}^{i} (x_j - y_j) \equiv 0 \pmod{q_2}.$$

Thus, we pair x_i to y_i modulo q_1, and then pair each x_i to the previous y_i modulo q_2, unless coincidentally all the x_j and y_j are already paired off modulo q_2, in which case x_{i+1} may take on any value modulo q_2. However, this coincidence will only occur once in $|N(q_1)N(q_2)|$ values by the Chinese Remainder Theorem, and so every prime q that divides C_n reduces the search space in each variable by a factor of $N(q)$, where $N(q)$ denotes the norm of the ideal $\langle q \rangle$. Therefore, divisibility results, particularly large prime factors, for C_n are very important for optimizing the search.

3.2 Divisibility Results for C_n

There are a number of results in the literature concerning divisibility of C_n for the $\mathbb{Z}$-PTE problem. For example, about half of the article by Rees and Smyth [27] is spent proving such results. Many of these results generalize immediately to $\mathcal{O}$, which we state below without proof. In the case where the result is more of an analogy than a generalization, we provide a proof.

The usual method of generalization is to view arithmetic modulo a prime power in $\mathbb{Z}$ as analogous to arithmetic in the appropriate finite field, which is then viewed as analogous to arithmetic modulo the algebraic norm of a prime in $\mathcal{O}$. Fermat's Little Theorem corresponds with Lagrange's Theorem and so on. This method was used in the proof of Theorem 3.1.2 in the previous section.

The next two results are generalizations of Proposition 2.3 and Proposition 3.1 in [27], respectively. Their proofs may be found in Appendix 2.

Theorem 3.2.1. *Let $q \in \mathcal{O}$ be a prime with $N(q) > 3$. Then $N(q) \mid C_{N(q)}$.*

Theorem 3.2.2. *Let $q \in \mathcal{O}$ be a prime such that*

$$n + 3 \leq N(q) < n + 3 + \frac{n-2}{6}.$$

Then $q \mid C_{n+1}$.

Note that Rees and Smyth use a "Multiplicity Lemma" to prove this result in [27]. The proof of this lemma also generalizes appropriately to $\mathcal{O}$, and so Theorem 3.2.2 remains valid.

We now prove a general divisibility result of C_n for powers of primes q. This result is based on the same techniques used in Proposition 2.4 of [27].

Proposition 3.2.3. *Suppose $q \in \mathcal{O}$ is a prime. If $q \mid C_n$, then*

$$q^{\lceil \frac{n}{N(q)} \rceil} \Big| C_n,$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x.

Proof. Suppose $X = \{a_1, \ldots, a_n\}$ and $Y = \{b_1, \ldots, b_n\}$ with $X =_{n-1} Y$, and $q \mid C_{n,X,Y}$. From Theorem 3.1.2, we can relabel the a_i and b_j such that $a_i \equiv b_i \pmod{q}$ for $i = 1, \ldots, n$. Note that $\mathcal{O}$ has $N(q)$ congruence classes modulo q, and so there is at least one congruence class with at least $\lceil n/N(q) \rceil$ elements from the set $\{b_1, \ldots, b_n\}$. Relabel this set so that $b_1, \ldots, b_{\lceil \frac{n}{N(q)} \rceil}$ are in the same congruence class modulo q. From Proposition 2.1.2 with $M = 1$, we may shift the a_i and b_i by $-b_1$ without changing the corresponding constant, and so $C_{n,X,Y} = a_1 a_2 \cdots a_n$. Then

$$\begin{aligned} a_1 &\equiv b_1 \equiv 0 \pmod{q} \\ a_2 &\equiv b_2 \equiv 0 \pmod{q} \\ &\vdots \\ a_{\lceil \frac{n}{N(q)} \rceil} &\equiv b_{\lceil \frac{n}{N(q)} \rceil} \equiv 0 \pmod{q}. \end{aligned}$$

Thus, $q^{\lceil \frac{n}{N(q)} \rceil} \mid C_{n,X,Y}$, and since X and Y were arbitrary, we have proved the result. □

Note that we can only apply Proposition 3.2.3 when we already have from another source that $q \mid C_n$.

We now prove a specific result for the divisibility of C_5 for powers of primes $q \in \mathcal{O}$, with $N(q) = 2$. This result is based on the same techniques used in Proposition 2.5 of [27].

Proposition 3.2.4. *Suppose $q \in \mathcal{O}$ is prime with $N(q) = 2$. Then $q^4 \mid C_5$.*

Proof. Suppose $X = \{a_1, \ldots, a_5\}$ and $Y = \{b_1, \ldots, b_5\}$ with $X =_4 Y$. As in the proof of Proposition 3.2.3, we can relabel the a_i and b_j such that $a_i \equiv b_i \pmod{q}$ for $i = 1, \ldots, 5$, and so that $b_1, \ldots, b_3$ are in the same congruence class modulo q. Again as above, we can shift the a_i and b_i by $-b_1$, giving $C_{5,X,Y} = a_1a_2a_3a_4a_5$. Assume that $q^4 \nmid C_{5,X,Y}$. Since we know that $q^3 \mid C_{5,X,Y}$. However, we can assume that $a_1 \equiv a_2 \equiv a_3 \equiv q \pmod{q^2}$ and $a_4 \equiv a_5 \equiv 1 \pmod{q}$. As usual, we have

$$(z-a_1)(z-a_2)(z-a_3)(z-a_4)(z-a_5) - z(z-b_2)(z-b_3)(z-b_4)(z-b_5) = C_{5,X,Y}. \quad (3.3)$$

Substituting $z = a_1$ into (3.3) gives

$$-a_1(a_1-b_2)(a_1-b_3)(a_1-b_4)(a_1-b_5) = C_{5,X,Y}.$$

Since a_1, a_1-b_2, a_1-b_3 are all equivalent to 0 modulo q, while a_1-b_4, a_1-b_5 are both equivalent to 1 modulo q and their product is not divisible by q^4, we must have $a_1 \equiv a_1-b_2 \equiv a_1-b_3 \equiv q \pmod{q^2}$. Since $a_1 \equiv q \pmod{q^2}$ already, this means that $b_2 \equiv b_3 \equiv 0 \pmod{q^2}$.

We now substitute $z = a_4$ into (3.3) giving

$$-a_4(a_4-b_2)(a_4-b_3)(a_4-b_4)(a_4-b_5) = C_{5,X,Y}.$$

Since a_4, a_4-b_2, a_4-b_3 are all equivalent to 1 modulo q, while a_4-b_4, a_4-b_5 are both equivalent to 0 modulo q, we can assume, without loss of generality, that $a_4 - b_5 \equiv q \pmod{q^2}$ and $a_4 - b_4 \equiv q^2 \pmod{q^3}$, i.e., $a_4 - b_4 \equiv 0 \pmod{q^2}$.

Finally, substituting $x = b_5$ into (3.3) gives

$$(b_5-a_1)(b_5-a_2)(b_5-a_3)(b_5-a_4)(b_5-a_5) = C_{5,X,Y}.$$

Only $b_5 - a_4$ and $b_5 - a_5$ are equivalent to 0 modulo q. However, we already have that $a_4 - b_5 \equiv q \pmod{q^2}$, and so we must have $a_5 - b_5 \equiv 0 \pmod{q^2}$. However, we have

$$\begin{aligned} 0 &= a_1 + a_2 + a_3 + a_4 + a_5 - (b_2 + b_3 + b_4 + b_5) \\ &\equiv q + q + q + b_4 + b_5 - 0 - 0 - b_4 - b_5 \equiv q \pmod{q^2}, \end{aligned}$$

which is a contradiction, proving the proposition. □

Not all results from the literature concerning C_n generalize to $\mathbb{Z}[i]$ or $\mathcal{O}$, and some must be addressed specifically depending on the ring of integers involved. Those relevant to our computer search for ideal solutions over $\mathbb{Z}[i]$ are discussed next.

3.3 Divisibility Results for C_n over $\mathbb{Z}[i]$

An important divisibility result for C_n over $\mathbb{Z}$ is that $n! \mid C_{n+1}$ (see Proposition 2.1 in [27], originally due to H. Kleiman in [23]). This fact demonstrates that C_n is highly composite and will contain some large prime factors. The proof that Rees and Smyth provide of Proposition 2.1 in [27] uses the obvious fact that if $t \in \mathbb{Z}$ then $t(t+1)(t+2)\cdots(t+n) \equiv 0 \pmod{(n+1)!}$. However, this depends on t being an integer. Unfortunately, this fact does not fully generalize to $\mathbb{Z}[i]$. Nevertheless, we are able to state an analogous lemma below. For completeness, we prove this result in greater generality than necessary, that is, for the ring of integers of an arbitrary quadratic number field.

We first recall some facts concerning quadratic number fields from Chapter 5 of [14]. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d \neq 1$ squarefree and let $D = d(K)$ denote the discriminant of K, and let $\mathcal{O}$ be its ring of integers. We also assume that $\mathcal{O}$ is a UFD, but note that this hypothesis is not required for Propositions 3.3.1 and 3.3.2 or Lemma 3.3.3. We have the following results:

Proposition 3.3.1.

(i) *If* $d \equiv 1 \pmod 4$, *then* $\{1, \frac{1+\sqrt{d}}{2}\}$ *is an integral basis for* $\mathcal{O}$ *and* $D = d$.

(ii) *If* $d \equiv 2$ *or* $3 \pmod 4$, *then* $\{1, \sqrt{d}\}$ *is an integral basis for* $\mathcal{O}$ *and* $D = 4d$.

Thus, we may write $\mathcal{O} = \mathbb{Z}[\omega]$, where $\omega = \frac{D+\sqrt{D}}{2}$.

Proposition 3.3.2. *Let* p *be a prime and* $\left(\frac{a}{p}\right)$ *be the Legendre symbol. Then the decomposition of prime ideals of* $\mathbb{Z}$ *in* $\mathcal{O}$ *is as follows:*

(i) *If* $p \mid D$, *i.e., if* $\left(\frac{D}{p}\right) = 0$, *then* p *is ramified, and we have* $p\mathcal{O} = \mathfrak{p}^2$, *where* $\mathfrak{p} = p\mathcal{O} + \omega\mathcal{O}$, *except when* $p = 2$ *and* $D \equiv 12 \pmod{16}$. *In this case* $\mathfrak{p} = p\mathcal{O} + (1+\omega)\mathcal{O}$.

(ii) *If* $\left(\frac{D}{p}\right) = -1$, *then* p *is inert, and hence* $\mathfrak{p} = p\mathcal{O}$ *is a prime ideal.*

(iii) *If* $\left(\frac{D}{p}\right) = 1$, *then* p *is split, and we have* $p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$, *where* $\mathfrak{p}_1 = p\mathcal{O} + \left(\omega - \frac{D+c}{2}\right)\mathcal{O}$ *and* $\mathfrak{p}_2 = p\mathcal{O} + \left(\omega - \frac{D-c}{2}\right)$, *and* c *is any solution to the congruence* $c^2 \equiv D \pmod{4p}$.

Lemma 3.3.3. *Let $p \in \mathbb{Z}$ be a prime that is either ramified or split in $\mathcal{O}$, i.e., is of type (i) or (iii) from Proposition 3.3.2. Let $s \in \mathbb{N}$. Then*

$$t(t+1)(t+2)(t+3)\cdots(t+sp-1) \in \begin{cases} \mathfrak{p}^s, & \text{where } p \text{ is type (i) and } p\mathcal{O} = \mathfrak{p}^2; \\ \mathfrak{p}_1^s, & \text{where } p \text{ is type (iii) and } p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2; \\ \mathfrak{p}_2^s, & \text{where } p \text{ is type (iii) and } p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2. \end{cases}$$

Proof. Define a map $\phi : \mathcal{O} \to \mathbb{R}^2$ by $\phi(a+b\omega) = (a,b)$, where $a, b \in \mathbb{Z}$. Because $\{1, \omega\}$ is an integral basis for $\mathcal{O}$, it is clear that ϕ is well defined. We now examine the image of ramified and split ideals $p\mathcal{O}$ under ϕ.

First note that ω satisfies the equation $\omega^2 = \frac{D-D^2}{4} + D\omega$.

Suppose p is ramified. Then from Proposition 3.3.2, we have $p\mathcal{O} = \mathfrak{p}^2$, where $\mathfrak{p} = p\mathcal{O} + \omega\mathcal{O}$, excluding the case that $p = 2$ and $D \equiv 12 \pmod{16}$. Thus, an arbitrary element $q \in \mathfrak{p}$ looks like

$$\begin{aligned} q &= p(a+b\omega) + \omega(e+f\omega) \\ &= ap + (bp+e)\omega + f\omega^2 \\ &= ap + (bp+e)\omega + f\left(\frac{D-D^2}{4} + D\omega\right) \\ &= ap + f\left(\frac{D-D^2}{4}\right) + (bp+e+Df)\omega, \end{aligned}$$

where $a, b, e, f \in \mathbb{Z}$. Thus, we have

$$\phi(q) = \left(ap + f\left(\frac{D-D^2}{4}\right), bp+e+Df\right).$$

In the case that $p = 2$ and $D \equiv 12 \pmod{16}$, we have $\mathfrak{p} = p\mathcal{O} + (1+\omega)\mathcal{O}$. Thus, an arbitrary element $q \in \mathfrak{p}$ looks like

$$\begin{aligned} q &= p(a+b\omega) + (1+\omega)(e+f\omega) \\ &= ap + e + (bp+e+f)\omega + f\omega^2 \\ &= ap + e + (bp+e+f)\omega + f\left(\frac{D-D^2}{4} + D\omega\right) \\ &= ap + e + f\left(\frac{D-D^2}{4}\right) + (bp+e+(D+1)f)\omega, \end{aligned}$$

where $a, b, e, f \in \mathbb{Z}$. Thus, we have

$$\phi(q) = \left(ap + e + f\left(\frac{D - D^2}{4}\right), bp + e + (D+1)f \right).$$

Alternatively, suppose p is split. Then from Proposition 3.3.2, we have $p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1 = p\mathcal{O} + \left(\omega - \frac{d+c}{2}\right)\mathcal{O}$ and $\mathfrak{p}_2 = p\mathcal{O} + \left(\omega - \frac{D-c}{2}\right)$ and c is any solution to the congruence $c^2 \equiv D \pmod{4p}$.

Thus, an arbitrary element of $q \in \mathfrak{p}_1$ (resp. $\mathfrak{p}_2$) looks like

$$\begin{aligned} q &= p(a + b\omega) + \left(\omega - \frac{D \pm c}{2}\right)(e + f\omega) \\ &= ap + bp\omega + e\omega + f\omega^2 + f\left(\frac{D - D^2}{4} + D\omega\right) - \left(\frac{D \pm c}{2}\right)e + \left(\frac{D \pm c}{2}\right)f\omega \\ &= ap + f\left(\frac{D - D^2}{4}\right) - \left(\frac{D \pm c}{2}\right)e + \left(bp + e + fD + \left(\frac{D \pm c}{2}\right)f\right)\omega, \end{aligned}$$

where $a, b, e, f \in \mathbb{Z}$. Thus, we have

$$\phi(q) = \left(ap + f\left(\frac{D - D^2}{4}\right) - \left(\frac{D \pm c}{2}\right)e, \left(bp + e + fD + \left(\frac{D \pm c}{2}\right)f\right)\right).$$

Now let $t \in \mathcal{O}$ and suppose $t = u + v\omega$ so that $\phi(t) = (u, v)$. Note that $D \pm c$ is always even, and if we pick f so that $f\left(\frac{D-D^2}{4}\right)$ is an integer, then $\phi(q) \in \mathbb{Z}^2$ in all three of the above cases. Further, in each case, we may solve the equations $bp + e + Df = v$, $bp + e + (D+1)f = v$ and $bp + e + fD + \left(\frac{D \pm c}{2}\right)f = v$ for b, e, f. Thus, in each case, it follows that the set

$$\{t + jp, t + jp + 1, t + jp + 2, t + jp + 3, \ldots, t + jp + (p-1)\}$$

contains an element that belongs to $\mathfrak{p}$ or $\mathfrak{p}_1$ or $\mathfrak{p}_2$ respectively, for $j = 0, \ldots, s-1$. Thus, the set $\{t, t+1, t+2, \ldots, t+sp-1\}$ contains s elements that belong to $\mathfrak{p}$ or $\mathfrak{p}_1$ or $\mathfrak{p}_2$ respectively, proving the lemma. □

Remark 3.3.4. Note that if p is inert, i.e. of type (ii), the expression $t(t+1)(t+2)(t+3)\ldots(t+n)$ need not belong to $p\mathcal{O}$. For example, when $K = \mathbb{Q}(i)$ and $\mathcal{O} = \mathbb{Z}[i]$, $p = 3$ and $t = i$, note that none of $i, 1+i, 2+i, \ldots, n+i$ contain a factor of 3.

Using the above characterization of primes in a quadratic number field, we have the following result for the $\mathcal{O}$-PTE problem analogous to $n! \mid C_{n+1}$:

Theorem 3.3.5. *Let C_{n+1} be the constant associated with the $\mathcal{O}$-PTE problem. Suppose p is either (i) ramified or (iii) split and let*

$$\mathfrak{p} = \begin{cases} \mathfrak{p}, & \text{where } p \text{ is type (i) and } p\mathcal{O} = \mathfrak{p}^2; \\ \mathfrak{p}_1, & \text{where } p \text{ is type (iii) and } p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2; \\ \mathfrak{p}_2, & \text{where } p \text{ is type (iii) and } p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2. \end{cases}$$

Let $s = \lfloor (n+1)/p \rfloor$ and let ℓ be the highest power such that $n+1 \in \mathfrak{p}^\ell$. Then $C_{n+1} \in \mathfrak{p}^{\max(s-\ell,0)}$.

We digress before proving Theorem 3.3.5. As stated earlier, many results on the $\mathcal{O}$-PTE problem involve Newton's identities and symmetric polynomials, including the proof of (2.1) $\iff$ (2.2). We need them for the proof of some results below, so although they are well known and easily found in the literature (for example see [36]), we repeat them here.

Let $n \in \mathbb{N}$. Let $s_1, \ldots, s_n$ be variables. Then for all integers $k \geq 1$, we define

$$p_k(s_1, \ldots, s_n) := s_1^k + s_2^k + \cdots + s_n^k,$$

the kth power sum in n variables. Similarly, for $k \geq 0$, we define

$$\begin{aligned} e_0(s_1, \ldots, s_n) &= 1 \\ e_1(s_1, \ldots, s_n) &= s_1 + s_2 + \cdots + s_n \\ e_2(s_1, \ldots, s_n) &= \sum_{i<j} s_i s_j \\ &\vdots \\ e_k(s_1, \ldots, s_n) &= \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq n} s_{j_1} \cdots s_{j_k} \\ &\vdots \\ e_n(s_1, \ldots, s_n) &= s_1 s_2 \cdots s_n \\ e_k(s_1, \ldots, s_n) &= 0, \forall k > n, \end{aligned}$$

to be the elementary symmetric polynomials in n variables. Then we have the result known as Newton's identities:

$$k e_k(s_1, \ldots, s_n) = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i}(s_1, \ldots, s_n) p_i(s_1, \ldots, s_n), \tag{3.4}$$

for all $k \geq 1$. Note that this can be rearranged to

$$p_k(s_1, \ldots, s_n) = (-1)^{k-1} k e_k(s_1, \ldots, s_n) + \sum_{i=1}^{k-1} (-1)^{k-i} e_{k-i}(s_1, \ldots, s_n) p_i(s_1, \ldots, s_n), \quad (3.5)$$

for $k \geq 2$. Another fact is the identity

$$\prod_{i=1}^{n} (t - s_i) = \sum_{k=0}^{n} (-1)^k e_k(s_1, \ldots, s_n) t^{n-k}. \quad (3.6)$$

Thus, the coefficients of a polynomial are elementary symmetric polynomials of its roots, and they depend on the power sums $p_i(s_1, \ldots, s_n)$.

We are now able to proceed with the proof of the Theorem.

Proof of Theorem 3.3.5. We closely emulate the proof of Proposition 2.1 in [27]. Suppose $X = \{x_1, \ldots, x_{n+1}\}$ and $Y = \{y_1, \ldots, y_{n+1}\}$ are subsets of $\mathcal{O}$, and $X =_n Y$. Then we have

$$(z - x_1) \cdots (z - x_{n+1}) - (z - y_1) \cdots (z - y_{n+1}) = C_{n+1,X,Y}$$

where $C_{n+1,X,Y} = (-1)^{n+1}(x_1 x_2 \cdots x_{n+1} - y_1 y_2 \cdots y_{n+1})$. Then from the identity (A.3), we have

$$(z - x_1) \cdots (z - x_{n+1}) = \sum_{k=0}^{n+1} (-1)^k e_k(x_1, \ldots, x_{n+1}) z^{n+1-k}$$
$$(z - y_1) \cdots (z - y_{n+1}) = \sum_{k=0}^{n+1} (-1)^k e_k(y_1, \ldots, y_{n+1}) z^{n+1-k}.$$

From the identity (A.2), it follows that

$$p_{k+1}(x_1, \ldots, x_{n+1}) = (-1)^k (k+1) e_{k+1}(x_1, \ldots, x_{n+1}) + \sum_{i=1}^{k} (-1)^{k+1-i} e_{k+1-i}(x_1, \ldots, x_{n+1}) p_i(x_1, \ldots, x_{n+1}), \quad (3.7)$$

and

$$p_{k+1}(y_1,\dots,y_{n+1}) = (-1)^k(k+1)e_{k+1}(y_1,\dots,y_{n+1}) + \sum_{i=1}^{k}(-1)^{k+1-i}e_{k+1-i}(y_1,\dots,y_{n+1})p_i(y_1,\dots,y_{n+1}). \quad (3.8)$$

By hypothesis, we have $p_k(x_1,\dots,x_{n+1}) = p_k(y_1,\dots,y_{n+1})$ and $e_k(x_1,\dots,x_{n+1}) = e_k(y_1,\dots,y_{n+1})$ for $1 \le k \le n$, and so subtracting (3.8) from (3.7) it follows that

$$p_{n+1}(x_1,\dots,x_{n+1}) - p_{n+1}(y_1,\dots,y_{n+1}) = (-1)^n(n+1)e_{n+1}(x_1,\dots,x_{n+1}) - (-1)^n(n+1)e_{n+1}(y_1,\dots,x_{y+1}). \quad (3.9)$$

Now noting that $C_{n+1,X,Y} = e_{n+1}(x_1,\dots,x_{n+1}) - e_{n+1}(y_1,\dots,y_{n+1})$, rearranging (3.9) we get

$$p_{n+1}(x_1,\dots,x_{n+1}) + (n+1)C_{n+1,X,Y} = p_{n+1}(y_1,\dots,y_{n+1}). \quad (3.10)$$

Since $s = \lfloor (n+1)/p \rfloor$, it follows that $sp < n+2$, and so from the above lemma we have

$$\sum_{k=0}^{n+1}(-1)^k e_k(0,-1,\dots,-n)t^{n+1-k} = t(t+1)(t+2)(t+3)\cdots(t+n) \in \mathfrak{p}^s. \quad (3.11)$$

Substituting $t = x_1, x_2, \dots, x_{n+1}$ into (3.11) and summing, and doing the same for $t = y_1, y_2, \dots, y_{n+1}$, we get

$$\sum_{i=1}^{n+1}\sum_{k=0}^{n+1}(-1)^k e_k(0,-1,\dots,-n)x_i^{n+1-k} \in \mathfrak{p}^s \quad (3.12)$$

and

$$\sum_{i=1}^{n+1}\sum_{k=0}^{n+1}(-1)^k e_k(0,-1,\dots,-n)y_i^{n+1-k} \in \mathfrak{p}^s. \quad (3.13)$$

Subtracting (3.13) from (3.12) and applying (3.10), we get

$$(n+1)C_{n+1,X,Y} \in \mathfrak{p}^s.$$

Since $n+1 \in \mathfrak{p}^\ell$ and $n+1 \notin \mathfrak{p}^{\ell+1}$, we have $C_{n+1,X,Y} \in \mathfrak{p}^{\max(s-\ell,0)}$, and because X and Y were arbitrary solutions to the $\mathcal{O}$-PTE problem, we have $C_{n+1} \in \mathfrak{p}^{\max(s-\ell,0)}$, proving the theorem. □

Table 3.1: Divisibility Results for the $\mathbb{Z}[i]$-PTE Problem

n	lower bound for C_n	upper bound for C_n
2	1	1
3	$(1+i)^2$	$(1+i)^2$
4	1	1
5	$(1+i)^4(2+i)(2-i)$	$(1+i)^5(2+i)(2-i)$
6	$(1+i)^3(2+i)(2-i)$	$(1+i)^4(2+i)^2(2-i)^2$
7	$(1+i)^4(2+i)(2-i)\cdot 3$	$(1+i)^6(2+i)^2(2-i)^2\cdot 3$
8	$(1+i)^4(2+i)(2-i)$	$(1+i)^8(2+i)^2(2-i)^2(3+2i)(3-2i)$
9	$(1+i)^5(2+i)(2-i)$ $\cdot 3^2\cdot(3+2i)(3-2i)$	$(1+i)^{18}(2+i)^2(2-i)^2\cdot 3^4\cdot 7^2\cdot 11\cdot(3+2i)$ $(3-2i)(4+i)(4-i)\cdot 23\cdot(5+2i)(5-2i)\,(*)$
10	$(1+i)^5(2+i)(2-i)$ $(3+2i)(3-2i)$	$(1+i)^{13}(2+i)^2(2-i)^2\cdot 3^2\cdot(3+2i)(-3+2i)$ $(4+i)(4-i)$
11	$(1+i)^6(2+i)^2(2-i)^2$	none known
12	$(1+i)^6(2+i)^2(2-i)^2$	$(1+i)^{24}(2+i)^3(2-i)^3\cdot 3^8\cdot 7^2\cdot 11^2\cdot(3+2i)^2$ $(-3+2i)^2(4+i)(4-i)\cdot 19\cdot 23\cdot(5+2i)$ $(5-2i)\cdot 31\,(*)$
13	$(1+i)^7(2+i)^2(2-i)^2$ $(3+2i)(3-2i)(4+i)(4-i)$	none known
14	$(1+i)^7(2+i)^2(2-i)^2$ $(3+2i)(3-2i)(4+i)(4-i)$	none known
15	$(1+i)^8(2+i)(2-i)$ $(3+2i)(3-2i)$	none known

The above divisibility results give lower bounds for C_n for the PTE problem over $\mathbb{Z}[i]$; these are stated in Table 3.1. When $(*)$ appears in Table 3.1, this means the upper bounds for C_n come from the upper bounds for C_n for the PTE problem over $\mathbb{Z}$ (compare to Table 3.2). In the next section we explain the upper bounds new to the $\mathbb{Z}[i]$-PTE problem. These have been determined by searching for solutions computationally.

Table 3.2, which appears as Table 5.1 later on and is explained in Chapters 4 and 5, shows that the constant for the $\mathbb{Z}$-PTE problem has many more factors than that for the $\mathbb{Z}[i]$- PTE problem. This demonstrates that the Gaussian integers are a much less restrictive setting for the PTE-problem than the ordinary integers.

However, it is clear from each table that for larger n, there is substantial gap in factors that appear in the upper bounds compared to the lower bounds. For example, for $n = 5$ in the $\mathbb{Z}$-PTE problem, the lower and upper bounds are equal, but for $n = 7$, there is an

Table 3.2: Divisibility Results for the $\mathbb{Z}$-PTE Problem

n	Lower bound for C_n	Upper bound for C_n	Upper bound divided by Lower Bound
2	1	1	1
3	2^2	2^2	1
4	$2^2 \cdot 3^2$	$2^2 \cdot 3^2$	1
5	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	1
6	$2^5 \cdot 3^2 \cdot 5^2$	$2^5 \cdot 3^2 \cdot 5^2$	1
7	$2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11$	$2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11$	1
8	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	$2^8 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	2^4
9	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	$2^9 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$ $\cdot 17 \cdot 23 \cdot 29$	$2^2 \cdot 3 \cdot 17 \cdot 23 \cdot 29$
10	$2^7 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17$	$2^{11} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$ $\cdot 17 \cdot 23 \cdot 37 \cdot 53 \cdot 61 \cdot 79$ $\cdot 83 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 191$	$2^4 \cdot 3^2 \cdot 11 \cdot 23 \cdot 37 \cdot 53$ $\cdot 61 \cdot 79 \cdot 83 \cdot 103 \cdot 107 \cdot 109$ $\cdot 113 \cdot 191$
11	$2^8 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$ $\cdot 17 \cdot 19$	none known	
12	$2^8 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 11^2$ $\cdot 17 \cdot 19$	$2^{12} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11^2 \cdot 13^2$ $\cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$	$2^4 \cdot 3^4 \cdot 13^2 \cdot 23 \cdot 29$ $\cdot 31$

extra factor of $2 \cdot 19$, and for $n = 12$ there are a number of additional factors.

3.4 Computer Search for Solutions

We may restrict the $\mathcal{O}$-PTE problem to a symmetric version. This is helpful because there are fewer variables, but at the same time, some ideal solutions may be missed. For odd n, this means finding solutions $x_1, \ldots, x_n \in \mathcal{O}$ with $\{x_1, \ldots, x_n\} =_{n-1} \{-x_1, \ldots, -x_n\}$. Since $x_i^{2k} = (-x_i)^{2k}$ for all $k \in \mathbb{N}$, this means we only need to consider solutions to $\sum_{i=1}^{n} x_i^e = 0$ for $e = 1, 3, \ldots, n-2$. For example, $\{3+3i, 3+4i, 3+5i, -2-8i, -7-4i\} =_4 \{-3-3i, -3-4i, -3-5i, 2+8i, 7+4i\}$ is an ideal symmetric solution of size 5.

Similarly, for even n, this means finding solutions $x_1, \ldots, x_{n/2}, y_1, \ldots, y_{n/2} \in \mathcal{O}$ such that $\{x_1, \ldots, x_{n/2}, -x_1, \ldots, -x_{n/2}\} =_{n-1} \{y_1, \ldots, y_{n/2}, -y_1, \ldots, -y_{n/2}\}$. As above, since $(-x_i)^{2e+1} = -x_i^{2e+1}$ for all $k \in \mathbb{N}$, we only need to consider solutions to $\sum_{i=1}^{n/2} x_i^e = \sum_{i=1}^{n/2} y_i^e$ for $e = 2, 4, \ldots, n-2$. For example, $\{\pm 1, \pm(4+i), \pm(3+i)\} =_5 \{\pm(7i), \pm(7+4i), \pm(7-3i)\}$ is an ideal symmetric solution of size 6.

Thus, the symmetric case of PTE problem involves half as many variables as the usual case. Some results concerning this case are discussed in [5, 9, 10].

In [5], BLP describe an algorithm for finding odd and even symmetric solutions to the $\mathbb{Z}$-PTE problem. We have adapted this algorithm for finding ordinary solutions as well as odd and even symmetric solutions to the $\mathbb{Z}[i]$-PTE problem. As the ideas behind the algorithms are not any different from the original, one may see [5] for an explanation. This was implemented first in *Maple* and then in `C++`, using the Class Library for Numbers.

The computer search was implemented to try to find solutions with real and imaginary parts between 0 and 30 for sizes 10 and 12. The above method is trivially parallelizable, so each search range was divided up into intervals, which were then submitted to a cluster of machines.

The following symmetric solutions of size 10 were found:

$$\begin{aligned}\{\pm(9+i), \pm(4+8i), \pm(8+4i), \pm(3-3i), \pm(1-9i)\} =_9 \\ \{\pm(5+7i), \pm 8, \pm(9+3i), \pm 8i, \pm(1-7i)\}\end{aligned}$$

which has constant

$$-(1+i)^{22}(2+i)^2(2-i)^2 3^2(3+2i)^2(3-2i)(4+i)(4-i)(5+2i),$$

and also

$$\begin{aligned}\{\pm(8+3i), \pm(9+4i), \pm(11+2i), \pm(1-7i), \pm(5+7i)\} =_9 \\ \{\pm(7+7i), \pm(11+1i), \pm(11+4i), \pm(1+6i), \pm 5i\}\end{aligned}$$

which has constant

$$i(1+i)^{13}(2+i)^2(2-i)^2 3^2(3+2i)^2(3-2i)(4+i)(4-i)(5+2i)(5-2i)(5+4i).$$

Additionally, by the remark at the end of Section 2, the complex conjugates of these solutions are also ideal PTE solutions of size 10. First note that none of these solutions lies on a line in the complex plane. Thus they cannot be equivalent to a $\mathbb{Z}$-PTE solution. By examining their constants and applying Proposition 2.1.2, they cannot be equivalent to each other either.

Further note that all the Gaussian integers in the first solution have norm ≤ 90, while in the second they all have norm ≤ 147. This contrasts with the ordinary integer case where from [5] there is no size 10 solution with height less than 313, and in fact, there are

only two inequivalent solutions with height less than 1500. This results corresponds to the intuition that Gaussian integer solutions should be "easier" to find.

We now explain the second column of Table 3.1 above, which lists the upper bounds for the divisibility of C_n.

For $n = 2$ and $n = 3$, the upper bound comes from Table 3.2.

For $n = 4$, the upper bound comes from the solution $\{0, 0, 0, 0\} =_3 \{1, -1, i, -i\}$.

For $n = 5$, the solutions

$$\{0, -5i, -3 - 4i, 1 + 3i, 1 + 3i\} =_4 \{-5 - 5i, 5, -4 + 3i, 1 - 7i, 2 + 6i\}$$

and

$$\{0, 2 - 4i, 3 - i, -6 - 3i, -4 - 7i\} =_4 \{-5 - 5i, -4 - 2i, 4 - 3i, -2 - 6i, 2 + i\}$$

have constants $-(1+i)^5(2-i)^2(2+i)^7$ and $i(1+i)^6(2-i)(2+i)^6$ respectively. The upper bound comes from taking the gcd of these constants, along with the constant associated to the complex conjugate of the second solution.

For $n = 6$, the solution

$$\{0, -5i, 2 - 4i, -4 - 2i, -6 + 2i, -4 + 3i, -5 - 5i\} =_5 \{-5 + 5i, 1 + 3i, -8 + i, 1 - 7i, 4 - 3i\}$$

has constant $-(1 + i)^4(2 - i)^2(2 + i)^8(-3 + 2i)$. The upper bound comes from taking the gcd of this constant and the constant associated to the complex conjugate of this solution.

For $n = 7$, the solution

$$\begin{aligned}\{3 + i, 2 + 4i, -3 - 4i, 2 - 3i, -5 + 2i, -5 + 3i, 6 - 3i\} =_6 \\ \{-3 - i, -2 - 4i, 3 + 4i, -2 + 3i, 5 - 2i, 5 - 3i, -6 + 3i\},\end{aligned}$$

has constant $(-i)(1 + i)^6(2 - i)^3(2 + i)^2 3(3 + 2i)(4 + i)(5 - 2i)$. The upper bound comes from taking the gcd of this constant and the constant associated to the complex conjugate of this solution.

For $n = 8$, the symmetric solution

$$\{\pm(2 + 2i), \pm 3, \pm 3i, \pm(2 - 2i)\} =_7 \{\pm 2, \pm 2i, \pm i, \pm 1\}$$

has constant $(1 + i)^8(2 - i)^2(2 + i)^2(3 + 2i)(-3 + 2i)$.

For $n = 10$, the upper bound is obtained taking the gcd of the constants from the solutions listed above, as well as their complex conjugates.

For $n = 9$ and $n = 12$, the upper bound is obtained from factoring the bounds listed in Table 3.2.

Note that for n in the range $4 \leq n \leq 8$, many other $\mathbb{Z}[i]$-PTE solutions are known, but they give no further information about the divisibility of C_n. In these cases, we have not been able to prove if these upper bounds are true in general.

Unfortunately, no new symmetric solutions of size 12 have been found. Considering that there is a symmetric solution of size 12 of height 151 in the integer case, the usual intuition implies that a Gaussian integer solution would not be much larger than the search range. However, the search for size 12 ideal solutions with real and imaginary parts between 0 and 30 took approximately 2 weeks on a cluster of 16 machines each with four 1Ghz. processors. Considering the magnitude of the solutions found in the integer case, this method does not seem likely to produce them in the Gaussian integer case.

Chapter 4

More Divisibility Results for C_n

As demonstrated in Chapter 3 (and as will be seen in Chapter 5), divisibility conditions for the constant C_n are important for searching for ideal PTE solutions computationally. In Chapter 3, we presented a number of such results over both general number fields and for quadratic number fields that are unique factorization domains. One of these results was a generalization of the "Multiplicity Lemma" of Rees and Smyth from [27].

First we review some other divisibility results for C_n from the literature. Most of these results rely on considering the existence of PTE solutions locally, that is, modulo a prime. The key observation is that every PTE solution over $\mathbb{Z}$ is also a PTE solution modulo any prime. Thus, given a prime p, if the constant corresponding to each local PTE solution is divisible by p, then $p \mid C_n$.

Thus, let p be a prime. Then we have four cases for p and n:

1. $p \leq n-1$.
2. $p = n$.
3. $p = n+1$.
4. $p \geq n+2$.

In the first case, we have Kleiman's result from [23] that $(n-1)! \mid C_n$. This gives that for every prime p with $p \leq n-1$, then p divides C_n. We further obtain higher powers for some of these primes.

The second case is determined by Theorem 4.0.2 below.

In the third case, with $n = p-1$, note that $\{0, \ldots, 0\} =_{p-2} \{1, \ldots, p-1\}$ is an ideal PTE solution of size $p-1$ modulo p. However, the corresponding constant is $1 \cdot 2 \cdots (p-1) \equiv -1 \pmod{p}$, and so we may not conclude $p \mid C_{n-1}$, by merely considering local PTE solutions alone. (Nevertheless, this "exceptional" local PTE solution is of interest for computation, as will be explained later.)

In the fourth case, Rees and Smyth prove in [27] that p divides C_n to at most the first power. They also prove the following results:

Theorem 4.0.1. *If p is a prime such that $pk < n$ for some positive integer k, then $p^{k+1} \mid C_n$.*

Theorem 4.0.2. *If $p > 3$ is prime and $n = p$, then $p \mid C_n$.*

Theorem 4.0.3. *We have $2^4 \mid C_5$ and $2^5 \mid C_6$.*

Theorem 4.0.4. *Let p be a prime satisfying*

$$n + 2 \leq p < n + 2 + \frac{n-3}{6}.$$

Then $p \mid C_n$.

In the same paper, Rees and Smyth also do some computations that prove the following divisibility results:

Theorem 4.0.5. *We have $11 \mid C_7$, $11 \mid C_8$, $13 \mid C_8$, $13 \mid C_9$ and $17 \mid C_{11}$.*

The proof of Theorem 4.0.4 and the algorithm on which Theorem 4.0.5 is based, rests upon the "Multiplicity Lemma", which is explained in the next section. Examining these results and extending the computations will be the main focus of this chapter.

Before proceeding further, we present Table 4.1, which summarizes these divisibility results. The second column contains a lower bound for C_n, and in particular, C_n must be divisible by this bound. This bound is derived theoretically, normally by local constraints, as described above. The third column contains an upper bound for C_n and C_n must divide this bound. This bound is derived by taking the gcd of constants constructed from explicit ideal PTE solutions of size n.

The bounds listed here largely come from [27] and [4], but have been updated to include new solution of size 12 found in [6, 29] and those explicitly given in [12].

Shuwen's solution from [29] is

$$\{\pm 35, \pm 47, \pm 94, \pm 121, \pm 146, \pm 148\} =_{11} \{\pm 22, \pm 61, \pm 86, \pm 127, \pm 140, \pm 151\},$$

which has constant $2^{12} \cdot 3^9 \cdot 5^3 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$. Meanwhile, Broadhurst's solution from [6] is

$$\begin{aligned}\{\pm 472, \pm 639, \pm 1294, \pm 1514, \pm 1947, \pm 2037\} &=_{11} \\ \{\pm 257, \pm 891, \pm 1109, \pm 1618, \pm 1896, \pm 2058\},&\end{aligned}$$

which has constant

$$2^{14} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 47 \cdot 61 \cdot 89 \cdot 191 \cdot 419.$$

In particular, the second constant has one less power of 3 than the constant coming from Shuwen's solution. The gcd of these constants is $2^{12} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$. It turns out that this number divides all the constants of all the solutions explicitly given in [12] as discussed in Chapter 6, and so it appears as the upper bound for C_{12} in the table.

The last column is third column divided by the second column. This indicates what is unknown about C_n in each case. For example, when the third column is 1 as in $n = 2, 3, 4, 5$, this shows the value of C_n is known exactly. Updated versions of this table will be found throughout the thesis to illustrate the progress that has been made.

We now proceed to improve the lower bounds for C_7.

4.1 $p = 2$

Following the methods of [27], we prove some divisibility results for $p = 2$ and $n = 7$. Recall we know that $2^4 \mid C_7$ since $6! \mid C_7$.

Theorem 4.1.1. $2^5 \mid C_7$.

Proof. Assume otherwise, that is, $C_7 \equiv 16 \pmod{32}$. Now suppose $\{x_1, \ldots, x_7\} =_6 \{y_1, \ldots, y_7\}$. Hence, we have

$$\prod_{i=1}^{7}(z - x_i) - \prod_{i=1}^{7}(z - y_i) \equiv 16 \pmod{32}. \tag{4.1}$$

Table 4.1: Divisibility Results for the $\mathbb{Z}$-PTE Problem

n	Lower bound for C_n	Upper bound for C_n	Upper bound divided by Lower Bound
2	1	1	1
3	2^2	2^2	1
4	$2^2 \cdot 3^2$	$2^2 \cdot 3^2$	1
5	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	1
6	$2^5 \cdot 3^2 \cdot 5^2$	$2^6 \cdot 3^2 \cdot 5^2$	2
7	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11$	$2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 19$	$2^2 \cdot 19$
8	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	$2^8 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	2^4
9	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	$2^9 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$ $\cdot 17 \cdot 23 \cdot 29$	$2^2 \cdot 3 \cdot 17 \cdot 23 \cdot 29$
10	$2^7 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 13$	$2^{11} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$ $\cdot 17 \cdot 23 \cdot 37 \cdot 53 \cdot 61 \cdot 79$ $\cdot 83 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 191$	$2^4 \cdot 3^2 \cdot 11 \cdot 17 \cdot 23 \cdot 37 \cdot 53$ $\cdot 61 \cdot 79 \cdot 83 \cdot 103 \cdot 107 \cdot 109$ $\cdot 113 \cdot 191$
11	$2^8 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$	none known	
12	$2^8 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 11^2$	$2^{12} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11^2 \cdot 13^2$ $\cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$	$2^4 \cdot 3^4 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29$ $\cdot 31$

Assume $y_1 = 0$. Then taking $z = 0$, we have $x_1 \cdots x_7 \equiv 16 \pmod{32}$. Without loss of generality, we may assume x_1, x_2, x_3, x_4 are even. Otherwise, suppose we have only x_1, x_2, x_3 even with x_4, x_5, x_6, x_7 odd. Since we know the y_i must match up with the x_i modulo 2, we must have y_2, y_3 even and y_4, y_5, y_6, y_7 odd. Now translating by $-x_4$, which does not change the constant, we obtain $x_1 - x_4, x_2 - x_4, x_3 - x_4, 0, x_5 - x_4, x_6 - x_4$, the first three of which are odd and the last three are even and $-x_4, y_2 - x_4, y_3 - x_4, y_4 - x_4, y_5 - x_4, y_6 - x_4, y_7 - x_4$, the first three of which are odd and the last four of which are even. Thus, we are now in exactly the same situation we have assumed above.

Since $x_1 \cdots x_7 \equiv 16 \pmod{32}$ and x_1, x_2, x_3, x_4 are even, they must each be congruent to 2 modulo 4. Further, we have x_5, x_6, x_7 are odd, and since we know the y_i must match up with the x_i modulo 2, we may assume that y_2, y_3, y_4 are even with y_5, y_6, y_7 odd.

Taking $z = x_1$, considering only the even factors in (4.1), we have

$$x_1(y_2 - x_1)(y_3 - x_1)(y_4 - x_1) \equiv 16 \pmod{32}.$$

We must have $y_i - x_1 \equiv 2 \pmod{4}$ for $i = 2, 3, 4$ and since $x_1 \equiv 2 \pmod{4}$, we must have $y_2, y_3, y_4 \equiv 0 \pmod{4}$.

Similarly, taking $z = x_5$, we have

$$x_5(x_5 - y_5)(x_5 - y_6)(x_5 - y_7) \equiv 16 \pmod{32}.$$

Since x_5 is odd, without loss of generality, we may assume $x_5 - y_5 \equiv 4 \pmod 8$ and so $x_5 - y_6, x_5 - y_7 \equiv 2 \pmod 4$. Thus, $x_5 \equiv y_5 \pmod 4$ and $y_6 \equiv y_7 \pmod 4$.

Further, taking $z = y_6$, we have

$$y_6(y_6 - x_5)(y_6 - x_6)(y_6 - x_7) \equiv 16 \pmod{32}.$$

Since $y_6 - x_5 \equiv 2 \pmod 4$, without loss of generality we may assume $y_6 - x_6 \equiv 4 \pmod 8$ and $y_6 - x_7 \equiv 2 \pmod 4$. Since $y_6 \equiv y_7 \pmod 4$ from above, it follows that $x_7 - y_7 \equiv 2 \pmod 4$. Thus we have

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 - (y_1 + y_2 + y_3 + y_4 + y_5 + y_6 + y_7) \\ &\equiv 2 + 2 + 2 + 2 + x_5 + x_6 + x_7 - (0 + 4 + 4 + 4 + y_5 + y_6 + y_7) \pmod 4 \\ &\equiv (x_5 - y_5) + (x_6 - y_6) + (x_7 - y_7) \pmod 4 \\ &\equiv 0 + 0 + 2 \equiv 2 \pmod 4, \end{aligned}$$

which is a contradiction since $\{x_1, \ldots, x_7\} =_6 \{y_1, \ldots, y_7\}$, proving the result. □

Using the same argument, we extend this result to obtain the following:

Theorem 4.1.2. $2^6 \mid C_7$.

Proof. Assume otherwise, that is, $C_7 \equiv 32 \pmod{64}$. Now suppose $\{x_1, \ldots, x_7\} =_6 \{y_1, \ldots, y_7\}$. Hence, we have

$$\prod_{i=1}^{7}(z - x_i) - \prod_{i=1}^{7}(z - y_i) \equiv 32 \pmod{64}. \tag{4.2}$$

Assume $y_1 = 0$. Then taking $z = 0$, we have $x_1 \cdots x_7 \equiv 32 \pmod{64}$. Without loss of generality, using the same argument as in the proof above, we may assume one of the two cases: (1) x_1, x_2, x_3, x_4, x_5 all congruent to 2 modulo 4 or (2) $x_1 \equiv 4 \pmod 8$ and $x_2, x_3, x_4 \equiv 2 \pmod 4$

For (1), we have x_6, x_7 odd, and as above, assume y_2, y_3, y_4, y_5 are even and y_6, y_7 are odd. Taking $z = x_1$, again considering only the even factors in (4.2), we have

$$x_1(x_1 - y_2)(x_1 - y_3)(x_1 - y_4)(x_1 - y_5) \equiv 32 \pmod{64}.$$

We must have $x_1 - y_i \equiv 2 \pmod 4$ for $i = 2, \ldots, 5$ and so $y_2, y_3, y_4, y_5 \equiv 0 \pmod 4$.

Similarly, taking $z = x_6$, we have

$$(x_6 - y_6)(x_6 - y_7) \equiv 32 \pmod{64}.$$

As both factors are even, we have one of two cases: (i) $x_6 - y_6 \equiv 2 \pmod 4$ and $x_6 - y_7 \equiv 16 \pmod{32}$ and (ii) $x_6 - y_6 \equiv 4 \pmod 8$ and $x_6 - y_7 \equiv 8 \pmod{16}$.

Taking $z = y_7$, we have

$$(y_7 - x_6)(y_7 - x_7) \equiv 32 \pmod{64}.$$

In case (i), as $x_6 - y_7 \equiv 16 \pmod{32}$, we must have $y_7 - x_7 \equiv 2 \pmod 4$ while in case (ii), we must have $y_7 - x_7 \equiv 4 \pmod 8$.

Taking $z = x_7$, we have

$$(x_7 - y_6)(x_7 - y_7) \equiv 32 \pmod{64}.$$

In case (i), as $x_7 - y_7 \equiv 2 \pmod 4$, we must have $x_7 - y_6 \equiv 16 \pmod{32}$, while in case (ii), we must have $x_7 - y_6 \equiv 8 \pmod{16}$.

Now note that if $a \equiv 2 \pmod 4$ then $a^2 \equiv 4 \pmod 8$. We consider the sums of squares of x_i and y_i modulo 8. In both case (i) and (ii) we have

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 - (y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2 + y_7^2) \\ &\equiv 5 \cdot 4 + x_6^2 + x_7^2 - (0 + 4 \cdot 16 + y_6^2 + y_7^2) \pmod 8 \\ &\equiv 4 + x_6^2 + x_7^2 - y_6^2 - y_7^2 \pmod 8. \end{aligned}$$

In case (i), we may rewrite the last line above as $4 + (x_6 - y_7)(x_6 + y_7) + (x_7 - y_6)(x_7 + y_6)$. Since we have $x_6 - y_7 \equiv 8 \pmod{16}$ and $x_7 - y_6 \equiv 16 \pmod{32}$, both the second and third terms are congruent to 0 modulo 8.

In case (ii), we may rewrite the last line above as $4 + (x_6 - y_6)(x_6 + y_6) + (x_7 - y_7)(x_7 + y_7)$ where we have $y_7 - x_7 \equiv 4 \pmod 8$ and $x_6 - y_6 \equiv 4 \pmod 8$. Since the respective sums are also even, again both the second and third terms are congruent to 0 modulo 8.

Thus, in either case, the above sum is congruent to 4 modulo 8, which is a contradiction.

For (2), we have x_5, x_6, x_7 odd and y_2, y_3, y_4 even and y_5, y_6, y_7 odd. Taking $z = x_1$, again considering only the even factors in (4.2), we have

$$x_1(x_1 - y_2)(x_1 - y_3)(x_1 - y_4) \equiv 32 \pmod{64}.$$

Since $x_1 \equiv 0 \pmod 4$, it follows that $x_1 - y_2, x_1 - y_3, x_1 - y_4 \equiv 2 \pmod 4$, and so $y_2, y_3, y_4 \equiv 2 \pmod 4$. Since $x_2, x_3, x_4 \equiv 2 \pmod 4$ also, translating this solution by 2, which does not change the constant, makes x_2, x_3, x_4 and y_2, y_3, y_4 all multiples of 4, and so $(2^2)^3 \mid C_7$, which is a contradiction.

Thus, in both cases (1) and (2), we have obtained a contradiction, proving the result. □

We now proceed to the introduce the "Multiplicity Lemma" to deal with the case of $p \geq n + 2$.

4.2 The "Multiplicity Lemma" and related results

In this section, we describe the "Multiplicity Lemma" of Rees and Smyth [27] and some related results also from Rees and Smyth. This section will also describe an algorithm that these results yield. For convenience, we repeat the proofs of each result. First, we have the following:

Lemma 4.2.1 (Multiplicity Lemma)**.** *Let p be a prime with $p > n$. Suppose that $q_1(x)$ and $q_2(x)$ are monic polynomials of degrees n in $(\mathbb{Z}/p\mathbb{Z})[x]$, both having all zeros in $\mathbb{Z}/p\mathbb{Z}$. Further, suppose*

$$q_1(x) - q_2(x) = C$$

in $(\mathbb{Z}/p\mathbb{Z})[x]$, where C is some integer with $C \not\equiv 0 \pmod p$. For $i = 1, 2$, let $M_i(a)$ denote the multiplicity of a zero $a \in \mathbb{Z}/p\mathbb{Z}$ of $q_i(x)$. Then we have

$$M_1(x) - M_2(x) \equiv h(x) \pmod p,$$

where $h(x)$ is some polynomial of degree exactly $k = p - n - 1$.

Proof. First we show that $M_1(x)$ must be of the form

$$M_1(x) = (x - x^p)\frac{q_1'(x)}{q_1(x)}$$

in $(\mathbb{Z}/p\mathbb{Z})[x]$. Note that $p > n$ and so $\deg q_1'(x) = \deg q_1(x) - 1$. Since $q_1(x)$ is monic and has all roots in $\mathbb{Z}/p\mathbb{Z}$, we may write it as

$$q_1(x) = \prod_{a=0}^{p-1}(x - a)^{m_a},$$

where m_a are nonnegative integers. Then since

$$q_1'(x) = \sum_{a=0}^{p-1} \frac{m_a}{x-a} q_1(x),$$

it follows that

$$\begin{aligned}(x-x^p)\frac{q_1'(x)}{q_1(x)} &= (x-x^p)\sum_{a=0}^{p-1}\frac{m_a}{x-a} = \sum_{a=0}^{p-1}\frac{m_a(x-a+a-x^p)}{x-a} \\ &= \sum_{a=0}^{p-1}\frac{m_a\left((x-a)-(x^p-a^p)\right)}{x-a} = \sum_{a=0}^{p-1}\frac{m_a\left((x-a)-(x-a)^p\right)}{x-a} \\ &= \sum_{a=0}^{p-1} m_a(1-(x-a)^{p-1}).\end{aligned}$$

It is clear that the last line of the above equation is equal to m_a whenever $x = a$, which is what we wanted to show. Similarly, we have

$$M_2(x) = (x-x^p)\frac{q_2'(x)}{q_2(x)}.$$

Since we assumed $q_1(x) - q_2(x) \equiv C \pmod{p}$, it follows that all their coefficients except the constant term are equivalent modulo p. Therefore, we have $q_1'(x) \equiv q_2'(x) \pmod{p}$ and so

$$\begin{aligned}M_1(x) - M_2(x) &\equiv (x-x^p)\left(\frac{q_1'(x)}{q_1(x)} - \frac{q_1'(x)}{q_2(x)}\right) \equiv (x-x^p)\left(\frac{q_1'(x)(q_2(x)-q_1(x))}{q_1(x)q_2(x)}\right) \\ &\equiv \frac{-C(x-x^p)q_1'(x)}{q_1(x)q_2(x)}.\end{aligned}$$

We write $h(x) = M_1(x) - M_2(x)$. Further, since $C \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, the numerator has degree $p+n-1$, the denominator has degree $2n$, and $p > n$, it follows that $h(x)$ is a nonzero polynomial of degree $p-n-1$, proving the result. □

Remark 4.2.2. Note that Lemma A.2.7 in Appendix 2 is a generalized version of the "Multiplicitly Lemma" for rings of integers of number fields that are unique factorization domains.

In [27], Rees and Smyth show that the "Multiplicity Lemma" has the following consequences:

Corollary 4.2.3. *If $C \not\equiv 0 \pmod{p}$, then for each $a \in \mathbb{Z}/p\mathbb{Z}$, we have $h(a) = M_1(a)$ or $h(a) = -M_2(a)$ for $a \in \mathbb{Z}/p\mathbb{Z}$.*

Proof. We may also write $q_1(x) = \prod_{i=1}^{n}(x - a_i)$ and so $m_a = 0$ for $a \neq a_1, \ldots, a_n$ and is nonzero otherwise. Similarly, the same is true for $q_2(x)$. Thus, since $C \not\equiv 0 \pmod{p}$, we have $\gcd(q_1(x), q_2(x)) = 1$, and so it follows that at least one of $M_1(x)$ and $M_2(x)$ is always zero, proving the result. □

Remark 4.2.4. The choice of $h(a) = M_1(a)$ or $h(a) = -M_2(a)$ depends on a and may differ for different a.

We need some more notation, again following [27]. First, let p be an odd prime. Given $a \in \mathbb{Z}/p\mathbb{Z}$, let $\langle a \rangle_p$ be the integer congruent to a modulo p in the interval $(-p/2, p/2)$. Secondly, for a polynomial $H(x)$, define $S(H, p)$ to be the sum

$$S(H, p) := \sum_{a=0}^{p-1} \left| \langle H(a) \rangle_p \right|.$$

We may now state the following:

Corollary 4.2.5. *For $h(x)$ from the "Multiplicity Lemma" and $C \not\equiv 0 \pmod{p}$, we have*

$$S(h, p) \leq 2n.$$

Proof. If $M_i(a) > 0$, then from the Corollary above, we have

$$M_i(a) = \pm h(a) = \pm \langle h(a) \rangle_p + \lambda p \geq \left| \langle h(a) \rangle_p \right|,$$

where λ is some nonnegative integer. Summing both sides of this inequality over $i = 1, 2$ and $a = 0, \ldots, p-1$ and noting that the polynomials $q_1(x)$ and $q_2(x)$ have $2n$ roots counting multiplicity, proves the result. □

In the next section, we proceed to describe an algorithm that uses Corollary 4.2.3 and the contrapositive of Corollary 4.2.5 to prove more divisibility results for C_n.

4.3 An Algorithm

Rees and Smyth note that Corollary 4.2.5 above yields an algorithm for computing divisors of C_n:

Let p be a prime with $p > n+1$ and suppose $a_1, \ldots, a_n, b_1, \ldots, b_n$ are in $\mathbb{Z}/p\mathbb{Z}$. We set $f(x) := (x-a_1)\ldots(x-a_n)$ and $g(x) := (x-b_1)\ldots(x-b_n)$. Now suppose that there exists $C \in \mathbb{Z}/p\mathbb{Z}$ with $C \neq 0$ such that

$$f(x) - g(x) = C.$$

That is, we have an ideal PTE solution of size n and constant C in $\mathbb{Z}/p\mathbb{Z}$. Further, it is clear we may apply the "Multiplicity Lemma" with $q_1(x) = f(x)$ and $q_2(x) = g(x)$ and obtain some polynomial $h(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ of degree $p-n-1$.

Corollary 4.2.5 above says that if $C \not\equiv 0 \pmod{p}$, then $S(h,p) \leq 2n$. From the contrapositive of this statement, it follows that if $S(h,p) > 2n$, then $p \mid C$.

Thus, if we construct all polynomials $h(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ of degree exactly $p-n-1$ that may possibly arise from an ideal PTE solution of size n modulo p, and every one of these polynomials satisfies $S(h,p) > 2n$, then we must have $p \mid C_n$.

In [27], Rees and Smyth considered this for some values of n and p that gave values of $p-n-1$ less than 5. We summarize their results in Table 4.2 below. Here, we define

$$m_{n,p} := \min_h S(h,p),$$

where the minimum is taken over all polynomials $h \in (\mathbb{Z}/p\mathbb{Z})[x]$ of degree exactly $p-n-1$.

In [27], Rees and Smyth note that given any polynomial $h(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ and $a, b \in \mathbb{Z}/p\mathbb{Z}$, so long as $a \not\equiv 0 \pmod{p}$, the sets of values $\{h(x) | x = 0, \ldots, p-1\}$ and $\{h(ax+b) | x = 0, \ldots, p-1\}$ are equal. Because our computation of $S(h,p)$ depends only on the set of values of $\{h(x) | x = 0, \ldots, p-1\}$, any such affine transformation $x \mapsto ax+b$ on $h(x)$ preserves $S(h,p)$. Therefore, we may reduce the polynomials $h(x)$ we must consider.

Suppose $h(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0$ is a polynomial in $(\mathbb{Z}/p\mathbb{Z})[x]$ of degree exactly $d = p-n-1$, so $a_d \neq 0$. As $p > n+1$, we have $1 \leq d = p-n-1 < p$, so d has a multipliciative inverse modulo p and so mapping $x \mapsto x - \frac{a_{d-1}}{d a_d}$ eliminates the x^{d-1} term.

Further, if every nonzero integer has a dth root modulo p, then we may substitute

$$x \mapsto \frac{x}{a_d^{1/d}}.$$

Note that this condition is equivalent to every integer occuring as a dth power modulo p, which is easy to check. For example this is true for $n = 7$ and $p = 11$ ($d = 3$), but for $n = 8$ and $p = 11$ ($d = 2$), only $1, 3, 4, 5, 9$ appear as a square modulo p.

If there is a nonzero integer that does not have a dth root modulo p, we may make a different substitution. If $a_1 \neq 0$, then we may substitute $x \mapsto x/a_1$. Thus, in this case, we need only consider $h(x)$ with degree 1 coefficients that are 0 or 1.

We will call the set of polynomials $\{x^d + a_{d-2}x^{d-2} + a_{d-3}x^{d-3} + \cdots + a_1x + a_0 \,|\, a_i \in \mathbb{Z}/p\mathbb{Z}\}$ "Type 1" polynomials and call $\{a_dx^d + a_{d-2}x^{d-2} + a_{d-3}x^{d-3} + \cdots + a_1x + a_0 \,|\, a_i \in \mathbb{Z}/p\mathbb{Z}, a_1 = 0, 1\}$ "Type 2" polynomials.

Thus, we have the following algorithm:

Algorithm 4.3.1. *Given a positive integer n and prime p with $p > n$ and a Boolean variable t that represents whether or not every nonzero element in $\mathbb{Z}/p\mathbb{Z}$ has a $(p-n-1)$th root, this algorithm computes $m_{n,p}$ as defined above and lists all polynomials $h(x) \in \mathbb{Z}/\mathbb{Z}_p[x]$ with $m_{n,p} = S(h, p)$.*

Input: n, p, t.
Output: $m_{n,p}$ as defined above and a list of all polynomials $h(x) \in \mathbb{Z}/\mathbb{Z}_p[x]$ (up to the above equivalence) with $m_{n,p} = S(h, p)$.

1. As a precomputation, compute all values $r \cdot s^w \pmod p$, where $0 \leq r \leq p-1$, $0 \leq s \leq p-1$, $0 \leq w \leq p-n-1$ and store them in a three-dimensional array.

2. Set $m = 10000$ and $a = 0$, and create the arrays `coeff` with $p-n$ entries and `values` with p entries, initializing each entry to 0.

3. Loop over all i from 0 to $p-1$, set $\texttt{coeff}[a] = i$ and within this loop, loop over all j from 0 to $p-1$ setting $\texttt{values}[j] = (\texttt{values}[j] + i \cdot j^a) \pmod p$. Increment a by 1 and repeat until $a = p - n$.

3a. Set $s = 0$. Loop over all i from 0 to $p-1$, and if $\texttt{values}[i] < p/2$, then set $s := s + \texttt{values}[i]$, otherwise set $s := s - (\texttt{values}[i] - p)$.

3b. If $s \leq m$, print s and `coeffs`.

To further explain this algorithm, we make the following remark, where each point corresponds to a step in the algorithm:

Remark 4.3.1.

1. Precomputing these values yields a substantial computational saving since within the loop, we may simply lookup values rather than repeatedly multiplying, exponentiating and reducing modulo p. Thus, the resulting algorithm only requires addition modulo p.

2. We choose $m = 10000$ simply as a large number that is certainly bigger than $m_{n,p}$. The array `coeff` will store the coefficients of $h(x)$, while the array `values` is precomputing evaluations of $h(x)$ at each element of $\mathbb{Z}/p\mathbb{Z}$ for $S(h,p)$. This also yields a substantial computational savings.

3. Loops are omitted in this step according to the Boolean variable t, so if $t = 1$, then we loop over all polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$ of the form $x^{p-n-1} + a_{p-n-3}x^{p-n-3} + \cdots a_0$ and otherwise, we loop over all polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$ of the form $a_{p-n-1}x^{p-n-1} + a_{p-n-3}x^{p-n-3} + \cdots + \epsilon x + a_0$, where $\epsilon = 0, 1$. Note the value $i \cdot j^a$ comes from the (i, j, a)th entry from the lookup table, and 0^0 is interpreted as 1.

3a. This step computes $S(h,p)$.

Thus, we have the following table where $(*)$ denotes the information that came from Rees and Smyth in [27], and ?? denotes a partial result of a computation that terminated after a week of computation. We use "Type 1" and "Type 2" as described before. The second last column gives the number of polynomials $h(x)$ found by the search with $S(h,p) = m_{n,p}$. Note that this number is up to the above equivalence. The last column of the table indicates whether the computation yields $p \mid C_n$, and if not, indicates whether the computation was incomplete or completed and remaining unknown.

Note that in the case of $n = 7$ and $p = 17$ and $n = 9$ and $p = 19$, it does not matter that the computation was incomplete, since it is known from Table 4.1 that these primes do not occur as factors of C_n in the respective cases. In other cases where we know the primes do not occur in the upper bounds for C_n, that is, as $n = 7$ and $p = 13$, $n = 8$ and $p = 17$, $n = 9$ and $p = 19$, and $n = 10$ and $p = 19$, we have included the computations for verification purposes.

The cases of $n = 9$ and $p = 17$ and $n = 11$ and $p = 23$ are examined in the section below. The question of whether 19 divides C_7 is addressed in the next chapter.

Table 4.2: Computing $m_{n,p}$

n	p	$m_{n,p}$	Type of Polynomial	A polynomial $h(x)$ with $S(h,p) = m_{n,p}$	# of $h(x)$ with $S(h,p) = m_{n,p}$	$p \mid C_n$?
7	11	16	Type 1	$x^3 + 6x$	1	Yes $(*)$
7	13	14	Type 1	$x^5 + 12x^3 + x^5$	1	No
7	17	≤ 16	Type 1	$3x + 4x^3 + 9x^5 + x^7 + x^9$	??	No
8	11	23	Type 1	$x^2 + 8$	11	Yes $(*)$
8	13	20	Type 2	$2x^4 + 2x^2$	24	Yes $(*)$
8	17	16	Type 2	x^8	22	No
9	13	24	Type 2	$4x^3 + 6$	8	Yes $(*)$
9	17	18	Type 1	$x + 7x^3 + 7x^5 + x^7$	1	Unknown
9	19	≤ 18	Type 2	$x + 7x^3 + 7x^5 + x^7$	?	No
10	13	32	Type 2	x^2	13	Yes $(*)$
10	17	24	Type 2	$4 + 3x^2 + 14x^4 + 13x^6$	16	Yes
10	19	20	Type 2	$2 + 2x^2 + 6x^4 + 17x^6 + 13x^8$	20	No
10	23	≤ 44	Type 2	??	??	Incomp.
11	17	30	Type 1	$x^5 + 12x^3 + 3x$	1	Yes $(*)$
11	19	28	Type 1	$3x + 18x^3 + 15x^5 + x^7$	2	Yes
11	23	≤ 22	Type 2	x^{11}	??	Unknown
12	17	37	Type 2	$12 + x^2 + 5x^4$	16	Yes
12	19	32	Type 2	$2 + x^2 + 16x^4 + 6x^6$	18	Yes
12	23	≤ 24	Type 2	$2 + x^2 + 8x^4 + 18x^6 + 2x^8 + 15x^{10}$	??	Unknown

Thus, we have the following Theorem:

Theorem 4.3.2. *We have* $17 \mid C_{10}$, $19 \mid C_{11}$, $17 \mid C_{12}$, *and* $19 \mid C_{12}$.

Hence, we may update Table 4.1 above to indicate the new results, where boxes and strike- throughs highlight the changed results:

Table 4.3: Divisibility Results for the $\mathbb{Z}$-PTE Problem

n	Lower bound for C_n	Upper bound for C_n	Upper bound divided by Lower Bound
2	1	1	1
3	2^2	2^2	1
4	$2^2 \cdot 3^2$	$2^2 \cdot 3^2$	1
5	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	1
6	$2^5 \cdot 3^2 \cdot 5^2$	$2^6 \cdot 3^2 \cdot 5^2$	2
7	$\boxed{2^6} \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11$	$2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 19$	$\cancel{2^2} \cdot 19$
8	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	$2^8 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	2^4
9	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	$2^9 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$ $\cdot 17 \cdot 23 \cdot 29$	$2^2 \cdot 3 \cdot 17 \cdot 23 \cdot 29$
10	$2^7 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot \boxed{17}$	$2^{11} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$ $\cdot 17 \cdot 23 \cdot 37 \cdot 53 \cdot 61 \cdot 79$ $\cdot 83 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 191$	$2^4 \cdot 3^2 \cdot 11 \cdot \cancel{17} \cdot 23 \cdot 37 \cdot 53$ $\cdot 61 \cdot 79 \cdot 83 \cdot 103 \cdot 107 \cdot 109$ $\cdot 113 \cdot 191$
11	$2^8 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$ $\cdot 17 \cdot \boxed{19}$	none known	
12	$2^8 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 11^2$ $\cdot \boxed{17} \cdot \boxed{19}$	$2^{12} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11^2 \cdot 13^2$ $\cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$	$2^4 \cdot 3^4 \cdot 13^2 \cdot \cancel{17} \cdot \cancel{19} \cdot 23 \cdot 29$ $\cdot 31$

We next describe a further extension to this algorithm.

4.3.1 A Further Extension

Suppose n and p are such that $m_{n,p} \leq 2n$, that is

$$2n \geq m_{n,p} = \min_h S(h,p).$$

In this case, we are not able to apply Corollary 4.2.5 to conclude that $p \mid C_n$. Let $H \subseteq (\mathbb{Z}/p\mathbb{Z})[x]$ be the set of all polynomials $h(x)$ with $S(h,p) = 2n$. We may every $h(x) \in H$ as arising from an ideal PTE solution modulo p. We may attempt to eliminate a particular $h(x) \in H$ from consideration by showing the possible ideal PTE solutions modulo p from which it arises does not have a constant that is not divisible by p.

From Corollary 4.2.3 above, we have either $h(a) = m_a$ or $h(a) = -m_b$ or 0, and this helps us to determine any corresponding PTE solutions.

An obvious case to apply this extension is for $n = 9$ and $p = 17$. Here $m_{n,p} = 18$, so we may not conclude that $17 \mid C_9$, but from our computation, there is only one polynomial,

up to transformation, $h(x)$ with $S(h,p) = m_{n,p}$, namely $h(x) = x + 7x^3 + 7x^5 + x^7$. It has the following table of values modulo 17:

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$h(a) \pmod{17}$	0	16	2	0	0	2	0	15	15	2	2	0	15	0	0	15	1

As mentioned above, since $h(a) = m_a$ or $h(a) = -m_b$ or 0, we interpret the values of 15 and 16 as -2 and -1, respectively, and so the corresponding PTE solution modulo 17 would be

$$\{1, 7, 7, 8, 8, 12, 12, 15, 15\} =_8 \{2, 2, 5, 5, 9, 9, 10, 10, 16\}.$$

It turns out that this is an ideal PTE solution of size 9 modulo 17, with kth powers each summing to $0, 13, 0, 14, 0, 6, 0, 1$ modulo 17, and has constant $88646400 = 2^8 \cdot 3^6 \cdot 5^2 \cdot 19$ which is not divisible by 17. Thus, we may not conclude that $17 \mid C_9$. However, this "exceptional" local solution will be useful later. Further note that this is easily observed to be a symmetric solution by subtracting 17 from every entry in the right hand side. Thus, this solution also shows that if we restrict C_9 to symmetric solutions only, we may not conclude that $17 \mid C_9$.

We may also apply this extension to the case of $n = 11$ and $p = 23$, where $m_{n,p}$ was found to be no more than 22. One example of $h(x)$ with $S(h,p) = 22$ is $h(x) = x^{11}$, which has the following values modulo 23:

$$h(x) = \begin{cases} 1, & \text{when } x = 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18; \\ 22, & \text{when } x = 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22. \end{cases}$$

Again interpreting 22 as -1, the corresponding PTE solution modulo 23 is

$$\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\} =_{10} \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}.$$

Again, it turns out that this is an ideal PTE solution of size 11 modulo 23, with kth powers all summing to 0 modulo 23. The corresponding constant is

$$-2412518606496 = -1 \cdot 2^5 \cdot 3^2 \cdot 43 \cdot 194809319.$$

Thus, we may not conclude that $23 \mid C_{11}$.

Another case to apply this extension is when $n = 12$ and $p = 23$, where $m_{n,p}$ was found to be no more than 24. One example of $h(x)$ with $S(h,p) = 24$ is $h(x) = 2 + x^2 + 8x^4 + 18x^6 + 2x^8 + 15x^{10}$, which has the following values modulo 23:

$$h(x) = \begin{cases} 0, & \text{when } x = 1, 2, 6, 7, 13, 16, 17, 21, 22; \\ 1, & \text{when } x = 8, 15; \\ 2, & \text{when } x = 0, 4, 5, 18, 19; \\ 21, & \text{when } x = 3, 9, 11, 12, 14, 20. \end{cases}$$

Again interpreting 21 as -2, the corresponding PTE solution modulo 23 is

$$\{0, 0, 4, 4, 5, 5, 8, 15, 18, 18, 19, 19\} =_{11} \{3, 3, 9, 9, 11, 11, 12, 12, 14, 14, 20, 20\}.$$

Again, it turns out that this is an ideal PTE solution of size 11 modulo 23, with kth powers summing to $0, 16, 0, 9, 5, 20, 0, 17, 0, 20, 0$ modulo 23. The corresponding constant is $2^{10} \cdot 3^8 \cdot 5^2 \cdot 7^2 \cdot 11^2$, and so we may not conclude that $23 \mid C_{12}$. Further note that this is easily observed to be a symmetric solution. This solution also shows that if we restrict C_{12} to symmetric solutions only, we may not conclude that $23 \mid C_{12}$.

4.4 Further Work

It is likely possible to extend the above results for $n = 7$ and $p = 2$ for larger n.

The search for $n = 10$ and $p = 23$ was incomplete and so this case could be further explored.

Since it is possible to generalize the "Multiplicity Lemma" to appropriate rings of integers of number fields (see Lemma A.2.7 in Appendix 2), it is likely this algorithm could be extended in that direction as well.

Additionally, we could use the profiles of the $h(x)$ found above with $S(h, p) = 2n$ to implement a search that would look for examples with $p \nmid C$.

To obtain results for powers of primes, we could search for ideal PTE solutions locally and then examine the corresponding constants. However, since there is no corresponding $h(x)$ polynomial, it is computationally demanding.

Since there are new prime divisors of C_n obtained in Theorem 4.3.2, this result could dramatically improve the BLP algorithm described in Chapter 3. For the computations that are incomplete or unknown, one could assume that these prime factors of C_n do exist, and attempt to find examples anyway.

Chapter 5

Another Computational Search

In the previous chapter, we examined divisibility results for C_n and presented tables which included information about upper bounds for what C_n must itself divide. In this chapter, we focus on lowering this upper bound through further computation.

In particular, we present a new algorithm which given a positive integer C finds any ideal PTE solutions of size n with constant C translated so that all values in the solution are nonnegative and the least value is 0, if they exist.

Thus, we may find the smallest constant C for which an ideal PTE solution exists, which is a question that has not been addressed in the literature. No other algorithm in the literature is as conclusive in this respect. The solutions we find also provide information that often lowers the upper bounds mentioned above.

We also work with some parametrized families of ideal PTE solutions to lower these upper bounds.

Some ideas in this chapter are from personal communication with Cameron L. Stewart [34].

5.1 A new algorithm

Let n be a positive integer and suppose $\{x_1, \ldots, x_n\} =_{n-1} \{y_1, \ldots, y_n\}$. Put

$$f(z) = \prod_{i=1}^{n}(z - x_i), \quad g(z) = \prod_{i=1}^{n}(z - y_i),$$

and so

$$f(z) - g(z) = C_{n,X,Y} = (-1)^n(x_1 \cdots x_n - y_1 \cdots y_n). \tag{5.1}$$

Without loss of generality, we may assume that y_1 is zero and that all x_i and the remaining y_i are positive. Since $y_1 = 0$, we see that $C_{n,X,Y} = (-1)^n x_1 \cdots x_n$. From the Interlacing Theorem (Theorem 2.1.3), we may also order the x_i and y_i as

$$0 < x_1 \leq x_2 < y_2 \leq y_3 < x_3 \leq x_4 < \cdots < x_{n-1} \leq x_n < y_n, \; n \text{ even},$$

$$0 < x_1 \leq x_2 < y_2 \leq y_3 < x_3 \leq x_4 < \cdots < x_{n-1} < y_{n-1} \leq y_n < x_n, \; n \text{ odd}.$$

Note that $C_{n,X,Y} \neq 0$, since $\{x_1, \ldots, x_n\}$ and $\{0, y_2, \ldots, y_n\}$ are disjoint.

For each positive integer $C = (-1)^n C_{n,X,Y}$, we can determine if there is a solution of (5.1) by first finding each representation of C as a product of n positive integers $x_1, \ldots, x_n$. For each representation, we then compute the polynomial

$$g(z) = f(z) - (-1)^n C = \prod_{i=1}^{n} (z - y_i),$$

and check to see whether or not $g(z)$ factors completely over $\mathbb{Q}$. That is, whether $g(z)$ has n non-negative integer roots. Since $y_2, \ldots, y_n$ must be positive, it suffices to check whether $g(z)/z$ has $n-1$ positive integer roots. If this is the case, then we have found an ideal PTE solution.

In practice, we rarely need to factor $g(z)$, since we may further exploit the interlacing of the roots, as given above. For example, we know $x_2 < y_2 \leq y_3 < x_3$, so $g(z)$ must have an integer root in the interval (x_2, x_3).

Thus, if we determine the integer i such that $x_{2i+1} - x_{2i}$ is minimized, we may simply test all integers in (x_{2i}, x_{2i+1}) to see if $g(z) = 0$. As above, if a root exists in this range, then we may try factoring $g(z)/z$ and seeing if it has $n-1$ positive integer roots. This was the method chosen for the algorithm for reasons that will be detailed below.

Thus, using this method, we can find all solutions of (5.1) for a fixed $C_{n,X,Y}$.

5.2 Details of the Algorithm

We now provide a step by step explanation of the algorithm. We first describe a precomputation. Its importance will be explained later.

Note that from the remark following the Interlacing Theorem, Theorem 2.1.3, it follows that the largest possible x_i will occur when the product of the other x_i's are as small as possible. This product will be minimized when $x_0 = x_1 = 1$, $x_2 = 3, x_3 = 3$, $x_4 = 5$, $x_5 = 5$ and so on. That is, given x_i, we pick x_{i+1} to be the next smallest possible integer, given the previous x_i's and our restrictions.

For example, for $n = 6$, the smallest possible x_i's are $1, 1, 3, 3, 5$, for $n = 7$, the smallest possible x_i's are $1, 1, 3, 3, 5, 5$, and so on. Since we assume that C_n divides C, so far these numbers have not depended on the choice of C, since we already know they appear as factors.

Thus, in the case $n = 6$, we only need to consider divisors of C up to and including $C/45$. This reduces the size of the loop slightly. However, we also note $C/45$ can only occur among the x_i when it is x_6 and in this case we must have $x_0 = x_1 = 1$, $x_2 = 3, x_3 = 3$, and $x_4 = 5$. Thus, we may check to see if $\{1, 1, 3, 3, 5, C/45\}$ corresponds to an ideal PTE solution of size 6 and constant C, and we no longer need to consider $C/45$ as a possible x_i.

Thus, we have eliminated the previously largest possible value for x_i. Continuing in this fashion for other large divisors of C, we can pre-check whether or not these occur as part of a PTE solution with constant C, and greatly reduce the size of the subsequent loops in the computation.

In general, this precomputation proceeds as follows:

Algorithm 5.2.1. *Given positive integers C, n and g with $g \mid C$, this algorithm outputs all ideal* PTE *solutions of size n and constant C where the largest x_i is greater than or equal to g, if any exist.*

Input: n, C, g

Output: All ideal PTE *solutions of size n and constant C where the largest x_i is greater than or equal to g, if any exist, and up to the above normalization.*

1. Set $k := 1$. (k will keep track of the number of x_i selected so far.)

2. If $k < n - 2$, compute the divisors of $C/(\prod_{i=1}^{k} x_i)$ and store them in an ordered list `X`. Set i to be the index of least element of `X` that is greater than or equal to x_k. Loop from $j = i$ so long as $\texttt{X}[j] < (C/(g \prod_{i=1}^{k} x_i))^{1/(n-k-1)}$ and set $x_{k+1} := \texttt{X}[j]$ and increment k by 1.

3. If $k = n - 2$, compute the divisors of $C/(\prod_{i=1}^{k} x_i)$ and store them in an ordered list `X`. Set i to be the index of least element of X that is greater than or equal to x_k.

Loop from $j = i$ so long as

$$\texttt{X}[j] < (C/(\prod_{i=1}^{k} x_i))^{1/(n-k)},$$

and set $x_{k+1} := \texttt{X}[j]$ and increment k by 1.

4. If $k = n-1$, set $x_n := C/(\prod_{i=1}^{k} x_i)$ and check if $\{x_1, \ldots, x_n\}$ forms a PTE solution of size n with constant C as explained above.

Remark 5.2.1. Note that for step 2. above, since we are only considering possible PTE solutions where x_n is greater than or equal to g, given $x_1, \ldots, x_k$, it follows that x_{k+1} must satisfy the bound in this step.

We may now proceed to explain the main algorithm:

Algorithm 5.2.2. *Based on the above ideas, given positive integers n and C, this algorithm will find all ideal* PTE *solutions of size n with constant C, if any exist.*

Input: n, C.

Output: All ideal PTE *solutions of size n with constant C, up to normalization, if any exist.*

1. Compute the prime factorization of C. Assume there are ℓ distinct prime divisors. Store this information in a $2 \times \ell$ array, call it `primdiv`. The first row of the array stores the primes and the second row stores the corresponding exponents.

2. Compute all the divisors of C and store them in an array.

3. Perform the precomputation described above to eliminate large divisors of C from consideration.

4. Store the shortened list of divisors in an array, and suppose it has length d.

5. Compute the prime factorization of each of these divisors, in terms of the original prime divisors of C, and store the exponents in this factorization as a vector of length ℓ along with the divisor. Store all such pairs in an array of size $d \times (\ell + 1)$, called `XX`.

6. Sort the array `XX` by ordering it lexicographically with respect to the vectors associated to the divisors.

7. Create an array of length d containing all 2's, called `usage`.

8a. Calculate the largest index i for which `XX`$[i]$ may be x_1, call this index m.

8b. Given the ordering on `XX`, loop from over i from 0 to ℓ and note the least j such that `XX`$[j][i] = 0$. Store these i in the array `entry`.

9a. If $k = 1$, loop over all `XX`$[i]$ for i from 0 to m, setting $x_1 =$ `XX`$[i]$, and subtract 1 from the ith entry of `usage`. Repeat step 9 with $k = 2$.

9b. If $2 \leq k < n$, loop over all `XX`$[j]$ for j from i to d. Given the information from `entry`, check that `XX`$[j]$ is lexicographically possible. If `XX`$[j]$ is lexicographically less than or equal to x_{k-1} and `XX`$[j]$ is lexicographically less than or equal to $C/(x_1 \cdots x_{k-1})$ and `usage`$[j] > 0$, then set $x_k =$ `XX`$[j]$ and subtract 1 from the jth entry of `usage`. Repeat step 9 with $k = k + 1$.

9c. If $k = n$, set $x_n = C/(x_1 \cdots x_{n-1})$.

10. Sort $x_1, \ldots, x_n$ into ascending order.

11. Find the index i that gives the smallest quantity among the $x_{2i+1} - x_{2i}$.

12. Loop over all integers t in (x_{2i}, x_{2i+1}).

12a. Calculate $D := \prod_{j=0}^{n-1}(t - x_j) - (-1)^n C$.

12b. If $D = 0$, then t is a root of the polynomial $g(z) = f(z) - C$ from above, so factor this polynomial completely over $\mathbb{Q}[x]$ and check to see if it has all integer roots.

12c. Print out the integer roots and these are an ideal PTE solution of size n.

We make the following remarks to fill in some details:

Remark 5.2.2.

3. "Large" here is a hard-coded value to keep the list of divisors relatively small. In practice, we have implemented g is the 100th smallest divisor of C or the $\lfloor \sigma(C)/6 \rfloor$th divisor of C, whichever is smallest.

5. For example, if $C = 14400 = 2^6 \cdot 3^2 \cdot 5^2$ and a divisor is $24 = 2^3 \cdot 3$, then the entry stored is $[24, [3, 1, 0]]$. The idea of these vectors is that instead of looking for positive integers that multiply to give C, we instead look for vectors that sum to the vector corresponding to C.

6. For example, we have $[3,1,0] >_L [2,2,1]$. This ordering will be useful later. *Sage* can sort a list with respect to the lexicographical ordering automatically.

7. From the Interlacing Theorem (Theorem 2.1.3), each x_i is allowed to occur at most twice in a PTE solution, and `usage` will keep track of this.

8a. Since we will loop through the `XX`$[i]$'s lexicographically, the first one in the outermost loop cannot have 0 as its first entry, so this reduces the size of this loop. Further, there must be enough subsequent `XX`$[i]$'s in the inner loops for their first entries to add up to the correct amount, and this reduces the size of the loop further.

9c. In practice, we perform two redundancy checks here to ensure there are no problems in the code. First, we ensure the value remaining is less than the previous vector and secondly, we check that the value remaining is nonnegative.

10. In practice, the list of x_i's is sorted each time a new one is assigned. This is clearly more efficient since because we are looping, the outermost x_i's are fixed, so when a new one is chosen, only a simple search and insertion are required to sort the list.

As an alternative to step 12, note the following idea. If $p \mid C$, then for some ordering of the y_i, we have $y_i \equiv x_i \pmod{p}$. Thus, instead of testing all $j \in (x_{2i}, x_{2i+1})$, simply test those j which are congruent to some x_k modulo p. To make this process more efficient, we may assume we compute the values of $x_i \pmod{p}$ as we select the x_i, and store them in an array.

This method appears to be more efficient when p and the interval length $x_{2i+1} - x_{2i}$ are both larger than $n-2$ (say at least twice as large). However, in practice, the shortest interval is usually around this size, so this alternative was not implemented.

This algorithm may also be parallelized by splitting the computation up in at each step of the outermost loop. That is, each time x_1 is selected, a new job is started. It is clear that besides the common precomputations, no communication between the jobs is required.

This parallelization has major computational advantages, and thus the algorithm is well-suited to submitted to high performance computing clusters with thousands of nodes operating serially.

The precomputation yields a significant improvement in the performance of the algorithm. For example, the previously smallest known ideal PTE solution of size 7 has constant 13967553600. However, this number has 2688 divisors. When we performed the main algorithm with no precomputation on this input, it did not terminate within a week. However,

performing the precomputation with g the 400th smallest divisor, the computation finished successfully in about 20 hours, and when g was chosen to be the 200th smallest divisor, the computation finished in about 40 minutes. In the second case, the precomputation did not take longer than about a half hour.

5.3 An Example

To illustrate the above algorithm, let us take $n = 6$ and $C = 14400$. Then note that $C = 2^6 \cdot 3^2 \cdot 5^2$, and so all divisors of C are

$$\{1, 2,3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25, 30, 32, 36, 40, 45, 48, 50, 60, 64, 72, 75, 80, 90, 96, 100, 120, 144, 150, 160, 180, 192, 200, 225, 240, 288, 300, 320, 360, 400, 450, 480, 576, 600, 720, 800, 900, 960, 1200, 1440, 1600, 1800, 2400, 2880, 3600, 4800, 7200, 14400\}.$$

The only divisors in this list that can occur as a part of a PTE solution are

$$\{1, 2,3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25, 30, 32, 36, 40, 45, 48, 50, 60, 64, 72, 75, 80, 90, 96, 100, 120, 144, 150, 160, 180, 192, 200, 225, 240, 288, 300, 320\}.$$

Now we represent each divisor in terms of the exponents of its prime factorization, relative to C. Thus, the vector $[6, 2, 2]$ represents C, while $[2, 1, 1]$ represents 60. Ordering these vectors lexicographically gives the list

$$\{192,320, 64, 288, 96, 160, 32, 144, 240, 48, 80, 16, 72, 120, 24, 200, 40, 8, 180, 36, 300, 60, 12, 100, 20, 4, 90, 18, 150, 30, 6, 50, 10, 2, 225, 45, 9, 75, 15, 3, 25, 5, 1\}$$

(omitting the vectors themselves). Now we loop over the elements in this array as described above.

When the programme assigns $8, 8, 15, 15, 1, 1$ to $x_1, \ldots, x_6$ (which is lexicographically ordered), we see $D = 0$ when $t = 3$ in step 12a above. Thus, we factor the polynomial $g(z)$ from step 12b and find that it has 6 integers roots: $0, 3, 5, 11, 13, 16$, and so $\{1, 1, 8, 8, 15, 15\} =_5 \{0, 3, 5, 11, 13, 16\}$ is an ideal PTE solution of size 6 with constant 14400.

5.4 Results of the computations

We have used this algorithm to search for new smaller PTE solutions in order to lower the upper bounds of the constant appearing in the table in the previous chapter.

5.4.1 $n = 6$

The lower bound for C_6 is 7200. The smallest previously known solution (after normalizing) according to [3] was $\{1, 1, 8, 8, 15, 15\} =_5 \{0, 3, 5, 11, 13, 16\}$, which has constant $14400 = 2^6 \cdot 3^2 \cdot 5^2 = 2 \cdot 7200$. In fact, all solutions previously found were of the form $2 \cdot k \cdot 7200$, and in [27], Rees and Smyth state that it was possible that $2^6 \mid C_6$. Hence, the previous upper bound of $2 \cdot 7200$. However, our search was able to find $\{0, 6, 8, 23, 25, 31\} =_5 \{1, 3, 11, 20, 28, 30\}$, which has constant $554400 = 2^5 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 = 77 \cdot 7200$. Thus, we have the following Theorem:

Theorem 5.4.1. $C_6 = 7200$.

5.4.2 $n = 7$

The lower bound for C_7 is 3326400 and the upper bound is $19 \cdot 3326400$. The smallest previously known solution (according to [3]) is

$$\{0, 18, 27, 58, 64, 89, 101\} =_6 \{1, 13, 38, 44, 75, 84, 102\}$$

which has constant $13967553600 = 4199 \cdot 3326400 = 13 \cdot 17 \cdot 19 \cdot 3326400$. This solution can be seen to be symmetric after translating by -51. The solution $\{0, 18, 19, 50, 56, 79, 81\} =_6 \{1, 11, 30, 39, 68, 70, 84\}$ was also found, but this is equivalent to the solution given above. We have the following theorem:

Theorem 5.4.2. *The smallest ideal* PTE *solution of size* 7*, up to normalization, is*

$$\{0, 14, 16, 45, 54, 73, 83\} =_6 \{3, 5, 28, 34, 65, 66, 84\},$$

which has constant $5145940800 = 2^6 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 = 1547 \cdot 3326400 = 7 \cdot 13 \cdot 17 \cdot 3326400$. *Therefore, the value of* C_7 *is* 3326400*. Also, besides the solutions mentioned above, there are no ideal* PTE *solutions of size* 7 *with constants less than or equal to* $3326400 \cdot 5500$.

5.4.3 $n = 8$

The lower bound for C_8 in this case is 75675600. The smallest known solution according to [3] is $\{0, 4, 9, 23, 27, 41, 46, 50\} =_7 \{1, 2, 11, 20, 30, 39, 48, 49\}$, which has constant $1210809600 = 2^4 \cdot 75675600$. We have the following Theorem:

Theorem 5.4.3. *There are no other ideal* PTE *solutions of size* 8 *with constants less than or equal to* $2^4 \cdot 75675600$*, up to normalization. Further, for* C *less than* $12000 \cdot 75675600$*, there are no solutions that have* C *not a multiple of* $2^4 \cdot 75675600$*.*

In fact, for constants C up to $12000 \cdot 75675600$, we found 9 ideal PTE solutions of size 8 with constants that are a multiple of $2^4 \cdot 75675600$.

5.4.4 $n = 9$

The lower bound for C_9 in this case is 46569600. The smallest known solution (according to [3]) is $\{0, 26, 42, 124, 166, 237, 293, 335, 343\} =_8 \{5, 13, 55, 111, 182, 224, 306, 322, 348\}$ which has constant $11911664856 \cdot 46569600$. We have searched multiples of 46569600 up to $1200 \cdot 46569600$. We have the following Theorem:

Theorem 5.4.4. *There are no ideal* PTE *solutions of size* 9 *with constants less than or equal to* $1200 \cdot 46569600$*.*

5.4.5 $n = 10$

The lower bound for C_{10} is $2^7 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17 = 2806876800$. We have the following Theorem:

Theorem 5.4.5. *There are no ideal* PTE *solutions of size* 10 *with constants less than or equal to* $100 \cdot 2806876800$*.*

We now present an updated table, Table 5.1, for C_n based on the results of this section.

5.5 Further Work

We attempted to determine new lower bounds for C_7 and C_8 using the parametrized families from [20] and [8], respectively. However, it turned out that the corresponding constants were always divisible by 2^7 and 2^9, respectively, which yields nothing new.

Relatively few computations were done in the size 10 case because they took so long. Although both the precomputation and main algorithm were written in `C++`, the search was inefficient at this size. A search for a typical value of C required about a week to

Table 5.1: Divisibility Results for the $\mathbb{Z}$-PTE Problem

n	Lower bound for C_n	Upper bound for C_n	Upper bound divided by Lower Bound
2	1	1	1
3	2^2	2^2	1
4	$2^2 \cdot 3^2$	$2^2 \cdot 3^2$	1
5	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	1
6	$2^5 \cdot 3^2 \cdot 5^2$	$\boxed{2^5} \cdot 3^2 \cdot 5^2$	~~2~~
7	$2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11$	$2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot$ ~~19~~	~~19~~
8	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	$2^8 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	2^4
9	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	$2^9 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$ $\cdot 17 \cdot 23 \cdot 29$	$2^2 \cdot 3 \cdot 17 \cdot 23 \cdot 29$
10	$2^7 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot \boxed{17}$	$2^{11} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$ $\cdot 17 \cdot 23 \cdot 37 \cdot 53 \cdot 61 \cdot 79$ $\cdot 83 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 191$	$2^4 \cdot 3^2 \cdot 11 \cdot$ ~~17~~ $\cdot 23 \cdot 37 \cdot 53$ $\cdot 61 \cdot 79 \cdot 83 \cdot 103 \cdot 107 \cdot 109$ $\cdot 113 \cdot 191$
11	$2^8 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$ $\cdot 17 \cdot \boxed{19}$	none known	
12	$2^8 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 11^2$ $\cdot \boxed{17} \cdot \boxed{19}$	$2^{12} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11^2 \cdot 13^2$ $\cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$	$2^4 \cdot 3^4 \cdot 13^2 \cdot$ ~~17~~ $\cdot$ ~~19~~ $\cdot 23 \cdot 29$ $\cdot 31$

complete. Therefore, searches were not attempted for $n \geq 11$. It will be subsequent work to extend the computations in the case of $n = 9$ and $n = 10$.

An alternative to searching every constant that is a multiple of the lower bound for C_n could be to only search "likely" multiples. That is, perhaps only consider constants with many smaller factors, say powers of 2 and 3 and no large factors, say ≥ 41.

Chapter 6

Connection to Elliptic Curves

In this chapter, we examine the connection between elliptic curves over $\mathbb{Q}$ and ideal PTE solutions. We explain work in the literature of Smyth [32] and Choudhry and Wróblewski [12] who both found infinite families of ideal PTE solutions of size 10 and 12, respectively.

We examine whether these families of solutions can be used to reduce the upper bounds for C_n. Further, we demonstrate how new ideal PTE solutions over number fields may be found by working with quadratic twists of the elliptic curves that arise in the above works.

First we explain a technique that is necessary for later use in this chapter.

6.1 Rational points on $Ax^2y^2 - Bx^2z^2 - By^2z^2 + Cz^4 = 0$

As we will explain in the sections below, both Smyth and Choudhry and Wróblewski reduce the problem of finding ideal PTE solutions to finding rational points on equations of the form

$$Ax^2y^2 - Bx^2z^2 - By^2z^2 + Cz^4 = 0. \tag{6.1}$$

In both papers, methods that seem to be specific to the case in question are used to transform this equation into an elliptic curve. In this section, we explain a more general method to achieve this.

The first step is to make the following substitution:

$$x = Uz, \quad y = \frac{Vz}{AU^2 - B}. \tag{6.2}$$

Then when equation (6.1) is set equal to 0 and simplified, we obtain

$$V^2 = ABU^4 - ACU^2 - B^2U^2 + CB. \tag{6.3}$$

This equation is a quartic model of an elliptic curve. In fact, Connell in [16] gives a standard method for transforming an equation like (6.3) into an elliptic curve in Weierstrass form, which we explain next.

Suppose we have a curve of the form $v^2 = f(u)$, where $f(u)$ is a quartic polynomial in u, and this curve has a rational point at $(u, v) = (p, q)$. First replace u by $u + p$ to obtain a curve in the form

$$v^2 = au^4 + bu^3 + cu^2 + du + q^2.$$

When $q \neq 0$, Connell proves that such a curve is birationally equivalent to a curve with the following Weierstrass equation:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

where

$$X = \frac{2q(v+q) + du}{u^2} \quad \text{and} \quad Y = \frac{4q^2(v+q) + 2q(du + cu^2) - \frac{d^2u^2}{2q}}{u^3},$$

and

$$a_1 = \frac{d}{q}, a_3 = 2qb, a_2 = c - \frac{d^2}{4q^2}, a_4 = -4q^2a, a_6 = a_2a_4.$$

The inverse transformations are

$$u = \frac{2q(X+c) - \frac{d^2}{2q}}{Y} \quad \text{and} \quad v = -q + \frac{u(uX - d)}{2q}.$$

Thus, in order to transform our curve above in (6.3) to Weierstrass form, we must find a rational point on the curve. Note that the right hand side of (6.3) factors as

$$ABU^4 - ACU^2 - B^2U^2 + CB = (BU^2 - C)(AU^2 - B),$$

and this will be equal to a square when $BU^2 - C = AU^2 - B$. Thus, taking $U = \sqrt{\frac{C-B}{B-A}}$ will give a rational point on (6.3) whenever U is an integer. Alternatively, we may attempt to find a rational point on (6.3) by a brute force search. In all examples we consider, finding a rational point is not an issue.

Once a rational point is found, the above method can be applied and a_1, a_2, a_3, a_4, a_6 are computed, putting the curve into Weierstrass form. Now we may use any number of methods to compute rational points on the resulting elliptic curve, and we can use the inverse transformations above to map such points back to rational points on (6.1), as desired.

6.2 Size 10 solutions

C. Smyth in [32] examines ideal symmetric PTE solutions of size 10 of the form

$$\{\pm x_1, \ldots, \pm x_5\} =_9 \{\pm y_1, \ldots, \pm y_5\}$$

by first making the substitutions

$$\begin{aligned}
x_1 &= xy + xz + yz - 11z^2, & y_1 &= xy + 3xz + 3yz - 11z^2,\\
x_2 &= xy - xz - yz - 11z^2, & y_2 &= xy - 3xz - 3yz - 11z^2,\\
x_3 &= xy - 3xz + 3yz + 11z^2, & y_3 &= xy - xz + yz + 11z^2,\\
x_4 &= xy + 3xz - 3yz + 11z^2, & y_4 &= xy + xz - yz + 11z^2,\\
x_5 &= 4xz + 4yz, & y_5 &= 4xz - 4yz.
\end{aligned}$$

The idea is to then examine the resulting differences of sums of powers and obtain some conditions on x, y, z. Thus, let

$$A_k := \left(\sum_{i=1}^{5} x_i^k\right) - \left(\sum_{i=1}^{5} y_i^k\right).$$

Note that since we have assumed a symmetric parametrization, we need only consider A_k for k even. To find an ideal PTE of size 10 with the above parametrization, we must have A_k equal to zero for $k = 2, 4, 6, 8, 10$. Calculating these values of A_k, we obtain the following:

$$\begin{aligned}
A_2 &= 0,\\
A_4 &= -384xyz^2(-13x^2z^2 - 13y^2z^2 + 121z^4 + x^2y^2),\\
A_6 &= -960xyz^2(y^2 + 11z^2)(x^2 + 11z^2)(-13x^2z^2 - 13y^2z^2 + 121z^4 + x^2y^2),\\
A_8 &= -1792xyz^2(-13x^2z^2 - 13y^2z^2 + 121z^4 + x^2y^2)(113y^4z^4 + 30x^2y^4z^2 + x^4y^4\\
&\qquad + 3630y^2z^6 + 84x^2y^2z^4 + 30x^4y^2z^2 + 14641z^8 + 3630x^2z^6 + 113x^4z^4).
\end{aligned}$$

Note that A_2 is identically 0, while A_4, A_6 and A_8 have

$$g(x, y, z) = -13x^2z^2 - 13y^2z^2 + 121z^4 + x^2y^2. \tag{6.4}$$

as a common factor. Now if $g(x, y, z) = 0$ for some $x, y, z \in \mathbb{Q}$, then all the $A_2, \ldots, A_8$ will be zero, and hopefully yield a nontrivial PTE solution.

Using the method described above, we first substitute

$$x = Uz, \qquad y = \frac{V}{U^2 - 13}$$

into (6.4) and simplify to obtain

$$V^2 = 13U^4 - 290U^2 + 1573.$$

This equation has a rational point at $(U, V) = (3, 4)$ and so replacing U by $u + 3$ and V by v, we obtain

$$v^2 = 13u^4 + 156u^3 + 412u^2 - 336u + 16.$$

Now from Connell's result explained above, this is birationally equivalent to

$$E_{10} : Y^2 - 84XY + 1248Y = X^3 - 1352X^2 - 832X + 1124864, \tag{6.5}$$

which is an elliptic curve over $\mathbb{Q}$.

Note that while working with (6.4) to obtain an elliptic curve, Smyth uses a different method which yields

$$\begin{aligned} E_S : Y^2 &= X^3 - 556011X + 159551910 \\ &= (X - 435)(X - 426)(X + 861). \end{aligned} \tag{6.6}$$

However, this curve has the same j-invariant,

$$\frac{8732907467857}{1656369},$$

as our curve (6.5) above. Thus, it follows that E_S and E_{10} are isomorphic over the algebraic closure of $\mathbb{Q}$.

Smyth proceeds to compute the Mordell-Weil group of these curves to be $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ so there are infinitely many rational points on E. Smyth then uses a combinatorial argument to show that these points in turn lead to infinitely many PTE solutions.

Smyth proceeds to explicitly construct two ideal PTE solutions of size 10. Smyth notes that the PTE solution

$$\{\pm 12, \pm 11881, \pm 20231, \pm 20885, \pm 23738\} =_9 \{\pm 436, \pm 11857, \pm 20449, \pm 20667, \pm 23750\}$$

found by Letac [20, p. 55] is obtained from the point $P = (x, y) = (-344, -9792)$, which is a generator of the non-torsion part of E_{10} and yields the rational point on $g(x, y, z) = 0$ of $(671/153, -869/191, 1)$

The other solution Smyth finds explicitly is

$$\{\pm 308520455907, \pm 87647378809, \pm 527907819623, \pm 243086774390, \pm 441746154196\} =_9$$
$$\{\pm 529393533005, \pm 133225698289, \pm 432967471212, \pm 338027122801, \pm 189880696822\}.$$

This is obained from the point $(62776/225, 15978304/3375)$ on E_{10}, which is twice the point P above, and yields the rational point $(296313/249661, -1264969/424999)$ on $g(x, y, z) = 0$ from equation (6.4).

6.3 Work of Chouhdry and Wróblewski

Chouhdry and Wróblewski [12] use the same ideas as Smyth to examine the ideal symmetric PTE problem of size 12. To search for solutions to $\{\pm x_1, \ldots, \pm x_6\} =_{11} \{\pm y_1, \ldots, \pm y_6\}$, they make the following substitutions:

$$\begin{aligned}
x_1 &= 2xy + xz + 2yz - 7z^2, & y_1 &= 2xy + 2xz + yz - 7z^2,\\
x_2 &= 2xy - xz - 2yz - 7z^2, & y_2 &= 2xy - 2xz - yz - 7z^2,\\
x_3 &= 2xy - 2xz + yz + 7z^2, & y_3 &= 2xy - xz + 2yz + 7z^2,\\
x_4 &= 2xy + 2xz - yz + 7z^2, & y_4 &= 2xy + xz - 2yz + 7z^2,\\
x_5 &= 3xz + 5yz, & y_5 &= 5xz + 3yz,\\
x_6 &= 5xz - 3yz, & y_6 &= 3xz - 5yz.
\end{aligned}$$

As above, the idea is to then examine the resulting differences of sums of powers and obtain some conditions on x, y, z. Thus, let

$$A_k = \left(\sum_{i=1}^{6} x_i^k\right) - \left(\sum_{i=1}^{6} y_i^k\right).$$

Note again that since our parametrization is symmetric, $A_1, A_3, A_5, A_7, A_9, A_{11}$ are all 0. To solve the PTE problem in this setting, we must have A_k to be equal to zero for $k =$

$2, 4, 6, 8, 10$. Calculating A_k in this range, we obtain

$$\begin{aligned}
A_2 &= 0,\\
A_4 &= 0,\\
A_6 &= 4320xyz^4(x-y)(x+y)(8x^2y^2-17x^2z^2+98z^4-17y^2z^2),\\
A_8 &= 5376xyz^4(x-y)(x+y)(8x^2y^2-17x^2z^2+98z^4-17y^2z^2)\\
&\qquad\times(8x^2y^2+37x^2z^2+37y^2z^2+98z^4),\\
A_{10} &= 10080xyz^4(x-y)(x+y)(8x^2y^2-17x^2z^2+98z^4-17y^2z^2).\\
&\quad(665y^4z^4+248x^2y^4z^2+32x^4y^4+3038y^2z^6+2384x^2z^4y^2+248x^4y^2z^2+4802z^8\\
&\quad+3038x^2z^6+665x^4z^4)
\end{aligned}$$

Note that again A_2 and A_4 are identically zero, while A_6, A_8, A_{10} all have a nontrivial common factor,

$$f(x,y,z) := 8x^2y^2-17x^2z^2+98z^4-17y^2z^2. \tag{6.7}$$

As above, solving $f(x,y,z)=0$ for $x,y,z\in\mathbb{Q}$ will lead to all the A_k to be zero, and hopefully yield a nontrivial PTE solution. (Note that $(x-y)(x+y)$ are also common factors of the A_k, but picking x and y to satisfy either $x-y=0$ or $x+y=0$ leads to a trivial PTE solution.)

Using the method described above, we solve $f(x,y,z)=0$ by making the substitutions $x=Uz$ and $y=Vz/(8U^2-17)$ and so after simplification (6.7) reduces to

$$V^2 = 136U^4-1073U^2+1666. \tag{6.8}$$

Now equation (6.8) has a rational point at $(U,V)=(3,55)$ and replacing U by $U+3$ and V by v, we obtain

$$v^2 = 136u^4+1632u^3+6271u^2+8250u+3025,$$

which from Connell's result is birationally equivalent to the elliptic curve over $\mathbb{Q}$

$$E_{12}: Y^2+150XY+179520Y = X^3+646X^2-1645600X-1063057600.$$

Note that Choudhry and Wróblewski use a different method to obtain an elliptic curve from (6.7) and they end up with

$$E_{CW}: Y^2 = X^3+X^2-1290080X+556370100.$$

Note that this curve has j-invariant

$$\frac{57971431973034407521}{850187506100625},$$

which is the same as our curve E_{12} above. Thus, it follows that E_{CW} and E_{12} are isomorphic over the algebraic closure of $\mathbb{Q}$.

Computing the Mordell-Weil group of E_{12} with *Sage* [33], we find that

$$E_{12}(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},$$

and two generators for the non-torsion part of E_{12} are $P = (-3355, 174735)$ and $Q = (-3190, 174900)$.

Choudhry and Wróblewski explain they used this method to find 113 ideal PTE solutions of size 12 with terms under 10^{100}, including 8 with terms under 10^{10}. These 8 solutions are given explicitly in [12]. We repeat these solutions in Table 6.3 below. The first row contains the coefficients of the linear combination of P and Q that yields the solution. The second and third rows are the X and Y coordinates of the rational point on E_{12} and the fourth through sixth rows are the values of x, y, z that yield the PTE solution. The remaining rows are the subsequent ideal PTE solution of size 12 that is obtaied after clearing denominators and removing any common factors.

Note that it is possible to find smaller values of X and Y that generate the same solution by using torsion points in addition to P and Q, but we do not include this. Further, the solutions arising from $-P+Q$ also arises from $-Q$ and the solution arising from $-2Q$ also arises from $-P+2Q$. The minus signs are included in the table to make it explicitly clear how the solution arises from the substitutions given for the x_i and y_i given above.

6.4 Upper bounds for C_n

In the previous chapter, we presented a new algorithm for finding ideal PTE solutions. A major application of this algorithm was to lower the upper bounds for C_n. In this section, we examine whether the solutions presented above can lower the upper bounds for C_{10} and C_{12}.

Table 6.1: Some Ideal PTE solutions of size 12 found by Choudhry and Wróblewski

(i,j)	$(0,2)$	$(0,-1)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(0,-2)$	$(0,3)$
X	2225	-3190	-3355	6050	$\frac{-9955}{4}$	$\frac{-147598}{289}$	2225	$\frac{-291723190}{130321}$
Y	-531135	124080	174735	-1271160	$\frac{1029105}{8}$	$\frac{-496499652}{4913}$	17865	$\frac{4959403249680}{47045881}$
x	$\frac{89}{37}$	$\frac{35}{47}$	$\frac{457}{353}$	$\frac{259}{107}$	$\frac{47}{33}$	$\frac{6587}{2309}$	$\frac{8209}{397}$	$\frac{18025}{13469}$
y	$\frac{-1}{9}$	$\frac{77}{29}$	$\frac{981}{223}$	$\frac{35}{151}$	$\frac{-263}{29}$	$\frac{-3787}{4135}$	$\frac{1511}{1041}$	$\frac{-19271}{3833}$
z	1	1	1	1	1	1	1	1
x_1	-891	293	570049	-3455	-23708	-7641076	15829981	-107581333
x_2	-1618	-886	-224448	-10112	-7713	-9033773	6084678	-43290994
x_3	257	1180	795069	4054	-14714	-3305329	5604633	-52219540
x_4	1896	953	652598	14693	-3309	5725910	22095904	4600567
x_5	1109	1510	1018599	9718	-19653	2713630	14318021	-778995430
x_6	2058	-413	-264662	13165	16426	11601341	20464122	80295173
y_1	-472	107	447858	-929	-18687	-5070974	19802832	-84106267
y_2	-2037	-700	-102257	-12638	-12734	-11603875	2111827	-66766060
y_3	639	1511	1019171	7115	-18372	-1984396	10177351	-65824631
y_4	1514	622	428496	11632	349	4404977	17523186	18205658
y_5	1947	1138	774217	14770	-9611	7853834	22263723	-30945298
y_6	1294	-1075	-712866	7043	23742	8959475	11318686	107505355

6.4.1 C_{10}

The two solutions found explicitly by Smyth have constants

$$2^{11} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 23 \cdot 37 \cdot 53 \cdot 61 \cdot 79 \cdot 83^2 \cdot 103 \cdot 107 \cdot 109^2 \cdot 113 \cdot 191$$

and

$$2^{11} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 43 \cdot 47^2 \cdot 53 \cdot 61 \cdot 79 \cdot 83 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 157 \cdot 191 \cdot 421^2 \cdot 541 \cdot 1381^2 \cdot 1699 \cdot 2297 \cdot 2707 \cdot 3217 \cdot 6299^2 \cdot 8609 \cdot 8761 \cdot 189949^2 \cdot 320687^2 \cdot 1264969,$$

which have gcd

$$2^{11} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 37 \cdot 53 \cdot 61 \cdot 79 \cdot 83 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 191.$$

As explained above, the first solution arises from the point $(-344, -9792)$ on E_{10}, which we shall call P. It turns out the second solution arises from $2 \times P$. Further, let $T_1, \ldots, T_8$ denote the 8 points of finite order on E_{10}. In order to find new ideal PTE solutions of size 10, we may examine points on E_{10} of the form $j \cdot P + T_i$, where $j \in \mathbb{Z}$ and $i = 1, \ldots, 8$.

It turns out that when $j \neq 0, 1$ is fixed, any choice of T_i lead to the same ideal PTE solution of size 10 after simplification. For $j = 0$, all T_i lead to the trivial solution $\{\pm 3, \pm 1, \pm 2, \pm 5, \pm 4\} =_9= \{\pm 5, \pm 1, \pm 3, \pm 4, \pm 2\}$ except when T_i is the point at infinity, when we do not obtain a solution at all.

For $j = 1$, all T_i lead to the first solution given above, except for the torsion point $(-520, -22464)$ which gives the point $(1352, 0)$ on E_{10} and which cannot be mapped back to a PTE solution using our method above since the Y-coordinate is zero.

For $j = -1$, we obtain the trivial solution mentioned above for any choice of T_i.

Searching over all $2 \leq j \leq 40$ and $-40 \leq j \leq -2$, we find a number of new ideal PTE solutions of size 10, but all have constants divisible by the upper bound given above.

6.4.2 C_{12}

As explained in a previous chapter, the constants of solutions found explicitly by Choudhry and Wróblewski in [12], given above, have gcd

$$2^{12} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31.$$

As explained above, the curve E_{12} has rank 2 and two generators are the points $(-3355, 174735), (-3190, 174900)$, which we will call P and Q respectively. Again, as above, let $T_1, \ldots, T_8$ denote the 8 points of finite order on E_{12}. Thus, in order to find new ideal PTE solutions of size 12, we may examine points on E_{12} of the form $j \cdot P + k \cdot Q + T_i$, where $j, k \in \mathbb{Z}$ and $i = 1, \ldots, 8$.

When $j = k = 0$, all T_i lead to the trivial solution $\{\pm 4, \pm 3, \pm 7, \pm 6, \pm 9, \ \pm 2\} =_{12} \{\pm 3, \pm 2, \pm 9, \pm 4, \pm 7, \pm 6\}$, except when T_i is the point at infinity, when we do not obtain a solution at all.

For $(j, k) = (0, -1)$ and $(j, k) = (-1, 0)$, all T_i lead to the trivial solution

$$\{\pm 14, \pm 5, \pm 1, \pm 8, \pm 11, \pm 10\} =_{12} \{\pm 11, \pm 8, \pm 1, \pm 10, \pm 5, \pm 14\}.$$

Now searching over all $j, k \in \mathbb{Z}$ in the interval $-20 < j, k < 20$ except $(j, k) = (0, 0)$, $(j, k) = (0, -1)$, $(j, k) = (-1, 0)$, we find many ideal PTE solutions of size 12, many of which were likely found by Choudhry and Wróblewski. However, all have constants divisible by the upper bound given above.

6.5 Elliptic Curves and PTE solutions over Number Fields

In the previous section, we found ideal PTE solutions over $\mathbb{Z}$ from rational points on elliptic curves. That is, we mapped elements of the group $E(\mathbb{Q})$ back to substitutions that yielded PTE solutions. Given an elliptic curve over $\mathbb{Q}$, we may also examine its group structure over a finite extension of $\mathbb{Q}$, i.e., some number field K. Using a computer algebra programme like *Sage* [33], it is possible directly examine the group $E(K)$. As in the case of $E(\mathbb{Q})$, it is easy to determine the torsion subgroup.

However, even in the case when K is a quadratic extension, it is computationally difficult to determine lower bounds for the rank of $E(K)$, for both theoretical and practical reasons. A discussion of some theoretical reasons can be found in [15], for example. A practical restriction is the availability of appropriate software. *Sage* computes $E(K)$ using `gp` scripts due to Denis Simon [31], which are naturally less quick than the corresponding computations for $E(\mathbb{Q})$ in *Sage*, since they are not implemented natively.

Instead, quadratic twists of elliptic curves may be used to find K-rational points, when K is a quadratic extension. Thus, in this section, we demonstrate how ideal PTE solutions over quadratic number fields can be found by finding rational points on quadratic twists of the elliptic curves appearing above. We proceed to explain some necessary background material.

Remark 6.5.1. Note that it is possible to compute cubic, quartic and sextic twists of elliptic curves, which can be used to find K-rational points for number fields K of higher degree. However, this is only possible when the j-invariant of the curve is 0, 1728 and 0, respectively (see [35], for example). Neither E_{10} nor E_{12} have these j-invariants and so these cases do not arise in our work.

6.5.1 Quadratic Twists

Following [30, Chapter X, Section 2], let K be a number field, and given an elliptic curve $E(K) : y^2 = f(x)$, and a quadratic extension of K, say $K(\sqrt{d})$, then the functions $x' = x$ and $y' = y/\sqrt{d}$ are fixed by $G_{\overline{K}/K}$, and satisfy the equation $dy'^2 = f(x')$. One can see the curves are isomorphic over $K(\sqrt{d})$ via the identification $(x', y') \mapsto (x', y'\sqrt{d})$. Then the equation $dy'^2 = f(x')$ is a representation of the *quadratic twist* of E by d, denoted E_d.

We have the following proposition from of [30, Chapter X, Section 6]:

Proposition 6.5.2. *Given an elliptic curve $E : y^2 = x^3 + Ax + B$ over a number field K and $d \in K^*$, then the quadratic twist of E corresponding to d has the Weierstrass equation*

$$E_d : y^2 = x^3 + d^2Ax + d^3B,$$

so long as the j-invariant of E, $j(E)$ is not equal to 0 or 1728.

Remark 6.5.3. In the cases that $j = 0$ or $j = 1728$, the Weierstrass equation for E_d takes a different form, but this case does not arise in our work.

For an elliptic curve that is not in short Weierstrass form, we follow [15]. Thus, let E be an elliptic curve defined over K, a number field, by an equation $y^2 = f(x)$, with $f(x)$ a cubic polynomial, $d \in K^*$. Then the *quadratic twist* of E by d is the elliptic curve with equation $dy^2 = f(x)$. Now if $f(x) = x^3 + ax^2 + bx + c$, we may multiply the equation $dy^2 = f(x)$ through by d^3 and set $Y = d^2y$ and $X = dx$ giving the Weierstrass equation

$$Y^2 = X^3 + adX^2 + bd^2X + cd^3.$$

Also note that both curves E_{10} and E_{12} are not in the form described above. To obtain this, we make the following transformations, as in Chapter III, Section 1 of [30]. Suppose

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{6.9}$$

is an elliptic curve with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$. To eliminate the xy and y terms, we may replace y by $\frac{1}{2}(2y_1 - a_1x - a_3)$ to obtain an elliptic curve of the form

$$y_1^2 = x^3 + \left(\frac{1}{4}a_1^2 + a_2\right)x^2 + \left(\frac{1}{2}a_1a_3 + a_4\right)x + \frac{1}{4}a_3^2 + a_6. \tag{6.10}$$

Finally, this curve has quadratic twist

$$y_1^2 = x^3 + \left(\frac{1}{4}a_1^2 + a_2\right)dx^2 + \left(\frac{1}{2}a_1a_3 + a_4\right)dx + \left(\frac{1}{4}a_3^2 + a_6\right)d^3. \tag{6.11}$$

Thus, we can find a point (X, Y) on (6.11), this corresponds to a point $(X, Y\sqrt{d})$ on (6.10) which corresponds to a point $(X, \frac{1}{2}(2Y\sqrt{d} - a_1X - a_3)$ on our original curve (6.9). Further, if (X, Y) is a point of infinite order on (6.11), then $(X, \frac{1}{2}(2Y\sqrt{d} - a_1X - a_3)$ is a $\mathbb{Q}(\sqrt{d})$ point of infinite order on (6.9). Since the y-coordinate of this point on (6.9) contains $\sqrt{d}$, but the x-coordinate does not, it is clear that the corresponding PTE solution will not reduce to a solution over $\mathbb{Z}$. Thus, if we can find d for which $E_{d\times n}$ (for $n = 10, 12$)

has rank at least 1, then it follows that there exists an ideal PTE solution of size n over $\mathbb{Q}(\sqrt{d})$.

Note that there are many deep, theoretical results concerning families of quadratic twists of a fixed elliptic curve. For example, Stewart and Top [35] have shown that if $E : y^2 = x^3 + ax + b$ is an elliptic curve with $ab \neq 0$, then there are infinitely many squarefree integers d such that $E_d(\mathbb{Q})$ has rank at least 2. They also provide an effective lower bound for the density of such d. See Rubin and Silverberg's review [28] for a summary of related results. Their article also briefly explains difficulties of computing the rank of $E(\mathbb{Q})$, as mentioned above.

Thus, we may conclude that there are infinitely many d for which there is an ideal PTE solution of size 10 (resp. 12) over $\mathbb{Q}(\sqrt{d})$ that is not equivalent to a $\mathbb{Z}$-PTE solution.

We now proceed to apply this theory to the elliptic curves appearing in the previous section. The examples we present explicitly are all in quadratic number fields with class number 1. Thus, it is possible to remove any common factors that might appear in the ideal PTE solutions. Of course, this method will still produce ideal PTE solutions over quadratic number fields that do not have class number 1, but we do not present this case.

6.5.2 $n = 10$

As explained above, the curve that Smyth used in [32] to find ideal PTE solutions of size 10 is

$$E_{10} := Y^2 - 84XY + 1248Y = X^3 - 1352X^2 - 832X + 1124864.$$

From above, using the substitution $y = \frac{1}{2}(2y_1 + 84x - 1248)$, the quadratic twist of E_{10} by d is

$$E_{10\times d} : y_1^2 = x^3 + 412dx^2 - 53248d^2x + 1514240d^3. \tag{6.12}$$

For example, when $d = 5$, we note the class number of $\mathbb{Q}(\sqrt{5})$ is 1 and we have

$$E_{10\times 5} : y^2 = x^3 + 2060x^2 - 1331200x + 189280000.$$

According to *Sage*, this curve has torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and rank 1 and generator $P = (-620, 39600$. This point corresponds to $(-124, 1584)$ on

$$5y^2 = x^3 + 412x^2 - 53248x + 1514240,$$

which corresponds to $(-124, 1584\sqrt{5})$ on

$$y_1^2 = x^3 + 412x^2 - 53248x + 1514240.$$

Now using the substitution $y = \frac{1}{2}(2y_1 - 84x + 1248)$, we obtain the point $(-124, -5832 + 1584\sqrt{5})$ on our original elliptic curve E_{10}. After clearing denominators and removing any common factors, we obtain the ideal PTE solution of size 10

$$\{\pm(20\sqrt{5}+129), \pm(48\sqrt{5}+108), \pm(24\sqrt{5}+205), \pm(-48\sqrt{5}+31), \pm(-56\sqrt{5}+42)\} =_9$$
$$\{\pm(-8\sqrt{5}+150), \pm(76\sqrt{5}+87), \pm 147, \pm(-24\sqrt{5}+89), \pm(-48\sqrt{5}-116)\},$$

which has constant

$$\left(-4\sqrt{5}-9\right)\cdot\left(\frac{9}{2}\sqrt{5}+\frac{1}{2}\right)^{10}\cdot\left(\frac{9}{2}\sqrt{5}-\frac{1}{2}\right)\cdot\left(\frac{3}{2}\sqrt{5}-\frac{1}{2}\right)^{14}\cdot\left(\frac{3}{2}\sqrt{5}+\frac{1}{2}\right)^{11}$$
$$\cdot\left(-2\sqrt{5}-1\right)\cdot\left(-2\sqrt{5}+1\right)\cdot 2^{31}\cdot\left(\frac{1}{2}\sqrt{5}-\frac{11}{2}\right)\cdot 3^2\cdot\left(\frac{5}{2}\sqrt{5}+\frac{1}{2}\right)\cdot\left(\frac{3}{2}\sqrt{5}+\frac{41}{2}\right)\cdot$$
$$\left(\frac{1}{2}\sqrt{5}+\frac{13}{2}\right)\cdot\left(\frac{1}{2}\sqrt{5}+\frac{41}{2}\right)\cdot\left(\frac{1}{2}\sqrt{5}-\frac{41}{2}\right)^{10}\cdot\left(-\sqrt{5}\right)^2\cdot\left(\frac{7}{2}\sqrt{5}+\frac{1}{2}\right)\cdot\left(\frac{7}{2}\sqrt{5}-\frac{1}{2}\right)$$
$$\cdot 7^2\cdot\left(\frac{1}{2}\sqrt{5}+\frac{17}{2}\right)^2.$$

Since 147 appears in the solution, there is no affine transformation that can possibly map this solution to a $\mathbb{Z}$-PTE solution. Thus, this solution is not equivalent to a a $\mathbb{Z}$-PTE solution.

Another example is when $d = -2$, where, as above, the class number of $\mathbb{Q}(\sqrt{-2})$ is 1. Then we have

$$E_{10\times -2} : y^2 = x^3 - 824x^2 - 212992x - 12113920,$$

which according to *Sage* has torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ and rank 1 with generator $P = (1340, 25080)$. This point corresponds to $(-670, 6270)$ on

$$-2y^2 = x^3 + 412x^2 - 53248x + 1514240,$$

which corresponds to $(-670, 6270\sqrt{-2})$ on

$$y_1^2 = x^3 + 412x^2 - 53248x + 1514240.$$

Now using the substitution $y = \frac{1}{2}(2y_1 + 84x - 1248)$, we obtain the point $(-670, 6270\sqrt{-2} - 28764)$ on our original elliptic curve E_{10}. After clearing denominators and removing any common factors, we obtain the ideal PTE solution of size 10

$$\{\pm(37117\sqrt{-2}+80083), \pm(43004\sqrt{-2}+53476), \pm(29985\sqrt{-2}+103025),$$
$$\pm(-40713\sqrt{-2}-12157), \pm(-11774\sqrt{-2}+53214)\} =_9$$
$$\{\pm(31230\sqrt{-2}+106690), \pm(48891\sqrt{-2}+26869), \pm(6419\sqrt{-2}+64631),$$
$$\pm(-17147\sqrt{-2}+26237), \pm(-47132\sqrt{-2}-76788)\},$$

which has constant

$$\begin{aligned}(-1)&\cdot(-\sqrt{-2}-3)\cdot(\sqrt{-2}-3)\cdot(-4\sqrt{-2}+9)\cdot(4\sqrt{-2}+9)\cdot(-60\sqrt{-2}-67)^2\\
&\cdot(5\sqrt{-2}-9)\cdot(-9\sqrt{-2}+1)\cdot(2\sqrt{-2}+3)\cdot(-2\sqrt{-2}+3)\cdot(3\sqrt{-2}+1)\cdot(3\sqrt{-2}-1)\\
&\cdot(6\sqrt{-2}-11)\cdot\sqrt{-2}^{58}\cdot(101\sqrt{-2}-15)^2\cdot(9\sqrt{-2}+11)\cdot(\sqrt{-2}+1)^6\cdot(\sqrt{-2}-1)^6\\
&\cdot(-24\sqrt{-2}+43)\cdot(12\sqrt{-2}+7)\cdot(-87\sqrt{-2}-149)^{10}\cdot(87\sqrt{-2}-149)\\
&\cdot(42\sqrt{-2}-23)\cdot(-42\sqrt{-2}-23)^{10}\cdot(4\sqrt{-2}-3)\cdot(-3\sqrt{-2}-5)\cdot(3\sqrt{-2}-5)\\
&\cdot(-289\sqrt{-2}+543)\cdot5^2\cdot(-40\sqrt{-2}-51)\cdot(-5\sqrt{-2}+3)^2\cdot7^2\cdot(-18\sqrt{-2}-11)^2\\
&\cdot(-18\sqrt{-2}-17)^2\end{aligned}$$

Further, note that the prime $(-60\sqrt{-2}-67)$ appears in the constant above, but its conjugate in $\mathbb{Q}(\sqrt{-2})$ does not. Thus, by Proposition 2.1.2, this solution cannot be equivalent to a $\mathbb{Z}$-PTE solution.

We present information about the quadratic twists of E_{10} by squarefree d with $2 \leq d \leq 35$ and $-35 \leq d \leq -1$ in Tables 6.5.2 and 6.5.2 respectively . In each table, the second column merely provides a lower bound for the rank of $E_{10\times d}$, since in some cases, this is all *Sage* is able to compute. We include the class number of $\mathbb{Q}(\sqrt{d})$ for reference. For convenience, we omit the row d when $E_{10\times d}$ has rank 0. Also, in every case, the torsion subgroup of $E_{10\times d}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

In particular, note that when $d=-1$, the curve $E_{10\times d}$ has rank 0, and so we are not able to obtain ideal PTE solutions in $\mathbb{Z}[i]$ using this method. Thus, the $\mathbb{Z}[i]$-PTE solutions found computationally in Chapter 3 do not arise from this elliptic curve.

6.5.3 $n = 12$

As explained above, the curve that Choudhry and Wróblewski used in [12] to find ideal PTE solutions of size 12 is

$$E_{12}: Y^2+150XY+179520Y = X^3+646X^2-1645600X-1063057600.$$

Table 6.2: Data for $E_{10\times d}$ for $d > 0$

d	class number of $\mathbb{Q}(\sqrt{d})$	Lower bound for the rank of $E_{10\times d}$	Generators for the free part of $E_{10\times d}(\mathbb{Q})$
5	1	1	$(-620, 39600)$
6	1	2	$(-1976, 77792), (-312, 33696)$
7	1	1	$(-208, 34320)$
11	1	1	$(-1976, 157248)$
13	1	1	$(740, 2400)$
15	2	1	$(-1560, 187200)$
17	1	1	$(1352, 43680)$
19	1	1	$(416, 61776)$
22	1	1	$(3260, 251160)$
26	2	1	$(-848, 253440)$
29	1	1	$(5720, 599040)$
30	2	1	$(-240, 230400)$
33	1	1	$(2040, 34560)$
35	2	3	$(-12480, 1086800), (-9380, 1058400),$ $(2184, -40768)$

Table 6.3: Data for $E_{10\times d}$ for $d < 0$

d	class number of $\mathbb{Q}(\sqrt{d})$	Lower bound for the rank of $E_{10\times d}$	Generators for the free part of $E_{10\times d}(\mathbb{Q})$
-2	1	1	$(1340, 25080)$
-10	2	1	$(-91400/169, -3326400/2197)$
-11	1	1	$(15812, 1648128)$
-14	4	1	$(11816, 846720)$
-15	2	1	$(-824, 2464)$
-22	2	1	$\left(\frac{4275088840}{370881}, \frac{26763312283840}{225866529}\right)$
-23	3	1	$(-1240, 5280)$
-30	4	1	$(-80400/49, -2534400/343)$
-31	3	1	$(-385976/225, -20782432/3375)$
-34	4	1	$(-16112/9, -189440/27)$

From above, using the substitution $y_1 = \frac{1}{2}(2y_1 - 150x - 179520)$, the quadratic twist of E_{12} by d is

$$E_{12\times d} : y^2 = x^3 + 6271dx^2 + 11818400d^2x + 6993800000d^3. \tag{6.13}$$

When $d = 2$, the curve

$$E_{12\times 2} : y^2 = x^3 + 12542x^2 + 47273600x + 55950400000$$

has torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and rank 1 with generator $P = (-2686, 8976)$. This point corresponds to $(-1343, 2244)$ on the curve

$$2y_1^2 = x^3 + 6271x^2 + 11818400x + 6993800000.$$

After using the substitution $y = \frac{1}{2}(2y_1 - 150x - 179520)$, we obtain the point

$$(-1343, 2244\sqrt{2} + 10965)$$

on E_{12}. This yields the ideal PTE solution

$$\begin{aligned}
&\{ \pm(12885\sqrt{2} + 34803), \pm(-45202\sqrt{2} + 81574), \pm(-118287\sqrt{2} + 89607),\\
&\quad \pm(-40408\sqrt{2} + 35380), \pm(83301\sqrt{2} - 66225), \pm(95434\sqrt{2} - 65818)\} =_{11}\\
&\{ \pm(30440\sqrt{2} + 23212), \pm(-62757\sqrt{2} + 93165), \pm(-93073\sqrt{2} + 70153),\\
&\quad \pm(-65622\sqrt{2} + 54834), \pm(118411\sqrt{2} - 89407), \pm(45006\sqrt{2} - 26910)\},
\end{aligned}$$

which has constant

$$\begin{aligned}
&(408\sqrt{2} - 577) \cdot (3\sqrt{2} - 11) \cdot (-23\sqrt{2} + 5) \cdot (23\sqrt{2} + 5)^{12} \cdot (-2\sqrt{2} + 103) \cdot 11^2 \cdot (8\sqrt{2} - 1)\\
&\cdot(9\sqrt{2} + 5) \cdot (58\sqrt{2} + 401) \cdot (\sqrt{2} - 13) \cdot (-3\sqrt{2} + 1) \cdot (-3\sqrt{2} - 1)^2 \cdot (10\sqrt{2} - 133)^{12}\\
&\cdot(10\sqrt{2} + 133) \cdot (11\sqrt{2} + 45) \cdot (\sqrt{2} + 43) \cdot \sqrt{2}^{47} \cdot (\sqrt{2} - 5)^2 \cdot (-\sqrt{2} - 5) \cdot (1121\sqrt{2} - 69)\\
&\cdot 3^7 \cdot (4\sqrt{2} - 1) \cdot (-4\sqrt{2} - 1) \cdot (-2\sqrt{2} + 7) \cdot (2\sqrt{2} + 7) \cdot (16\sqrt{2} + 7) \cdot (-16\sqrt{2} + 7)\\
&\cdot(\sqrt{2} - 7) \cdot (\sqrt{2} + 7) \cdot (5964\sqrt{2} + 23519) \cdot (50\sqrt{2} + 9) \cdot 5 \cdot (16\sqrt{2} + 3) \cdot (-2\sqrt{2} + 1)^2\\
&\quad \cdot (-2\sqrt{2} - 1)^2 \cdot (2\sqrt{2} + 9) \cdot (-61\sqrt{2} - 7) \cdot (21\sqrt{2} - 5) \cdot (-7\sqrt{2} + 3) \cdot (-7\sqrt{2} - 3)\\
&\cdot(-7\sqrt{2} - 1) \cdot (-7\sqrt{2} - 33).
\end{aligned}$$

By the same argument as above, since the prime $(3\sqrt{2} - 11)$ appears in the constant but its conjugate in $\mathbb{Q}(\sqrt{2})$ does not, it follows from Proposition 2.1.2 that this solution cannot be equivalent to any $\mathbb{Z}$-PTE solution.

When $d = -3$, the curve

$$E_{12\times -3} : y^2 = x^3 - 18813x^2 + 106365600x - 188832600000$$

has torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and rank 1 with generator $P = (4150, 7150)$. This point corresponds to $(-4150/3, 7150/9)$ on the curve

$$-3y_1^2 = x^3 - 18813x^2 + 106365600x - 188832600000.$$

After using the substitution $y = \frac{1}{2}(2y_1 - 150x - 179520)$, we obtain the point

$$\left(\frac{-4150}{3}, \frac{7150}{9}\sqrt{-3} + 13990\right)$$

on E_{12}. This yields the ideal PTE solution

$$\left\{ \pm(4898\sqrt{-3} + 74149), \pm\left(\frac{59665}{2}\sqrt{-3} - \frac{58869}{2}\right), \pm\left(\frac{81119}{2}\sqrt{-3} - \frac{361115}{2}\right)\right.$$
$$\left. \pm(21548\sqrt{-3} - 85143), \pm(-34316\sqrt{-3} + 144200), \pm\left(-\frac{44443}{2}\sqrt{-3} + \frac{227361}{2}\right)\right\} =_{11}$$
$$\left\{ \pm(1688\sqrt{-3} + 92415), \pm\left(\frac{66085}{2}\sqrt{-3} - \frac{95401}{2}\right), \pm(31178\sqrt{-3} - 139941),\right.$$
$$\left. \pm\left(\frac{61859}{2}\sqrt{-3} - \frac{251519}{2}\right), \pm(-40736\sqrt{-3} + 180732), \pm\left(-\frac{6917}{2}\sqrt{-3} + \frac{64895}{2}\right)\right\},$$

which has constant

$$\left(-\frac{1}{2}\sqrt{-3}+\frac{1}{2}\right)\cdot\left(\frac{11}{2}\sqrt{-3}+\frac{7}{2}\right)\cdot\left(\frac{37}{2}\sqrt{-3}+\frac{5}{2}\right)\cdot 11^2\cdot\left(-\frac{13}{2}\sqrt{-3}-\frac{1}{2}\right)\cdot\left(2\sqrt{-3}-1\right)^2$$
$$\cdot\left(-2\sqrt{-3}-1\right)^2\cdot\left(-20\sqrt{-3}-11\right)\cdot\left(\frac{13}{2}\sqrt{-3}-\frac{7}{2}\right)\cdot\left(\frac{133}{2}\sqrt{-3}+\frac{67}{2}\right)\cdot\left(-7\sqrt{-3}+2\right)\cdot\left(-7\sqrt{-3}-2\right)$$
$$\cdot\left(\frac{5}{2}\sqrt{-3}+\frac{1}{2}\right)^2\cdot\left(-\frac{5}{2}\sqrt{-3}+\frac{1}{2}\right)\cdot\left(-24999\sqrt{-3}+6236\right)\cdot 2^{18}\cdot\left(\frac{163}{2}\sqrt{-3}-\frac{61}{2}\right)^{12}\cdot\left(-\frac{163}{2}\sqrt{-3}-\frac{61}{2}\right)$$
$$\cdot\left(-\frac{17}{2}\sqrt{-3}-\frac{5}{2}\right)\cdot\left(\frac{179}{2}\sqrt{-3}-\frac{19}{2}\right)\cdot\left(\frac{179}{2}\sqrt{-3}+\frac{19}{2}\right)^{12}\cdot\left(-\frac{161}{2}\sqrt{-3}-\frac{155}{2}\right)\cdot\left(-\frac{19}{2}\sqrt{-3}-\frac{1}{2}\right)$$
$$\cdot\left(-\frac{19}{2}\sqrt{-3}-\frac{5}{2}\right)\cdot\left(-\sqrt{-3}\right)^{11}\cdot\left(3\sqrt{-3}-2\right)\cdot\left(-3\sqrt{-3}-2\right)\cdot\left(-\frac{7}{2}\sqrt{-3}+\frac{1}{2}\right)\cdot\left(-\frac{7}{2}\sqrt{-3}-\frac{1}{2}\right)$$
$$\cdot\left(-\frac{21}{2}\sqrt{-3}-\frac{19}{2}\right)\cdot\left(\frac{21}{2}\sqrt{-3}-\frac{19}{2}\right)\cdot\left(-\frac{7}{2}\sqrt{-3}-\frac{5}{2}\right)\cdot\left(-12\sqrt{-3}+1\right)\cdot\left(\frac{71}{2}\sqrt{-3}-\frac{67}{2}\right)\cdot 5$$
$$\cdot\left(-132\sqrt{-3}+43\right)\cdot\left(-\frac{27}{2}\sqrt{-3}-\frac{1}{2}\right)\cdot\left(13\sqrt{-3}-8\right)\cdot\left(-\frac{9}{2}\sqrt{-3}-\frac{1}{2}\right)\cdot\left(-\frac{3}{2}\sqrt{-3}-\frac{1}{2}\right)^2$$
$$\cdot\left(\frac{3}{2}\sqrt{-3}-\frac{1}{2}\right)^3\cdot\left(\frac{9}{2}\sqrt{-3}-\frac{7}{2}\right)\cdot\left(-\frac{9}{2}\sqrt{-3}-\frac{7}{2}\right)\cdot\left(5\sqrt{-3}+2\right)\cdot\left(-\frac{11}{2}\sqrt{-3}-\frac{5}{2}\right)\cdot\left(\frac{101}{2}\sqrt{-3}-\frac{91}{2}\right).$$

Again following the same argument as above, since the prime $-\frac{1}{2}\sqrt{-3}+\frac{1}{2}$ appears in the constant but its conjugate in $\mathbb{Q}(\sqrt{-3})$ does not, it follows from Proposition 2.1.2 that this solution cannot be equivalent to any $\mathbb{Z}$-PTE solution.

As above, we present information about the quadratic twists of E_{12} by squarefree d with $2 \leq d \leq 35$ and $-35 \leq d \leq -1$ in Tables 6.5.3 and 6.5.3 respectively. In each table, the second column merely provides a lower bound for the rank of $E_{12\times d}$, since in some cases, this is all *Sage* is able to compute. We include the class number of $\mathbb{Q}(\sqrt{d})$ for reference. For convenience, we omit the row d when $E_{12\times d}$ has rank 0. Also, in every case, the torsion subgroup of $E_{12\times d}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

6.6 Further Work

One direction for further work could be to examine both E_{10} and E_{12} over cubic number fields. This was attempted over $K=\mathbb{Q}(\sqrt[3]{2})$, but the computation to find K-rational points on E_{12} did not terminate after three hours.

An exercise could be to explicitly prove that adding any of the torsion points to a point of infinite order on E_{10} or E_{12}, the same ideal PTE solution is obtained. This should be

Table 6.4: Data for $E_{12\times d}$ for $d > 0$

d	class number of $\mathbb{Q}(\sqrt{d})$	Lower bound for the rank of $E_{12\times d}$	Generators for the free part of $E_{12\times d}(\mathbb{Q})$
2	1	1	$(-2686, 8976)$
5	1	2	$(-11330, 311850), (-7755, 47300)$
7	1	1	$(-18700, 617100)$
11	1	1	$(-76395/4, 3507185/8)$
13	1	1	$(9350, -6479550)$
17	1	1	$\left(\frac{-49430150}{2209}, \frac{-34126591950}{103823}\right)$
22	1	1	$(-34000, -408000)$
23	1	1	$(-39644, 1272348)$
26	2	2	$(-39270, -254320), (620350, -553675500)$
29	1	1	$(-43520, -165240)$
30	2	1	$(-39134, -874276)$
31	1	2	$(-88660, 5708340), (-69700, 4748100)$
33	1	2	$(-27150, -5868450), \left(\frac{-120326}{25}, \frac{-1741378918}{125}\right)$
35	2	1	$\left(\frac{-116875}{4}, \frac{-50139375}{8}\right)$

Table 6.5: Data for $E_{12\times d}$ for $d > 0$

d	class number of $\mathbb{Q}(\sqrt{d})$	Lower bound for the rank of $E_{12\times d}$	Generators for the free part of $E_{12\times d}(\mathbb{Q})$
-2	1	1	$(2768, 4032)$
-3	1	1	$(4150, 7150)$
-6	2	1	$\left(\frac{35673}{4}, \frac{-168399}{8}\right)$
-13	2	1	$\left(\frac{9583288}{529}, \frac{-1113079968}{12167}\right)$
-14	4	1	$(51920, 2090880)$
-15	2	1	$(108834, -20993742)$
-17	4	1	$(24200, 184800)$
-22	2	2	$\left(\frac{502225}{16}, \frac{-17562825}{64}\right), (32750, -130500)$
-23	3	1	$(32714, -289674)$
-29	6	1	$(212135, 57448710)$
-30	4	2	$(42000, -360000), \left(\frac{2016498000}{18769}, \frac{12201068880000}{2571353}\right)$
-33	4	2	$(46104, 396576), (501000, 282852000)$
-34	4	2	$(174768, 30635264), (242114, 68753100)$

straightforward since the addition of points on an elliptic curve is given explicitly by the group law.

One could also attempt to try to find other families of ternary quadratic forms to use as substitutions. Attempting to do this for size 10, we proved that that all families with the same symmetry as the one given by Smyth lead to an elliptic curve with the same j-invariant as E_{10} anyway. No new solution arise in this way.

We also tried to do this for size 12, but we were not able to show this explicitly. However, all other families found did lead to elliptic curves with the same j-invariant as E_{12}, and no new solutions were found. For both cases $n = 10$ and $n = 12$, we also searched for substitutions that had coefficients in $\mathbb{Z}[i]$, but none were found.

Using similar symmetries as Smyth and Choudhry and Wróblewski, we searched for substitutions that would lead to ideal solutions for sizes $n = 14$ and $n = 16$. We were not able to find any appropriate substitutions for $n = 14$. For $n = 16$, we found a substitution that yield common factors for sixth and eighth powers, but not higher. Further, the resulting elliptic curve has rank 0 over $\mathbb{Q}$, and the smallest d for which this elliptic curve had nonzero rank is -3. Thus all we found in this case is a PTE solution of size 16 and degree 9 over $\mathbb{Q}(\sqrt{-3})$. This is an obscure case of the problem so we do not go into further detail.

Recall that in the size 10 case, we were not able to improve the upper bounds for C_{10} from the single solution. It is known that multiples of points of infinite order on elliptic curves are connected to linear recurrent sequences called elliptic divisibility sequences (see the exercises at the end of Chapter III in [30] for a definition). One could examine whether the properties of these sequences prevent new upper bounds from being obtained.

In [8], Chernick worked with a parametrized family of size 6 ideal PTE solutions to produce a parametrized family of size 7 ideal PTE solutions. It may be possible to connect these ideas with the work of Smyth and Choudhry and Wróblewski to produce a family of size 9 solutions.

Chapter 7

Conclusion

In this thesis, we have used both theoretical and computational techniques to examine the Prouhet-Tarry-Escott problem. The problem has been generalized to rings of integers of number fields and we have adapted ideas from the literature for this setting in Chapter 3.

A vital piece of information for the problem is the constant C_n and in Chapters 4 and 5, we employed an armamentarium of algorithms to examine this aspect of the problem. In Chapter 4, in Section 4.1, we proved that $2^6 \mid C_7$. It is likely possible to extend this result to larger n. In fact, since this thesis was submitted, we have obtained $2^7 \mid C_8$ and further expect $2^8 \mid C_8$. Also, in Section 4.3, we extended an algorithm from the literature that improves lower bounds for C_n. It is possible this search could be extended further, especially in the case of $n = 10$ and $p = 23$, which was incomplete. Alternatively, this algorithm could be extended to the number field case. Since there are new prime divisors of C_n obtained in Theorem 4.3.2, this result could dramatically improve the BLP algorithm described in Chapter 3.

In Chapter 5, we present a new algorithm that determines whether a PTE solution of size n with constant C exists. This algorithm allows us to improve the upper bounds for C_n. In Section 5.4, we completely determine the value of C_6 and C_7. For $n = 7$ and $n = 8$, we use this algorithm to determine the smallest constant C for which a PTE solution exists.

Further work would also be to extend the computations in the cases of $n = 9$ and $n = 11$.

It may also be possible to extend the algorithm of Chapter 5 to the number field case. The algorithm depends upon the "Interlacing Theorem" and being able to factor an integer into primes uniquely, which both hold in the case that $\mathcal{O} \subseteq \mathbb{R}$ and a $\mathcal{O}$ is a UFD.

Some open questions from Chapter 4 and 5 include the exact value of C_n for $n \geq 7$ and finding the smallest C for which a PTE solution exists for $n = 9, 10, 12$.

The connection between the PTE problem and elliptic curves was further examined in Chapter 6. We largely focused on explaining results from the literature, and demonstrated how quadratic twists of elliptic curves could be used to find PTE solutions over quadratic number fields.

The fundamental question of whether solutions exist at all for $n = 11$ and $n \geq 13$ remain unanswered. However, the algorithms from Chapter 5 could be applied to these cases in the future. Additionally, it may be possible to adapt some of the ideas from Chapter 6 and similar works in the literature to find infinite families of solutions of size 9, as well as $n = 11$ and $n \geq 13$.

Appendix A

Proof of Background Results

This appendix contains the proof of some background results.

A.1 Preliminaries – Newton's Identities

Many results on the $\mathcal{O}$-PTE problem involve Newton's identities and symmetric polynomials. Although they are well known and easily found in the literature, we will repeat them here for convenience.

Let $n \in \mathbb{N}$. Let $s_1, \ldots, s_n$ be variables. Then for all integers $k \geq 1$, we define

$$p_k(s_1, \ldots, s_n) := s_1^k + s_2^k + \ldots + s_n^k,$$

the kth power sum in n variables. Similarly, for $k \geq 0$, we define

$$\begin{aligned}
e_0(s_1, \ldots, s_n) &= 1 \\
e_1(s_1, \ldots, s_n) &= s_1 + s_2 + \ldots + s_n \\
e_2(s_1, \ldots, s_n) &= \sum_{i<j} s_i s_j \\
&\vdots \\
e_n(s_1, \ldots, s_n) &= s_1 s_2 \cdots s_n \\
e_k(s_1, \ldots, s_n) &= 0, \forall k > n,
\end{aligned}$$

the elementary symmetric polynomials in n variables. Then we have the result known as Newton's identities:

$$ke_k(s_1,\ldots,s_n) = \sum_{i=1}^{k}(-1)^{i-1}e_{k-i}(s_1,\ldots,s_n)p_i(s_1,\ldots,s_n), \tag{A.1}$$

for all $k \geq 1$. Note that this can be rearranged to

$$p_k(s_1,\ldots,s_n) = (-1)^{k-1}ke_k(s_1,\ldots,s_n) + \sum_{i=1}^{k-1}(-1)^{k-i}e_{k-i}(s_1,\ldots,s_n)p_i(s_1,\ldots,s_n), \tag{A.2}$$

for $k \geq 2$. Another fact is the identity

$$\prod_{i=1}^{n}(t-s_i) = \sum_{k=0}^{n}(-1)^k e_k(s_1,\ldots,s_n)t^{n-k}. \tag{A.3}$$

Thus, the coefficients of a polynomial are elementary symmetric polynomials of its roots, and because of (A.1), they depend on the power sums $p_i(s_1,\ldots,s_n)$. This is a crucial observation for some later work.

A.2 Some Easy Results

At this point, we will give basic results that are normally stated over $\mathbb{Z}$, but also hold when one considers the PTE problem over any $\mathcal{O}$. It is more convenient to state these results in a general way.

Lemma A.2.1. *Suppose $X = \{x_1,\ldots,x_n\}$ and $Y = \{y_1,\ldots,y_n\}$ are subsets of $\mathcal{O}$, and $k \in \mathbb{N}$ with $k \leq n-1$. Then the following are equivalent:*

$$(i) \quad \sum_{i=1}^{n} x_i^j = \sum_{i=1}^{n} y_i^j \quad \text{for } j = 1,2,\ldots,k$$

$$(ii) \quad \deg\left(\prod_{i=1}^{n}(z-x_i) - \prod_{i=1}^{n}(z-y_i)\right) \leq n-k-1$$

$$(iii) \quad (z-1)^{k+1} \mid \sum_{i=1}^{n} z^{x_i} - \sum_{i=1}^{n} z^{y_i}$$

Remark A.2.2. Note that for any $c \in \mathbb{C}$, we have $z^c = e^{c\ln(z)}$. Since

$$(z^c)' = (e^{c\ln(z)})' = c\frac{1}{z}e^{c\ln(z)} = cz^{c-1},$$

and all we need for the proof is differentiation, we can use this fact formally. Similarly, since the terms in (iii) are not polynomials, we consider the division to refer to the order of the zero at 1.

Proof. $((i) \Rightarrow (ii))$ Suppose (i) holds. Now we examine the polynomial

$$\prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i).$$

Note that from the identity (A.3), the coefficient of x^j in this polynomial is

$$(-1)^{n-j}e_{n-j}(x_1, \ldots, x_n) - (-1)^{n-j}e_{n-j}(y_1, \ldots, y_n).$$

We make the following claim:

Claim: $e_j(x_1, \ldots, x_n) - e_j(y_1, \ldots, y_n) = 0$ for $j = 1, \ldots, k$.

Proof of Claim: We use induction on j. For $j = 1$, it follows from (A.1) and our hypothesis that

$$e_1(x_1, \ldots, x_n) - e_1(y_1, \ldots, y_n) = p_1(x_1, \ldots, x_n) - p_1(y_1, \ldots, y_n) = 0.$$

Now suppose our claim is true for $j = 1, \ldots, l$, for some $l < k$. Once again, from (A.1) we

have

$$\begin{aligned}
&(l+1)(e_{l+1}(x_1,\ldots,x_n) - e_{l+1}(y_1,\ldots,y_n)) \\
&\quad = \sum_{i=1}^{l+1}(-1)^{i-1}e_{l+1-i}(x_1,\ldots,x_n)p_i(x_1,\ldots,x_n) \\
&\quad\quad - \sum_{i=1}^{l+1}(-1)^{i-1}e_{l+1-i}(y_1,\ldots,y_n)p_i(y_1,\ldots,y_n) \\
&\quad = \sum_{i=1}^{l+1}(-1)^{i-1}e_{l+1-i}(x_1,\ldots,x_n)p_i(x_1,\ldots,x_n) \\
&\quad\quad - \sum_{i=1}^{l+1}(-1)^{i-1}e_{l+1-i}(x_1,\ldots,x_n)p_i(y_1,\ldots,y_n) \\
&\quad = \sum_{i=1}^{l+1}(-1)^{i-1}e_{l+1-i}(x_1,\ldots,x_n)(p_i(x_1,\ldots,x_n) - p_i(y_1,\ldots,y_n)) \\
&\quad = 0,
\end{aligned}$$

proving the claim.

Thus, the coefficient of z^j is zero for $j = n-k,\ldots,n$, as desired.

$((ii) \Rightarrow (i))$ We more or less use the reverse of the above argument. Suppose (ii) holds. Thus, the coefficient of z^j is zero for $j = n-k,\ldots,n$. From the identity (A.3), it follows that $e_j(x_1,\ldots,x_n) - e_j(y_1,\ldots,y_n) = 0$ for $j = 1,\ldots,k$. We make the following claim, which will be sufficient to prove (i):

Claim: $p_j(x_1,\ldots,x_n) - p_j(y_1,\ldots,y_n) = 0$ for $j = 1,\ldots,k$.

Proof of Claim: We use induction on j. For $j = 1$, it follows from the definition of the first symmetric polynomial that

$$p_1(x_1,\ldots,x_n) - p_1(y_1,\ldots,y_n) = e_1(x_1,\ldots,x_n) - e_1(y_1,\ldots,y_n) = 0.$$

Now suppose our claim is true for $j = 1, \ldots, l$, for some $l < k$. From (A.2), we have

$$\begin{aligned}
&p_{l+1}(x_1, \ldots, x_n) - p_{l+1}(y_1, \ldots, y_n) \\
&\quad = (-1)^l (l+1) e_{l+1}(x_1, \ldots, x_n) + \sum_{i=1}^{l} (-1)^{l+1-i} e_{l+1-i}(x_1, \ldots, x_n) p_i(x_1, \ldots, x_n) \\
&\qquad - (-1)^l (l+1) e_{l+1}(y_1, \ldots, y_n) - \sum_{i=1}^{l} (-1)^{l+1-i} e_{l+1-i}(y_1, \ldots, y_n) p_i(y_1, \ldots, y_n) \\
&\quad = \sum_{i=1}^{l} (-1)^{l+1-i} e_{l+1-i}(x_1, \ldots, x_n) p_i(x_1, \ldots, x_n) \\
&\qquad - \sum_{i=1}^{l} (-1)^{l+1-i} e_{l+1-i}(y_1, \ldots, y_n) p_i(x_1, \ldots, x_n) \\
&\quad = \sum_{i=1}^{l} (-1)^{l+1-i} p_i(x_1, \ldots, x_n) (e_{l+1-i}(x_1, \ldots, x_n) - e_{l+1-i}(y_1, \ldots, y_n)) \\
&\quad = 0,
\end{aligned}$$

proving the claim.

$((i) \Rightarrow (iii))$ Suppose (i) holds. We now examine the object

$$\sum_{i=1}^{n} z^{x_i} - \sum_{i=1}^{n} z^{y_i}. \tag{A.4}$$

Note that (A.4) is necessarily a polynomial only when $\mathcal{O} = \mathbb{Z}$. The jth derivative with respect to z of (A.4) is

$$\sum_{i=1}^{n} x_i (x_i - 1) \cdots (x_i - j + 1) z^{x_i - j} - \sum_{i=1}^{n} y_i (y_i - 1) \cdots (y_i - j + 1) z^{y_i - j}. \tag{A.5}$$

Substituting $z = 1$ into (A.5), applying identity (A.3) and grouping terms gives

$$\begin{aligned}
&\sum_{i=1}^{n} x_i(x_i-1)\cdots(x_i-j+1) - \sum_{i=1}^{n} y_i(y_i-1)\cdots(y_i-j+1) \\
&\quad = \sum_{i=1}^{n}\sum_{l=0}^{j}(-1)^l e_l(0,1,\ldots,j-1)x_i^{j-l} - \sum_{i=1}^{n}\sum_{l=0}^{j}(-1)^l e_l(0,1,\ldots,j-1)y_i^{j-l} \\
&\quad = \sum_{i=1}^{n}\sum_{l=0}^{j}(-1)^l e_l(0,1,\ldots,j-1)(x_i^{j-l} - y_i^{j-l}). \qquad \text{(A.6)}
\end{aligned}$$

It follows from our hypothesis that for $j = 1,\ldots,k$ (A.6) is zero, and so (A.5) has a root at 1 for $j = 1,\ldots,k$. Hence, (A.4) has a root of order $k+1$ at $z = 1$, proving (iii).

$((iii) \Rightarrow (i))$ Once again, we use more or less the reverse argument. Suppose (iii) holds. Then we have

$$\sum_{i=1}^{n}\sum_{l=0}^{j-1}(-1)^l e_l(0,1,\ldots,j-1)(x_i^{j-l} - y_i^{j-l}) = 0 \qquad \text{(A.7)}$$

for $j = 1,\ldots,k$. (Note that the $l = j$ term has been omitted since it is identically zero.) We make the following claim, which will be sufficient to prove (i):

Claim: $p_j(x_1,\ldots,x_n) - p_j(y_1,\ldots,y_n) = 0$ for $j = 1,\ldots,k$.

Proof of Claim: We use induction on j. For $j = 1$, (A.7) gives us

$$0 = \sum_{i=1}^{n} e_0(0)(x_i - y_i) = \sum_{i=1}^{n} x_i - \sum_{i=1}^{n} y_i,$$

since $e_0(0) = 1$. Now assume our claim is true for $j = 1,\ldots,m$ for some $m < k$. Once again, from (A.7), we have

$$\begin{aligned}
0 &= \sum_{i=1}^{n}\sum_{l=0}^{m}(-1)^l e_l(0,1,\ldots,m)(x_i^{m+1-l} - y_i^{m+1-l}) \\
&= \sum_{i=1}^{n} e_0(0,1,\ldots,m)(x_i^{m+1} - y_i^{m+1}) \\
&= \sum_{i=1}^{n} x_i^{m+1} - \sum_{i=1}^{n} y_i^{m+1},
\end{aligned}$$

proving the claim. □

We have the following results, found in both [17] and [4], originally due to M. Frolov.

Proposition A.2.3. *Suppose* $\{x_1, \ldots, x_n\}$ *and* $\{y_1, \ldots, y_n\}$ *are subsets of* $\mathcal{O}$*. If*

$$\{x_1, \ldots, x_n\} =_k \{y_1, \ldots, y_n\}$$

then

$$\{x_1, \ldots, x_n, y_1 + M, \ldots, y_n + M\} =_{k+1} \{x_1 + M, \ldots, x_n + M, y_1, \ldots, y_n\},$$

for any $M \in \mathcal{O}$*.*

Proof. Suppose $\{x_1, \ldots, x_n\} =_k \{y_1, \ldots, y_n\}$. Then from Lemma A.2.1, we have that

$$\sum_{i=1}^{n} z^{x_i} - \sum_{i=1}^{n} z^{y_i}$$

has a zero of order k at $z = 1$. Since $z^M - 1$ has a zero of order at least one at $z = 1$, it follows that

$$(z^M - 1)\left(\sum_{i=1}^{n} z^{x_i} - \sum_{i=1}^{n} z^{y_i}\right) = \left(\sum_{i=1}^{n} z^{x_i+M} + \sum_{i=1}^{n} z^{y_i}\right) - \left(\sum_{i=1}^{n} z^{y_i+M} + \sum_{i=1}^{n} z^{x_i}\right)$$

has a zero of order at least $k + 1$ at $z = 1$, which again by Lemma A.2.1 proves the proposition. □

Proposition A.2.4. *Suppose* $\{x_1, \ldots, x_n\}$ *and* $\{y_1, \ldots, y_n\}$ *are subsets of* $\mathcal{O}$*. If*

$$\{x_1, \ldots, x_n\} =_k \{y_1, \ldots, y_n\},$$

then

$$\{Mx_1 + K, \ldots, Mx_n + K\} =_k \{My_1 + K, \ldots, My_n + K\},$$

for any $M, K \in \mathcal{O}$*.*

Proof. Let $j \in \{1, \ldots, k\}$. Then we have

$$\begin{aligned}\sum_{i=1}^{n}(Mx_i + K)^j - \sum_{i=1}^{n}(My_i + K)^j &= \sum_{i=1}^{n}\sum_{l=0}^{j}\binom{j}{l}(Mx_i)^l K^{j-l} - \sum_{i=1}^{n}\sum_{l=0}^{j}\binom{j}{l}(My_i)^l K^{j-l} \\ &= \sum_{l=0}^{j}\binom{j}{l}M^l K^{j-l}\left(\sum_{i=1}^{n}x_i^l - \sum_{i=1}^{n}y_i^l\right) \\ &= 0,\end{aligned}$$

proving the proposition. □

We now prove Theorems 3.2.1 and 3.2.2 which were stated in Chapter 3 and are generalizations of Proposition 2.3 and 3.1 from [27] for the $\mathcal{O}$-PTE problem:

Theorem A.2.5 (3.2.1)**.** *Suppose $\mathcal{O}$ is a* UFD*. Let $q \in \mathcal{O}$ be a prime with $N(q) > 3$. Then $N(q) \mid C_{N(q)}$.*

Proof. As discussed above, we have that $\langle q \rangle$ is a prime ideal of $\mathcal{O}$, and so $F_q := \mathcal{O}/\langle q \rangle$ is a finite field of order $N(q)$. Recall that Lagrange's Theorem says that for any nonzero element $a \in F_q$, we have $a^{N(q)-1} = 1$. This is the observation that allows us to generalize Proposition 2.3 from [27].

Thus suppose $X\{x_1, \ldots, x_{N(q)}\}$ and $Y = \{y_1, \ldots, y_{N(q)}\}$ are subsets of $\mathcal{O}$, and

$$\{x_1, \ldots, x_{N(q)}\} =_{N(q)-1} \{y_1, \ldots, y_{N(q)}\}$$

is a solution to the $\mathcal{O}$-PTE problem. From Proposition A.2.3, without loss of generality, we can assume that $y_1 = 0$. Suppose $N(q) \nmid x_i$ for all $i = 1, \ldots, N(q)$, and thus, $N(q) \nmid C_{N(q),X,Y}$. Then

$$p_{N(q)-1}(x_1, \ldots, x_{N(q)}) = \sum_{i=1}^{N(q)} x_i^{N(q)-1} \equiv 0 \pmod{N(q)},$$

since it is a sum of $N(q)$ terms all congruent to 1 modulo $N(q)$. By hypothesis, we have

$$p_{N(q)-1}(y_1, \ldots, y_{N(q)}) = p_{N(q)-1}(x_1, \ldots, x_{N(q)}) \equiv 0 \pmod{N(q)}.$$

However, since $y_1 = 0$, it follows that $p_{N(q)-1}(y_1, \ldots, y_{N(q)})$ is a sum of at most $N(q) - 1$ nonzero terms all congruent to 0 or 1 modulo $N(q)$, which sum to 0 modulo $N(q)$. Thus, each of the terms is zero modulo $N(q)$ and we have $y_i \equiv 0 \pmod{N(q)}$ for $i = 1, \ldots, N(q)$.

From Lemma A.2.1, we have

$$(x-x_1)\cdots(x-x_{N(q)})-(x-y_1)\cdots(x-y_{N(q)})=C_{N(q),X,Y}.$$

Considering this modulo $N(q)$, we get

$$(x+C_{N(q),X,Y})^{N(q)}\equiv(x-x_1)\cdots(x-x_{N(q)}) \pmod{N(q)},$$

and since $F_q[x]$ is a unique factorization domain, it follows that

$$x_1\equiv\ldots\equiv x_{N(q)}\equiv -C_{N(q),X,Y} \pmod{N(q)}.$$

Let $x_i=-C_{N(q),X,Y}+a_iN(q)$ for some $a_i\in\mathcal{O}$ for $i=1,\ldots,N(q)$, and note that $p_k(y_1,\ldots,y_{N(q)})=p_k(x_1,\ldots,x_{N(q)})\equiv 0 \pmod{N(q)^2}$ for $k\geq 2$. Thus, taking $k=2$ and $k=3$, it follows that

$$N(q)C_{N(q),X,Y}^2-2C_{N(q),X,Y}N(q)\sum_{i=1}^{N(q)}a_i\equiv\sum_{i=0}^{N(q)}(-C_{N(q),X,Y}+a_iN(q))^2\equiv 0 \pmod{N(q)^2} \tag{A.8}$$

and

$$-N(q)C_{N(q),X,Y}^3+3C_{N(q),X,Y}^2N(q)\sum_{i=1}^{N(q)}a_i\equiv\sum_{i=0}^{N(q)}(-C_{N(q),X,Y}+a_iN(q))^3\equiv 0 \pmod{N(q)^2}. \tag{A.9}$$

From our assumption that $N(q)\nmid x_i$ for all $i=1,\ldots,N(q)$, it follows that $N(q)\nmid C_{N(q),X,Y}$, and so we can divide (A.8) and (A.9) through by the appropriate power of $C_{N(q),X,Y}$ getting

$$C_{N(q),X,Y}+2\sum_{i=1}^{N(q)}a_i\equiv C_{N(q),X,Y}+3\sum_{i=1}^{N(q)}a_i\equiv 0 \pmod{N(q)}.$$

It follows immediately from this that $C_{N(q),X,Y}\equiv 0 \pmod{N(q)}$, which is a contradiction, proving the result. □

Theorem A.2.6 (3.2.2). *Suppose $\mathcal{O}$ is a* UFD. *Let $q\in\mathcal{O}$ be a prime such that*

$$n+3\leq N(q)<n+3+\frac{n-2}{6}.$$

Then $q\mid C_{n+1}$.

Before we prove this result, we need to prove a Lemma. As above, let $\mathbb{F}_q$ denote the field $\mathcal{O}/\langle q \rangle$, of size $N(q)$.

Lemma A.2.7. *Let $q \in \mathcal{O}$ with $N(q) > n+1$. Suppose $p_1(x)$ and $p_2(x)$ are monic polynomials in $\mathbb{F}_q[x]$ such that all their zeroes are in $\mathbb{F}_q$, and which satisfy $p_1(x) - p_2(x) = C$, for some nonzero $C \in \mathbb{F}_q$, and let $\mathcal{M}_i(a)$ denote the multiplicity of a zero $a \in \mathbb{F}_q$ of p_i. Then it follows that*

$$\mathcal{M}_1(x) - \mathcal{M}_2(x) = h(x)$$

where $h(x) \in \mathbb{F}_q[x]$ of degree exactly $N(q) - n - 2$.

Proof. We first make the following claim:
Claim: $\mathcal{M}_1(x) = (x - x^{N(q)})p_1'(x)/p_1(x)$
Proof of Claim: Let $p_1(x) = \prod_{a=0}^{N(q)-1}(x-a)^{m_a}$. Then we have that

$$\begin{aligned}(x - x^{N(q)})p_1'(x)/p_1(x) = (x - x^{N(q)}) \sum_{a=0}^{N(q)-1} \frac{m_a}{x-a} &= \sum_{a=0}^{N(q)-1} \frac{m_a}{x-a}((x-a) - (x-a)^{N(q)}) \\ &= \sum_{a=0}^{N(q)-1} m_a(1 - (x-a)^{N(q)-1}).\end{aligned}$$

We note that at $x = a$, this is equal to m_a, proving the claim.

Similarly, we have $\mathcal{M}_2(x) = (x - x^{N(q)})p_2'(x)/p_2(x)$. Since $p_1(x) - p_2(x)$ is a constant in $\mathbb{F}_q$, it follows that $p_1'(x) = p_2'(x)$, and so we have

$$\mathcal{M}_1(x) - \mathcal{M}_2(x) = \frac{C(x^{N(q)} - x)p_1'(x)}{p_1(x)p_2(x)}. \tag{A.10}$$

We define the right hand side of (A.10) to be $h(x)$, and we have

$$\deg h(x) = N(q) + n - 2(n+1) = N(q) - n - 2,$$

proving the Lemma. □

We now proceed with the proof of the Theorem:

Proof. Suppose $X = \{\alpha_1, \ldots, \alpha_{n+1}\}$ and $Y = \{\beta_1, \ldots, \beta_{n+1}\}$ are subsets of $\mathcal{O}$ with $X =_n Y$, with particular associated constant $C_{n+1,X,Y}$. Also, suppose that $N(q) \geq n+3$ and $q \nmid C_{n+1,X,Y}$. From Lemma A.2.1 we have that

$$(x-\alpha_1)\cdots(x-\alpha_{n+1}) - (x-\beta_1)\cdots(x-\beta_{n+1}) = C_{n+1,X,Y}.$$

We now take $p_1(x) = (x-\alpha_1)\cdots(x-\alpha_{n+1})$ and $p_2(x) = (x-\beta_1)\cdots(x-\beta_{n+1})$ and apply Lemma A.2.7. For $j = 0, 1, \ldots, n+1$, let

$$N_j := \#\{\text{roots of } p_1 \text{ of multiplicity } j\} + \#\{\text{roots of } p_2 \text{ of multiplicity } j\}.$$

Then for $j > 0$, it follows that

$$N_j \leq \#\{a : h(a) = j \in \mathbb{F}_q\} + \#\{a : h(a) = -j \in \mathbb{F}_q\} \leq 2\deg h(x) = 2(N(q) - n - 2).$$

Similarly, by counting the elements of $\mathbb{F}_q$, we see that $N_0 \leq N(q) - n - 2$. Thus, we get that $\sum_{j=0}^{n+1} N_j = N(q)$ and $\sum_{j=0}^{n+1} jN_j = \deg p_1(x) + \deg p_2(x) = 2(n+1)$. Hence, we have

$$\begin{aligned} N_1 + N_2 + N_3 + \ldots + N_{n+1} &= p - N_0 \geq (p - (N(q) - n - 2)) - n = n + 2 \\ N_2 + N_3 + \ldots + N_{n+1} &\geq n + 2 - N_1 \geq n + 2 - 2(N(q) - n - 2) \\ N_3 + \ldots + N_{n+1} &\geq n + 2 - 2k - N_2 = n + 2 - 4(N(q) - n - 2) \end{aligned}$$

Adding these inequalities gives

$$2(n+1) = \sum_{j=0}^{n+1} \geq N_1 + 2N_2 + 3(N_3 + \ldots + N_{n+1} \geq 3n + 6 - 6(N(q) - n - 2),$$

that is, $N(q) - n - 2 \geq (n+4)/6$, giving $N(q) \geq n + 2 + (n+4)/6 = n + 3 + (n-2)/6$. Thus, if $N(q) < n + 3 + (n-2)/6$, then we must have $q \mid C_{n,X,Y}$, and since X and Y were arbitrary, we have proved the Theorem. □

References

[1] A. Alpers and R. Tijdeman. The two-dimensional Prouhet-Tarry-Escott problem. *J. Number Theory*, 123(2):403–412, 2007.

[2] B. Borchert, P. McKenzie, and K. Reinhardt. Few product gates but many zeros. In *Mathematical foundations of computer science 2009*, volume 5734 of *Lecture Notes in Comput. Sci.*, pages 162–174. Springer, Berlin, 2009.

[3] P. Borwein. *Computational excursions in analysis and number theory*. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, 10. Springer-Verlag, New York, 2002.

[4] P. Borwein and C. Ingalls. The Prouhet-Tarry-Escott problem revisited. *Enseign. Math. (2)*, 40(1-2):3–27, 1994.

[5] P. Borwein, P. Lisoněk, and C. Percival. Computational investigations of the Prouhet-Tarry-Escott problem. *Math. Comp.*, 72(244):2063–2070, 2003.

[6] D. Broadhurst. A Chinese Prouhet-Tarry-Escott solution. http://physics.open.ac.uk/~dbroadhu/cpte.pdf, 2007.

[7] T. Caley. The Prouhet-Tarry-Escott problem for Gaussian integers. *Math. Comp.*, to appear.

[8] J. Chernick. Ideal Solutions of the Tarry-Escott Problem. *Amer. Math. Monthly*, 44(10):626–633, 1937.

[9] A. Choudhry. Ideal solutions of the Tarry-Escott problem of degree four and a related Diophantine system. *Enseign. Math. (2)*, 46(3-4):313–323, 2000.

[10] A. Choudhry. Ideal solutions of the Tarry-Escott problem of degrees four and five and related Diophantine systems. *Enseign. Math. (2)*, 49(1-2):101–108, 2003.

[11] A. Choudhry. Matrix analogues of the Tarry-Escott problem, multigrade chains and the equation of Fermat. *Math. Student*, 75(1-4):215–224 (2007), 2006.

[12] A. Choudhry and J. Wróblewski. Ideal solutions of the Tarry-Escott problem of degree eleven with applications to sums of thirteenth powers. *Hardy-Ramanujan J.*, 31:1–13, 2008.

[13] M. Cipu. Upper bounds for norms of products of binomials. *LMS J. Comput. Math.*, 7:37–49, 2004.

[14] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[15] H. Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[16] I. Connell. Addendum to a paper of K. Harada and M.-L. Lang: "Some elliptic curves arising from the Leech lattice" [J. Algebra **125** (1989), no. 2, 298–310; MR1018947 (90g:11072)]. *J. Algebra*, 145(2):463–467, 1992.

[17] L. E. Dickson. *History of the theory of numbers. Vol. II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966.

[18] H. L. Dorwart and O. E. Brown. The Tarry-Escott Problem. *Amer. Math. Monthly*, 44(10):613–626, 1937.

[19] M. Frolov. Égalités à deux degrés. *Bull. Soc. Math. France*, 17:69–83, 1889.

[20] A. Gloden. *Mehrgradige Gleichungen*. Noordhoff, Berlin, 1982.

[21] S. Hernández and F. Luca. Integer roots chromatic polynomials of non-chordal graphs and the Prouhet-Tarry-Escott problem. *Graphs Combin.*, 21(3):319–323, 2005.

[22] L. K. Hua. *Introduction to number theory*. Springer-Verlag, Berlin, 1982. Translated from the Chinese by Peter Shiu.

[23] H. Kleiman. A note on the Tarry-Escott problem. *J. Reine Angew. Math.*, 278/279:48–51, 1975.

[24] R. Maltby. Pure product polynomials and the Prouhet-Tarry-Escott problem. *Math. Comp.*, 66(219):1323–1340, 1997.

[25] Z. A. Melzak. A note on the Tarry-Escott problem. *Canad. Math. Bull.*, 4:233–237, 1961.

[26] S. Prugsapitak. The Tarry-Escott problem of degree two. *Period. Math. Hungar.*, 65(1):157–165, 2012.

[27] E. Rees and C. Smyth. On the constant in the Tarry-Escott problem. In *Cinquante ans de polynômes (Paris, 1988)*, volume 1415 of *Lecture Notes in Math.*, pages 196–208. Springer, Berlin, 1990.

[28] K. Rubin and A. Silverberg. Ranks of elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 39(4):455–474 (electronic), 2002.

[29] C. Shuwen. The Prouhet-Tarry-Escott Problem. http://euler.free.fr/eslp/TarryPrb.htm.

[30] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[31] D. Simon. Programme de calcul du rang des courbes elliptiques dans les corps de nombres. http://www.math.unicaen.fr/~simon/, 2011.

[32] C. J. Smyth. Ideal 9th-order multigrades and Letac's elliptic curve. *Math. Comp.*, 57(196):817–823, 1991.

[33] W. A. et al. Stein. Sage Mathematics Software (version 4.6.2). http://www.sagemath.org, 2012.

[34] C. L. Stewart. personal communication, 2011.

[35] C. L. Stewart and J. Top. On ranks of twists of elliptic curves and power-free values of binary forms. *J. Amer. Math. Soc.*, 8(4):943–973, 1995.

[36] I. Stewart and D. Tall. *Algebraic number theory and Fermat's last theorem*. A K Peters Ltd., Natick, MA, third edition, 2002.

[37] A. Černý. On Prouhet-Like Solutions to the Prouhet-Tarry-Escott Problem, to appear.

[38] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.

[39] E. M. Wright. On Tarry's problem (i). *Quart. J. Math., Oxford Ser.*, 6:261–267, 1935.