2015

# Nonexistence of Solutions to Certain Families of Diophantine Equations

Eva G. Goedhart
*Bryn Mawr College*

# The Nonexistence of Solutions to Certain Families of Diophantine Equations

by

Eva G. Goedhart

May 2015

Submitted to the Faculty of Bryn Mawr College
in partial fulfillment of the requirements for
the degree of Doctor of Philosophy

# ABSTRACT

In this work, I examine specific families of Diophantine equations and prove that they have no solutions in positive integers. The proofs use a combination of classical elementary arguments and powerful tools such as Diophantine approximations, Lehmer numbers, the modular approach, and earlier results proved using linear forms in logarithms. In particular, I prove the following three theorems.

**Main Theorem I.** *Let $a$, $b$, $c$, $k \in \mathbb{Z}^+$ with $k \geq 7$. Then the equation*

$$(a^2cX^k - 1)(b^2cY^k - 1) = (abcZ^k - 1)^2$$

*has no solutions in integers $X$, $Y$, $Z > 1$ with $a^2X^k \neq b^2Y^k$.*

**Main Theorem II.** *Let $L$, $M$, $N \in \mathbb{Z}^+$ with $N > 1$. Then the equation*

$$NX^2 + 2^L3^M = Y^N$$

*has no solutions with $X$, $Y \in \mathbb{Z}^+$ and $\gcd(NX, Y) = 1$.*

**Main Theorem III.** *Let $p$ be an odd rational prime and let $N$, $\alpha$, $\beta$, $\gamma \in \mathbb{Z}$ with $N > 1$, $\alpha \geq 1$, and $\beta$, $\gamma \geq 0$. Then the equation*

$$X^{2N} + 2^{2\alpha}5^{2\beta}p^{2\gamma} = Z^5$$

*has no solutions with $X$, $Z \in \mathbb{Z}^+$ and $\gcd(X, Z) = 1$.*

# DEDICATION

*To my family*

# ACKNOWLEDGMENTS

Starting as a freshman, I thought I would be either an art major or a mathematics major. When I realized that I would have to sell my artwork to make a living, I decided mathematics was much more appealing. In the years that followed, I took every pure mathematics course at James Madison University and was still thirsty for more. Thanks to the recommendations of Carl Droms and Gary Peterson, I continued to quench that thirst for knowledge at Wake Forest University, where I worked with Kenneth Berenhaut and Fred Howard.

It was Fred who helped to determine the next step on my path to a mathematics career. While at a conference in Germany, Fred introduced me to Helen Grundman. He sat me down next to her and encouraged us to get to know each other. I had no idea that Fred had just set me up on a date with my future.

It was because of that meeting that I applied to Bryn Mawr College to work with Helen Grundman, and she has been my adviser ever since. She has let me choose my own way while guiding me around road blocks and obstacles, even if that meant occasionally turning me around entirely. I do not know enough words to express how much she has taught me, though she has also taught me many words and the grammar to go with them. I am grateful for her innumerable hours of hard work, encouragement, and countless cookies over the years.

I would not have made it to the finish line without the additional knowledge and support of my professors and mentors Paul Melvin, Leslie Cheng, Lisa Traynor, Rhonda Hughes, Djordje Milićević, Robert Styer, and Marvin Knopp. Though Marvin is no longer with us, he and the members of the local number theory community have been inspiring.

I thank the entire Bryn Mawr Mathematics Department for being encouraging at

every step, especially the past and present graduate students. They have been my personal cheerleading squad, of which Daniel Wisniewski and Beth Campbell-Hetrick have always been the co-captains.

Finally, I would like to thank my family. I am especially grateful to my husband, Erik, and my young daughter, Aedlin, who has never known me not to be working on my dissertation.

# Contents

# Chapter 1

# Introduction

In Alexandria, circa 250 A.D., Diophantus authored the multi-volume book *Arithmetica*, sparking the development of mathematical notation and algebraically solving various equations [23]. It is for this reason that equations solved in integers are named for Diophantus. Specifically, a *Diophantine equation* is a polynomial equation in one or more variables with integer coefficients. *Diophantine analysis* is the process of solving Diophantine equations and inequalities for integer solutions.

In the early seventeenth century, Pierre de Fermat wrote, in the margins of his edition of *Arithmetica*, that he had proven that the Diophantine equation

$$X^N + Y^N = Z^N$$

has no integer solutions with $XYZ \neq 0$ and $N > 2$. His claim was named *Fermat's Last Theorem* and remained unsolved for hundreds of years. The final piece of the proof was completed by A. Wiles [81] and Taylor and Wiles [71]. Now, the proof is one of the most widely known examples of how Diophantine analysis has led to new tools and techniques in mathematics.

Diophantine analysis continues to provide a multitude of alluring problems and beautiful results. In this work, we prove three new results, as stated in the abstract, showing that some specific families of Diophantine equations have no positive integer solutions (see also [36–38]).

In Chapter 2, we review definitions and results that are relevant to the proofs of the main theorems. Specifically, in Section 2.1, we review some algebraic number theory including binary quadratic forms, which are used to construct Lehmer pairs in the proof of Main Theorem II. In Section 2.2, we describe some results on Diophantine approximations used to prove Main Theorem I. Lehmer pairs are defined and discussed in Section 2.3. Finally, in Section 2.4, we state versions of the Modularity Theorem. This theorem is key to the modular approach used in proving Main Theorem III.

In each of the next three chapters, we restate one of the main results, give a brief history of the problem, provide the necessary related results, and present the proof of that main theorem.

# Chapter 2

# Background

## 2.1 Algebraic Number Theory

In this section, we give a short review of relevant terminology and results from algebraic number theory. We define binary quadratic forms and relate these forms to the class numbers of quadratic number fields (see [52,68] for more information on algebraic number theory and [25,27,40] specifically for binary quadratic forms).

A number $\alpha \in \mathbb{C}$ is called an *algebraic number* if it is a zero of a nonzero polynomial $f(X) = \sum_{i=0}^{k} a_i X^i \in \mathbb{Q}[X]$ with $a_k \neq 0$. If $f(X)$ is an irreducible polynomial, then $f(X)$ is called the *minimal polynomial* of $\alpha$, $a_k$ is the *leading coefficient* of $f(X)$, and $deg(f(X)) = k$ is its *degree*. We also say that $k$ is the degree of $\alpha$. The set of algebraic numbers forms a subring of $\mathbb{C}$, denoted $\overline{\mathbb{Q}}$. Fix $\overline{\mathbb{Q}}$ for the remainder of this work.

A *number field* is a finite extension field of the rational numbers $\mathbb{Q}$ contained in $\mathbb{C}$. Let $K$ be an arbitrary number field. Let $\alpha \in K$ and let $f(X)$ be its minimal polynomial. The zeros of $f(X)$, denoted $\alpha^{(j)}$ for $1 \leq j \leq deg(f(X))$ are called the *conjugates* of $\alpha$. The product of all of the conjugates of $\alpha$ is given by the norm map. For $\theta \in K$, the *norm*, $N : K \to \mathbb{Q}$ is defined by $N(\theta) = \prod_{j=1}^{k} \theta^{(j)} \in \mathbb{Q}$.

If $\alpha$ is a zero of some nonzero monic polynomial in $\mathbb{Z}[X]$, then $\alpha$ is called an *algebraic integer*. The *ring of integers* of $K$, denoted $\mathcal{O}_K$, is the set of all algebraic integers in $K$. It is well-known that $\mathcal{O}_K$ is a finitely generated free abelian group and thus has an integral basis $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ where $k = [K : \mathbb{Q}]$. The *discriminant* of $\mathcal{O}_K$ is $\text{disc}(\mathcal{O}_K) = (\det[\alpha_i^{(j)}])^2$, for $1 \leq i, j \leq k$.

In $\mathcal{O}_K$, every nonzero ideal can be factored uniquely (up to order) into a product of prime ideals. Let $F \subseteq K$ be number fields and let $\mathfrak{p} \subseteq \mathcal{O}_K$ and $\mathfrak{q} \subseteq \mathcal{O}_F$ be prime ideals. If $\mathfrak{q}\mathcal{O}_K \subseteq \mathfrak{p}$, then we say that $\mathfrak{p}$ *lies over* $\mathfrak{q}$ or $\mathfrak{q}$ *lies under* $\mathfrak{p}$. Further, since every number field contains $\mathbb{Q}$, each prime ideal $\mathfrak{p}$ lies over a unique rational prime $p$.

Given two ideals $I$, $J \subseteq \mathcal{O}_K$, the usual sum and product of I and J are the ideals defined by

$$I + J = \{a + b \,|\, a \in I, b \in J\}$$

and

$$IJ = \left\{ \sum_{i=1}^{d} a_i b_i \,|\, a_i \in I, b_i \in J, d \in \mathbb{Z}^+ \right\}.$$

Ideals $I$ and $J$ are *equivalent* if and only if $\alpha I = \beta J$ for some $\alpha$, $\beta \in \mathcal{O}_K$. The equivalence class of $I$, denoted $[I]$, is called an *ideal class*. The ideal classes form the *ideal class group* under the multiplication induced by the product of ideals, $[I][J] = [IJ]$. The identity element is the class of principal ideals, $[\mathcal{O}_K]$. Therefore, $s \in \mathbb{Z}^+$ is the *order* of an ideal class $[I]$ if and only if $s$ is the smallest integer such that $I^s$ is a principal ideal. The size of the ideal class group, $h_K$, is called the *class number* of $K$. Thus, if $s$ is the order of an ideal class, then $s \mid h_K$. Note that $h_K = 1$ if and only if $\mathcal{O}_K$ is a principal ideal domain.

A *quadratic field* is a number field of degree 2 over $\mathbb{Q}$. We recall the following well-known properties of quadratic fields. Each quadratic field can be written in the form $F = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ is square-free. Let $d \in \mathbb{Z} - \{0\}$ be square-free. If

$d \neq -1$ or $-3$, then the only roots of unity in $\mathbb{Q}(\sqrt{d})$ are 1 and $-1$. Further, if $d \not\equiv 1 \pmod 4$, then $\mathcal{O}_F = \mathbb{Z}[\sqrt{d}]$ and has $\text{disc}(\mathcal{O}_F) = 4d$, while if $d \equiv 1 \pmod 4$, $\mathcal{O}_F = \mathbb{Z}[(1+\sqrt{d})/2]$ and has $\text{disc}(\mathcal{O}_F) = d$. So, in either case, $\alpha \in \mathcal{O}_F$ can be written as $\alpha = U + V\sqrt{d}$ where $U$, $V \in \mathbb{Z}$ or $U$, $V \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$.

The class numbers of quadratic fields are closely related to the class numbers of quadratic forms. A *binary quadratic form* is a polynomial in $\mathbb{Z}[X, Y]$,

$$f(X, Y) = aX^2 + bXY + cY^2,$$

often denoted as $f = [a, b, c]$. The *discriminant* of $f = [a, b, c]$ is $D = b^2 - 4ac$. The form is called *positive definite* if $a > 0$ and $D < 0$. If $\gcd(a, b, c) = 1$, then $f$ is said to be *primitive*. Two quadratic forms $f$ and $g$ are *equivalent*, $f \sim g$, if and only if there exist $u$, $v$, $w$, $z \in \mathbb{Z}$ with $uz - vw = 1$ such that $g(X, Y) = f(uX + vY, wX + zY)$.

An integer, $D \in \mathbb{Z}$, is a *fundamental discriminant* if $D$ is a discriminant of a ring of integers of some quadratic number field. In other words, $D$ is a fundamental discriminant if $D \neq 1$, is square-free, and $D \equiv 1 \pmod 4$ or if $D/4 \equiv 2$ or $3 \pmod 4$, is square-free. It is easy to see that if $f$ has a fundamental discriminant $D$, then $f$ is primitive.

Let $k$, $x_0$, $y_0 \in \mathbb{Z}$ with $\gcd(x_0, y_0) = 1$ and let $f = [a, b, c]$ with $f(x_0, y_0) = k$. Then the expression $f(x_0, y_0)$ is called a *representation* of $k$. By [40, Theorem 11.4.1], there exist $u$, $v$, $\ell \in \mathbb{Z}$ such that

$$x_0 u - y_0 v = 1, \quad \ell = (2ax_0 + by_0)v + (bx_0 + 2cy_0)u, \text{ and } 0 \leq \ell < 2k. \tag{2.1}$$

The uniquely defined number $\ell$ is called the *characteristic number* of the representa-

tion $k = f(x_0, y_0)$. By [40, Section 11.4], $\ell = \ell(f, x_0, y_0)$ also satisfies

$$\ell^2 \equiv D \pmod{4k} \tag{2.2}$$

and

$$2ax_0 + by_0 \equiv -\ell y_0 \pmod{2k}. \tag{2.3}$$

Further, if two representations of $k$, $f(x_0, y_0) = k = g(x_1, y_1)$, have the same characteristic number, $\ell(f, x_0, y_0) = \ell(g, x_1, y_1)$, then $f \sim g$.

The following lemma, used in the proof of Theorem 22, is a special case of [40, Theorem 11.4.3].

**Lemma 1.** *Let $a$, $c$, $k \in \mathbb{Z}^+$. Let $f = [a, 0, c]$ be a primitive quadratic form of discriminant $D$ with $|D| > 4$. Let $x_0$, $y_0$, $x_1$, $y_1 \in \mathbb{Z}$ with $\gcd(x_0, y_0) = \gcd(x_1, y_1) = 1$ be such that $f(x_0, y_0)$ and $f(x_1, y_1)$ are two representations of $k$. Then, $\ell(f, x_0, y_0) = \ell(f, -x_0, -y_0)$. Further, if $\ell(f, x_0, y_0) = \ell(f, x_1, y_1)$, then*

$$(x_0, y_0) = (x_1, y_1) \text{ or } (x_0, y_0) = (-x_1, -y_1).$$

Let $[f]$ denote the equivalence class of a binary quadratic form $f$. It can be shown that any two equivalent binary quadratic forms have the same discriminant. Thus, all of the binary quadratic forms in an equivalence class have the same discriminant. We call this the discriminant of the class. We now describe a binary operation on equivalence classes of quadratic forms (see [25, Lemma 14.2.3]).

For equivalence classes $[f]$ and $[g]$ of discriminant $D$, there exist primitive forms $f' = [a, b, c] \in [f]$ and $g' = [r, s, t] \in [g]$ such that $\gcd(a, r) = 1$ and $b = s$. Using this notation, define the *composition* of equivalence classes by $[f][g] = [fg]$ where $fg = [ar, b, (b^2 - D)/4ar]$. The set of equivalence classes of positive definite binary quadratic

forms of discriminant $D$ forms a finite abelian group of under this composition. For a fixed $D$, let $f_D$ be a binary quadratic form of discriminant $D$ such that $f_D(x, y) = 1$ is a representation, for some $x$, $y \in \mathbb{Z}$. Then $[f_D]$ is the identity element of the group. It contains all binary quadratic forms of discriminant $D$ that can represent 1.

The number of equivalence classes of positive definite binary quadratic forms of discriminant $D$ is the *class number*, denoted $h(D)$. If $D$ is a fundamental discriminant, then $h(D) = h_F$, where $F = \mathbb{Q}(\sqrt{D})$ (see [27, Theorem 5.2.8]).

Let $D \in \mathbb{Z}$. Let the *Dirichlet character* mod $|D|$, $\chi : \mathbb{Z} \to \mathbb{C}$, be defined by $\chi(n) = \left(\frac{D}{n}\right)$, where $\left(\frac{D}{\cdot}\right)$ is Kronecker's extension of the Legendre symbol. The *Dirichlet L-function* of $\chi$ is defined by $L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$, for $s \in \mathbb{C}$ with $\Re(s) > 1$. Since the Dirichlet characters are periodic and take only roots of unity as values, it can be shown that, for $|D| \geq 3$,

$$L(1, \chi) < 2 + \log(|D|)$$

(see [55, Lemma 8.16] for the proof). If $D < 0$ is the discriminant of a positive definite binary quadratic form $f$, then $h(D)$ is given by the formula

$$h(D) = \frac{w\sqrt{|D|}}{2\pi} L(1, \chi),$$

where $w$ is the number of pairs $(x, y)$ such that $f(x, y) = k$ is a representation, which all have the same characteristic number (see [40, Theorem 11.4.3 & Theorem 12.10.1]). Further, if $D$ is a fundamental discriminant, then the *class number formula* for a quadratic field $F = \mathbb{Q}(\sqrt{D})$ with $D < 0$ is given by

$$h_F = \frac{\omega\sqrt{|D|}}{2\pi} L(1, \chi),$$

where $\omega$ is the number of roots of unity contained in $F$.

Combining each of the class number formulas and the bound for the Dirichlet $L$-function above yields a bound for the class numbers, stated explicitly in the lemma below.

**Lemma 2.** *Let $D \in \mathbb{Z}$ such that $D < 0$ and $|D| \geq 3$. Then*

$$h(D) < \frac{w\sqrt{|D|}}{\pi}\left(1 + \log\left(\sqrt{|D|}\right)\right).$$

*If $D$ is the discriminant of a field $F$, then*

$$h_F < \frac{\omega\sqrt{|D|}}{\pi}\left(1 + \log\left(\sqrt{|D|}\right)\right).$$

We use the following two lemmas in proving special cases that arise in Chapter 4. This first lemma [77, Lemma 3] is used in the proof of Theorem 27.

**Lemma 3** (Wang and Wang)**.** *Let $d \in \mathbb{Z}^+$ be square-free. If $d > 1$, then $h(-4d) < d$.*

*Sketch of proof.* Let $d \in \mathbb{Z}^+$ be square-free with $d > 1$. For a contradiction, suppose that $16 \leq d \leq h(-4d)$. Since $d > 1$, $-4d < -4$ and so, by [40, Theorem 11.4.3], $w = 2$. Then, by Lemma 2,

$$d \leq h(-4d) < \frac{2\sqrt{|-4d|}}{\pi}\left(1 + \log\left(\sqrt{|-4d|}\right)\right) = \frac{4\sqrt{d}}{\pi}\log\left(2e\sqrt{d}\right).$$

Let $f : [4, \infty) \to \mathbb{R}$ be defined by $f(z) = z - 4\log(2ez)/\pi$. The authors prove that $f$ is positive and increasing for $z \geq 4$. Thus, $z > 4\log(2ez)/\pi$ for $z \geq 4$. Since $d \geq 16$, $\sqrt{d} \geq 4$ and so $d > 4\sqrt{d}\log(2e\sqrt{d})/\pi$. Comparing this lower bound for $d$ with the upper bound yields

$$\frac{4\sqrt{d}}{\pi}\log\left(2e\sqrt{d}\right) < \frac{4\sqrt{d}}{\pi}\log\left(2e\sqrt{d}\right),$$

a contradiction.

For the remaining possible values of $d$, Wang and Wang list the values of $h(-4d)$ and verify that $d > h(-4d)$. □

The next lemma is used in the proof of Main Theorem II. Its proof is similar to that of Lemma 3.

**Lemma 4.** *Let $F = \mathbb{Q}(\sqrt{-mn})$ with $m$, $n > 1$ square-free relatively prime integers. If $m \leq 6$, then $h_F < 2n$.*

*Proof.* Let $F$ be as in the statement of the lemma. Then, $|D| = |\operatorname{disc}(\mathcal{O}_F)| \leq 4mn \leq 24n$, since $m \leq 6$. Also, since $mn \geq 2 \cdot 2 = 4$, the only roots of unity in $F = \mathbb{Q}(\sqrt{-mn})$ are 1 and $-1$, and so $\omega = 2$. Suppose, for a contradiction, that $2n \leq h_F$. By Lemma 2,

$$2n \leq h_F < \frac{2\sqrt{24n}}{\pi}\left(1 + \log\sqrt{24n}\right),$$

and so

$$1 < \frac{2\sqrt{6}}{\pi\sqrt{n}}\left(1 + \log\sqrt{24n}\right). \tag{2.4}$$

Define $f : [1, \infty) \to \mathbb{R}$ by $f(r) = (2\sqrt{6}/\pi\sqrt{r})\left(1 + \log\sqrt{24r}\right)$. The derivative of $f$ at $r \geq 1$ is

$$f'(r) = \frac{-\sqrt{6}}{\pi r\sqrt{r}}\left(\log\sqrt{24r}\right) < 0.$$

So, $f$ is a decreasing function. By a direct calculation, $f(51) < 0.995$, and therefore $f(r) < 1$ for $r \geq 51$. Now, from inequality (2.4), $1 < f(n)$. Hence, $n \leq 50$.

It follows that since $m \leq 6$, we have $mn \leq 300$. For arbitrary $d \in \mathbb{Z}^+$, there are class number tables for $\mathbb{Q}(\sqrt{-d})$ (see for example [18, Table 4]). By checking the values of class numbers for $\mathbb{Q}(\sqrt{-d})$ for $0 < d \leq 300$, we find that $h_{\mathbb{Q}(\sqrt{-d})} \leq 22$. Since $F = \mathbb{Q}(\sqrt{-mn})$ with $mn \leq 300$, $h_F \leq 22$. By assumption, $2n \leq h_F$, and so this

implies that $n \leq 11$. Again, using $m \leq 6$ we conclude that $mn \leq 66$. So, this time checking the table for $d \leq 66$, we find that $h_F \leq 8$. Again, by assumption $2n \leq h_F$ and so $n \leq 4$. Repeating this procedure, we find that $n \leq 1$, which is a contradiction. Hence, $h_F < 2n$. □

We now define and review some facts about biquadratic fields. We then prove Lemma 5 which is used in the proof of Main Theorem II. A *biquadratic field* is a degree 4 extension of $\mathbb{Q}$ with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$. Let $K$ be a biquadratic field. Then, there exist $m$, $n \in \mathbb{Z}$ distinct and square-free such that $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$. It is easy to see that $K$ contains exactly three quadratic fields, $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$, and $\mathbb{Q}(\sqrt{mn})$.

Information about $\mathcal{O}_K$ can be gleaned from information about the quadratic subfields of $K$, as in the following lemma.

**Lemma 5.** *Let $K = \mathbb{Q}(\sqrt{m}, \sqrt{-n})$ with $m \not\equiv 1 \pmod 4$ and $n > 1$ positive square-free relatively prime integers. If $\gamma \in \mathcal{O}_K$, then*

$$\gamma = A\sqrt{m} + B\sqrt{-n} + C\sqrt{-mn} + D$$

*for some $A$, $B$, $C$, $D \in \frac{1}{4}\mathbb{Z}$. Further, if $\gamma^2 \in \mathbb{Q}(\sqrt{-mn})$, then $A = B = 0$ or $C = D = 0$.*

*Proof.* Let $K$ be as in the lemma and assume that $\gamma \in \mathcal{O}_K$. Let $E_1 = \mathbb{Q}(\sqrt{m})$, and $E_2 = \mathbb{Q}(\sqrt{-n})$. Since $m \not\equiv 1 \pmod 4$, $\mathcal{O}_{E_1} = \mathbb{Z}[\sqrt{m}]$ and $\mathrm{disc}(\mathcal{O}_{E_1}) = 4m$.

If $n \equiv 1$ or $2 \pmod 4$, then $\mathcal{O}_{E_2} = \mathbb{Z}[\sqrt{-n}]$ and $\mathrm{disc}(\mathcal{O}_{E_2}) = -4n$. Since $\gcd(m, n) = 1$, we have $\gcd(4m, -4n) = 4$ and so, by [52, Theorem 12],

$$\mathcal{O}_K \subseteq \frac{1}{4}\mathbb{Z}\left[\sqrt{m}\right]\mathbb{Z}\left[\sqrt{-n}\right].$$

Therefore, $\gamma = A\sqrt{m} + B\sqrt{-n} + C\sqrt{-mn} + D$ for some $A$, $B$, $C$, $D \in \frac{1}{4}\mathbb{Z}$.

If $n \equiv 3 \pmod 4$, then $\mathcal{O}_{E_2} = \mathbb{Z}[(1+\sqrt{-n})/2]$ and $\operatorname{disc}(\mathcal{O}_{E_2}) = -n$. Since $\gcd(m,n) = 1$, we have $\gcd(4m,-n) = 1$. By [52, Theorem 12],

$$\mathcal{O}_K \subseteq \mathbb{Z}\left[\sqrt{m}\right]\mathbb{Z}\left[\frac{1+\sqrt{-n}}{2}\right].$$

Hence, $\gamma = A\sqrt{m} + B\sqrt{-n} + C\sqrt{-mn} + D$ for some $A$, $B$, $C$, $D \in \frac{1}{2}\mathbb{Z}$, completing the first part of the lemma.

Now, assume that $\gamma^2 \in \mathbb{Q}(\sqrt{-mn})$. Letting $\gamma = A\sqrt{m} + B\sqrt{-n} + C\sqrt{-mn} + D$, we have

$$\begin{aligned}\gamma^2 &= \left(A\sqrt{m} + B\sqrt{-n} + C\sqrt{-mn} + D\right)^2 \\ &= 2(AD - BCn)\sqrt{m} + 2(ACm + BD)\sqrt{-n} + 2(AB + CD)\sqrt{-mn} \\ &\qquad + (A^2m - B^2n - C^2mn + D^2)\end{aligned}$$

Since $\gamma^2 \in \mathbb{Q}(\sqrt{-mn})$, the coefficients of $\sqrt{-n}$ and $\sqrt{m}$ in this equation must be zero. So,

$$AD - BCn = 0 \tag{2.5}$$

and

$$ACm + BD = 0. \tag{2.6}$$

Combining these equations, we have $AD^2 + AC^2mn = 0$, implying that either $A = 0$ or $D^2 + C^2mn = 0$.

Assume that $C$ and $D$ are not both zero. Then, we have that $D^2 + C^2mn > 0$ and so $A = 0$. By equations (2.5) and (2.6), this implies that $BC = BD = 0$. Since $C$ and $D$ are not both zero, $B = 0$. Therefore, we have that $A = B = 0$.

Hence, either $A = B = 0$ or $C = D = 0$. □

## 2.2 Diophantine Approximation

*Diophantine approximation* is the study of how closely an algebraic number $\alpha$ can be approximated by a rational number $r/s$. In this section, we discuss some early results on Diophantine approximation, we fix notation for and review some standard properties of continued fractions, and state two results used in Chapter 3. (See [17] for a brief history and see [45,56] for details on continued fractions.)

Let $\alpha \in \overline{\mathbb{Q}} - \mathbb{Q}$ be of degree $n \geq 3$ and let $r/s \in \mathbb{Q}$. Since 1844, mathematicians sought lower bounds for the difference between $\alpha$ and $r/s$ of the form

$$\left|\alpha - \frac{r}{s}\right| > \frac{c}{s^{\lambda}} \tag{2.7}$$

with $c = c(\alpha, \lambda)$ and $\lambda \in \mathbb{R}$. Liouville's work [46], one of the earliest to be published, proves such a lower bound with $\lambda = n$ and with an effectively computable value of $c$. In 1918, Thue [73] improved the exponent to $\lambda = n/2 + 1$, but his proof was not constructive. In years following, Siegel [64], Dyson [34], Gel'fond [35], and Roth [62] all made significant improvement toward $\lambda = 2 + \varepsilon$, for $\epsilon > 0$. But again, the results were ineffective, proving only the existence of some $c$.

On the other hand, given an algebraic number, $\alpha$, continued fractions provide one approach to finding rational approximations $r/s \in \mathbb{Q}$ such that $|\alpha - r/s|$ is small. Let $\alpha \in \overline{\mathbb{Q}}$. The *simple continued fraction expansion* of $\alpha$,

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}},$$

with $a_0 \in \mathbb{Z}$ and $a_j \in \mathbb{Z}^+$, for $j \geq 1$, is denoted $\alpha = [a_0, a_1, a_2, \ldots]$. For $j \geq 0$, the number $a_j$ is called the *j-th partial quotient* of $\alpha$ and the value

$$\frac{p_j}{q_j} = [a_0, a_1, \ldots, a_j] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_j}}},$$

where $\gcd(p_j, q_j) = 1$, is the *j-th convergent* of $\alpha$. The sequence of denominators, $q_j$ satisfies the recursive formula, for $j > 1$,

$$q_j = a_j q_{j-1} + q_{j-2}, \tag{2.8}$$

with initial values $q_0 = 1$ and $q_1 = a_1$. This implies that the sequence $q_j$ is increasing for $j > 1$,

$$q_0 \leq q_1 < q_2 < \ldots < q_j.$$

The convergents of $\alpha$ satisfy

$$\frac{1}{q_j(q_j + q_{j+1})} < \left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j^2}. \tag{2.9}$$

In fact, the convergents are the best approximations of $\alpha$. More precisely, if $r/s \in \mathbb{Q}$ satisfies the inequality

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2}, \tag{2.10}$$

then $r/s$ must be equal to one of the continued fraction convergents of $\alpha$.

Combining inequalities (2.8) and (2.9), there is a standard lower bound using the $j+1$-st partial quotient, for each $j > 1$,

$$\left|\alpha - \frac{p_j}{q_j}\right| > \frac{1}{q_j^2(a_{j+1} + 2)}. \tag{2.11}$$

So, the convergents are very good rational approximations of $\alpha$, yet we still have lower bounds for the difference between $\alpha$ and its convergents.

Another property of continued fractions that we use in Chapter 3 includes the following. The odd indexed convergents decrease toward $\alpha$. Similarly, the even indexed convergents increase toward $\alpha$. So, for each $j \geq 0$, we have

$$\frac{p_{2j}}{q_{2j}} < \alpha < \frac{p_{2j+1}}{q_{2j+1}}. \tag{2.12}$$

Returning to the problem of finding lower bounds for $|\alpha - r/s|$, we consider results with $\alpha$ restricted to being of a particular form. In 1964, Baker [4] found an effectively computable bound for the difference between any rational number and $\alpha = (a/b)^{m/n}$ with $a$, $b$, $m$, $n \in \mathbb{Z}^+$. In Chapter 3, we work with an algebraic number of the form $\sqrt[n]{1 + 1/N}$ with $n$, $N \in \mathbb{Z}^+$, and apply Baker's theorem to obtain bounds.

First, for an integer $n \geq 2$, define

$$\mu_n = \prod_{\substack{p \text{ prime} \\ p|n}} p^{1/(p-1)}. \tag{2.13}$$

It is easy to see that $\mu_n$ is a multiplicative function, meaning that for $m$, $n \in \mathbb{Z}^+$ relatively prime, $\mu_n \mu_m = \mu_{nm}$.

The following special case of Baker's theorem [4] is used in the proof of Theorem 16.

**Theorem 6** (Baker)**.** *Let $n$, $N \in \mathbb{Z}^+$ such that $n \geq 3$. If $4N \geq n^2 \mu_n$, then for any $r/s \in \mathbb{Q}$,*

$$\left| \sqrt[n]{1 + \frac{1}{N}} - \frac{r}{s} \right| > \frac{1}{4n(2N+1)(2s)^{\lambda}},$$

*where*

$$\lambda = 1 + \frac{\log\left(2n\mu_n\left(2N+1\right)\right)}{\log\left(4N/\left(n^2\mu_n\right)\right)}.$$

*Sketch of Proof.* Let $n$, $N \in \mathbb{Z}^+$, as in the theorem. Let $\alpha = (1 + 1/N)^{1/n}$. Define a hypergeometric function by

$$F(a, b, c, x) = \sum_{j=0}^{\infty} \left( \prod_{k=0}^{j-1} \frac{(a+k)(b+k)}{(1+k)(c+k)} \right) x^j,$$

for $x \in \mathbb{R}$ and $a$, $b$, $c$, $k \in \mathbb{Q}$. Note that $F$ satisfies the differential equation

$$x(x-1)\frac{d^2F}{dx^2} + ((1+a+b)x - c)\frac{dF}{dx} + abF = 0.$$

From the function $F$, Baker obtains sequences of single variable functions indexed by a parameter $t \in \mathbb{Z}^+$. For example, he defines $A_t(x) = F(1/n - t, -t, -2t, x)$. Using these sequences of functions, he proves the existence of a pair of positive integers $(r_t, s_t)$, for each $t \geq 1$, satisfying $0 < |\alpha - r_t/s_t| < c_t/s_t$ with $c_t = 3\mu_n/(4N(4N)^t)$. Then, for a given $r/s \in \mathbb{Q}$, Baker finds $t_0 \in \mathbb{Z}^+$ such that $(4N)^{t_0} < 2s < (4N)^{t_0+1}$. Using $(r_{t_0}, s_{t_0})$, he derives the inequality in the theorem. □

In 1997, Bennett [7, Theorem 1.3] improved upon the special case of Baker's result given in Theorem 6. In the proof, Bennett uses diagonal Padé approximants, contour integrals, and counting primes in particular intervals, among other techniques, to derive a sequence of good rational approximations to numbers of the form $\alpha = (1 + 1/N)^{1/n}$. He applies some of Rickert's work [61] to generate an effective lower bound of $|\alpha - r/s|$ from the sequence of rational approximations.

**Theorem 7** (Bennett)**.** *Let $n$ and $N$ be positive integers with $n \geq 3$. If $\left(\sqrt{N} + \sqrt{N+1}\right)^{2(n-2)} > (n\mu_n)^n$, then, for $r$, $s \in \mathbb{Z}^+$,*

$$\left| \sqrt[n]{1 + \frac{1}{N}} - \frac{r}{s} \right| > \frac{1}{(8n\mu_n N)s^\lambda}$$

*with*

$$\lambda = 1 + \frac{\log\left(\left(\sqrt{N}+\sqrt{N+1}\right)^2 n\mu_n\right)}{\log\left(\left(\sqrt{N}+\sqrt{N+1}\right)^2/\left(n\mu_n\right)\right)}.$$

## 2.3 Linear Forms in Logarithms and Lehmer Pairs

In this section, after giving some definitions and a little bit of history, we state some results on linear forms in two logarithms. These results are used later in this section and in Chapter 3. We also discuss Lehmer pairs and use them in Chapter 4. (See [28] for an overview of linear forms in logarithms and [15] for more on Lehmer pairs.)

Throughout this section, for $\alpha \in \overline{\mathbb{Q}}$, let $\log \alpha$ denote the branch of the logarithm in which $-\pi < \Im(\log \alpha) \leq \pi$. A *linear form in logarithms* is an expression of the form

$$\sum_{j=1}^{n} b_j \log \alpha_j,$$

with $n \in \mathbb{Z}^+$ and, for $1 \leq j \leq n$, $\alpha_j \in \overline{\mathbb{Q}}$ and $b_j \in \mathbb{Z}$. Let

$$D = \frac{[\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) : \mathbb{Q}]}{[\mathbb{R}(\alpha_1, \alpha_2, \ldots, \alpha_n) : \mathbb{R}]}.$$

For $\alpha \in \overline{\mathbb{Q}}$, let $k$ be the degree of $\alpha$, $a_k$ the leading coefficient of the minimal polynomial of $\alpha$, and $\alpha^{(j)}$ the conjugates of $\alpha$, for $1 \leq j \leq k$, as in Section 2.1. The *absolute logarithmic height* of $\alpha$ is defined by

$$h(\alpha) = \frac{1}{k}\left(\log|a_k| + \sum_{j=1}^{k} \max\left\{\log\left|\alpha^{(j)}\right|, 0\right\}\right).$$

In 1935, Gel'fond was the first to publish a lower bound for a linear form in two logarithms [28]. In 1966, Baker [5] improved on this by finding lower bounds for linear

forms in logarithms for arbitrary $n \in \mathbb{Z}^+$. Many results arose from Baker's work, including bounds by Waldschmidt [76] and Laurent, Mignotte, and Nesterenko [41]. Below, we state two such results. The first, used in the proof of Theorem 16, is one of Mignotte's refinements [53, Theorem 2] of Laurent, Mignotte, and Nesterenko's work on linear forms in two logarithms.

**Theorem 8** (Mignotte)**.** *Let $b_1$, $b_2 \in \mathbb{Z}^+$ and $\alpha_1$, $\alpha_2 \in \overline{\mathbb{Q}} - \{0\}$ such that*

$$\Lambda = b_2 \log \alpha_1 - b_1 \log \alpha_1 \neq 0.$$

*Let $a_1$, $a_2$, $H$, $t$, $\rho \in \mathbb{R}^+$ with $\rho > 1$. Set $\lambda = \log \rho$ and $c = H/\lambda$ and let $c_0 \geq 0$ such that $c \geq c_0$. Also, set*

$$v = 4c + 4 + \frac{1}{c} \quad \text{and} \quad m = \max\left\{2^{5/2}\left(1+c\right)^{3/2}, \left(1+2c\right)^{5/2}/c\right\}.$$

*Define $f : (1, \infty) \to \mathbb{R}$ by*

$$f(x) = \log \frac{\sqrt{x}(1+\sqrt{x-1})}{x-1} + \frac{\log x}{6x(x-1)} + \frac{3}{2} + \log\left(\frac{3}{4}\right) + \frac{\log x - \log(x-1)}{x-1}.$$

*Further, assume that*

$$H \geq D\left(\log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \log\lambda + f(\lceil K_0 \rceil)\right) + 0.023,$$

$$a_i \geq \max\left\{1, \rho|\log\alpha_i| - \log|\alpha_i| + 2Dh(\alpha_i)\right\} \quad (i = 1, 2),$$

$$a_1 a_2 \geq \lambda^2, \qquad A = \max\{a_1, a_1\},$$

*and*

$$t = \frac{1}{\lambda^2}\left(\frac{1+2c}{3c}\right)^2 + \frac{1}{\lambda}\left(\frac{2+2\sqrt{1+2c}}{3c}\right),$$

*where*

$$K_0 = \frac{1}{\lambda}\left(\frac{\sqrt{2+2c_0}}{3} + \sqrt{\frac{2\,(1+c_0)}{9} + \frac{2\lambda}{3}\left(\frac{1}{a_1}+\frac{1}{a_2}\right) + \frac{4\lambda\sqrt{2+c_0}}{3\sqrt{a_1 a_2}}}\right)^2 a_1 a_2.$$

*Then*

$$\begin{aligned}\log|\Lambda| \geq & -\frac{1}{\lambda}\left(\frac{v^2}{9} + \frac{4\lambda v}{3}\left(\frac{1}{a_2}+\frac{1}{a_2}\right) + \frac{8\lambda m}{3\sqrt{a_1 a_2}}\right)^2 a_1 a_2 \\ & - \max\left\{\lambda\,(1.5+2c) + \log(((2+2c)^{3/2} + (2+2c)^2\sqrt{t})A + (2+2c)), D\log 2\right\}.\end{aligned}$$

The other one of Mignotte's refinements [15, Theorem A.1.3] of Laurent, Mignotte, and Nesterenko's work is the following theorem which is used in the proof of Theorem 11.

**Theorem 9** (Mignotte)**.** *Let $b_1$, $b_2 \in \mathbb{Z}^+$ and $\alpha \in \overline{\mathbb{Q}}$ such that $|\alpha| = 1$, but $\alpha$ is not a root of unity. Let*

$$\Lambda = b_1 i\pi - b_2 \log\alpha.$$

*Let $\lambda \in \mathbb{R}$ such that $1.8 \leq \lambda < 4$ and set*

$$\rho = e^{\lambda}, \quad a = 0.5\pi\rho + Dh(\alpha), \quad B = \max\{b_1, b_2, 13\},$$

$$t = \frac{1}{6\pi\rho} - \frac{1}{48\pi\rho(1+\pi\rho/3\lambda)}, \quad m = \left(\frac{1/3 + \sqrt{1/9 + 2\lambda t}}{\lambda}\right)^2,$$

$$\begin{aligned}H = \max\Bigg\{3\lambda, D\left(\log B + \log\left(\frac{1}{\pi\rho}+\frac{1}{2a}\right) - \log\sqrt{m} + 0.886\right) \\ + \frac{3\lambda}{2} + \frac{1}{m}\left(\frac{1}{6\pi\rho}+\frac{1}{3a}\right) + 0.023\Bigg\}.\end{aligned}$$

*Then*

$$\log|\Lambda| > -(8m\pi\rho\lambda^{-1}H^2 + 0.23)a - 2H - 2\log H + 0.5\lambda + 2\log\lambda - (D+2)\log 2.$$

Baker [6] applied his work on linear forms in logarithms to solving Thue equations. A *Thue equation* is a Diophantine equation of the form $F(X,Y) = M$, where $M \in \mathbb{Z}$ and $F(X,Y) \in \mathbb{Z}[X,Y]$ is a homogeneous irreducible polynomial of degree at least 3. The *auxiliary polynomial* of $F$ is the polynomial $f(X) = F(X,1) \in \mathbb{Z}[X]$. In 1909, Thue [72] proved that any such equation has at most a finite number of solutions. His proof was not constructive and so did not lead to a method for finding solutions. In 1968, Baker [6] proved an effective version of Thue's result. By using linear forms in logarithms, Baker bound the magnitudes of the solutions for a given Thue equation. However, the bounds were often too large to be practical [74].

It was Baker's breakthrough that allowed Tzanakis and de Weger [74] to develop an algorithm for solving Thue equations. They use a combination of lower bounds for linear forms in logarithms, continued fractions, and a lattice-based reduction method by Lenstra, Lenstra, and Lovász [44] (the LLL-algorithm). Tzanakis and de Weger's algorithm was modified by Bilu and Hanrot [14], who replaced the LLL-algorithm with another continued fraction argument. They used this method with Voutier to solve Thue equations in order to prove Theorem 11 on Lehmer pairs. We define Lucas and Lehmer pairs next.

First, a *Lucas pair* is a pair $(\alpha, \beta)$ where $\alpha,\ \beta \in \mathbb{C}$ are the distinct zeros of a polynomial of the form

$$X^2 - PX + Q$$

where $P,\ Q \in \mathbb{Z} - \{0\}$ are relatively prime with $|P^2 - 4Q| > 4$. Given a Lucas pair

$(\alpha, \beta)$, define a sequence recursively with $U_0 = 0$ and $U_1 = 1$, by

$$U_n = PU_{n-1} - QU_{n-2},$$

for $n \geq 2$. It is easy to show that, for all $n \in \mathbb{Z}^+$,

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

In 1930, D. H. Lehmer [43] observed that if $P$ is replaced by $\sqrt{R}$, where $R \in \mathbb{Z} - \{0\}$ is not a square, then the recursive definition of $U_n$ implies that $U_{2n+1} \in \mathbb{Z}$ and $U_{2n} \in \sqrt{R}\mathbb{Z}$. Since $\alpha + \beta = \sqrt{R}$, $U_{2n}/(\alpha + \beta) \in \mathbb{Z}$. For $n \in \mathbb{Z}^+$, the *n-th Lehmer number* is defined by

$$L_n(\alpha, \beta) = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta}, & \text{if } n \text{ is odd,} \\ \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, & \text{if } n \text{ is even.} \end{cases} \tag{2.14}$$

So, $L_n(\alpha, \beta) \in \mathbb{Z}$. Today, the definition of Lehmer pairs includes that of the Lucas pairs. Specifically, a *Lehmer pair* is now defined to be a pair $(\alpha, \beta)$ where $\alpha$, $\beta \in \mathbb{C}$ satisfy the following

$$\alpha\beta, (\alpha + \beta)^2 \in \mathbb{Z} - \{0\}, \tag{2.15}$$

$$\gcd(\alpha\beta, (\alpha + \beta)^2) = 1, \tag{2.16}$$

and

$$\frac{\alpha}{\beta} \text{ is not a root of unity.} \tag{2.17}$$

Two Lehmer pairs $(\alpha_1, \beta_1)$ and $(\alpha_2, \beta_2)$ are *equivalent* if $\alpha_1/\alpha_2 = \beta_1/\beta_2 = i^k$ with $0 \leq k \leq 3$.

Lehmer used his extension of the Lucas numbers to test the primality of integers, but he did not study the prime divisors of the Lehmer numbers in depth. In the late nineteenth century and early twentieth, the prime divisors of the Lucas numbers had been studied by Zsigmondy [83], Carmichael [24] and others. It was not until 1955 that Ward [78] studied the prime divisors of Lehmer numbers extensively.

A prime divisor, $p$, of a Lehmer number, $L_n(\alpha, \beta)$ is called a *primitive divisor* if

$$p \nmid (\alpha^2 - \beta^2)^2 L_1(\alpha, \beta) \dots L_{n-1}(\alpha, \beta). \tag{2.18}$$

If $L_n(\alpha, \beta)$ has no primitive divisors, then $(\alpha, \beta)$ is called an *$n$-defective* Lehmer pair. Note, in particular, that if $L_n(\alpha, \beta) = \pm 1$, then $L_n(\alpha, \beta)$ has no prime divisors and thus $(\alpha, \beta)$ is $n$-defective.

In 1974, Schinzel [63] proved the existence of a constant such that, for each $n$ greater than that constant, there are no $n$-defective Lehmer pairs. Let $n_0 \in \mathbb{Z}^+$ be the smallest such constant. A few years later, Stewart [67] proved that $n_0 \leq e^{452} 4^{67}$. In his paper, Stewart described how to reduce the problem of listing all $n$-defective Lehmer pairs to a problem of solving certain Thue equations.

In 1995, Voutier [75] used Stewart's idea and, solving Thue equations with the algorithms developed by Tzanakis and de Weger [74], determined a complete list of the $n$-defective Lehmer pairs for most of the values of $n \leq 30$, as seen below.

**Theorem 10** (Voutier)**.** *Let $n \in \mathbb{Z}^+$ such that $6 < n \leq 30$ and $n \neq 8$, 10, or 12. If $(\alpha, \beta)$ is an $n$-defective Lehmer pair, then for some $k \in \{0, 1, 2, 3\}$, $i^k\alpha$ is one of the values listed in Table 2.1.*

In this same paper, Voutier conjectured that $n_0 = 30$. A few years later, Voutier proved that $n_0 \leq 30030$, but it was not until 2001 that he, Bilu, and Hanrot [15] proved his conjecture.

Table 2.1: Possible values of $i^k\alpha$ determined by Voutier.

| $n$ | $i^k\alpha$, for $k \in \{0,1,2,3\}$ | | |
|---|---|---|---|
| 7 | $\frac{1\pm\sqrt{-7}}{2}$ | $\frac{1\pm\sqrt{-19}}{2}$ | $\frac{\sqrt{3}\pm\sqrt{-5}}{2}$ |
| | $\frac{\sqrt{5}\pm\sqrt{-7}}{2}$ | $\frac{\sqrt{13}\pm\sqrt{-3}}{2}$ | $\frac{\sqrt{14}\pm\sqrt{-22}}{2}$ |
| 9 | $\frac{\sqrt{5}\pm\sqrt{-3}}{2}$ | $\frac{\sqrt{7}\pm\sqrt{-1}}{2}$ | $\frac{\sqrt{7}\pm\sqrt{-5}}{2}$ |
| 13 | $\frac{1\pm\sqrt{-7}}{2}$ | | |
| 14 | $\frac{\sqrt{3}\pm\sqrt{-13}}{2}$ | $\frac{\sqrt{5}\pm\sqrt{-3}}{2}$ | $\frac{\sqrt{7}\pm\sqrt{-1}}{2}$ |
| | $\frac{\sqrt{7}\pm\sqrt{-5}}{2}$ | $\frac{\sqrt{19}\pm\sqrt{-1}}{2}$ | $\frac{\sqrt{22}\pm\sqrt{-14}}{2}$ |
| 15 | $\frac{\sqrt{7}\pm\sqrt{-1}}{2}$ | $\frac{\sqrt{10}\pm\sqrt{-2}}{2}$ | |
| 18 | $\frac{1\pm\sqrt{-7}}{2}$ | $\frac{\sqrt{3}\pm\sqrt{-5}}{2}$ | $\frac{\sqrt{5}\pm\sqrt{-7}}{2}$ |
| 24 | $\frac{\sqrt{3}\pm\sqrt{-5}}{2}$ | $\frac{\sqrt{5}\pm\sqrt{-3}}{2}$ | |
| 26 | $\frac{\sqrt{7}\pm\sqrt{-1}}{2}$ | | |
| 30 | $\frac{1\pm\sqrt{-7}}{2}$ | $\frac{\sqrt{2}\pm\sqrt{-10}}{2}$ | |

**Theorem 11** (Bilu, Hanrot, and Voutier)**.** *If a Lehmer pair is $n$-defective for $n \in \mathbb{Z}^+$, then $n \leq 30$.*

*Sketch of Proof.* Suppose, for a contradiction, that there is an $n$-defective Lehmer pair $(\alpha, \beta)$ with $n > 30$. Bilu, Hanrot, and Voutier show that there exists a primitive $n$-th root of unity $\xi$ such that the value of $|\arg((\beta/\alpha)\xi^{-1})|$ is less than a bound that they determine by using Stewart's reduction to Thue equations. This implies an upper bound for $|\arg((\beta/\alpha)^n)|$. The authors prove that, without loss of generality, they may assume that $\pi/n < \arg(\beta/\alpha) < \pi$. Define $b_1$ to be the nearest even integer to $n\arg(\beta/\alpha)/\pi$. Thus, $0 < b_1 \leq n$ and $|\arg((\beta/\alpha)^n)| = |b_1\pi i - n\log(\beta/\alpha)|$. Letting $\Lambda = b_1\pi i - n\log(\beta/\alpha)$, they apply Theorem 9. From this, the authors derive a contradiction for all but a finite number of $n$. The remaining possible values of $n$ are eliminated by solving many Thue equations using Bilu and Hanrot's modifications [14] of the algorithm by Tzanakis and de Weger. □

## 2.4 Elliptic Curves and Modular Forms

In this section, we review elliptic curves and modular forms while defining the notation and terminology needed to state various versions of the Modularity Theorem. The Modularity Theorem is the backbone of the modular approach, the method we use to prove Main Theorem III. (See [65,79] for additional information on elliptic curves, [51] for details on modular forms, and [33] for an expanded discussion of versions of the Modularity Theorem.)

We use the following standard notation. Let $m \in \mathbb{Z}$ and let $G$ be an arbitrary additive abelian group. For any $P \in G$, $mP$ is the sum of $m$ copies of $P$ in $G$, while $G[m]$ denotes the subgroup of the elements of $G$ whose order divides $m$. Recall that $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$.

Let $K$ be a field. Let $E$ be a cubic curve defined by the equation

$$Y^2Z = X^3 + AXZ^2 + BZ^3, \tag{2.19}$$

with $A$, $B \in K$. We view $E$ as the set of solutions to this equation in $\mathbb{P}^2$, projective 2-space. Since $A$, $B \in K$, we say $E$ is a curve *defined over* $K$. The *discriminant* of $E$ is $\Delta_E = -16(4A^3 + 27B^2)$. We say that $E$ is *nonsingular* if $\Delta_E \neq 0$; that $E$ has a *cusp singularity* if $\Delta_E = 0$ and $A = 0$; and that $E$ has a *node singularity* if $\Delta_E = 0$ and $A \neq 0$.

If $E$ is nonsingular, then it is called an *elliptic curve*. If $P = [x, y, z] \in E$ with $x$, $y$, $z \in K$, then we say that $P$ is a *$K$-rational point* of $E$. The set of $K$-rational points of $E$ is denoted by $E(K)$.

For the remainder of this section, we let $E$ be a fixed elliptic curve defined, over $\mathbb{Q}$, by equation (2.19). The intersection of $E$ and the projective line defined by $Z = 0$

is the *point at infinity*, $\mathcal{O} = [0, 1, 0]$. All other points in $\mathbb{P}^2$ satisfying equation (2.19) can be written in the form $P = [x, y, 1]$. When convenient, we view these points as being in affine space, $\mathbb{A}^2$, with $[x, y, 1] \in \mathbb{P}^2$ corresponding to $(x, y) \in \mathbb{A}^2$. These points are solutions to the equation

$$Y^2 = X^3 + AX + B,$$

obtained by setting $Z = 1$ in equation (2.19).

It is well-known that the equation for $E$, defined over $\mathbb{Q}$, can be written as in equation (2.19) with $A$, $B \in \mathbb{Z}$. The points of $E$ form an abelian group with a well-defined addition. The subgroup of $\mathbb{Q}$-rational points, $E(\mathbb{Q})$, is called the *Mordell-Weil group*.

Let $\ell \in \mathbb{Z}$ be an arbitrary prime. For each $R \in \mathbb{Z}$, let $\widetilde{R}$ denote the reduction of $R$ modulo $\ell$. Using this notation, reducing the coefficients of the equation for $E$ modulo $\ell$ yields the equation

$$Y^2Z = X^3 + \widetilde{A}XZ^2 + \widetilde{B}Z^3.$$

We call the curve defined by this equation $\widetilde{E}$. Since $\widetilde{A}$, $\widetilde{B} \in \mathbb{F}_\ell$, $\widetilde{E}$ is defined over $\mathbb{F}_\ell$. If $\Delta_{\widetilde{E}} \neq 0$, then we say that $E$ is *stable*. If $\Delta_{\widetilde{E}} = 0$ and $\widetilde{A} \neq 0$, then $E$ is *semistable*. If $\Delta_{\widetilde{E}} = 0$ and $\widetilde{A} = 0$, then $E$ is *unstable*. The *trace* of $E$ is defined by

$$a_\ell(E) = \ell + 1 - |\widetilde{E}(\mathbb{F}_\ell)|.$$

Next, we define congruence subgroups of $SL_2(\mathbb{Z})$, modular curves, and other terminology, before defining modular forms.

Let

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

A subgroup $\Gamma \subseteq SL_2(\mathbb{Z})$ is a *congruence subgroup* of $SL_2(\mathbb{Z})$ if, for some $N \in \mathbb{Z}^+$, $\Gamma(N) \subseteq \Gamma$. If $N$ is the smallest such integer, we say that $\Gamma$ is a congruence subgroup of *level* $N$. Two congruence subgroups of level $N$, of importance here, are

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| c \equiv 0 \pmod{N} \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| a \equiv d \equiv 1 \pmod{N}, c \equiv 0 \pmod{N} \right\}.$$

Let $\mathcal{H} = \{z \in \mathbb{C} | \Im(z) > 0\}$ be the complex upper half plane and $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$. The *modular curve* of $\Gamma_1(N)$ is

$$X_1(N) = \Gamma_1(N) \setminus \mathcal{H}^*.$$

As is well-known, the modular curve $X_1(N)$ can be described as an algebraic curve defined over $\mathbb{Q}$. This means that it has properties analogous to those of elliptic curves (see [33, Chapter 7] for a discussion of this).

The *divisor group* of $X_1(N)$ is defined by

$$Div(X_1(N)) = \coprod_{P \in X_1(N)} \mathbb{Z}(P).$$

So, an arbitrary element of $Div(X_1(N))$ is of the form $D = \sum m_p(P)$ with $m_P \in \mathbb{Z}$ and where the sum is taken over all $P \in X_1(N)$. Note that $(P)$ indicates that this is a formal linear combination of points on $X_1(N)$ with integer coefficients. The *degree*-0 *divisor group* of $X_1(N)$ is the subgroup defined by

$$Div^0(X_1(N)) = \left\{ \sum_{P \in X_1(N)} m_P(P) \in Div(X_1(N)) \middle| \sum_{P \in X_1(N)} m_P = 0 \right\}.$$

Let $P \in X_1(N)$ and let $g_0$ and $h_0$ be nonzero polynomials in the coordinate ring $\overline{\mathbb{Q}}[X_1(N)]$. For $M_P$, the maximal ideal of the local ring $\overline{\mathbb{Q}}[X_1(N)]_P$ at $P$, the *valuation* of $g_0$ at $P$ is defined by $\nu_P(g_0) = \max\{d \in \mathbb{Z} | g_0 \in M_P^d\}$. The valuation is extended to the function field of $X_1(N)$, $\overline{\mathbb{Q}}(X_1(N))$, by $\nu_P(g_0/h_0) = \nu_P(g_0) - \nu_P(h_0)$. So, a *principal divisor* of $Div^0(X_1(N))$ is an element of the form $div(g/h) = \sum \nu_P(g/h)(P)$, for some nonzero $g/h \in \overline{\mathbb{Q}}(X_1(N))$. The quotient of the degree-0 divisor group by the set of principal divisors is the *(degree-0) Picard group* of $X_1(N)$, denoted by $Pic^0(X_1(N))$. (See [33, Section 7.2 & 7.3] for more details.)

Now, we define modular forms with respect to a congruence subgroup. For $k$, $N \in \mathbb{Z}^+$, a *modular form* of *weight* $k$ with respect to $\Gamma_0(N)$ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that

$$f(Mz) = f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \text{ for each } M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \text{ and } z \in \mathcal{H},$$

and, letting $q = e^{2\pi i z}$, $f$ has a Fourier expansion,

$$f(z) = \sum_{n=0}^{\infty} a_n(f) q^n.$$

The modular form $f$ is of *level* $N$, if $N$ is the smallest integer such that the above

conditions hold. If $a_0(f) = 0$, then $f$ is called a *cusp form*. If, in addition, $a_1(f) = 1$, then $f$ is a *normalized cusp form*. Further, $f$ is called *rational* if for all $n \in \mathbb{Z}$, $a_n(f) \in \mathbb{Q}$. The vector space of cusp forms of weight 2 and level $N$ is denoted by $S_2(\Gamma_0(N))$.

If $N$, $N'$, $d \in \mathbb{Z}^+$ such that $dN' = N$, then the degeneracy map $\alpha_d : S_2(\Gamma_0(N')) \to S_2(\Gamma_0(N))$ is defined by $f(q) \mapsto f(q^d)$. The cusp forms contained in the image of $\alpha_d$ are called *oldforms*. The orthogonal complement under the Petersson inner product of the subspace of oldforms is the subspace $S_2(\Gamma_0(N))^{\text{new}}$. A basis for this space is a set of normalized Hecke eigenforms. We follow the standard practice and call those basis elements *newforms* of level $N$.

There is an explicit formula for the dimension of $S_2(\Gamma_0(N))^{\text{new}}$ (see for example [28, Proposition 15.1.1]). As a corollary, we have the following lemma.

**Lemma 12.** *There are no newforms of level $N$ if and only if*

$$N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60\}.$$

If $f \in S_2(\Gamma_0(N))$ is a newform for some $N \in \mathbb{Z}^+$ with Fourier expansion $\sum a_n(f)q^n$, then the *Dirichlet L-function* of $f$ is defined by $L(s, f) = \sum_{n=1}^{\infty} a_n(f)n^{-s}$ for $s \in \mathbb{C}$ with $\Re(s) > 1$. Since $f$ is a newform, its $L$-function has an Euler product

$$L(s, f) = \prod_{\ell \text{ prime}} \left(1 - a_\ell(f)\ell^{-s} + \chi_0(\ell)\ell^{1-2s}\right)^{-1},$$

where $\chi_0$ is the trivial Dirichlet character mod $N$.

Now, we define Galois representations. For $d$, $\ell \in \mathbb{Z}^+$ with $\ell$ prime, a $d$-dimensional *$\ell$-adic Galois representation* is a continuous homomorphism $\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_d(\mathbb{Q}_\ell)$. Two representations are *equivalent*, $\rho \sim \rho'$, if and only if there exists $M \in GL_d(\mathbb{Q}_\ell)$

such that $\rho'(\sigma) = M^{-1}\rho(\sigma)M$ for all $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. We outline the construction of two important $\ell$-adic Galois representations, $\rho_{E,\ell} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Q}_\ell)$ for an elliptic curve $E$ and $\rho_{X_1(N),\ell} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_{2g}(\mathbb{Q}_\ell)$, for $N \in \mathbb{Z}^+$ and $g$, the genus of $X_1(N)$. (See [33, Section 3.1] for information about the genus.)

First, we construct $\rho_{E,\ell}$. Define the multiplication-by-$\ell$ map,

$$[\ell] : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}}) \text{ by } [\ell]P = \ell P.$$

Note that $[\ell]$ is a group homomorphism. For arbitrary $P \in E[\ell^{n+1}]$, $\ell^{n+1}P = \mathcal{O}$. Hence, $\ell^n([\ell]P) = \ell^{n+1}P = \mathcal{O}$ and so $[\ell]P \in E[\ell^n]$. Thus, the homomorphism $[\ell]$ restricts to a homomorphism $E[\ell^{n+1}] \to E[\ell^n]$, which we also denote by $[\ell]$.

It is well-known that, for each $n \in \mathbb{Z}^+$, $E[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^2$. We choose compatible bases $\{P_n, Q_n\}_{n\in\mathbb{Z}^+}$ so that, for each $n \in \mathbb{Z}^+$,

$$\{P_n, Q_n\} \text{ is a basis for } E[\ell^n], [\ell]P_{n+1} = P_n, \text{ and } [\ell]Q_{n+1} = Q_n. \tag{2.20}$$

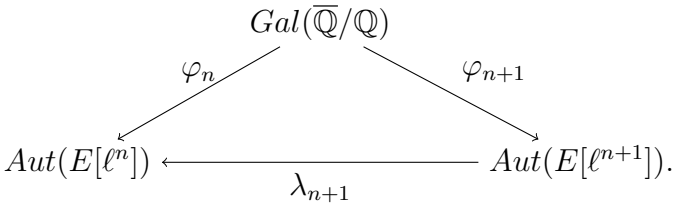
Now fix $n \in \mathbb{Z}^+$. For $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, $\sigma$ induces an automorphism $\sigma_n : E[\ell^n] \to E[\ell^n]$ defined by $\sigma_n([x, y, z]) = [\sigma(x), \sigma(y), \sigma(z)]$. This action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[\ell^n]$ induces

$$\varphi_n : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut(E[\ell^n]) \text{ defined by } \varphi_n(\sigma) = \sigma_n.$$

Let $\lambda_{n+1} : Aut(E[\ell^{n+1}]) \to Aut(E[\ell^n])$ be defined by

$$\lambda_{n+1}(\tau) = [\ell]\tau[\ell]^{-1} \text{ for all } \tau \in Aut(E[\ell^{n+1}]).$$

Note that even though $[\ell]^{-1}$ is not a single-valued function, $\lambda_{n+1}$ is a well-defined homomorphism. For each $n \in \mathbb{Z}^+$, we obtain the diagram



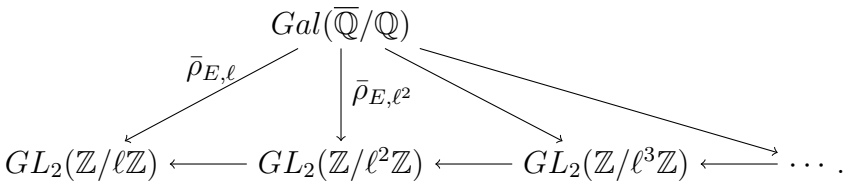

Since $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ is a homomorphism, equations (2.20) imply that the diagram commutes.

For each $n \in \mathbb{Z}^+$, let $\psi_n : GL_2(\mathbb{Z}/\ell^n\mathbb{Z}) \to Aut(E[\ell^n])$ be the standard isomorphism determined by the basis $\{P_n, Q_n\}$ for $E[\ell^n]$. In other words, for $M \in GL_2(\mathbb{Z}/\ell^n\mathbb{Z})$, $\psi_n(M) = \tau_M$ where $M(P_n, Q_n)^t = (\tau_M(P_n), \tau_M(Q_n))^t$.

For all $n \in \mathbb{Z}^+$, define a *mod* $\ell^n$ *Galois representation of* $E$,

$$\bar{\rho}_{E,\ell^n} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/\ell^n\mathbb{Z})$$

by $\bar{\rho}_{E,\ell^n} = \psi_n\varphi_n$, which yields the inverse system




The inverse limit of this system is the representation $\rho'_{E,\ell} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_\ell)$. Finally, letting $\iota : GL_2(\mathbb{Z}_\ell) \to GL_2(\mathbb{Q}_\ell)$ be inclusion, we have the $\ell$-adic Galois representation that arises from $E$

$$\rho_{E,\ell} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Q}_\ell)$$

defined by $\rho_{E,\ell} = \iota\rho'_{E,\ell}$.

Next, we outline the construction of $\rho_{X_1(N),\ell}$, for $N \in \mathbb{Z}^+$. Viewing $X_1(N)$ as an

algebraic curve of genus $g$, the construction of the representation is similar to that of the elliptic curve, which has genus 1.

Let $[\ell] : Pic^0(X_1(N))[\ell^{n+1}] \to Pic^0(X_1(N))[\ell^n]$ be multiplication by $\ell$ (repeated addition) in the group $Pic^0(X_1(N))[\ell^{n+1}]$. Choosing compatible bases of $Pic^0(X_1(N))[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$, for all $n \in \mathbb{Z}^+$, we obtain the commutative diagram

$$\begin{array}{ccc} & Gal(\overline{\mathbb{Q}}/\mathbb{Q}) & \\ \swarrow & & \searrow \\ Aut(Pic^0(X_1(N))[\ell^n]) & \longleftarrow & Aut(Pic^0(X_1(N))[\ell^{n+1}]). \end{array}$$

Together with the standard isomorphism $GL_{2g}(\mathbb{Z}/\ell^n\mathbb{Z}) \to Aut(Pic^0(X_1(N))[\ell^n])$, this yields the inverse system

$$\begin{array}{ccccccc} & & Gal(\overline{\mathbb{Q}}/\mathbb{Q}) & & & & \\ & \swarrow & \downarrow & \searrow & & \searrow & \\ GL_{2g}(\mathbb{Z}/\ell\mathbb{Z}) & \longleftarrow & GL_{2g}(\mathbb{Z}/\ell^2\mathbb{Z}) & \longleftarrow & GL_{2g}(\mathbb{Z}/\ell^3\mathbb{Z}) & \longleftarrow & \cdots . \end{array}$$

The inverse limit composed with the inclusion map is the $\ell$-adic Galois representation arising from the modular curve $X_1(N)$ with $N \in \mathbb{Z}^+$,

$$\rho_{X_1(N),\ell} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_{2g}(\mathbb{Q}_\ell).$$

(For details of this construction see [33, Section 9.5]).

From $\rho_{X_1(N),\ell}$, for a rational newform, $f \in S_2(\Gamma_0(N))$, one obtains the $\ell$-adic Galois representation arising from $f$, $\rho_{f,\ell} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Q}_\ell)$, and the mod $\ell$ Galois representation, $\bar{\rho}_{f,\ell} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/\ell\mathbb{Z})$. It is $\rho_{E,\ell}$ and $\rho_{f,\ell}$ that are at the heart of the proof of the Modularity Theorem, providing the connection between newforms and elliptic curves.

An elliptic curve $E$ defined over $\mathbb{Q}$ is *modular* if there exists a rational newform $f$ such that $\rho_{E,\ell} \sim \rho_{f,\ell}$, for some prime $\ell \in \mathbb{Z}^+$. In 1995, Wiles [81] and Taylor and Wiles [71] proved that every semistable elliptic curve is modular. This was the last missing piece to the proof of Fermat's Last Theorem (see Chapter 1). In 2001, Breuil, Conrad, Diamond, and Taylor [16, Theorem 1] extended the proof of Taylor and Wiles to include all elliptic curves defined over $\mathbb{Q}$. First, they prove that $\bar{\rho}_{E,\ell}$ is modular, meaning $\bar{\rho}_{E,\ell} \sim \bar{\rho}_{f,\ell}$, for some prime $\ell \in \mathbb{Z}^+$. Then, they extend their construction to proving that $\rho_{E,\ell}$ is modular. Thus, proving the initial version of the *Modularity Theorem*.

**Theorem 13** (Breuil, Conrad, Diamond, and Taylor)**.** *If $E$ is an elliptic curve defined over $\mathbb{Q}$, then $E$ is modular.*

From Theorem 13, it can be shown that given an elliptic curve $E$ defined over $\mathbb{Q}$, there exists a rational newform $f$ of weight 2 and level $N \in \mathbb{Z}^+$ such that $\rho_{E,\ell} \sim \rho_{f,\ell}$. The smallest such integer $N$ is called the *conductor* of $E$.

There are many equivalent definitions of modular that lead to equivalent formulations of the Modularity Theorem (see [33] for even more versions). The following version is proved from Theorem 13 by using images of Frobenius elements under representations. Let $F$ be a finite Galois extension of $\mathbb{Q}$ in $\mathbb{C}$ and let $\mathfrak{p}$ be a maximal ideal in $\mathcal{O}_F$ lying over a rational prime, $p$. A *Frobenius element* of $Gal(F/\mathbb{Q})$ is any element $Frob_{\mathfrak{p}} \in Gal(F/\mathbb{Q})$ such that $Frob_{\mathfrak{p}}(x) \equiv x^p \pmod{\mathfrak{p}}$ for all $x \in \mathcal{O}_F$.

For an elliptic curve $E$ defined over $\mathbb{Q}$ with conductor $N$, if $\ell$, $p \in \mathbb{Z}^+$ are primes such that $p \nmid \ell N$, an *absolute Frobenius element* of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ is any element of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ that restricts to a Frobenius element of $Gal(F/\mathbb{Q})$ for some finite Galois extension $F$ over $\mathbb{Q}$. It can be shown that $\bar{\rho}_{E,\ell}(Frob_{\mathfrak{p}})$ has characteristic polynomial $X^2 - a_p(E)X + p = 0$.

If $f \in S_2(\Gamma_0(N))$ is a rational newform and $\ell$, $p \in \mathbb{Z}^+$ are primes such that $p \nmid \ell N$, then $\bar{\rho}_{f,\ell}(Frob_{\mathfrak{p}})$ has characteristic polynomial $X^2 - a_p(f)X + p = 0$ and so Theorem 14 [33, Theorem 8.8.1] follows.

**Theorem 14** (Modularity Theorem for $a_\ell$)**.** *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with conductor $N$. Then, for some rational newform $f \in S_2(\Gamma_0(N))$, $a_\ell(f) = a_\ell(E)$ for all primes $\ell$.*

For an elliptic curve $E$, the conductor $N$ and the values $a_\ell(E)$ are encoded in the *Hasse-Weil L-function* of $E$, defined by

$$L(s, E) = \prod_{\ell \text{ prime}} \left(1 - a_\ell(E)\ell^{-s} + \chi_0(\ell)\ell^{1-2s}\right)^{-1},$$

where, again, $\chi_0$ is the trivial Dirichlet character modulo $N$.

If, for each $\ell$ prime, $a_\ell(f) = a_\ell(E)$, as in Theorem 14, then it is easy to see that the $L$-functions for $f$ and $E$ must also be equal. Thus, we have the following version of the Modularity Theorem on $L$-functions [33, Theorem 8.8.3].

**Theorem 15** (Modularity Theorem for $L$)**.** *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with conductor $N$. Then, for some rational newform $f \in S_2(\Gamma_0(N))$, $L(s, f) = L(s, E)$.*

This version is quite interesting in that $L(s, E)$ is conjectured to contain extra information about the curve $E$. In particular, Birch and Swinneton-Dyer conjectured that the rank of the Mordell-Weil group $E(\mathbb{Q})$ is the order of vanishing of $L(s, E)$ at $s = 1$ (see [33, Conjecture 8.8.5] for more details on the Birch-Swinnerton-Dyer Conjecture).

# Chapter 3

# Main Theorem I

In this chapter, we prove Main Theorem I using Diophantine approximation. First, we give a brief history of the problem. In Section 3.1, we state the known results that lead up to the main theorem, and in Section 3.2, we present the proof of Main Theorem I. (See [20,21] for a more detailed history and Section 2.2 for a discussion of Diophantine approximation notation and results.)

It is reported [21] that Diophantus knew that the set $\{1/16, 33/16, 17/4, 105/16\}$ has the property that one plus the product of any two elements in the set is a perfect square. Fermat found a set of integers, $\{1, 3, 8, 120\}$, with this same property. We are interested in triples of integers of the form $\{1, A, B\}$ with $1 < A < B$ such that one plus the product of any two elements is a $k$-th power, for some integer $k \geq 2$. The existence of such a set is equivalent to the existence of $x$, $y$, $z \in \mathbb{Z}^+$ satisfying $A + 1 = x^k$, $B + 1 = y^k$, and $AB + 1 = z^k$ and so $(x^k - 1)(y^k - 1) = z^k - 1$.

Bugeaud [20] observed that for an integer $r > 1$, the equation

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

provides a formula to find infinitely many solutions to the Diophantine equation $(X^k-1)(Y^k-1) = Z^k-1$ for $k = 2$. In that same paper, Bugeaud [20, Theorem 2] considered triples of positive integers of the form $\{1, A, A^2B\}$ such that $A+1$, $A^2B+1$, and $AB+1$ are all $k$-th powers. The existence of such a triple is equivalent to the existence of a solution to the Diophantine equation $(X^k-1)(Y^k-1) = (Z^k-1)^2$ with $X^k-1$ dividing $Z^k-1$.

Bennett [9] improved Bugeaud's results and Zhang [82, Theorem 1.1] adapted Bennett's methods to prove results for a generalization of $(X^k-1)(Y^k-1) = Z^k-1$, namely, $(aX^k-1)(bY^k-1) = abZ^k-1$ with $a, b \in \mathbb{Z}^+$.

We consider the following generalization of the equation $(X^k-1)(Y^k-1) = (Z^k-1)^2$.

**Main Theorem I.** *Let $a$, $b$, $c$, $k \in \mathbb{Z}^+$ with $k \geq 7$. The equation*

$$(a^2cX^k-1)(b^2cY^k-1) = (abcZ^k-1)^2$$

*has no solutions in integers $X$, $Y$, $Z > 1$ with $a^2X^k \neq b^2Y^k$.*

Note that given the prior results, it seems likely that there are also no solutions for $4 \leq k \leq 6$.

## 3.1 Preliminary Results

In 2004, Bugeaud [20, Theorem 1] proved the following two results using linear forms in logarithms (see Section 2.3).

**Theorem 16** (Bugeaud)**.** *Let $k \in \mathbb{Z}^+$.*

*(a) For $k \geq 75$, the Diophantine equation*

$$(X^k - 1)(Y^k - 1) = (Z^k - 1)$$

*has no solutions in positive integers $X$, $Y$, $Z$ with $Z > 1$. Furthermore, if $\min\{X, Y\}$ is sufficiently large, then the equation has no solutions for $k \geq 5$.*

*(b) For $k \geq 150$, the equation*

$$(X^k - 1)(Y^k - 1) = (Z^k - 1)^2$$

*has no solutions in positive integers $X$, $Y$, $Z$ with $1 < X < Y$ and $X^k - 1$ dividing $Z^k - 1$. Furthermore, if $X$ is sufficiently large, then the equation has no solutions for $k \geq 8$.*

The proofs of parts (a) and (b) are very similar. We describe the method that is used for both.

*Sketch of Proof.* For a contradiction, suppose that a positive integer solution $x$, $y$, $z$ exists. Derive a lower bound for $y^k$ in terms of $x$ and $k$. For large values of $k$, combine the lower bound for $y^k$ with a bound derived from Theorem 8 with $\Lambda = \log(1 + 1/(x^k - 1)) - k \log(xy/z)$, to reach a contradiction.

For the remaining small values of $k$, suppose that $\min\{x, y\}$ or $x$ is large enough to satisfy the hypothesis of Theorem 6 with $n = k$ and $N = x^k - 1$. Theorem 6 implies that, for integers $n \geq 3$, $N \geq c_1$, and real number $\varepsilon > 0$,

$$\left| \sqrt[n]{1 + \frac{1}{N}} - \frac{r}{s} \right| > \frac{c_2}{s^{2+\varepsilon}}, \tag{3.1}$$

where $c_1 = n^2 \mu_n / 4$, and $c_2 = 1/(16n(2N + 1)(2)^{\varepsilon})$ are computable. From this,

Bugeaud derives an upper bound for $y^k$. Combining this upper bound with the lower bound mentioned above, leads to a contradiction. □

In 2007, Bennett [9, Theorem 1.1] improved both of Bugeaud's results.

**Theorem 17** (Bennett)**.** *Let $k \in \mathbb{Z}^+$.*

*(a) For $k \geq 3$, equation*

$$(X^k - 1)(Y^k - 1) = Z^k - 1$$

*has only the solutions $(X, Y, Z, k) = (-1, 4, -5, 3)$ and $(4, -1, -5, 3)$ in integers $X$, $Y$, and $Z$ with $|Z| > 1$.*

*(b) For $k \geq 4$, equation*

$$(X^k - 1)(Y^k - 1) = (Z^k - 1)^2$$

*has no solutions in integers $X$, $Y$, and $Z$ with $|Z| > 1$ and $X \neq \pm Y$.*

We sketch the proof of part (a) for $k \geq 4$. The case $k = 3$ is handled separately using continued fractions. In his paper, Bennett briefly describes the changes that would be required to prove part (b), using a similar method.

*Sketch of Proof.* Suppose, for a contradiction, that there is a solution $x$, $y$, $z$ in positive integers, with $k \geq 4$. Rather than using linear forms in logarithms, Bennett derives an upper bound for $y^k$ using Theorem 7 with $n = k$ and $N = x^k - 1$. Combining this bound with a lower bound, leads to a contradiction for all but a finite number of values of $x$ and $k$. For each of those remaining possible values of $x$ and $k$, Bennett uses Theorem 7 again. This time he combines the bound he derives with bounds that he obtains from the properties of continued fractions to reach a contradiction.

As Bennett indicates, the proof for the negative values of $x$, $y$, and $z$ requires only minor adjustments to the argument described above, except in the special case where

$x$ or $y$ is $-1$. This final case is quite different from the rest. It requires completely solving the Thue equations, $X^k - 2Y^k = m$ with $k \geq 4$ and $|m| \leq 100$. This is achieved both through computer calculations and the modular approach. □

In 2014, Zhang [82, Theorem 1] considered a generalization of the equation in Theorem 17, part (a). Zhang expands Bennett's methods to bound the extra components and prove the theorem.

**Theorem 18** (Zhang)**.** *Let $a$, $b$, $k \in \mathbb{Z}^+$. For $k \geq 4$, the equation*

$$(aX^k - 1)(bY^k - 1) = abZ^k - 1$$

*has no solutions in integers $X$, $Y$, and $Z$ with $|X| > 1$ and $|Y| > 1$.*

Notice that $k \geq 4$ is the best possible, since, from Bennett's work, the case $a = b = 1$ has solutions for $k = 3$.

*Sketch of Proof.* Let $a$, $b$, $k \in \mathbb{Z}^+$. For a hypothetical solution, $x$, $y$, $z$, Zhang derives a lower bound for $by^k$ in terms of $a$, $b$, $x$, and $k$. Applying Theorem 7 with $n = k$ and $N = ax^k - 1$, he obtains an upper bound for $by^k$. Comparing the bounds, Zhang finds a contradiction for all but a finite number of values of $a$, $x$, and $k$. For the remaining finite set of possible values, he uses various methods similar to those used by Bennett to reach a contradiction. □

In preparation for proving Main Theorem I, we show that the hypotheses of Theorem 7 are satisfied for $N \geq 2^n$ and $n \geq 7$.

**Lemma 19.** *Let $N$, $n \in \mathbb{Z}^+$ such that $N \geq 2^n$ and $n \geq 7$. Then*

$$\left(\sqrt{N} + \sqrt{N+1}\right)^{2(n-2)} > (n\mu_n)^n.$$

*Proof.* Let $N$, $n \in \mathbb{Z}^+$ such that $N \geq 2^n$ and $n \geq 7$. Then, we have

$$\sqrt{N} + \sqrt{N+1} = \sqrt{N+1}\left(\sqrt{\frac{N}{N+1}} + 1\right) = \sqrt{N+1}\left(\sqrt{1 - \frac{1}{N+1}} + 1\right).$$

Since $N \geq 2^n \geq 128$, a direct calculation yields

$$\sqrt{N+1}\left(\sqrt{1 - \frac{1}{N+1}} + 1\right) \geq \sqrt{N+1}\left(\sqrt{1 - \frac{1}{128+1}} + 1\right) > \sqrt{2^n}\left(2^{1/1.01}\right)$$

Thus,

$$\left(\sqrt{N} + \sqrt{N+1}\right)^{2(n-2)} > 2^{n(n-2)+(2(n-2)/1.01)}.$$

Since $n \geq 7$, we have

$$n(n-2) + (2(n-2)/1.01) > n(n-2+(2/1.01)-(4/(1.01 \cdot 7))) > n(n-0.6).$$

Hence,

$$\left(\sqrt{N} + \sqrt{N+1}\right)^{2(n-2)} > (2^{n-0.6})^n.$$

Define $f : [7, \infty) \to \mathbb{R}$ by $f(t) = (t - 0.6)/\log t$. The first derivative of $f$ is

$$f'(t) = \frac{t \log t - t + 0.6}{t(\log t)^2}.$$

Since $t \log t > t \geq 7$, $f$ is an increasing function. Therefore, $n \geq 7$ implies that $f(n) = (n - 0.6)/\log n \geq (7 - 0.6)/\log 7 > 2/\log 2$. Thus, $(n - 0.6)\log 2 > 2 \log n$ and so $2^{n-0.6} > n^2$. Finally, since $n \geq \mu_n$, we have

$$\left(\sqrt{N} + \sqrt{N+1}\right)^{2(n-2)} > (2^{n-0.6})^n > n^{2n} \geq (n\mu_n)^n,$$

as desired. □

In the proof of Main Theorem I, there are a number of bounds that involve $\mu_n$ for $n \geq 7$. We use the following lemma to bound $\mu_n$. Recall that $\mu_n$ is a multiplicative function (see equation (2.13) in Section 2.2 for its definition).

**Lemma 20.** *If $n \geq 7$ is an integer, then $\mu_n \leq \sqrt{n}$.*

*Proof.* Let $q \in \mathbb{Z}^+$ be an odd prime. Since $q \geq 3$,

$$\mu_q = q^{1/(q-1)} \leq q^{1/2}.$$

Next, notice that for $e \in \mathbb{Z}^+$with $e \geq 2$, we have

$$\mu_2 = 2 \leq 2^{e/2}.$$

Now, let $n \in \mathbb{Z}^+$ such that $n \geq 7$. Let $e \in \mathbb{Z}$ with $e \geq 0$ and let $e_i$, $q_i$, $t \in \mathbb{Z}^+$ with $q_i$ distinct odd primes, for $1 \leq i \leq t$, such that $n = 2^e \prod_{i=1}^{t} q_i^{e_i}$.

If $n$ is odd, then $e = 0$ and so the multiplicative property of $\mu_n$, implies that

$$\mu_n = \prod_{i=1}^{t} \mu_{q_i} \leq \prod_{i=1}^{t} q_i^{1/2} = \left( \prod_{i=1}^{t} q_i \right)^{1/2} \leq n^{1/2}.$$

If $4 \mid n$, then $e \geq 2$. Again, since $\mu_n$ is multiplicative,

$$\mu_n = \mu_2 \prod_{i=1}^{t} \mu_{q_i} \leq 2 \prod_{i=1}^{t} q_i^{1/2} \leq 2^{e/2} \left( \prod_{i=1}^{t} q_i \right)^{1/2} \leq n^{1/2}.$$

Hence, it remains to consider $n$ such that $e = 1$. Since $n \geq 7$, either there exists $e_1 \geq 2$ such that $n = 2 \cdot 3^{e_1}$ or there exists a prime $q \geq 5$ such that $q \mid n$. First,

assume that $n = 2 \cdot 3^{e_1}$ with $e_1 \geq 2$. Then,

$$\mu_n = \mu_2\mu_3 = 2 \cdot 3^{1/2} < (2 \cdot 3^{e_1})^{1/2} = n^{1/2}.$$

Finally, assume that $q \mid n$ such that $q \geq 5$. Then $n = 2q^{e_2}r$, for $e_2$, $r \in \mathbb{Z}^+$ with $\gcd(2q, r) = 1$. Since $r$ is odd, we have $\mu_r \leq r^{1/2}$. Thus, by the multiplicative property of $\mu_n$,

$$\mu_n = \mu_2\mu_q\mu_r = 2q^{1/(q-1)}\mu_r < 2^{1/2}5^{1/4}q^{1/(q-1)}r^{1/2} \leq (2q^{e_2}r)^{1/2} = n^{1/2},$$

as desired. □

## 3.2 Proof of Main Theorem I

Now, we prove Main Theorem I using the results in Sections 2.2 and 3.1 and the ideas in the proofs of Theorems 17 and 18.

*Proof of Theorem I.* Let $a$, $b$, $c$, $k \in \mathbb{Z}^+$ such that $k \geq 7$. Suppose, for a contradiction, that $(X, Y, Z) = (x, y, z)$ is a solution to the equation $(a^2cX^k - 1)(b^2cY^k - 1) = (abcZ^k - 1)^2$ with $x$, $y$, $z > 1$ and $a^2x^k \neq b^2y^k$. So,

$$(a^2cx^k - 1)(b^2cy^k - 1) = (abcz^k - 1)^2. \tag{3.2}$$

Since the right side of this equation is a square, there exist $u$, $v$, $w \in \mathbb{Z}^+$ such that

$$a^2cx^k - 1 = uv^2 \tag{3.3}$$

and

$$b^2cy^k - 1 = uw^2. \tag{3.4}$$

By equation (3.2), the product of $uv^2$ and $uw^2$ is

$$(uvw)^2 = \left(abcz^k - 1\right)^2. \tag{3.5}$$

Since $a^2x^k \neq b^2y^k$, $v \neq w$ and so, without loss of generality, we assume that $v < w$. Then, we have that $v^2 + w^2 = (w - v)^2 + 2vw > 2vw$. So, using equations (3.3)–(3.5), we have

$$\begin{aligned}(a^2cx^k)(b^2cy^k) &= (uv^2 + 1)(uw^2 + 1)\\ &= (uvw)^2 + u(v^2 + w^2) + 1\\ &> (uvw)^2 + 2uvw + 1 = (uvw + 1)^2 = (abcz^k)^2.\end{aligned}$$

Thus, $a^2b^2c^2(xy)^k > a^2b^2c^2z^{2k}$, implying that

$$xy > z^2, \tag{3.6}$$

and so $xy/z^2 > 1$. This rational number is what we use to approximate the number $\sqrt[k]{1 + 1/uv^2} > 1$. For convenience in notation, let

$$\alpha = \sqrt[k]{1 + \frac{1}{uv^2}} \tag{3.7}$$

and

$$\beta = \frac{xy}{z^2}. \tag{3.8}$$

Now, $k \geq 7$ and $uv^2 > a^2cx^k \geq 2^k$, since $x > 1$. Thus, by Lemma 19, the

hypotheses of Theorem 7 with $n = k$ and $N = uv^2$, are satisfied. Therefore, by Theorem 7, we have that

$$|\alpha - \beta| = \left| \sqrt[k]{1 + \frac{1}{uv^2}} - \frac{xy}{z^2} \right| > \frac{1}{8k\mu_k uv^2 z^{2\lambda}}, \tag{3.9}$$

with

$$\lambda = 1 + \frac{\log\left(\left(\sqrt{uv^2} + \sqrt{uv^2+1}\right)^2 k\mu_k\right)}{\log\left(\left(\sqrt{uv^2} + \sqrt{uv^2+1}\right)^2/(k\mu_k)\right)}. \tag{3.10}$$

So, we have a lower bound for $|\alpha - \beta|$ that involves $\lambda$. To bound $\lambda$, we define the following functions.

For each $K \geq 7$, define the function $\Lambda_K : [2^K, \infty) \to \mathbb{R}$ by

$$\Lambda_K(D) = 2 + \frac{2\log(K\mu_K)}{2\log(\sqrt{D-1} + \sqrt{D}) - \log(K\mu_K)}. \tag{3.11}$$

It is easily seen that, for each value of $K$, $\Lambda_K$ is a decreasing function.

Define the function $\Lambda : [7, \infty) \to \mathbb{R}$ by

$$\Lambda(K) = 2 + \frac{6\log K}{2(K+1)\log 2 - 3\log K}.$$

A straightforward calculation yields

$$\Lambda'(K) = \frac{6}{K}\left(\frac{2(K+1)\log 2 - 2K\,(\log 2)\,(\log K)}{(2(K+1)\log 2 - 3\log K)^2}\right).$$

Since $K \geq 7$,

$$2(K+1)\log 2 - 2K\,(\log 2)\,(\log K) = (2\log 2)(K + 1 - K\log K) < 0.$$

Thus, $\Lambda'(K) < 0$ and so $\Lambda$ is a decreasing function.

Rewriting $\lambda$, from equation (3.10), we have

$$\lambda = 1 + \frac{2\log\left(\sqrt{uv^2} + \sqrt{uv^2+1}\right) + \log(k\mu_k)}{2\log\left(\sqrt{uv^2} + \sqrt{uv^2+1}\right) - \log(k\mu_k)},$$

and so

$$\lambda = 2 + \frac{2\log(k\mu_k)}{2\log\left(\sqrt{uv^2} + \sqrt{uv^2+1}\right) - \log(k\mu_k)} = \Lambda_k(uv^2+1) = \Lambda_k(a^2cx^k).$$

Since $k \geq 7$, $\Lambda_k$ is a decreasing function. So, since $a^2cx^k \geq 2^k$,

$$\lambda = \Lambda_k(a^2cx^k) \leq \Lambda_k(2^k). \tag{3.12}$$

By Lemma 20, $\mu_k \leq \sqrt{k}$ and so $k\mu_k \leq k^{3/2}$. From equations (3.11) and (3.12),

$$\lambda \leq \Lambda_k(2^k) \leq 2 + \frac{2\log(k^{3/2})}{2\log\left(\sqrt{2^k-1} + \sqrt{2^k}\right) - \log k^{3/2}}.$$

Since $2^k - 1 > 2^{k-1}$, we have

$$\sqrt{2^k-1} + \sqrt{2^k} > 2^{(k-1)/2} + 2^{k/2} > 2^{(k-1)/2} + 2^{(k-1)/2} = 2^{(k+1)/2}.$$

Hence,

$$\lambda < 2 + \frac{2\log(k^{3/2})}{2\log(2^{(k+1)/2}) - \log k^{3/2}} < 2 + \frac{6\log k}{2(k+1)\log 2 - 3\log k} = \Lambda(k). \tag{3.13}$$

We use the bounds for $\lambda$ in bounding inequality (3.23) for various values of $k$.

Next, we use $\alpha^k$ and $\beta^k$ to derive an upper bound for $|\alpha - \beta|$. We have

$$\alpha^k - \beta^k = \left(\sqrt[k]{1 + \frac{1}{uv^2}}\right)^k - \left(\frac{xy}{z^2}\right)^k = 1 + \frac{1}{uv^2} - \frac{(a^2cx^k)(b^2cy^k)}{(abcz^k)^2}.$$

Using equations (3.3)–(3.5), we write this equation in terms of $u$, $v$, and $w$,

$$\alpha^k - \beta^k = \frac{uv^2 + 1}{uv^2} - \frac{(uv^2 + 1)(uw^2 + 1)}{(uvw + 1)^2} = \frac{uv^2(2uvw - uv^2) + (2uvw + 1)}{uv^2(uvw + 1)^2} \quad (3.14)$$

Since $w > v$, we have $2uvw > uv^2$, implying that $\alpha^k > \beta^k$. Hence, $\alpha > \beta$.

Since $uv^2 > 0$, it follows from equation (3.14) that

$$\begin{aligned}\alpha^k - \beta^k &< \frac{uv^2(2uvw + 2) + (2uvw + 2)}{uv^2(uvw + 1)^2} = \frac{(uv^2 + 1)(2uvw + 2)}{uv^2(uvw + 1)^2} \\ &= \left(1 + \frac{1}{uv^2}\right)\frac{2}{uvw + 1}.\end{aligned}$$

Since $\alpha^k = 1 + (1/uv^2)$, we obtain

$$\alpha^k - \beta^k < \frac{2\alpha^k}{uvw + 1}. \quad (3.15)$$

Note that $\alpha^k - \beta^k$ factors as

$$\alpha^k - \beta^k = (\alpha - \beta)\sum_{i=0}^{k-1} \alpha^{k-1-i}\beta^i. \quad (3.16)$$

For each $0 \le i \le k - 1$, we have $\alpha^{k-1-i}\beta^i > 1$, implying that

$$\alpha^k - \beta^k > (\alpha - \beta)\sum_{i=0}^{k-1} 1 = (\alpha - \beta)k.$$

Thus, $\alpha - \beta < (\alpha^k - \beta^k)/k$ and so inequality (3.15) yields

$$\alpha - \beta < \frac{2\alpha^k}{k(uvw+1)}. \tag{3.17}$$

We combine the upper and lower bound for $|\alpha - \beta|$, namely, inequality (3.9) and the above inequality to obtain

$$\frac{1}{8k\mu_k uv^2 z^{2\lambda}} < \frac{2\alpha^k}{k(uvw+1)} < \frac{2\alpha^k}{kuvw}. \tag{3.18}$$

Our next step is to work towards an inequality depending only on the values $a$, $c$, $x$, $k$, and $\lambda$. First, we solve for $w$ to find that

$$w < 2^4 \mu_k \alpha^k v z^{2\lambda}. \tag{3.19}$$

Next, we find an upper bound for $z$, so that we can eliminate it from this inequality.

From equation (3.5),

$$z^k = \frac{uvw+1}{abc} \leq uvw + 1 = uvw\left(1 + \frac{1}{uvw}\right).$$

Since $w > v$, $1 + (1/uvw) < 1 + (1/uv^2) = \alpha^k$ and so $z^k < \alpha^k uvw$. Combining this with inequality (3.19) yields $w^k < 2^{4k}\mu_k^k \alpha^{k^2} v^k \left(\alpha^k uvw\right)^{2\lambda}$. Again, solving for $w$, we obtain

$$w^{k-2\lambda} < 2^{4k}\mu_k^k \alpha^{k(k+2\lambda)} u^{2\lambda} v^{k+2\lambda}. \tag{3.20}$$

Next, we find a lower bound for $w$. Using equations (3.3) and (3.4), we have

$$\begin{aligned}(uv^2+1)(uw^2+1)-(uvw+1)^2 &= (a^2cx^k)(b^2cy^k)-(abcz^k)^2\\ &= a^2b^2c^2[(xy)^k-(z^2)^k].\end{aligned}$$

Since, by inequality (3.6), $xy > z^2$,

$$a^2b^2c^2[(xy)^k-(z^2)^k] \geq a^2b^2c^2[(z^2+1)^k-(z^2)^k].$$

Expanding $(z^2+1)^k$ yields

$$a^2b^2c^2[(z^2+1)^k-(z^2)^k] = a^2b^2c^2\left(\sum_{i=0}^{k}\binom{k}{i}z^{2i}-z^{2k}\right) = a^2b^2c^2\sum_{i=0}^{k-1}\binom{k}{i}z^{2i}.$$

Since all of the terms in the sum are positive, we have

$$\begin{aligned}a^2b^2c^2\sum_{i=0}^{k-1}\binom{k}{i}z^{2i} &> a^2b^2c^2\left[\binom{k}{k-1}z^{2(k-1)}+\binom{k}{k-2}z^{2(k-2)}\right]\\ &= a^2b^2c^2\left(kz^{2(k-1)}+\frac{k(k-1)}{2}z^{2(k-2)}\right).\end{aligned}$$

Hence,

$$(uv^2+1)(uw^2+1)-(uvw+1)^2 > a^2b^2c^2kz^{2(k-1)}+a^2b^2c^2\frac{k(k-1)}{2}z^{2(k-2)}. \quad (3.21)$$

Since $a$, $b$, $c \geq 1$, and $k \geq 7$,

$$a^2b^2c^2\frac{k(k-1)}{2}z^{2(k-2)} > abcz^k.$$

From equation (3.5), $uvw = abcz^k - 1$ and $w > v$, and so $abcz^k = uvw + 1 > uv^2$.

Therefore,

$$a^2b^2c^2\frac{k(k-1)}{2}z^{2(k-2)} > uv^2.$$

Note that $uv^2+uw^2 = (uv^2+1)(uw^2+1)-(uvw+1)^2+2uvw$. Thus, inequality (3.21) implies that

$$uv^2 + uw^2 > a^2b^2c^2kz^{2(k-1)} + a^2b^2c^2\frac{k(k-1)}{2}z^{2(k-2)} > a^2b^2c^2kz^{2(k-1)} + uv^2.$$

Hence, $uw^2 > a^2b^2c^2kz^{2(k-1)}$. Again, using $abcz^k > uvw$, we obtain

$$(uw^2)^k > \left(a^2b^2c^2kz^{2(k-1)}\right)^k > k^k\left(abcz^k\right)^{2(k-1)} > k^k(uvw)^{2(k-1)},$$

implying that

$$w^2 > k^k u^{(k-2)}v^{2(k-1)}. \tag{3.22}$$

Combining this lower bound and the upper bound for $w$, from inequality (3.20), yields

$$\left(k^k u^{k-2}v^{2(k-1)}\right)^{k-2\lambda} < \left(2^{4k}\mu_k^k\alpha^{k(k+2\lambda)}u^{2\lambda}v^{k+2\lambda}\right)^2,$$

and so

$$\left(uv^2\right)^{(k-2\lambda-2)} < 2^8\mu_k^2\alpha^{2(k+2\lambda)}k^{-(k-2\lambda)}.$$

Since $uv^2 = a^2cx^k - 1$ and $\alpha^k = 1 + (1/uv^2) = 1 + 1/\left(a^2cx^k - 1\right)$, this implies that

$$\left(a^2cx^k - 1\right)^{(k-2\lambda-2)} < 2^8\mu_k^2\left(1 + \frac{1}{a^2cx^k - 1}\right)^{2+(4\lambda/k)}k^{-(k-2\lambda)}. \tag{3.23}$$

Having deduced an inequality dependent only on $a$, $c$, $x$, $k$, and $\lambda$, we next show that there is only a finite number of possible values of $k$ and $a^2cx^k$ that satisfy this

inequality. Let

$$S = \{(7, d) | d < 1035 \cdot 2^7\} \cup \{(8, d) | d < 10 \cdot 2^8\}.$$

Using inequality (3.23), we prove that $(k, a^2cx^k) \in S$.

Suppose, for a contradiction, that $k \geq 10$. Recalling that $\Lambda$ is a decreasing function and that, from inequality (3.13), $\lambda < \Lambda(k)$, $k \geq 10$ implies that $\Lambda(k) \leq \Lambda(10)$. A straightforward calculation yields $\Lambda(10) < 3.7$. Hence $\lambda < 3.7$. Since $x > 1$, by assumption, $a^2cx^k \geq 2^{10}$. Thus, bounding the left hand side of inequality (3.23) we have

$$\left(a^2cx^k - 1\right)^{(k-2\lambda-2)} > \left(a^2cx^k - 1\right)^{10-2\cdot 3.7-2} \geq (2^{10} - 1)^{0.6} > 63.$$

On the other hand, by Lemma 20 , $\mu_k \leq \sqrt{k}$, and so, bounding the right hand side we have

$$2^8\mu_k^2 \left(1 + \frac{1}{a^2cx^k - 1}\right)^{2+(4\lambda/k)} k^{-(k-2\lambda)} \leq 2^8 \left(1 + \frac{1}{a^2cx^k - 1}\right)^{2+(4\lambda/k)} k^{-(k-2\lambda-1)}.$$

Again, using $a^2cx^k \geq 2^{10}$, $\lambda < 3.7$, and $k \geq 10$,

$$2^8 \left(1 + \frac{1}{a^2cx^k - 1}\right)^{2+(4\lambda/k)} k^{-(k-2\lambda-1)} < 2^8 \left(1 + \frac{1}{2^{10} - 1}\right)^{3.48} 10^{-1.6} < 7.$$

Thus, inequality (3.23) implies that $63 < 7$, a contradiction. Hence, $k \leq 9$.

Using a similar method, suppose that $k = 9$. Then, from inequality (3.12) with $a^2cx^9 \geq 2^9$ and a calculation, $\lambda \leq \Lambda_9(2^9) < 3.2$. Since $\mu_9 = \sqrt{3}$, inequality (3.23) yields

$$\left(a^2cx^9 - 1\right)^{(9-2\lambda-2)} > (2^9 - 1)^{9-2\cdot 3.2-2} > 42$$

and

$$2^8\mu_9^2\left(1+\frac{1}{a^2cx^9-1}\right)^{2+(4\lambda/9)}9^{-(9-2\lambda)} < 2^8\sqrt{3}^2\left(1+\frac{1}{2^9-1}\right)^{2+(4\cdot 3.2/9)}9^{-(9-2\cdot 3.2)}$$
$$= 2^8\cdot 3\left(1+\frac{1}{2^9-1}\right)^{3.43}9^{-2.6} < 3.$$

This is another contradiction. Hence, $k \neq 9$. Since $k \geq 7$, by hypothesis, it remains to consider $k = 7$ and 8.

Again, for a contradiction, suppose that $k = 8$ and $(8, a^2cx^8) \notin S$. From the definition of $S$, this implies that $a^2cx^8 \geq 10\cdot 2^8$. Also, recalling that $\Lambda_8$ is a decreasing function, inequality (3.12) yields $\lambda \leq \Lambda_8(10\cdot 2^8) < 2.86$. Then, since $\mu_8 = 2$, inequality (3.23) implies that

$$9 < (10\cdot 2^8-1)^{8-2\cdot 2.86-2} < 2^8\cdot 2^2\left(1+\frac{1}{10\cdot 2^8-1}\right)^{2+4\cdot 2.86/8}8^{-(8-2\cdot 2.86)} < 9,$$

another contradiction. Therefore, if $k = 8$, then $(8, a^2cx^8) \in S$.

Finally, suppose $k = 7$ and $(7, a^2cx^7) \notin S$. Then, by the definition of $S$, $a^2cx^7 \geq 1035\cdot 2^7$. So, as before, we calculate that $\lambda \leq \Lambda_7(1035\cdot 2^7) < 2.4162$ and $\mu_7 = 7^{1/6}$. Thus, from inequality (3.23), we find that

$$7.218 < (1035\cdot 2^7-1)^{7-2\cdot 2.4162-2} < 2^8 7^{1/3}\left(1+\frac{1}{1035\cdot 2^7-1}\right)^{2+4\cdot 2.4162/7}7^{-(7-2\cdot 2.4162)}$$
$$< 7.213,$$

a contradiction. Hence, $(k, a^2cx^k) \in S$.

Since $S$ is a specific finite set, knowing that $(k, a^2cx^k) \in S$, yields a finite set of possible values of $a$, $c$, $x$, and $k$. We use continued fractions to complete the proof.

From equation (3.2), we have

$$(a^2cx^k - 1)b^2cy^k - a^2cx^k = (abcz^k)^2 - 2abcz^k. \tag{3.24}$$

Recalling that $a^2cx^k - 1 = uv^2$, we have

$$(uv^2)b^2cy^k - a^2cx^k = a^2b^2c^2z^k\left(z^k - \frac{2}{abc}\right).$$

Now, since $a^2cx^k > 0$ and $b \geq 1$, we obtain $(uv^2)b^2cy^k \geq a^2b^2c^2z^k(z^k - 2/(ac))$. Multiplying both sides by $x^k/(uv^2b^2cz^{2k})$ results in

$$\left(\frac{xy}{z^2}\right)^k > \frac{a^2cx^k}{uv^2z^k}\left(z^k - \frac{2}{ac}\right).$$

Again, since $a^2cx^k = uv^2 + 1$ and $z \geq 2$, we have

$$\left(\frac{xy}{z^2}\right)^k > \frac{a^2cx^k}{uv^2}\left(\frac{z^k - 2/ac}{z^k}\right) = \frac{uv^2+1}{uv^2}\left(1 - \frac{2}{acz^k}\right) \geq \alpha^k\left(\frac{2^kac - 2}{2^kac}\right).$$

For convenience, let

$$R = R(k, a, c) = \left(\frac{2^kac - 2}{2^kac}\right)^{1/k}.$$

Then,

$$\beta^k = \left(\frac{xy}{z^2}\right)^k > \alpha^kR^k.$$

Hence, $\beta > \alpha R$.

Recalling that $\alpha > \beta$, we have

$$\alpha^k - \beta^k = (\alpha - \beta)\sum_{i=0}^{k-1}\alpha^{k-1-i}\beta^i > (\alpha - \beta)\sum_{i=0}^{k-1}(\alpha R)^{k-1} = (\alpha - \beta)k\alpha^{k-1}R^{k-1}.$$

Therefore, $(\alpha - \beta) < (\alpha^k - \beta^k)/(k\alpha^{k-1}R^{k-1})$. Together with the upper bound for $\alpha^k - \beta^k$ from inequality (3.17), this implies that

$$\alpha - \beta < \frac{2\alpha}{kR^{k-1}(uvw+1)}.$$

Since $uvw + 1 = abcz^k \geq acz^k$,

$$\frac{\alpha}{x} - \frac{\beta}{x} \leq \frac{2\alpha}{xkacz^k} R^{-k+1}. \tag{3.25}$$

From the definition of $R$, we have that

$$R^{-k+1} = \left(\frac{2^k ac}{2^k ac - 2}\right)\left(\frac{2^k ac - 2}{2^k ac}\right)^{1/k} < \left(\frac{2^k ac}{2^{k-1} ac}\right)\left(\frac{2^k ac}{2^k ac}\right)^{1/k} = 2.$$

It is also easy to see that $\alpha = \sqrt[k]{1 + 1/(a^2 c x^k - 1)} < 2$. Further, recalling that $a$, $c \geq 1$, $k \geq 7$, and $x$, $z > 1$, we deduce that

$$\frac{\alpha}{x} - \frac{\beta}{x} \leq \frac{2\alpha}{xkacz^k} R^{-k+1} < \frac{1}{2z^4}.$$

Hence, inequality (2.10) is satisfied, implying that $\beta/x = y/z^2$ is a convergent of the continued fraction of $\alpha/x$.

Fix $J \geq 0$ such that $y/z^2 = p_J/q_J$. Since $p_J/q_J$ is in lowest terms, we have $q_J \leq z^2$. Next, since $\alpha > \beta$, we have $\alpha/x > \beta/x$. Therefore, inequality (2.12) implies that $J$ is even. Further, since $\alpha < 2$ and $x > 1$, $\alpha/x < 1$. Thus, from the definition of the 0-th convergent, $p_0/q_0 = a_0 = 0$. But $p_J/q_J = y/z^2 > 0$ and so $J \neq 0$. Hence, $J$ is even and strictly positive.

Next, we determine an upper bound for $J$ by bounding the value of $q_J$. Since $q_J \leq z^2$, we first derive an upper bound for $z^2$ by combining an upper and lower

bound for $|\alpha/x - \beta/x|$.

The lower bound for $|\alpha - \beta|$ from inequality (3.9) implies that

$$\frac{1}{8k\mu_k uv^2 z^{2\lambda} x} < \frac{\alpha}{x} - \frac{\beta}{x}.$$

Combining this with inequality (3.25), we have

$$\frac{1}{8k\mu_k uv^2 z^{2\lambda} x} < \frac{2\alpha}{kacz^k x} R^{-k+1}.$$

Solving for $z$ yields

$$z^{k-2\lambda} < \frac{16\mu_k \alpha u v^2}{ac} R^{-k+1}.$$

Thus,

$$q_J \leq z^2 < \left(\frac{16\mu_k \alpha u v^2}{ac} R^{-k+1}\right)^{2/(k-2\lambda)}. \tag{3.26}$$

Now, for each possible $(a, c, x, k)$ such that $(k, a^2 c x^k) \in S$, we use SAGE [66] to compute the first fifteen partial quotients $a_j$ of $\alpha/x$. Then, we compute the corresponding values of $q_j$. Comparing those $q_j$ values with the upper bound for $q_J$, we find that, for some $J_{\max} \leq 14$,

$$q_{J_{\max}} < (16\mu_k \alpha u v^2 R^{-k+1}/(ac))^{2/(k-2\lambda)} \leq q_{J_{\max}+1}.$$

Since $q_j$ is increasing for $j > 1$ and $q_J$ satisfies inequality (3.26), $J \leq J_{\max}$. Hence, for each $(k, a^2 c x^k) \in S$, we have determined a finite set of possible values of $J$.

Next, we derive a lower bound for the $J+1$-st partial quotient, $a_{J+1}$. By inequality (2.11),

$$\frac{\alpha}{x} - \frac{y}{z^2} > \frac{1}{q_J^2 (a_{J+1} + 2)} \geq \frac{1}{z^4 (a_{J+1} + 2)}.$$

Combining this with the upper bound in inequality (3.25) yields

$$\frac{1}{z^4(a_{J+1}+2)} < \frac{2\alpha}{xkacz^k} R^{-k+1}.$$

Solving for $\alpha_{J+1}$, we find

$$a_{J+1} > \frac{xkacz^{k-4}}{2\alpha} R^{k-1} - 2. \tag{3.27}$$

In order to eliminate $z$ from this inequality, we derive a lower bound for $z$ by using the lower bound for $w$. From inequality (3.22), $w^2 > k^k u^{(k-2)} v^{2(k-1)}$ and so $(uvw)^2 > k^k u^k v^{2k}$. Since $abcz^k = uvw + 1 > uvw$,

$$abcz^k > k^{k/2} u^{k/2} v^k.$$

Reducing equation (3.24) modulo $b$, we find that $a^2 cx^k \equiv 0 \pmod{b}$ and so $b \leq a^2 cx^k$. Combining this with the inequality above, we have $a^2 cx^k z^k > k^{k/2} u^{k/2} v^k$. So,

$$z > \frac{\sqrt{kuv^2}}{a^{3/k} c^{2/k} x}.$$

Thus, by inequality (3.27), we have

$$a_{J+1} > \frac{xkac}{2\alpha} \left( \frac{\sqrt{kuv^2}}{a^{3/k} c^{2/k} x} \right)^{k-4} R^{k-1} - 2.$$

For each possible value of $(a, c, x, k, J)$, we compute $a_{J+1}$ for $\alpha/x$ and calculate this lower bound for $a_{J+1}$. In each case, we find that $a_{J+1}$ is smaller than the bound, a contradiction. Hence, there are no possible values and so the theorem is proved. $\square$

# Chapter 4

# Main Theorem II

This chapter focuses on Main Theorem II, which we state below. The proof depends heavily on the results for Lehmer pairs presented in Section 2.3.

In 1992, Cohn [29] enumerated all of the integer solutions to the equation $X^2+2^L = Y^N$ with $L \in \mathbb{Z}^+$ odd and $N \geq 3$. Arif and Abu Muriefah [1] made some progress on the $L$ even case in 1997, proving many special cases. After Bilu, Hanrot, and Voutier's major work [15, Theorem 1.4] on Lucas and Lehmer pairs, Arif and Abu Muriefah [2, Theorem 1] proved the remaining cases.

The following year, Luca [47, Theorem 2.1] solved the equation $X^2 + 2^L 3^M = Y^N$ with $L$, $M$, $N \in \mathbb{Z}^+$ and $N \geq 3$. Other results on equations of this form were subsequently solved where the second term has a small number of prime divisors (see for example [50,57,69]).

In 2011, Wang and Wang [77], considered a variation of the equation studied by Arif and Abu Muriefah, $NX^2 + 2^L = Y^N$ with $L$, $N \in \mathbb{Z}^+$, $N > 1$, $L$ even, and $N$ odd. The case, in which $L$ is odd was solved by Wu [80] and independently by Luca and Soydan [48, Theorem 1].

Inspired by Wang and Wang's work, in the following theorem we consider a vari-

ation of Luca's equation.

**Main Theorem II.** *Let $L$, $M$, $N \in \mathbb{Z}^+$ with $N > 1$. Then the equation*

$$NX^2 + 2^L 3^M = Y^N, \tag{4.1}$$

*has no solutions with $X$, $Y \in \mathbb{Z}^+$ and $\gcd(NX, Y) = 1$.*

In the next two sections, we discuss earlier results and prove a special case of the main theorem before presenting the proof of Main Theorem II, in the last section.

## 4.1 Preliminary Results

In this section, we present some results that we use in the proof of Main Theorem II, then state and prove two technical lemmas. We use the following result of Luca [47, Theorem 2.1], in proving Lemma 25.

**Theorem 21** (Luca)**.** *Let $L$, $M$, $N \in \mathbb{Z}^+$ with $N \geq 5$. Then the equation*

$$X^2 + 2^L 3^M = Y^N$$

*has no solutions with $X$, $Y \in \mathbb{Z}^+$ and $\gcd(X, Y) = 1$.*

Luca lists all of the solutions for $N = 3$ and 4, but the statement above is sufficient for our purposes here. The proofs for $N = 3$ and 4 are applications of results by de Weger that appear in his dissertation [32].

*Sketch of proof.* Suppose for a contradiction, that a solution exists with $N \geq 5$. Luca constructs a Lucas pair from the hypothetical solution and shows that it is an $N$-defective Lucas pair. By Theorem 11, this implies that $N \leq 30$. A contradiction is

reached by examining Voutier's list in [15, Table 1] of Lucas pairs. □

Wang and Wang [77] proved that the equation $NX^2 + 2^L = Y^N$ has no solutions for $L$ even. We state their theorem and sketch the proof below. We use a similar method to prove Theorem 27 in which we consider equation (4.1) for $L$ and $M$ both even. Key to their proof is the following result by Heuberger and Le [39, Theorem 6.1 & 6.2]. (See Section 2.1 for a review of binary quadratic forms.)

**Theorem 22** (Heuberger and Le)**.** *Let $d \in \mathbb{Z}^+$ with $d > 1$ square-free and let $k > 1$ be an odd integer such that $\gcd(d, k) = 1$. If the equation*

$$X^2 + dY^2 = k^Z$$

*has a solution with $X, Y, Z \in \mathbb{Z}$, $\gcd(X, Y) = 1$, and $Z > 0$, then there exist $A, B, s, t \in \mathbb{Z}^+$ such that*

$$Z = st,$$

$$X + Y\sqrt{-d} = \lambda_1(A + \lambda_2 B\sqrt{-d})^t, \text{ with } \lambda_1, \lambda_2 \in \{-1, +1\},$$

$$A^2 + dB^2 = k^s,\ \gcd(A, B) = 1, \text{ and } s \mid h(-4d),$$

*where $h(-4d)$ is the class number of positive definite binary quadratic forms of discriminant $-4d$.*

*Sketch of the Proof.* Let $d$, $k \in \mathbb{Z}^+$ be given as in the theorem. Let

$$f(X, Y) = X^2 + dY^2.$$

So, $f = [1, 0, d]$ is a positive definite primitive binary quadratic form with discriminant $-4d$. For each $x$, $y$, $z \in \mathbb{Z}$ such that $\gcd(x, y) = 1$, $z > 0$, and $x^2 + dy^2 = k^z$, we have

that $f(x,y)$ is a representation of $k^z$. From equation (2.1), there exist $u$, $v$, $\ell \in \mathbb{Z}$ such that

$$xu - yv = 1, \quad \ell = 2axv + 2dyu, \text{ and } 0 \leq \ell < 2k.$$

Then, by congruence (2.2), $\ell^2 \equiv -4d \pmod{4k^z}$. Notice that $2 \mid \ell$. By [39, Lemma 5.1], there exists a unique $\bar{\ell} = \bar{\ell}(f,x,y) \in \mathbb{Z}^+$ such that $\bar{\ell} \equiv \pm\ell/2 \pmod{k}$, $0 < \bar{\ell} < k/2$,

$$\bar{\ell}^2 \equiv -d \pmod{k}, \tag{4.2}$$

and $\gcd(k, 2\bar{\ell}, (\bar{\ell}^2 + d)/k) = 1$. By equation (2.3), $2x \equiv -\ell y \pmod{2k^z}$, implying that

$$x \equiv \pm\bar{\ell}y \pmod{k}. \tag{4.3}$$

Assume that $x_0$, $y_0$, $z_0 \in \mathbb{Z}$ such that $\gcd(x_0, y_0) = 1$, $z_0 > 0$, and $f(x_0, y_0) = k^{z_0}$. Since $f(x_0, y_0) = f(-x_0, y_0)$, Heuberger and Le assume, using congruence (4.3), that $x_0 \equiv -\bar{\ell}y_0 \pmod{k}$.

Define

$$S = \{(x,y,z) \in \mathbb{Z}^3 | f(x,y) = k^z, \gcd(x,y) = 1, z > 0, \bar{\ell}(f,x,y) = \bar{\ell}(f,x_0,y_0)\},$$

$$S^+ = \{(x,y,z) \in S | x \equiv -\bar{\ell}y \pmod{k}\},$$

and

$$S^- = \{(x,y,z) \in S | x \equiv \bar{\ell}y \pmod{k}\}.$$

For convenience, let

$$T^+ = \{z \in \mathbb{Z}^+ | \exists x, y \in \mathbb{Z} \text{ s.t. } (x,y,z) \in S^+\}$$

and

$$T^- = \{z \in \mathbb{Z}^+ | \exists x, y \in \mathbb{Z} \text{ s.t. } (x, y, z) \in S^-\}.$$

Note that by congruence (4.3), $S = S^+ \cup S^-$. Also, $(x_0, y_0, z_0) \in S^+$ and so $S^+ \neq \emptyset$. Thus $T^+ \neq \emptyset$. Let $(\hat{x}, \hat{y}, \hat{z}) \in S^+$ such that $\hat{z}$ is the minimum of $T^+$.

Let $g = [k, 2\bar{\ell}, (\bar{\ell}^2 + d)/k]$. Then, $g$ is a primitive binary quadratic form with discriminant $-4d$. Heuberger and Le prove that for each $z \in T^+$, $[g]^z = [f]$. Since $f = [1, 0, d]$, $f(1, 0) = 1$ is a representation of 1 and so $[f] = [f_0]$, the identity element in the group of equivalence classes of binary quadratic forms of discriminant $-4d$. Since $z_0$, $\hat{z} \in T^+$, this implies that $[g]^{z_0} = [g]^{\hat{z}} = [f_0]$. By [39, Lemma 6.4], the order of $[g]$ is in $T^+$. Since $\hat{z} \in T^+$ is the minimum, $|[g]| = \hat{z}$. So, $\hat{z} \mid h(-4d)$ and $\hat{z} \mid z_0$. Let $t \in \mathbb{Z}^+$ such that

$$z_0 = \hat{z}t.$$

Then $f(x_0, y_0) = k^{z_0} = (k^{\hat{z}})^t = f(\hat{x}, \hat{y})^t$.

Let $x_t$, $y_t \in \mathbb{Z}$ such that

$$x_t + y_t\sqrt{-d} = (\hat{x} + \hat{y}\sqrt{-d})^t. \tag{4.4}$$

Notice that $x_t + y_t\sqrt{-d}$, $\hat{x} + \hat{y}\sqrt{-d} \in \mathbb{Q}(\sqrt{-d})$. Applying the norm map to equation (4.4) yields $f(x_t, y_t) = (f(\hat{x}, \hat{y}))^t = (k^{\hat{z}})^t = k^{z_0}$.

Expanding equation (4.4) and comparing the real and imaginary parts,

$$x_t = \sum_{j=0}^{[t/2]} \binom{t}{2j} \hat{x}^{t-2j} \hat{y}^{2j} (-d)^j$$

and

$$y_t = \sum_{j=0}^{[(t-1)/2]} \binom{t}{2j+1} \hat{x}^{t-2j-1} \hat{y}^{2j+1} (-d)^j.$$

Since $(\hat{x}, \hat{y}, \hat{z}) \in S^+$ with $\bar{\ell} = \bar{\ell}(f, x_0, y_0)$, $\hat{x} \equiv -\bar{\ell}\hat{y} \pmod{k}$. Then, congruence (4.2) implies that

$$x_t \equiv \hat{x}^t \sum_{j=0}^{[t/2]} \binom{t}{2j} \equiv 2^{t-1}\hat{x}^t \pmod{k},$$

since $\sum_{j=0}^{[t/2]} \binom{t}{2j} = 2^{t-1}$. Similarly, $y_t \equiv 2^{t-1}\hat{x}^{t-1}\hat{y} \pmod{k}$. Combining the congruences yields $x_t \equiv -\bar{\ell}y_t \pmod{k}$.

Suppose that $q$ is prime dividing $\gcd(x_t, y_t)$. Then, $q \mid f(x_t, y_t)$ and so $q \mid k$. Hence, $0 \equiv x_t \equiv 2^{t-1}\hat{x}^t \pmod{q}$. Since $k$ is odd, $q$ is also odd. Thus, this implies that $q \mid \hat{x}$. It follows that $q \mid \hat{y}$. But this is a contraction, since $\gcd(\hat{x}, \hat{y}) = 1$. Hence, $gcd(x_t, y_t) = 1$ and therefore $f(x_t, y_t) = k^{z_0}$ is a representation.

Finally, it is easy to show that $\ell(f, x_t, y_t) = \ell(f, x_0, y_0)$. Since the representations $f(x_t, y_t) = k^{z_0} = f(x_0, y_0)$ have the same characteristic number, by Lemma 1, $x_0 + y_0\sqrt{-d} = \pm(x_t + y_t\sqrt{-d})$. Set $A = |\hat{x}|$ and $B = |\hat{y}|$, and let $\lambda_1$, $\lambda_2 \in \{1, -1\}$ such that

$$x_0 + y_0\sqrt{-d} = \lambda_1(A + \lambda_2 B\sqrt{-d})^t.$$

The theorem follows by setting $s = \hat{z}$. □

**Theorem 23** (Wang and Wang)**.** *Let $L$, $N \in \mathbb{Z}^+$ with $L$ even and $N > 1$. The equation*

$$NX^2 + 2^L = Y^N$$

*has no solutions with $X$, $Y \in \mathbb{Z}^+$ and $\gcd(NX, Y) = 1$.*

*Sketch of Proof.* Using Theorem 22, Wang and Wang construct a $t$-defective Lehmer pair $(\alpha, \beta)$ for an integer $t$ dividing $N$. Using Theorems 10 and 11, they show that $t$ must be one of only a few values. They use congruence arguments to derive a contradiction for each of these values. □

Wu [80] proved that the equation $NX^2 + 2^L = Y^N$ has no solutions for $L$ odd and $N > 3$. He used the same type of arguments that are used in the proof of Theorem 23, but replaced Theorem 22 with an earlier result of Le [42, Theorem 3]. Luca and Soydan [48, Theorem 1] independently proved a slightly stronger result.

**Theorem 24** (Luca and Soydan)**.** *Let $L$, $N \in \mathbb{Z}^+$ with $L$ odd and $N > 3$. The equation*

$$NX^2 + 2^L = Y^N$$

*has no solutions with $X$, $Y \in \mathbb{Z}^+$ and $\gcd(X, Y) = 1$.*

*Sketch of proof.* From a hypothetical solution with $N \neq 5$ or 15, Luca and Soydan construct a $2t$-defective Lehmer pair for some $t$, with $t \mid N$. Then, the results in Theorem 10 and 11 yield a contradiction. For each of the remaining $N$, they translate the problem to one of either solving a Thue equation or finding points on an elliptic curve, both of which they solve with computer calculations. □

Next, we show that in proving Main Theorem II, it is sufficient to consider $N$ square-free.

**Lemma 25.** *Let $L$, $M$, $N$, $X$, $Y \in \mathbb{Z}^+$ with $N > 1$ and $\gcd(NX, Y) = 1$. If $NX^2 + 2^L 3^M = Y^N$, then there exist $N'$, $X'$, $Y' \in \mathbb{Z}^+$ with $N' > 1$ square-free and $\gcd(N'X', Y') = 1$ such that $N'(X')^2 + 2^L 3^M = Y'^{N'}$.*

*Proof.* Suppose that $(N, X, Y, L, M) = (n, x, y, \ell, m)$ is a solution in positive integers to the equation $NX^2 + 2^L 3^M = Y^N$ so that

$$nx^2 + 2^\ell 3^m = y^n \tag{4.5}$$

with $n$, $x$, $y$, $\ell$, $m \in \mathbb{Z}^+$, $n > 1$, and $\gcd(nx, y) = 1$.

Let $p = 2$ or 3. The assumption that $\ell,\ m \geq 1$ implies that $p \mid 2^{\ell}3^{m}$. By equation (4.5), $p \mid (y^n - nx^2)$. Thus, we see that $p \mid y$ if and only if $p \mid nx$. Since $\gcd(nx, y) = 1$, $p \nmid y$ and $p \nmid nx$. Hence, $\gcd(nxy, 6) = 1$, and so $n \geq 5$.

Let $u,\ v \in \mathbb{Z}^+$ such that $n = uv^2$ with $u$ square-free. Suppose that $u = 1$. Then $n = v^2$ and so, by equation (4.5), $(vx)^2 + 2^{\ell}3^{m} = y^{v^2}$. Notice that $\gcd(vx, y) = 1$ and $v^2 = n \geq 5$. Thus, $(N, X, Y, L, M) = (v^2, vx, y, \ell, m)$ is an integer solution to $X^2 + 2^L 3^M = Y^N$, with $N \geq 5$. By Theorem 21, this is a contradiction. Therefore, $u > 1$.

Since $n = uv^2$ with $u > 1$ and $\gcd(nx, y) = 1$, we have $\gcd(uvx, y^{v^2}) = 1$. Equation (4.5) implies that $u(vx)^2 + 2^{\ell}3^{m} = (y^{v^2})^u$. Therefore, $(N, X, Y, L, M) = (u, vx, y^{v^2}, \ell, m)$ is a solution to the equation $NX^2 + 2^L 3^M = Y^N$ with $N = u > 1$ square-free, as desired. □

For completeness, we include a proof of the following technical lemma on sums of certain binomial coefficients.

**Lemma 26.** *If $t \in \mathbb{Z}^+$, then*

*(a)* $\sum_{j=0}^{t} \binom{2t+1}{2j+1} = 2^{2t}$ *and*

*(b)* $\sum_{j=0}^{t} \binom{2t+1}{2j+1}(-1)^j = \pm 2^t$.

*Proof of* (a). Let $t \in \mathbb{Z}^+$. Let $f_1(t) = \sum_{j=0}^{t} \binom{2t+1}{2j}$ and $g_1(t) = \sum_{j=0}^{t} \binom{2t+1}{2j+1}$. Then,

$$\begin{aligned} f_1(t) + g_1(t) &= \sum_{j=0}^{t} \binom{2t+1}{2j} + \sum_{j=0}^{t} \binom{2t+1}{2j+1} = \sum_{k=0}^{2t+1} \binom{2t+1}{k} \\ &= \sum_{k=0}^{2t+1} \binom{2t+1}{k} 1^{2t+1-k} 1^k = (1+1)^{2t+1} = 2^{2t+1}. \end{aligned} \tag{4.6}$$

Similarly, we find that

$$\begin{aligned} f_1(t) - g_1(t) &= \sum_{j=0}^{t} \binom{2t+1}{2j} - \sum_{j=0}^{t} \binom{2t+1}{2j+1} \\ &= \sum_{j=0}^{t} \binom{2t+1}{2j}(-1)^{2j} + \sum_{j=0}^{t} \binom{2t+1}{2j+1}(-1)^{2j+1} \\ &= \sum_{k=0}^{2t+1} \binom{2t+1}{k}(-1)^{k} = \sum_{k=0}^{2t+1} \binom{2t+1}{k}1^{2t+1-k}(-1)^{k} = (1-1)^{2t+1} = 0. \end{aligned}$$

Thus, $f_1(t) - g_1(t) = 0$ and so $f_1(t) = g_1(t)$. Combining this with equation (4.6), we have that $2g_1(t) = 2^{2t+1}$. Hence, $g_1(t) = 2^{2t}$, as desired. ■

*Proof of* (b). Let $t \in \mathbb{Z}^+$. Let $f_2(t) = -i\sum_{j=0}^{t}\binom{2t+1}{2j}(-1)^j$ and $g_2(t) = \sum_{j=0}^{t}\binom{2t+1}{2j+1}(-1)^j$. Then,

$$\begin{aligned} if_2(t) + ig_2(t) &= \sum_{j=0}^{t} \binom{2t+1}{2j}(-1)^{j} + i\sum_{j=0}^{t} \binom{2t+1}{2j+1}(-1)^{j} \\ &= \sum_{j=0}^{t} \binom{2t+1}{2j}i^{2j} + \sum_{j=0}^{t} \binom{2t+1}{2j+1}i^{2j+1} \\ &= \sum_{k=0}^{2t+1} \binom{2t+1}{k}i^{k} = \sum_{k=0}^{2t+1} \binom{2t+1}{k}1^{2t+1-k}i^{k} = (1+i)^{2t+1}. \end{aligned}$$

Similarly,

$$\begin{aligned} if_2(t) - ig_2(t) &= \sum_{j=0}^{t} \binom{2t+1}{2j}(-1)^{j} - i\sum_{j=0}^{t} \binom{2t+1}{2j+1}(-1)^{j} \\ &= \sum_{j=0}^{t} \binom{2t+1}{2j}(-i)^{2j} + \sum_{j=0}^{t} \binom{2t+1}{2j+1}(-i)^{2j+1} \\ &= \sum_{k=0}^{2t+1} \binom{2t+1}{k}(-i)^{k} = (1-i)^{2t+1}. \end{aligned}$$

Combining these two equations yields

$$\begin{aligned} 2ig_2(t) &= (1+i)^{2t+1} - (1-i)^{2t+1} = (1+i)^{2t}(1+i) - (1-i)^{2t}(1-i) \\ &= (2i)^t(1+i) - (-2i)^t(1-i) = (2i)^t\left((1+i) - (-1)^t(1-i)\right) \\ &= \begin{cases} 2^t(\pm i)2, & \text{if } t \text{ is odd,} \\ 2^t(\pm 1)(2i), & \text{if } t \text{ is even,} \end{cases} \\ &= \pm 2^t(2i). \end{aligned}$$

Therefore, $g_2(t) = \pm 2^t$. □

## 4.2 Proof of a Special Case

We now prove the special case of Main Theorem II in which $L$ and $M$ are both even.

**Theorem 27.** *Let $L$, $M$, $N \in \mathbb{Z}^+$ such that $L$ and $M$ are both even and $N > 1$. The equation*

$$NX^2 + 2^L 3^M = Y^N \tag{4.7}$$

*has no solutions with $X$, $Y \in \mathbb{Z}^+$ and $\gcd(NX, Y) = 1$.*

*Proof.* Let $\ell$, $m$, $n \in \mathbb{Z}^+$ with $\ell$ and $m$ both even and $n > 1$. For a contradiction, suppose that $(N, X, Y, L, M) = (n, x, y, \ell, m)$ is a solution to equation (4.7) with $x$, $y \in \mathbb{Z}^+$ and $\gcd(nx, y) = 1$. So, we have

$$nx^2 + 2^\ell 3^m = y^n. \tag{4.8}$$

By Lemma 25, we assume that $n$ is square-free. Since $\ell$, $m \geq 1$, as in the proof of Lemma 25, $\gcd(nxy, 6) = 1$, and so $n \geq 5$.

By assumption, $\ell$ and $m$ are both even. Therefore, there exist $k$, $k' \in \mathbb{Z}^+$ such that $\ell = 2k$ and $m = 2k'$. So, equation (4.8) can be rewritten as

$$\left(2^k 3^{k'}\right)^2 + nx^2 = y^n. \tag{4.9}$$

Since $n > 1$ is square-free, $y > 1$ is odd, and $\gcd(n, y) = 1$, the hypotheses of Theorem 22 are satisfied. Hence, there exist $A$, $B$, $s$, $t \in \mathbb{Z}^+$ such that

$$n = st, \tag{4.10}$$

$$2^k 3^{k'} + x\sqrt{-n} = \lambda_1(A + \lambda_2 B\sqrt{-n})^t, \text{ with } \lambda_1, \lambda_2 \in \{+1, -1\}, \tag{4.11}$$

$$A^2 + nB^2 = y^s, \ \gcd(A, B) = 1, \tag{4.12}$$

and

$$s \mid h(-4n). \tag{4.13}$$

Let

$$\gamma = A + B\sqrt{-n}$$

and

$$\delta = -A + B\sqrt{-n}$$

in $\mathbb{Q}(\sqrt{-n})$. We prove that $(\gamma, \delta)$ is a $t$-defective Lehmer pair, after proving some preliminary results. First, we show that $t > 1$.

Suppose, for a contradiction that $t = 1$. Then by equation (4.10), $n = s$. Since $n > 1$ is square-free, Lemma 3 implies that $n > h(-4n)$. However, by equation (4.13) we have $n \mid h(-4n)$ and so $n \leq h(-4n)$, a contradiction. Therefore, $t > 1$.

Since $\gcd(n, 6) = 1$, equation (4.10) implies that $t$ is odd. Let $t_1 \in \mathbb{Z}$ such that

$t = 2t_1 + 1$. Since $t > 1$, we have that $t_1 \geq 1$. Expanding $\lambda_1 \left(A + \lambda_2 B\sqrt{-n}\right)^t$ in equation (4.11) yields

$$\begin{aligned} 2^k 3^{k'} + x\sqrt{-n} &= \lambda_1 \sum_{i=0}^{t} \binom{t}{i} A^{t-i} \left(\lambda_2 B\sqrt{-n}\right)^i \\ &= \lambda_1 \left( \sum_{j=0}^{t_1} \binom{t}{2j} A^{t-2j} (\lambda_2 B\sqrt{-n})^{2j} + \sum_{j=0}^{t_1} \binom{t}{2j+1} A^{t-2j-1} (\lambda_2 B\sqrt{-n})^{2j+1} \right). \end{aligned}$$

Comparing the real and imaginary parts, we find that

$$2^k 3^{k'} = \lambda_1 \sum_{j=0}^{t_1} \binom{t}{2j} A^{t-2j} (\lambda_2 B\sqrt{-n})^{2j}$$

and

$$x\sqrt{-n} = \lambda_1 \sum_{j=0}^{t_1} \binom{t}{2j+1} A^{t-2j-1} (\lambda_2 B\sqrt{-n})^{2j+1}.$$

Factoring and taking the absolute value of each sum, noting that $A$ and $B$ are positive and $\lambda_1$, $\lambda_2 \in \{\pm 1\}$, we find that

$$2^k 3^{k'} = A \left| \sum_{j=0}^{t_1} \binom{t}{2j} A^{t-2j-1} (-nB^2)^j \right|$$

and

$$x = B \left| \sum_{j=0}^{t_1} \binom{t}{2j+1} A^{t-2j-1} (-nB^2)^j \right|.$$

Thus, $A \mid 2^k 3^{k'}$ and $B \mid x$. For ease in notation, let

$$\mathcal{S} = \sum_{j=0}^{t_1} \binom{t}{2j} A^{t-2j-1} (-nB^2)^j$$

and so

$$2^k 3^{k'} = A|\mathcal{S}|. \tag{4.14}$$

Our next goal is to show that $A = 2^k 3^{k'}$ and $\mathcal{S} = \pm 1$. Since $\gcd(nxy, 6) = 1$, $x^2 \equiv 1 \pmod 6$ and $y^n \equiv y \pmod 6$. By equation (4.9), $n \equiv y \pmod 6$ and $n \equiv y \equiv y^s \pmod 6$, since $s$ is odd. Then, considering equation (4.12) modulo 6, we have

$$A^2 + nB^2 \equiv n \pmod 6. \tag{4.15}$$

Since $\gcd(x, 6) = 1$ and $B \mid x$, $\gcd(B, 6) = 1$, and so $B^2 \equiv 1 \pmod 6$. Hence, $A^2 + n \equiv n \pmod 6$. Thus, $A^2 \equiv 0 \pmod 6$, and so $6 \mid A$.

Reducing $\mathcal{S}$ modulo 6 yields

$$\mathcal{S} = \sum_{j=0}^{t_1} \binom{t}{2j} A^{t-2j-1}(-nB^2)^j \equiv \binom{t}{t-1}(-nB^2)^{t_1} \equiv t(-nB^2)^{t_1} \pmod 6. \tag{4.16}$$

We know that $\gcd(n, 6) = 1$ and $t \mid n$, so $n \equiv \pm 1 \pmod 6$ and $t \equiv \pm 1 \pmod 6$. Additionally, since $B^2 \equiv 1 \pmod 6$, $t(-nB^2)^{t_1} \equiv \pm 1 \pmod 6$. Therefore, congruence (4.16) yields $\mathcal{S} \equiv \pm 1 \pmod 6$. By equation (4.14), $S \mid 2^k 3^{k'}$ and therefore

$$\mathcal{S} = \pm 1 \quad \text{and} \quad A = 2^k 3^{k'}. \tag{4.17}$$

**Lemma 28.** *The pair $(\gamma, \delta)$ is a $t$-defective Lehmer pair.*

*Proof.* In order to show that $(\gamma, \delta)$ is a Lehmer pair as defined in Section 2.3, we show that the conditions (2.15)–(2.17) are satisfied. In other words, we show that $\gamma$ and $\delta$ are algebraic integers such that $(\gamma + \delta)^2$ and $\gamma\delta$ are relatively prime nonzero integers, and that $\gamma/\delta$ is not a root of unity.

Recall that $\mathbb{Q}(\sqrt{-n})$. Since $A$, $B \in \mathbb{Z}^+$, $A + B\sqrt{-n} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$ and so $\gamma$ and $\delta$

are nonzero algebraic integers. From the definition of $\gamma$ and $\delta$, we have

$$(\gamma+\delta)^2 = \left[\left(A+B\sqrt{-n}\right)+\left(-A+B\sqrt{-n}\right)\right]^2 = -4nB^2 \in \mathbb{Z}-\{0\}$$

and

$$\gamma\delta = \left(A+B\sqrt{-n}\right)\left(-A+B\sqrt{-n}\right) = -A^2-nB^2 = -y^s \in \mathbb{Z}-\{0\}. \tag{4.18}$$

Suppose, for a contradiction, that $p$ is a prime dividing $\gcd((\gamma+\delta)^2, \gamma\delta) = \gcd(4nB^2, y^s)$. It follows that $p \mid \gcd(2nB, y)$ and so, since $B \mid x$, $p \mid \gcd(2nx, y)$. But $\gcd(nx, y) = 1$ and $y$ is odd, so this is a contradiction. Hence, $\gcd((\gamma+\delta)^2, \gamma\delta) = 1$.

Now, $\gamma/\delta \in \mathbb{Q}(\sqrt{-n})$. Since $n \geq 5$, the only roots of unity in $\mathbb{Q}(\sqrt{-n})$ are 1 and $-1$. Since $A$ and $B$ are nonzero,

$$\gamma = A+B\sqrt{-n} \neq \pm\left(-A+B\sqrt{-n}\right) = \pm\delta$$

and so $\gamma/\delta \neq \pm 1$. Hence, $\gamma/\delta$ is not a root of unity. Therefore, $(\gamma, \delta)$ is a Lehmer pair.

It remains to show that $(\gamma, \delta)$ is $t$-defective. Since $t$ is odd, the $t$-th Lehmer number is

$$L_t(\gamma, \delta) = \frac{\gamma^t - \delta^t}{\gamma - \delta}. \tag{4.19}$$

Recalling that $t = 2t_1 + 1$ yields

$$\begin{aligned}
\gamma^t - \delta^t &= (A + B\sqrt{-n})^t - (-A + B\sqrt{-n})^t \\
&= \sum_{i=0}^{t} \binom{t}{i} A^{t-i}(B\sqrt{-n})^i - \sum_{i=0}^{t} \binom{t}{i} (-A)^{t-i}(B\sqrt{-n})^i \\
&= \sum_{i=0}^{t} \binom{t}{i} \left(A^{t-i} - (-A)^{t-i}\right)(B\sqrt{-n})^i \\
&= 2\sum_{j=0}^{t_1} \binom{t}{2j} A^{t-2j}(-nB^2)^j \\
&= 2A\sum_{j=0}^{t_1} \binom{t}{2j} A^{t-2j-1}(-nB^2)^j = 2A\mathcal{S}. \qquad (4.20)
\end{aligned}$$

Since $\gamma - \delta = 2A$, $\gamma^t - \delta^t = (\gamma - \delta)\mathcal{S}$. Therefore,

$$L_t(\gamma, \delta) = \frac{\gamma^t - \delta^t}{\gamma - \delta} = \mathcal{S} = \pm 1,$$

by equation (4.17). Thus, $L_t(\gamma, \delta) = \pm 1$ has no prime divisors and, as noted in Section 2.3, this means that $L_t(\gamma, \delta)$ has no primitive divisors. Hence, $(\gamma, \delta)$ is a $t$-defective Lehmer pair. ■

By Theorem 11, $t$-defective Lehmer pairs can only exist for $t \leq 30$. For $0 \leq d \leq 3$, we compare $i^d\gamma = i^d(A + B\sqrt{-n})$ to the values in Table 2.1. Since with $6 \mid A$ and $\gcd(B, 6) = 1$, we conclude that $t \leq 6$ or $t \in \{8, 10, 12\}$. However, $\gcd(t, 6) = 1$ and $t > 1$. Thus, $t = 5$.

Finally, by equation (4.17), $A = 2^k 3^{k'}$ and $\mathcal{S} = \pm 1$. So, $t = 5$ implies that

$$\pm 1 = \mathcal{S} = \sum_{j=0}^{2} \binom{5}{2j} A^{5-2j-1}(-nB^2)^j = 2^{4k}3^{4k'} - 10 \cdot 2^{2k}3^{2k'}nB^2 + 5n^2B^4.$$

Recalling that $k \geq 1$ and $2 \nmid nB$, we have that $\pm 1 \equiv 5n^2B^4 \equiv 5 \pmod 8$, a contra-

diction.

Hence, there are no solutions to equation (4.7) with $L$, $M \in \mathbb{Z}^+$ even. □

## 4.3 Proof of Main Theorem II

Finally, we prove the main result of this chapter. We use Theorem 27 and results from Section 4.1.

*Proof of Main Theorem II.* Let $\ell$, $m$, $n \in \mathbb{Z}^+$ with $n > 1$. For a contradiction, suppose that $(N, X, Y, L, M) = (n, x, y, \ell, m)$ is a solution to equation (4.1), with $x$, $y \in \mathbb{Z}^+$ and $\gcd(nx, y) = 1$. So,

$$nx^2 + 2^\ell 3^m = y^n. \tag{4.21}$$

Using Lemma 25, we assume that $n$ is square-free and, using Theorem 27, we assume that $\ell$ and $m$ are not both even. As in the proof of Lemma 25, $\ell$, $m \geq 1$ implies that $\gcd(nxy, 6) = 1$ and so $n \geq 5$. Note that, $\ell$, $m \geq 1$, also implies that $y > 1$.

We use the following notation. Let $k$, $k' \in \mathbb{Z}^+$ and $e$, $e' \in \{0, 1\}$ such that $\ell = 2k+e$ and $m = 2k' + e'$. Let $K = \mathbb{Q}(\sqrt{w}, \sqrt{-n})$, and let $F = \mathbb{Q}(\sqrt{-wn})$ with $w = 2^e 3^{e'}$. Since $\ell$ and $m$ are not both even, $e$ and $e'$ are not both zero. So, $w \in \{2, 3, 6\}$.

Rewriting equation (4.21), we have

$$2^{2k+e} 3^{2k'+e'} + nx^2 = y^n.$$

Factoring this equation in $K$ yields

$$\left(2^k 3^{k'} \sqrt{w} + x\sqrt{-n}\right)\left(2^k 3^{k'} \sqrt{w} - x\sqrt{-n}\right) = y^n.$$

Let

$$a = 2^k 3^{k'} \sqrt{w} + x\sqrt{-n}$$

and

$$b = 2^k 3^{k'} \sqrt{w} - x\sqrt{-n},$$

and so $ab = y^n$. Note that $b$ is the complex conjugate of $a$. Since $x \neq 0$, we have $a$, $b \in K - F$, whereas,

$$a^2 = \left(2^k 3^{k'} \sqrt{w} + x\sqrt{-n}\right)^2 = 2^\ell 3^m - nx^2 + 2^{k+1} 3^{k'} x\sqrt{-wn} \tag{4.22}$$

and

$$b^2 = \left(2^k 3^{k'} \sqrt{w} - x\sqrt{-n}\right)^2 = 2^\ell 3^m - nx^2 - 2^{k+1} 3^{k'} x\sqrt{-wn}, \tag{4.23}$$

are elements of $F$.

Next, we prove that $a^2\mathcal{O}_F$ and $b^2\mathcal{O}_F$ are relatively prime by working in the biquadratic field, $K$. First, suppose, for a contradiction, that $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$ such that $\mathfrak{p}$ divides each of the ideals $a\mathcal{O}_K$ and $b\mathcal{O}_K$. So, $\mathfrak{p}$ divides the product and the sum of $a\mathcal{O}_K$ and $b\mathcal{O}_K$. In particular, $\mathfrak{p}$ divides $(a\mathcal{O}_k)(b\mathcal{O}_K) = ab\mathcal{O}_K = (y^n)\mathcal{O}_K = (y\mathcal{O}_K)^n$ and so $\mathfrak{p} \mid y\mathcal{O}_K$. Let $p \in \mathbb{Z}$ be the prime lying under $\mathfrak{p}$. Then, $p \mid y$. The ideal $a\mathcal{O}_K + b\mathcal{O}_K$ contains the element $a + b$ and so contains the ideal $(a + b)\mathcal{O}_K = (2^{k+1}3^{k'}\sqrt{w})\mathcal{O}_K$. Therefore, $\mathfrak{p} \mid (2^{k+1}3^{k'}\sqrt{w})\mathcal{O}_K$. Since $w \in \{2, 3, 6\}$, $\mathfrak{p} \mid 6\mathcal{O}_K$. Thus, $p \mid 6$ and so $p \mid \gcd(y, 6)$. This is a contradiction, since $\gcd(y, 6) = 1$. Hence, $a\mathcal{O}_K$ and $b\mathcal{O}_K$ are relatively prime.

Now, suppose, for a contradiction, that $\mathfrak{q}$ is a prime ideal in $\mathcal{O}_F$ such that $\mathfrak{q}$ divides both $a^2\mathcal{O}_F$ and $b^2\mathcal{O}_F$. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal that lies over $\mathfrak{q}$. Then, $\mathfrak{p} \mid a^2\mathcal{O}_K$ and $\mathfrak{p} \mid b^2\mathcal{O}_K$. Since $a, b \in K$, $a^2\mathcal{O}_K = (a\mathcal{O}_K)^2$ and $b^2\mathcal{O}_K = (b\mathcal{O}_K)^2$ and so $\mathfrak{p} \mid a\mathcal{O}_K$ and $\mathfrak{p} \mid b\mathcal{O}_K$. However, $a\mathcal{O}_K$ and $b\mathcal{O}_K$ are relatively prime, so this is a contraction.

Hence, $a^2\mathcal{O}_F$ and $b^2\mathcal{O}_F$ are relatively prime.

Since $ab = y^n$, $(a^2\mathcal{O}_F)(b^2\mathcal{O}_F) = (a^2b^2)\mathcal{O}_F = y^{2n}\mathcal{O}_F = (y\mathcal{O}_F)^{2n}$. Therefore, since $a^2\mathcal{O}_F$ and $b^2\mathcal{O}_F$ are relatively prime, there exists an ideal $I \subseteq \mathcal{O}_F$ such that $a^2\mathcal{O}_F = I^{2n}$. Let $s \in \mathbb{Z}^+$ be the order of $I$ in the ideal class group of $\mathcal{O}_F$. So, $I^s$ is a principal ideal. Let $\alpha \in \mathcal{O}_F$ generate $I^s$,

$$\alpha\mathcal{O}_F = I^s.$$

Since $I^{2n} = a^2\mathcal{O}_F$ is also principal, we have that $s \mid 2n$. Let $t \in \mathbb{Z}$ such that

$$2n = st.$$

Then,

$$a^2\mathcal{O}_F = I^{2n} = I^{st} = (I^s)^t = (\alpha\mathcal{O}_F)^t = \alpha^t\mathcal{O}_F.$$

Therefore, there exists a unit, $\varepsilon \in \mathcal{O}_F^\times$ such that $a^2 = \varepsilon\alpha^t$. Since $F = \mathbb{Q}(\sqrt{-wn})$ is a quadratic field with $wn \geq 2 \cdot 5 = 10$, the only units in $\mathcal{O}_F$ are 1 and $-1$. Hence, $\varepsilon = \pm 1$.

To see that $t > 1$, first recall that $h_F$ is the class number $\mathcal{O}_F$. Since $s$ is the order of $I$ in the ideal class group of $\mathcal{O}_F$, $s \mid h_F$ and so $s \leq h_F$. By Lemma 4, $n > 1$ implies that $h_F < 2n = st \leq h_F t$. Thus, $t > 1$.

Next, suppose for a contradiction that $t$ is even. Then there exists $t_0 \in \mathbb{Z}^+$ such that $t = 2t_0$. Since $\varepsilon = \pm 1$, we have that $a^2 = \pm\alpha^{2t_0}$. This implies that $(a/\alpha^{t_0})^2 = \pm 1$ in $K$. Suppose that $(a/\alpha^{t_0})^2 = -1$. Then $K$ contains an element whose square is $-1$, meaning that $i \in K$. Since $i$ is of degree 2 over $\mathbb{Q}$, it must be in one of the quadratic subfields of $K$. Since $w > 1$ and $n \geq 5$, the only roots of unity in the subfields $\mathbb{Q}(\sqrt{w})$, $\mathbb{Q}(\sqrt{-n})$, and $\mathbb{Q}(\sqrt{-wn})$ are 1 and $-1$. So, $i \notin K$. Thus, $(a/\alpha^{t_0})^2 = 1$, implying that

$a = \pm\alpha^{t_0}$. Since $\alpha \in F$, this implies $a \in F$, which is a contradiction. Therefore, $t$ is odd.

Since $t$ is odd and $\varepsilon = \pm 1$, $\varepsilon = \varepsilon^t$ and so $a^2 = \varepsilon\alpha^t = (\varepsilon\alpha)^t = (\pm\alpha)^t$. Noting that $-\alpha$ and $\alpha$ both generate $I^s$, we can rename $-\alpha$ as $\alpha$. Thus, we assume that

$$a^2 = \alpha^t. \tag{4.24}$$

Let $t_1 \in \mathbb{Z}^+$ such that $t = 2t_1 + 1$. Now, we define a pair $(\gamma, \delta)$ by

$$\gamma = \frac{a}{\alpha^{t_1}}$$

and

$$\delta = \overline{\gamma}.$$

Our goal is to prove that $(\gamma, \delta)$ is a $2t$-defective Lehmer pair. First, we prove several preliminary results.

Since $a \in K - F$ and $\alpha \in F$, we have that $\gamma \in K$. Further, the equation $a^2 = \alpha^t$ implies that

$$\gamma^2 = \left(\frac{a}{\alpha^{t_1}}\right)^2 = \frac{\alpha^t}{\alpha^{2t_1}} = \alpha. \tag{4.25}$$

Thus, $\gamma$ is a zero of the monic polynomial $X^2 - \alpha$ with $\alpha \in \mathcal{O}_F$. By [68, Theorem 2.10], this implies that $\gamma \in \mathcal{O}_K$. Since $\delta = \overline{\gamma}$, $\delta \in \mathcal{O}_K$, as well.

Applying Lemma 5, we have $\gamma = A\sqrt{w} + B\sqrt{-n} + C\sqrt{-wn} + D$ for some $A$, $B$, $C$, $D \in \frac{1}{4}\mathbb{Z}$. Further, since $\gamma^2 = \alpha \in \mathcal{O}_F$, Lemma 5 implies that $A = B = 0$ or $C = D = 0$.

Suppose, for a contradiction, that $A = B = 0$. Then $\gamma = C\sqrt{-wn} + D \in \mathcal{O}_F$. So,

we have

$$(\gamma\mathcal{O}_F)^2 = \gamma^2\mathcal{O}_F = \alpha\mathcal{O}_F = I^s.$$

Since $st = 2n$ and $t$ is odd, $s$ is even. Thus, $\gamma\mathcal{O}_F = I^{s/2}$, a principal ideal. But this is a contradiction to $s$ being the order of $I$. Therefore, $\gamma \notin \mathcal{O}_F$ and so $C = D = 0$.

Hence, we have $A$, $B \in \frac{1}{4}\mathbb{Z}$ such that

$$\gamma = \frac{a}{\alpha^{t_1}} = A\sqrt{w} + B\sqrt{-n}, \tag{4.26}$$

and so

$$\delta = A\sqrt{w} - B\sqrt{-n}. \tag{4.27}$$

Since $\alpha \in \mathcal{O}_F = \mathbb{Z}[\sqrt{-wn}]$, there exist $U$, $V \in \mathbb{Z}$ or $U$, $V \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$ such that

$$\alpha = U + V\sqrt{-wn}.$$

Combining this with equations (4.25) and (4.26), we have $A^2w - B^2n + 2AB\sqrt{-wn} = U + V\sqrt{-wn}$. Comparing the real and imaginary parts, we find that

$$U = A^2w - B^2n \tag{4.28}$$

and

$$V = 2AB. \tag{4.29}$$

**Lemma 29.** *Let $A$, $B$, $U$, $V$ be defined as above.*

*(a) If $U$, $V \in \mathbb{Z}$, then $A$, $B \in \mathbb{Z}$.*

*(b) If $U$, $V \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$, then $w = 3$, $n \equiv 1 \pmod 4$, and $A$, $B \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$.*

*Proof.* Since $A$, $B \in \frac{1}{4}\mathbb{Z}$, there exist $r$, $s \in \mathbb{Z}$ such that $A = r/4$ and $B = s/4$. By

equations (4.28) and (4.29), we have

$$16U = r^2w - s^2n \tag{4.30}$$

and

$$8V = rs. \tag{4.31}$$

First, assume $U$, $V \in \mathbb{Z}$. Equation (4.31) implies that $8 \mid rs$ and so at least one of $r$ or $s$ is even. We consider multiple cases based on the parity of $r$ and $s$. If $r$ is odd, then $r^2 \equiv 1 \pmod 8$ and $s^2 \equiv 0 \pmod 8$. Reducing equation (4.30) modulo 8 yields $0 \equiv 16U \equiv r^2w - s^2n \equiv w \pmod 8$. Since $w \in \{2, 3, 6\}$, this is a contradiction. Similarly, if $s$ is odd, then equation (4.30) implies that $0 \equiv 16U \equiv r^2w - s^2n \equiv -n \pmod 8$, another contradiction. Hence, $r$ and $s$ are both even and so $r = 2r_1$ and $s = 2s_1$ for some $r_1$, $s_1 \in \mathbb{Z}$. Since $8 \mid rs$ at least one of $r_1$ and $s_1$ is also even.

If $r_1$ is odd, then $r_1^2 \equiv 1 \pmod 4$ and $s_1^2 \equiv 0 \pmod 4$. Therefore, equation (4.30) yields $0 \equiv 16U \equiv 4r_1^2w - 4s_1^2n \equiv 4w \pmod{16}$, again a contradiction. Similarly, if $s_1$ is odd, then equation (4.30) implies that $0 \equiv 4r_1^2w - 4s_1^2n \equiv -4n \pmod{16}$, a contradiction. Thus, $r_1$ and $s_1$ are both even. In other words, $r$ and $s$ are both divisible by 4 and so $A = r/4$ and $B = s/4$ are both rational integers. Hence, $A$, $B \in \mathbb{Z}$.

Next, assume $U$, $V \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$. Since $\alpha = U + V\sqrt{-wn} \in \mathcal{O}_F$, we have $-wn \equiv 1 \pmod 4$. So, $w \in \{2, 3, 6\}$ implies that

$$w = 3 \quad \text{and} \quad n \equiv 1 \pmod 4.$$

Reducing equation (4.31) modulo 4 yields $0 \equiv 4(2V) \equiv rs \pmod 4$. Therefore, at least one of $r$ and $s$ is even. If $r$ is odd, then equation (4.30) implies that $0 \equiv 8(2U) \equiv$

$3r^2 - s^2 \equiv 3 \pmod 4$, a contradiction. Similarly, if $s$ is odd then equation (4.30) implies that $0 \equiv 8(2U) \equiv 3r^2 - s^2 \equiv -1 \pmod 4$, another contradiction. Thus, $r$ and $s$ are both even. Since $V \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$, using equation (4.31), we have $2V = (r/2)(s/2)$ is odd, implying that $r/2$ and $s/2$ are both odd. Hence, $A$, $B \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$. ■

Combining equations (4.22) and (4.24), and multiplying by $2^t$,

$$2^t\alpha^t = 2^{t+\ell}3^m - 2^t nx^2 + 2^{t+k+1}3^{k'}x\sqrt{-wn}. \tag{4.32}$$

Since $\alpha = U + V\sqrt{-wn}$, expanding as usual, we have

$$\begin{aligned} 2^t\alpha^t &= (2U + 2V\sqrt{-wn})^t = \sum_{i=0}^{t} \binom{t}{i} (2U)^{t-i}(2V\sqrt{-wn})^i \\ &= \sum_{j=0}^{t_1} \binom{t}{2j} (2U)^{t-2j}(2V\sqrt{-wn})^{2j} + \sum_{j=0}^{t_1} \binom{t}{2j+1} (2U)^{t-2j-1}(2V\sqrt{-wn})^{2j+1}, \end{aligned} \tag{4.33}$$

where $2U$, $2V \in \mathbb{Z}$. Comparing the real and imaginary parts of equations (4.32) and (4.33), we find that

$$2^{t+\ell}3^m - 2^t nx^2 = (2U)\sum_{j=0}^{t_1} \binom{t}{2j} (2U)^{t-2j-1}(2V)^{2j}(-wn)^j \tag{4.34}$$

and

$$2^{t+k+1}3^{k'}x = (2V)\sum_{j=0}^{t_1} \binom{t}{2j+1} (2U)^{t-2j-1}(2V)^{2j}(-wn)^j. \tag{4.35}$$

For ease in notation, let $\mathcal{T} = \sum_{j=0}^{t_1} \binom{t}{2j+1} (2U)^{t-2j-1}(2V)^{2j}(-wn)^j$ so that

$$2^{t+k+1}3^{k'}x = (2V)\mathcal{T}. \tag{4.36}$$

Since $x > 0$, this implies that $2V \neq 0$. So, by equation (4.29),

$$A \neq 0 \text{ and } B \neq 0.$$

Suppose, for a contradiction, that $3 \nmid 2Vw$. Since $w = 2^e 3^{e'}$, this implies that $e' = 0$. Since $m = 2k' + e' > 0$, we have $k' > 0$. Then, 3 divides equation (4.36) and so $3 \mid \mathcal{T}$. Next, since $3 \nmid nx$, equation (4.34) implies that $3 \nmid 2U$. This, together with the supposition that $3 \nmid 2V$, yields

$$\mathcal{T} \equiv \sum_{j=0}^{t_1} \binom{t}{2j+1} (2U)^{t-2j-1} (2V)^{2j} (-wn)^j \equiv \sum_{j=0}^{t_1} \binom{t}{2j+1} (\pm 1)^j \pmod 3.$$

By Lemma 26, $\sum_{j=0}^{t_1} \binom{t}{2j+1} (\pm 1)^j = 2^{t-1}$ or $\pm 2^{t_1}$ and so $\mathcal{T} \equiv \sum_{j=0}^{t_1} \binom{t}{2j+1} (\pm 1)^j \equiv \pm 1 \pmod 3$. However, $3 \mid \mathcal{T}$ and so we have a contradiction. Thus,

$$3 \mid 2Vw. \tag{4.37}$$

From equation (4.26) and (4.27), we have that $\gamma + \delta = 2A\sqrt{w}$ and so

$$\frac{\gamma + \delta}{\sqrt{w}} = 2A \in \mathbb{Z}. \tag{4.38}$$

Combining equation (4.24) with the definition of $\gamma$ and $t = 2t_1 + 1$, we have

$$\gamma^t = \left(\frac{a}{\alpha^{t_1}}\right)^t = \frac{a^t}{a^{2t_1}} = \frac{a^{2t_1+1}}{a^{2t_1}} = a. \tag{4.39}$$

Recalling that $ab = y^n$ and $b = \bar{a}$, we have $\delta^t = \overline{\gamma}^t = \overline{a} = b$. Thus, $\gamma^t + \delta^t = a + b = 2^{k+1} 3^{k'} \sqrt{w}$ and so

$$\frac{\gamma^t + \delta^t}{\sqrt{w}} = 2^{k+1} 3^{k'} \in \mathbb{Z}. \tag{4.40}$$

Let $S = \sum_{i=0}^{t-1}(-1)^i\gamma^{t-1-i}\delta^i = (\gamma^t + \delta^t)/(\gamma+\delta)$. Since $\gamma$, $\delta \in \mathcal{O}_K$, we have $S \in \mathcal{O}_K$. Since $K = \mathbb{Q}(\sqrt{w}, \sqrt{-n})$, there are four automorphisms of $K$ over $\mathbb{Q}$, each determined by where it sends $\sqrt{w}$ and $\sqrt{-n}$. These automorphisms send $\gamma = A\sqrt{w} + B\sqrt{-n}$ to $\gamma$, $\delta$, $-\delta$, and $-\gamma$. Thus, $S$ is fixed by each of the automorphisms. Hence, $S \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. Then, since

$$\frac{(\gamma^t + \delta^t)/\sqrt{w}}{(\gamma + \delta)/\sqrt{w}} = \frac{\gamma^t + \delta^t}{\gamma + \delta} = S \in \mathbb{Z},$$

as integers $(\gamma + \delta)/\sqrt{w}$ divides $(\gamma^t + \delta^t)/\sqrt{w}$. By equations (4.38) and (4.40),

$$2A \mid 2^{k+1}3^{k'} \tag{4.41}$$

and so

$$\frac{\gamma^t + \delta^t}{\gamma + \delta} = \frac{2^{k+1}3^{k'}}{2A} \in \mathbb{Z}. \tag{4.42}$$

We are now ready to prove the following lemma.

**Lemma 30.** *The pair $(\gamma, \delta)$ is a $2t$-defective Lehmer pair.*

*Proof.* First, we verify that $(\gamma, \delta)$, satisfies the conditions (2.15)–(2.17). Starting with condition (2.15), we write $\gamma$ and $\delta$ in terms of $A$, $B \in \frac{1}{2}\mathbb{Z} - \{0\}$ and find that

$$\gamma\delta = \left(A\sqrt{w} + B\sqrt{-n}\right)\left(A\sqrt{w} - B\sqrt{-n}\right) = A^2w + B^2n \in \mathbb{Q}^+, \tag{4.43}$$

$$(\gamma + \delta)^2 = \left[(A\sqrt{w} + B\sqrt{-n}) + (A\sqrt{w} - B\sqrt{-n})\right]^2 = \left(2A\sqrt{w}\right)^2 = (2A)^2w \in \mathbb{Q}^+,$$

and

$$\frac{\gamma}{\delta} = \frac{\gamma^2}{\gamma\delta} = \frac{A^2w - B^2n + 2AB\sqrt{-wn}}{A^2w + B^2n}.$$

This shows that $\gamma\delta$ and $(\gamma + \delta)^2 \in \mathbb{Q} - \{0\}$. Since they are also in $\mathcal{O}_K$, we have

$\gamma\delta$, $(\gamma+\delta)^2 \in \mathbb{Z}-\{0\}$. Now, suppose that $p \in \mathbb{Z}$ is a prime dividing $\gcd(\gamma\delta, (\gamma+\delta)^2)$. Since $2A \mid 2^{k+1}3^{k'}$ and $w \mid 6$, we have that $(\gamma+\delta)^2 \mid 6(2^{k+1}3^{k'})^2$. Therefore, $p \mid (\gamma+\delta)^2$ yields $p = 2$ or 3. Further, $p \mid \gamma\delta$. From equation (4.39), $(\gamma\delta)^t = \gamma^t\delta^t = ab = y^n$. Therefore, $p \mid \gcd(y, 6)$, a contraction since $\gcd(y, 6) = 1$. Thus, $\gcd(\gamma\delta, (\gamma+\delta)^2) = 1$.

Notice that $\gamma/\delta \in F$. Since $A \neq 0$ and $B \neq 0$, we have $\gamma = A\sqrt{w} + B\sqrt{-n} \neq \pm\left(A\sqrt{w} - B\sqrt{-n}\right) = \pm\delta$. Since the roots of unity in $F = \mathbb{Q}(\sqrt{-wn})$ with $wn \geq 2 \cdot 5 = 10$ are 1 and $-1$, and since $\gamma/\delta \neq \pm 1$, $\gamma/\delta$ is not a root of unity. Hence, $(\gamma, \delta)$ is a Lehmer pair.

Finally, we show that $(\gamma, \delta)$ is $2t$-defective. For a contradiction, let $p$ be a rational prime such that $p \mid L_{2t}(\gamma, \delta)$ and $p \nmid (\gamma^2 - \delta^2)^2 L_1(\gamma, \delta) \ldots L_{2t-1}(\gamma, \delta)$. From the definition of $L_{2t}(\gamma, \delta)$,

$$L_{2t}(\gamma, \delta) = \frac{\gamma^{2t} - \delta^{2t}}{\gamma^2 - \delta^2} = \frac{(\gamma^t + \delta^t)}{(\gamma + \delta)} \frac{(\gamma^t - \delta^t)}{(\gamma - \delta)}.$$

Since $t$ is odd, $L_t(\gamma, \delta) = (\gamma^t - \delta^t)/(\gamma - \delta)$ and from equation (4.42), we have that $(\gamma^t + \delta^t)/(\gamma + \delta) = 2^{k+1}3^{k'}/2A$. So,

$$L_{2t}(\gamma, \delta) = \frac{2^{k+1}3^{k'}}{2A} L_t(\gamma, \delta).$$

Thus, $p \in \{2, 3\}$ or $p \mid L_t(\gamma, \delta)$. By supposition, $p \nmid L_t(\gamma, \delta)$ and so $p = 2$ or 3.

To show that $p \neq 3$, consider

$$\begin{aligned}(\gamma^2 - \delta^2)^2 &= \left[\left(A\sqrt{w} + B\sqrt{-n}\right)^2 - \left(A\sqrt{w} - B\sqrt{-n}\right)^2\right]^2 \\ &= \left[\left(A^2w - B^2n + 2AB\sqrt{-wn}\right) - \left(A^2w - B^2n - 2AB\sqrt{-wn}\right)\right]^2 \\ &= \left(4AB\sqrt{-wn}\right)^2 = -4(2AB)^2wn = -4V^2wn = -(2V)^2wn\end{aligned}$$

since $V = 2AB$. By equation (4.37), $3 \mid 2Vw$ and so $3 \mid (\gamma^2 - \delta^2)^2$. Hence, $p \neq 3$.

It remains to consider the case $p = 2$. Suppose that $V \in \mathbb{Z}$. Then $(\gamma^2 - \delta^2)^2 = -(2V)^2 wn$ is even implying that $2 \mid (\gamma^2 - \delta^2)^2 L_1(\gamma, \delta) \ldots L_{2t-1}(\gamma, \delta)$, contradicting the assumption. Hence, $V \notin \mathbb{Z}$.

Since $V \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$, by Lemma 29, we have that $w = 3$, $n \equiv 1 \pmod 4$, and $A$, $B \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$. Hence, $2A$ and $2B$ are odd integers, and so $(2A)^2 \equiv (2B)^2 \equiv 1 \pmod 8$. From equation (4.43), $4\gamma\delta \equiv (2A)^2 \cdot 3 + (2B)^2 n \equiv 3 + n \pmod 8$. Since $(\gamma\delta)^t = y^n$ is odd, $4\gamma\delta \equiv 4 \pmod 8$. Hence,

$$n \equiv 1 \pmod 8. \tag{4.44}$$

By the definition of $L_3(\gamma, \delta)$, $4L_3(\gamma, \delta) = 4(\gamma^3 - \delta^3)/(\gamma - \delta) = 4\,(\gamma^2 + \gamma\delta + \delta^2)$. Then,

$$\begin{aligned} 4L_3(\gamma, \delta) &= 4\left((A\sqrt{3} + B\sqrt{-n})^2 + (3A^2 + B^2 n) + (A\sqrt{3} - B\sqrt{-n})^2\right) \\ &= 4\left(2(3A^2 - B^2 n) + (3A^2 + B^2 n)\right) \\ &= 4\left(9A^2 - B^2 n\right) \\ &= 9(2A)^2 - (2B)^2 n \\ &\equiv 9 - n \equiv 0 \pmod 8, \end{aligned}$$

since $n \equiv 1 \pmod 8$. Thus, $2 \mid L_3(\gamma, \delta)$, contradicting the supposition, since $t \geq 3$.

Hence, for all primes $p \mid L_{2t}(\gamma, \delta)$, we have $p \mid (\gamma^2 - \delta^2)^2 L_1(\gamma, \delta) \ldots L_{2t-1}(\gamma, \delta)$ and so $(\gamma, \delta)$ is $2t$-defective, as claimed. ■

Theorem 11 implies that the Lehmer pair $(\gamma, \delta)$ can be $2t$-defective only if $2t \leq 30$. For $0 \leq d \leq 3$, we compare the possible values of $i^d\gamma = i^d(A\sqrt{w} + B\sqrt{-n})$ to the

values in Table 2.1 for $2t \leq 30$. Since $2A \mid 2^{k+1}3^{k'}$, we conclude that $i^d\gamma$ is not listed in the table. Therefore, $2t \in \{2, 4, 6, 8, 10, 12\}$. Since $\gcd(t, 6) = 1$ and $t > 1$, this implies that $2t = 10$ and so $t = 5$. Thus, it remains to prove the following lemma.

**Lemma 31.** *Let $A$, $B$, $U$, $V$, and $t$ be defined as above. Then $t \neq 5$.*

*Proof.* For a contradiction, suppose that $t = 5$. We rewrite equations (4.34) and (4.35) as

$$2^\ell 3^m - nx^2 = U\left(U^4 - 10U^2V^2wn + 5V^4w^2n^2\right) \tag{4.45}$$

and

$$2^{k+1}3^{k'}x = V\left(5U^4 - 10U^2V^2wn + V^4w^2n^2\right). \tag{4.46}$$

Next, combining equations (4.26) and (4.39), and comparing the real and imaginary parts, we find that

$$2^{k+1}3^{k'} = A\left(A^4w^2 - 10A^2B^2wn + 5B^4n^2\right) \tag{4.47}$$

and

$$x = B\left(5A^4w^2 - 10A^2B^2wn + B^4n^2\right). \tag{4.48}$$

First, assuming that $U$, $V \in \mathbb{Z}$, by Lemma 29, $A$, $B \in \mathbb{Z}$. So, equation (4.29) implies that $V$ is even. Since $2 \nmid nx$ and $\ell \geq 1$, $2 \nmid (2^\ell 3^m - nx^2)$ and so, by equation (4.45), $2 \nmid U$. Then, $2 \nmid (5U^4 - 10U^2V^2wn + V^4w^2n^2)$ and so equation (4.46) implies that $2^{k+1} \mid V$.

Since $x$ is odd and $B \mid x$, we have that $B$ is odd. If $k > 0$, then $2^{k+1} \mid V$ implies that $4 \mid V$. So, $V = 2AB$ implies that $4 \mid 2AB$. Then, since $2 \nmid B$, $2 \mid A$. If $k = 0$, then $\ell = 2k + e = e$. So, $\ell \geq 1$ with $e \in \{0, 1\}$ yields $e = 1$. Thus, $w = 2^e3^{e'}$ is even. Hence, in either case, $2 \mid Aw$.

By equation (4.47), $(A^4w^2 - 10A^2B^2wn + 5B^4n^2) \mid 2^{k+1}3^{k'}$. Since $2 \mid Aw$ and $2 \nmid Bn$, we consider $A^4w^2 - 10A^2B^2wn + 5B^4n^2$ modulo 8. First, if $2 \mid A$, then it easy to see that

$$A^4w^2 - 10A^2B^2wn + 5B^4n^2 \equiv 5 \pmod 8.$$

Now, if $2 \nmid A$, then $2 \mid w$, and so

$$A^4w^2 - 10A^2B^2wn + 5B^4n^2 \equiv 4 - 4 + 5 \equiv 5 \pmod 8.$$

Thus, $2 \nmid (A^4w^2 - 10A^2B^2wn + 5B^4n^2)$ implying that $A^4w^2 - 10A^2B^2wn + 5B^4n^2 = 3^j$ for some $0 \leq j \leq k'$. So, for any integer $j$,

$$5 \equiv A^4w^2 - 10A^2B^2wn + 5B^4n^2 = 3^j \equiv 1 \text{ or } 3 \pmod 8,$$

which is a contradiction. Hence, $U$, $V \notin \mathbb{Z}$.

Next, since $U$, $V \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$, by Lemma 29, we have $w = 3$, $n \equiv 1 \pmod 4$, and $A$, $B \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$. Multiplying equations (4.47) and (4.48) by $2^5$ yields

$$2^{k+6}3^{k'} = 2A\left((2A)^4 \cdot 3^2 - 10(2A)^2(2B)^2 \cdot 3n + 5(2B)^4n^2\right)$$

and

$$32x = 2B\left(5(2A)^4 \cdot 3^2 - 10(2A)^2(2B)^2 \cdot 3n + (2B)^4n^2\right). \tag{4.49}$$

Since $2B$ is odd, equation (4.49) implies that 32 divides $5(2A)^4w^2 - 10(2A)^2(2B)^2wn +$

$(2B)^4n^2$. We have

$$5(2A)^4 \cdot 3^2 - 10(2A)^2(2B)^2 \cdot 3n + (2B)^4n^2$$
$$= 4((2A)^2 \cdot 3)^2 + ((2A)^2 \cdot 3 - (2B)^2n)^2 - 8(2A)^2(2B)^2 \cdot 3n. \quad (4.50)$$

We now reduce each term in this expression modulo 32. First, we have $((2A)^2 \cdot 3)^2 \equiv 1 \pmod 8$ and so

$$4((2A)^2 \cdot 3)^2 \equiv 4 \pmod{32}.$$

Since $V \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$, by congruence (4.44), $n \equiv 1 \pmod 8$. Thus, $(2A)^2 \cdot 3 - (2B)^2n \equiv 2 \pmod 8$ implying that

$$((2A)^2 \cdot 3 - (2B)^2n)^2 \equiv 4 \pmod{32}.$$

Similarly, $-(2A)^2(2B)^2 \cdot 3n \equiv 5 \pmod 8$ implies that

$$-8(2A)^2(2B)^2 \cdot 3n \equiv 8 \pmod{32}.$$

Hence,

$$0 \equiv 4((2A)^2 \cdot 3)^2 + ((2A)^2 \cdot 3 - (2B)^2n)^2 - 8(2A)^2(2B)^2 \cdot 3n$$
$$\equiv 4 + 4 + 8 \equiv 16 \pmod{32},$$

a contradiction. ■

Hence, the theorem is proved. □

# Chapter 5

# Main Theorem III

In this chapter, we describe the modular approach to solving Diophantine equations, state some results that use that approach, and prove Main Theorem III. The modular approach can be used to solve many kinds of Diophantine equations, especially those that are variations on the equation in Fermat's Last Theorem. One such extension is called a generalized Fermat equation.

Let $r,\ s,\ t \geq 2$ be integers. A *generalized Fermat equation* is an equation of the form $X^r + Y^s = Z^t$. We say that the *signature* of this equation is $(r, s, t)$. Darmon and Granville [31, Theorem 2] proved that given a generalized Fermat equation of fixed signature $(r, s, t)$ satisfying $1/r + 1/s + 1/t < 1$, there are only a finite number of solutions $X,\ Y,\ Z \in \mathbb{Z} - \{0\}$ with $\gcd(X, Y, Z) = 1$.

There are numerous papers proving that for a specific signature $(r, s, t)$ the generalized Fermat equation has no solutions in relatively prime integers. For instance, Bennett, Chen, Dahmen, and Yazdani [11, Propositions 21–22] studied equations with the signatures $(2m, 2, 10)$ and $(2m, 2, 15)$, for $m > 1$. Earlier, Poonen [58, Theorem 1] considered equations with signature $(5, 5, 2)$. (See [11, Tables 1–3] for a list of currently known results of this form.)

For equations of signature $(2, 2, n)$, there are many results where $Y$ is restricted to product of specific primes. For example, Arif and Abu Murifah [2, Theorem 1] studied the equation $X^2 + 2^{2\ell} = Z^n$, with $\ell$, $n \in \mathbb{Z}^+$, and Luca and Togbé [50, Theorem 1.1] considered $X^2 + 2^\ell 5^m = Z^n$, with $\ell$, $m$, $n \in \mathbb{Z}^+$. (For other examples, see [47,49,57,70].) Solving such equations typically uses the construction of Lucas and Lehmer pairs, as seen in Chapter 4. A key to those proofs is knowing exactly which primes divide $Y$. When those primes are large, this method can have too many cases to be practical. It is also ineffective for treating the case in which $Y$ has an arbitrary prime divisor.

In this chapter, we consider a generalized Fermat equation of signature $(2N, 2, 5)$, with $N > 1$, where $Y$ is restricted to being an integer with a small number of prime divisors, possibly an unspecified prime, as in the theorem below.

**Main Theorem III.** *Let $p$ be an odd prime and let $N$, $\alpha$, $\beta$, $\gamma \in \mathbb{Z}^+$ such that $N > 1$, $\alpha \geq 1$, and $\beta$, $\gamma \geq 0$. The equation*

$$X^{2N} + 2^{2\alpha} 5^{2\beta} p^{2\gamma} = Z^5 \tag{5.1}$$

*has no solutions with $X$, $Z \in \mathbb{Z}^+$ and $\gcd(X, Z) = 1$.*

## 5.1 Preliminary Results

In this section, we present a number of results that we use in proving Main Theorem III. Many of these rely on the modular approach, which we describe below.

Note that the term modular approach pertains to solving any equation of the form $aX^r + bY^s = cZ^t$, for $r$, $s$, $t \in \mathbb{Z}^+$, using this type of method. We outline the approach

for an equation of the form $aX^n+bY^n = cZ^2$, for $a$, $b$, $c$, $n \in \mathbb{Z}$ and $n \geq 7$ prime. First, suppose that a solution exists, say $ax^n + by^n = cz^2$. This solution is used to define an elliptic curve, $E$, with rational coefficients. By Theorem 13, there exists a newform $f$ of weight 2 and level $N$, where $N$ is the conductor of the elliptic curve such that $\rho_{E,\ell} \sim \rho_{f,\ell}$, for some prime $\ell \in \mathbb{Z}^+$. By Ribet's Level-lowering Theorem [59, Theorem 1.1], there exists a newform $f'$ of weight 2 and level $N_n$, where $N_n \mid N$. If this level-lowering is successful, then there are a number of results, that can be used to find solutions or to reach contradictions. In 2007, Siksek [28, Chapter 15], summarized this method for solving certain Diophantine equations. He compiled many results from the work of Bennett and Skinner [12] into a single theorem [28, Theorem 15.8.2], of which we state a special case.

**Theorem 32** (Bennett-Skinner)**.** *Let $a$, $b$, $c$, $n$, $x$, $y$, $z \in \mathbb{Z}$ with $n \geq 7$ prime, $c$ square-free,* $\gcd(ax, by, cz) = 1$*, and*

$$ax^n + by^n = cz^2.$$

*If, for all rational primes $q$, $v_q(a)$, $v_q(b) < n$, $v_2(by^n) \geq 6$, $z \equiv c \pmod 4$, and $xy \neq \pm 1$, then the elliptic curve, $E$, given by the equation*

$$Y^2 + XY = X^3 + \frac{cz-1}{4}X^2 + \frac{bcy^n}{64}X$$

*is nonsingular and has conductor*

$$N = \begin{cases} 2^{-1}c^2\, rad(abxy), & \text{if } v_2(by^7) = 6, \\ c^2\, rad(abxy), & \text{if } v_2(by^7) \geq 7. \end{cases}$$

*Further, there exists a newform, $f$, of weight 2 and level*

$$N_n = \begin{cases} c^2\, rad(ab), & \text{if } v_2(b) \neq 0, 6, \\ 2c^2\, rad(ab), & \text{if } v_2(b) = 0, \\ 2^{-1}c^2\, rad(ab), & \text{if } v_2(b) = 6 \end{cases}$$

*associated to $E$.*

In their paper, Bennett and Skinner apply the modular approach to prove the following two results [12, Theorem 1.2 & Theorem 1.5].

**Theorem 33** (Bennett and Skinner)**.**

*(a) Let $N \geq 7$ be a rational prime. If $\alpha \in \mathbb{Z}^+$ such that $\alpha \geq 6$, then the equation*

$$X^N + 2^\alpha Y^N = 5Z^2$$

*has no solutions in nonzero pairwise relatively prime integers $X$, $Y$, $Z$ with $XY \neq \pm 1$.*

*(b) Let $N \geq 11$ be a rational prime, $p$ an odd prime, $\alpha$, $\beta$, integers with $\alpha \geq 6$ and $\beta \geq 1$. Then the equation*

$$X^N + 2^\alpha 5^\beta Y^N = Z^2$$

*has no solutions in pairwise relatively prime integers $X$, $Y$, $Z$.*

*Sketch of Proof.* For a contradiction, suppose that a solution exists. Applying the modular approach to that solution produces a newform of weight 2 and level $N_n$. For part (a), the particular value of the level $N_n$ is one found in the set in Lemma 12, an immediate contradiction. For part (b), Bennett and Skinner take advantage of

various results relating the Fourier coefficients of the newform to the trace of the elliptic curve to reach a contradiction. □

The following lemma is a classical parametrization that we use in the proof of Main Theorem III and in Theorem 35 (see [28, Section 14.2.2] for a discussion of this parametrization). We include the details of the proof.

**Lemma 34.** *Let $a$, $b$, $c \in \mathbb{Z} - \{0\}$ such that $\gcd(a, b) = 1$ and $a^2 + b^2 = c^5$. Then, there exist $u$, $v \in \mathbb{Z} - \{0\}$ that are relatively prime and of opposite parity such that*

$$a = u(u^4 - 10u^2v^2 + 5v^4) \text{ and } b = v(v^4 - 10u^2v^2 + 5u^4).$$

*Proof.* Let $a$, $b$, $c \in \mathbb{Z} - \{0\}$ satisfy $\gcd(a, b) = 1$ and

$$a^2 + b^2 = c^5. \tag{5.2}$$

Without loss of generality, we assume that $a$ and $b$ are positive integers. Since $\gcd(a, b) = 1$, $a$ and $b$ are not both even. If $a \equiv b \equiv 1 \pmod 2$, then $2 \equiv c^5 \pmod 8$ which is impossible. Therefore, $a$ and $b$ are not both odd and so $c$ is odd. Factoring equation (5.2) in $\mathbb{Z}[i]$, we have

$$(a + bi)(a - bi) = c^5.$$

Suppose that $q \in \mathbb{Z}[i]$ is a prime such that $q$ divides $a+bi$ and $a-bi$. Then, $q$ divides $2a$ and $2bi$. Since $\gcd(a, b) = 1$, $q \mid 2$. So, $N(q) \mid N(2)$. Since 2 splits in $\mathbb{Z}[i]$, $N(q) = 2$. But $q \mid (a + bi)$ implies that $2 \mid N(a + bi)$. Since $N(a + bi) = (a + bi)(a - bi) = c^5$, $2 \mid c$, a contradiction. Therefore, $(a + bi)$ and $(a - bi)$ are relatively prime.

Thus, there exist $0 \leq k \leq 3$ and $\alpha \in \mathbb{Z}[i]$ such that $a + bi = i^k\alpha^5$. Notice

that $(i^k)^5 = i^k$ and so $i^k\alpha^5 = (i^k\alpha)^5$. Let $u$, $v \in \mathbb{Z}$ such that $i^k\alpha = u + iv$. So, $a + bi = (i^k\alpha)^5 = (u + iv)^5$. Comparing the real and imaginary parts yields

$$a = u(u^4 - 10u^2v^2 + 5v^4)$$

and

$$b = v(v^4 - 10u^2v^2 + 5u^4).$$

Since $a$ and $b$ are nonzero, relatively prime, so are $u$ and $v$.

Since $a$ and $b$ are of opposite parity, we assume, without loss of generality, that $2 \mid a$. Then, $2 \nmid b$. Since $v \mid b$, we have that $2 \nmid v$. Similarly, $2 \nmid (v^4 - 10u^2v^2 + 5u^4)$. Now, if $2 \nmid u$, then $2 \mid (v^4 - 10u^2v^2 + 5u^4)$, a contradiction. Therefore, $2 \mid u$. Hence, $u$ and $v$ are also of opposite parity. □

In 2006, Bennett [8, Theorem 1] used the modular approach in proving the following theorem.

**Theorem 35** (Bennett)**.** *If $N \geq 2$ is an integer, then the Diophantine equation*

$$X^{2N} + Y^{2N} = Z^5$$

*has no solutions in nonzero integers $X$, $Y$, and $Z$, with* $\gcd(X, Y) = 1$.

*Sketch of Proof.* For a hypothetical solution $x$, $y$, $z$ and $n \geq 2$, Bennett uses Lemma 34 to write $x^n$ and $y^n$ in terms of integers $u$ and $v$. For $n \geq 7$, Bennett applies the modular approach [12] to reach a contradiction. For the remaining $3 \leq n \leq 6$, Bennett uses various known results on equations of this form and for $n = 2$ he uses a 2-descent argument. □

The following results of Bruin [19, Theorem 1.1] and Bennett and Chen [10, Theorem 1] imply that Main Theorem III holds for $N = 2$ and 3.

**Theorem 36** (Bruin)**.** *The equation*

$$X^2 + Y^4 = Z^5$$

*has no solutions* $X$, $Y$, $Z \in \mathbb{Z}$ *with* $\gcd(X, Y, Z) = 1$ *and* $XYZ \neq 0$.

*Sketch of Proof.* For a finite extension $L$ of a number field $K$, Bruin uses the arithmetic of an elliptic curve, $E$ over $L$, to find $K$-rational points on an algebraic curve that covers $E$. Then, using $p$-adic analytic methods, Bruin finds that there are no solutions. □

**Theorem 37** (Bennett and Chen)**.** *Let* $N \geq 3$ *be an integer. Then the equation*

$$X^2 + Y^6 = Z^N$$

*has no solutions* $X$, $Y$, $Z \in \mathbb{Z}^+$ *with* $\gcd(X, Y) = 1$.

*Sketch of Proof.* Suppose that a solution $x$, $y$, $z$, and $n \geq 3$ exists. Bennett and Chen use this solution to define multiple elliptic curves defined over number fields, not necessarily $\mathbb{Q}$. Using a broader variant of the modular approach, they examine the associated Galois representations and newforms to derive contradictions for $n \geq 7$. For the small values of $n$, the authors apply congruence arguments and prior results to finish the proof. □

In the proof of Main Theorem III, we use the following two theorems to show that it is sufficient to prove the result for $N$ prime. Both theorems are proved using Lucas pairs in a technique that is similar to the proof of Main Theorem II (see

Section 2.3 for the definition of a Lucas pair). First, we state Arif and Abu Muriefah's result [2, Theorem 1].

**Theorem 38** (Arif and Abu Muriefah)**.** *Let $L$, $N \in \mathbb{Z}^+$ with $L$ even and $N > 1$ odd. Then the Diophantine equation*

$$X^2 + 2^L = Y^N$$

*has a unique solution $X$, $Y \in \mathbb{Z}$ with $\gcd(X, Y) = 1$, namely, with $N = 3$, $(L, X, Y) = (1, 11, 5)$.*

Next, we state a simplified version of a result of Luca and Togbé [50, Theorem 1.1].

**Theorem 39** (Luca and Togbé)**.** *Let $L$, $M$, $N \in \mathbb{Z}^+$ with $N \geq 3$. The equation*

$$X^2 + 2^L 5^M = Y^N$$

*has a finite number of solutions with $X$, $Y \in \mathbb{Z}^+$ and $\gcd(X, Y) = 1$. In particular, for $N = 4$, there are two solutions $(L, M, X, Y) = (4, 1, 1, 3)$ and $(6, 1, 79, 9)$, and for $N = 5$, $(L, M, X, Y) = (1, 3, 401, 11)$.*

Finally, we present a lemma for resolving a particular case in the proof of Main Theorem III. We prove this using a sequence of congruence arguments, though it could instead be proved by solving a Thue equation with computer software.

**Lemma 40.** *Let $p \neq 5$ be an odd prime, $\alpha \geq 1$, and $\beta$, $\gamma \geq 0$ be integers. If $u$, $v \in \mathbb{Z}$ such that $v$ is even, $\gcd(u, v) = 1$, and $2^\alpha 5^\beta p^\gamma = v(v^4 - 10u^2v^2 + 5u^4)$, then*

$$v^4 - 10u^2v^2 + 5u^4 \neq 5.$$

*Proof.* Assuming the hypothesis, suppose for a contradiction that

$$v^4 - 10u^2v^2 + 5u^4 = 5. \tag{5.3}$$

Note that this implies that $\beta > 0$. Combining $2^\alpha 5^\beta p^\gamma = v(v^4 - 10u^2v^2 + 5u^4)$ and equation (5.3), we have $2^\alpha 5^\beta p^\gamma = 5v$ which yields

$$v = 2^\alpha 5^{\beta-1} p^\gamma. \tag{5.4}$$

Now, adding $4v^4$ to equation (5.3) yields $5(v^2-u^2)^2 = 5+4v^4$ and so $5 \mid v$. Combining this with equation (5.4), dividing by 5 and subtracting 1 yields $(v^2 - u^2)^2 - 1 = 2^{4\alpha+2}5^{4\beta-5}p^{4\gamma}$. Factoring we find that

$$(u^2 - v^2 + 1)(u^2 - v^2 - 1) = 2^{4\alpha+2}5^{4\beta-5}p^{4\gamma}. \tag{5.5}$$

Let $d = \gcd(u^2 - v^2 + 1, u^2 - v^2 - 1)$, then $d$ divides the difference $(u^2 - v^2 + 1) - (u^2 - v^2 - 1) = 2$. Therefore, $d = 1$ or 2. Since $v$ is even and $u$ is odd, by hypothesis, $u^2 - v^2 + 1$ and $u^2 - v^2 - 1$ are even. Thus, $\gcd(u^2 - v^2 + 1, u^2 - v^2 - 1) = 2$. Further, $u^2 - v^2 + 1 \equiv 2 \pmod 4$, so that $2 \mid\mid (u^2 - v^2 + 1)$. So, by equation (5.5), $2^{4\alpha+1} \mid\mid (u^2 - v^2 - 1)$. Therefore, there exist $k$, $k'$, $\ell$, $\ell' \in \mathbb{Z}^+$ such that

$$u^2 - v^2 + 1 = 2 \cdot 5^k p^\ell \tag{5.6}$$

and

$$u^2 - v^2 - 1 = 2^{4\alpha+1}5^{k'}p^{\ell'}. \tag{5.7}$$

Since $\gcd(u^2 - v^2 + 1, u^2 - v^2 - 1) = 2$, $\{k, k'\} = \{0, 4\beta - 5\}$ and $\{\ell, \ell'\} = \{0, 4\gamma\}$.

Combining (5.6) and (5.7) we have $2 \cdot 5^k p^\ell - 2^{4\alpha+1} 5^{k'} p^{\ell'} = 2$ implying that

$$5^k p^\ell - 2^{4\alpha} 5^{k'} p^{\ell'} = 1. \tag{5.8}$$

By assumption, $p \neq 5$ is prime and so $p^4 \equiv 1 \pmod 5$. Then, since $\{\ell, \ell'\} = \{0, 4\gamma\}$, $p^\ell \equiv p^{\ell'} \equiv 1 \pmod 5$.

Reducing equation (5.8) modulo 5 yields $5^k - 5^{k'} \equiv 1 \pmod 5$. Therefore, $k = 0$ and $k' = 4\beta - 5$, yielding

$$p^\ell - 2^{4\alpha} 5^{4\beta-5} p^{\ell'} = 1.$$

So, $\ell > 0$ implying that $\ell = 4\gamma$ and $\ell' = 0$. Thus, rewriting this equation, we have

$$1 + 2^{4\alpha} 5^{4\beta-5} = p^{4\gamma}. \tag{5.9}$$

Hence, $(L, M, X, Y) = (4\alpha, 4\beta-5, 1, p^\gamma)$ is a solution to the equation $X^2+2^a \cdot 5^b = Y^N$ with $N = 4$. Since $\gcd(1, p^\gamma) = 1$, and $\alpha$ and $4\beta-5$ are positive integers, equation (5.9) satisfies the hypotheses of Theorem 39. Therefore, $(4\alpha, 4\beta - 5, 1, p^\gamma)$ is equal to one of the solutions listed for $N = 4$. In particular, $(4\alpha, 4\beta - 5, 1, p^\gamma) = (4, 1, 1, 3)$ or $(6, 1, 79, 9)$. Since $\beta \in \mathbb{Z}^+$, we have a contradiction. Hence, $v^4 - 10u^2v^2 + 5u^4 \neq 5$. $\square$

## 5.2 Proof of Main Theorem III

*Proof of Main Theorem III.* Let $p$ be an odd prime, and let $\alpha \geq 1$, $\beta$, $\gamma \geq 0$ be integers. Suppose, for a contradiction, that $(N, X, Z) = (n, x, z)$ is a solution to the equation $X^{2N} + 2^{2\alpha} 5^{2\beta} p^{2\gamma} = Z^5$ with $n > 1$ and $\gcd(x, z) = 1$. Then,

$$x^{2n} + 2^{2\alpha} 5^{2\beta} p^{2\gamma} = z^5. \tag{5.10}$$

We first show that it is sufficient to prove the theorem for $n$ prime. Since $n > 1$, $n$ has a prime divisor $\ell$. So, $n = \ell d$ for some $d \in \mathbb{Z}^+$, and we have

$$(x^d)^{2\ell} + 2^{2\alpha}5^{2\beta}p^{2\gamma} = z^5.$$

Since $\ell > 1$ and $1 = \gcd(x, z) = \gcd(x^d, z)$, we have that $(N, X, Z) = (\ell, x^d, z)$ is a solution to the equation $X^{2N} + 2^{2\alpha}5^{2\beta}p^{2\gamma} = Z^5$ with $N = \ell$ prime. Thus, we assume that $n$ is prime. Further, by Theorems 36 and 37 (switching order of $X$ and $Y$), $n \neq 2$ or 3. Hence, we assume that $n \geq 5$.

Let $q \in \mathbb{Z}^+$ be a prime such that $q \mid 2^{2\alpha}5^{2\beta}p^{2\gamma}$. By equation (5.10), $q \mid (z^5 - x^{2n})$. Thus, $q \mid z$ if and only if $q \mid x$. But $\gcd(x, z) = 1$, by assumption, and so $q \nmid z$ and $q \nmid x$. Hence, $\gcd(xz, 2^{\alpha}5^{\beta}p^{\gamma}) = 1$.

Suppose for a contradiction that $p = 5$ or $\gamma = 0$, then equation (5.10) implies that

$$x^{2n} + 2^{2\alpha}5^{2(\beta+\gamma)} = z^5.$$

If $\beta+\gamma > 0$, then $(L, M, X, Y) = (2\alpha, 2(\beta+\gamma), x^n, z)$ is a solution to $X^2+2^L5^M = Y^N$ with $N = 5$. Since $\gcd(x, z) = 1$, Theorem 39 implies that $(2\alpha, 2(\beta + \gamma), x^n, z) = (1, 3, 401, 11)$. This is a contradiction, since $\alpha \in \mathbb{Z}^+$.

If $\beta+\gamma = 0$, then equation (5.10) yields $x^{2n}+2^{2\alpha} = z^5$ and so $(L, X, Y) = (\alpha, x^n, z)$ is a solution to the equation $X^2 + 2^L = Y^N$, with $N = 5$. By Theorem 38, this is another contradiction. Hence, $p \neq 5$ and $\gamma \neq 0$.

Assume, for now, that $n \geq 7$. This allows us to use Theorems 32 and 33. At the end of the proof, we use congruence arguments to show that $n \neq 5$. (Alternatively, the case $n = 5$ could be eliminated using [58, Theorem 1].)

Rewriting equation (5.10) as $(x^n)^2+\left(2^{\alpha}5^{\beta}p^{\gamma}\right)^2 = z^5$, we apply Lemma 34 to obtain

$u$, $v \in \mathbb{Z} - \{0\}$, such that $\gcd(u, v) = 1$, $u \not\equiv v \pmod 2$,

$$x^n = u(u^4 - 10u^2v^2 + 5v^4), \tag{5.11}$$

and

$$2^\alpha 5^\beta p^\gamma = v(v^4 - 10u^2v^2 + 5u^4). \tag{5.12}$$

We use these equations to determine the possible values of $v$.

Since $\gcd(xz, 2^\alpha 5^\beta p^\gamma) = 1$ and $\alpha \geq 1$, $2 \nmid x$. By equation (5.11), we have $2 \nmid u$. Since $u$ and $v$ have opposite parity, $2 \mid v$ and so $2 \nmid (v^4 - 10u^2v^2 + 5u^4)$. Thus, equation (5.12) implies that $2^\alpha \mid\mid v$.

Note that $\gcd(v, v^4 - 10u^2v^2 + 5u^4) = \gcd(v, 5u^4)$. Since $\gcd(u, v) = 1$, $\gcd(v, 5u^4) = \gcd(v, 5) = 1$ or 5. We consider these two cases separately.

First, if $5 \mid v$, then $5 \nmid u$ and $\gcd(v, v^4 - 10u^2v^2 + 5u^4) = \gcd(v, 5) = 5$. Further, $v^4 - 10u^2v^2 + 5u^4 \equiv 5u^4 \equiv 5 \pmod{25}$ and so $5 \mid\mid (v^4 - 10u^2v^2 + 5u^4)$. Since, from equation (5.12), $5^\beta \mid\mid v(v^4 - 10u^2v^2 + 5u^4)$, we have $5^{\beta-1} \mid\mid v$.

Still assuming that $5 \mid v$, suppose for a contradiction that $p^\gamma \mid v$. Since $2^\alpha \mid\mid v$, this implies that $v = 2^\alpha 5^{\beta-1} p^\gamma$ and $v^4 - 10u^2v^2 + 5u^4 = \pm 5$. Since $v^4 - 10u^2v^2 + 5u^4 \equiv 5 \pmod{25}$, it must be that $v^4 - 10u^2v^2 + 5u^4 = 5$, which contradicts Lemma 40. Therefore, $p^\gamma \nmid v$. Thus, when $5 \mid v$,

$$v^4 - 10u^2v^2 + 5u^4 = \pm 5p^\gamma$$

and

$$v = \pm 2^\alpha 5^{\beta-1}. \tag{5.13}$$

On the other hand, if $5 \nmid v$, then $\gcd(v, v^4 - 10u^2v^2 + 5u^4) = \gcd(v, 5) = 1$. Since

$5 \nmid v$, $5 \nmid (v^4 - 10u^2v^2 + 5u^4)$. So, equation (5.12) implies that $\beta = 0$. Again, suppose for a contradiction that $p^\gamma \mid v$. Then, by equation (5.12), $v^4 - 10u^2v^2 + 5u^4 = \pm 1$ and $v = \pm 2^\alpha p^\gamma$. Since $2 \mid v$ and $2 \nmid u$, $\pm 1 \equiv v^4 - 10u^2v^2 + 5u^4 \equiv 5 \pmod 8$ which is a contradiction. Therefore, when $5 \nmid v$,

$$v^4 - 10u^2v^2 + 5u^4 = \pm p^\gamma$$

and

$$v = \pm 2^\alpha. \tag{5.14}$$

Hence, letting $k = 0$ if $5 \nmid v$ and $k = \beta - 1$ if $5 \mid v$, we have that

$$v = \pm 2^\alpha 5^k. \tag{5.15}$$

Next, we consider equation (5.11). For ease in notation, let $w \in \mathbb{Z}$ such that $w = u^2 - 5v^2$. Note that $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = \gcd(u, 5v^4) = 1$ or 5. So, again, we have two cases: when $5 \mid u$ and when $5 \nmid u$. In each case, we use the information gained from equation (5.15).

Suppose, for a contradiction that $5 \mid u$. Then $5 \nmid v$ and $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = \gcd(u, 5) = 5$. So, $u^4 - 10u^2v^2 + 5v^4 \equiv 5v^4 \equiv 5 \pmod{25}$. Therefore, $5 \,||\, (u^4 - 10u^2v^2 + 5v^4)$ and $5^{n-1} \mid u$, by equation (5.11). Again, by equation (5.11) and $\gcd(u/5^{n-1}, (u^4 - 10u^2v^2 + 5v^4)/5) = 1$, we find that each of these is an $n$-th power. So, there exist $A, B \in \mathbb{Z}$ such that

$$u/5^{n-1} = A^n,$$

and

$$(u^4 - 10u^2v^2 + 5v^4)/5 = B^n \tag{5.16}$$

where $5 \nmid B$. (Note that since $n$ is odd, a factor of $-1$ can be absorbed into the integers $A$ and $B$.) Multiplying equation (5.16) by 5, then adding $20v^4$ yields $(u^2 - 5v^2)^2 = 5B^n + 20v^4$. Since $(u^2 - 5v^2)^2 = w^2$, this implies that

$$w^2 = 5B^n + 20v^4. \tag{5.17}$$

Hence, $5 \mid w$, and so let $w_1 = w/5 \in \mathbb{Z}$. Since $w_1 = u^2/5 - v^2$, and $5 \nmid v$, $5 \nmid w_1$. Further, from equation (5.15) with $k = 0$, we have that $v = \pm 2^\alpha$. Consequently, equation (5.17) yields

$$B^n + 2^{4\alpha+2} = 5w_1^2. \tag{5.18}$$

Recalling that $v$ is even and $u$ is odd, $w_1$ is also odd. This then implies that $B$ is odd. So, by equation (5.18), $B$, $5w_1$, and 2 are pairwise relatively prime. Reducing equation (5.18) modulo 8, we have that $B \equiv B^n \equiv 5 \pmod 8$ implying that $B \neq \pm 1$. Also, $\alpha \geq 1$ and so $4\alpha + 2 \geq 6$. Therefore, $(N, X, Y, Z) = (n, B, 1, w_1)$ is a solution in positive integers to the equation $X^N + 2^{4\alpha+2}Y^N = 5Z^2$ with $N = n \geq 7$. By Theorem 33 (a), this is a contradiction. Thus, $5 \nmid u$.

Since $5 \nmid u$, $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1$. So, equation (5.11) implies that there exist $C$, $D \in \mathbb{Z} - \{0\}$ relatively prime such that $x = CD$,

$$u = C^n,$$

and

$$u^4 - 10u^2v^2 + 5v^4 = D^n. \tag{5.19}$$

(Again, the unit $-1$ can be absorbed into the integers $C$ and $D$.) Adding $20v^4$ to equation (5.19),

$$w^2 = (u^2 - 5v^2)^2 = D^n + 20v^4. \tag{5.20}$$

Since $5 \nmid u$, $5 \nmid w$. Similarly, since $v$ is even and $u$ is odd, $w$ is odd. Therefore, $\gcd(w, 10) = 1$, and so $D$, $w$, and 10 are pairwise relatively prime.

By equation (5.15), $v = \pm 2^\alpha 5^k$ and so equation (5.20) yields

$$D^n + 2^{4\alpha+2}5^{k+1} = w^2. \tag{5.21}$$

Since $4\alpha + 2 \geq 6$, $(N, X, Y, Z) = (n, D, 1, w)$ is a positive integer solution to $X^N + 2^{4\alpha+2}5^{k+1}Y^N = Z^2$, with $N = n \geq 7$. By Theorem 33 (b), there are no solutions for $n \geq 11$ prime and so $n \leq 7$. Since, by assumption, $n \geq 7$, $n = 7$.

Now, recalling that $5 \nmid u$, by equation (5.21),

$$D^7 + 2^{4\alpha+2}5^{k+1} = w^2. \tag{5.22}$$

We use Theorem 32, to derive a contradiction. In order to do this, we rewrite the exponents of 2 and 5 in the above equation. Let $r_1$, $r_2$, $s_1$, $s_2 \in \mathbb{Z}$ with $0 \leq r_1, r_2 < 7$ such that $4\alpha + 2 = 7s_1 + r_1$ and $k + 1 = 7s_2 + r_2$. Then, equation (5.22) is equivalent to

$$D^7 + 2^{r_1}5^{r_2}\left(2^{s_1}5^{s_2}\right)^7 = w^2. \tag{5.23}$$

Since $\gcd(u, v) = 1$, $u$ and $v$ are not both divisible by 3. Therefore, $w^2 \equiv (u^2 - 5v^2)^2 \equiv 1 \pmod 3$. Reducing equation (5.22) modulo 3 yields $D^7 + 2 \equiv 1 \pmod 3$ so that $D \equiv -1 \pmod 3$. Thus, $D \neq 1$. Further, since $\alpha \geq 1$ and $w$ is odd, reducing equation (5.22) modulo 8 yields $D^7 \equiv 1 \pmod 8$ and so $D \neq -1$. Hence, $D \neq \pm 1$.

Applying Theorem 32 to equation (5.23) with $b = 2^{r_1}5^{r_2}$, we find that there exists a newform $f$ of weight 2 and level $N_7$. Notice that $\text{rad}(b) = \text{rad}(2^{r_1}5^{r_2}) \in \{1, 2, 5, 10\}$. Thus, since $c = 1$, $N_7 \in \{1, 2, 5, 10\}$. However, by Lemma 12 there do not exist newforms of weight 2 and level 1, 2, 5, or 10. Hence, we have a contradiction.

Finally, suppose $n = 5$. Then, equation (5.10) is simply

$$x^{10} + 2^{2\alpha}5^{2\beta}p^{2\gamma} = z^5.$$

Thus,

$$2^{2\alpha}5^{2\beta}p^{2\gamma} = z^5 - x^{10}, \tag{5.24}$$

implying that

$$2^{2\alpha}5^{2\beta}p^{2\gamma} = (z - x^2)(z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8). \tag{5.25}$$

Dividing $z - x^2$ into $z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8$, we find that

$$(z - x^2)(4z^3 + 3z^2x^2 + 2zx^4 + x^6) + (z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8) = 5z^4,$$

and so $\gcd(z - x^2, z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8) = \gcd(z - x^2, 5z^4)$. Since $\gcd(x, z) = 1$, we have $\gcd(z - x^2, z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8) = 1$ or 5.

Since $2 \nmid xz$, $z - x^2$ is even and $z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8$ is odd. Thus, equation (5.25) implies that $2^{2\alpha} \,||\, (z - x^2)$. We consider two cases.

First, if $\beta = 0$, then equation (5.25) yields

$$2^{2\alpha}p^{2\gamma} = (z - x^2)(z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8)$$

and $\gcd(z - x^2, z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8) = 1$. For a contradiction, suppose that

$p^{2\gamma} \mid (z - x^2)$. Then, $z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8 = \pm 1$. This is impossible, since $x$ and $z \geq 1$. Therefore, when $\beta = 0$,

$$z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8 = p^{2\gamma}$$

and

$$z - x^2 = 2^{2\alpha}. \tag{5.26}$$

Next, if $\beta \neq 0$, then from equation (5.24), $5 \mid (z^5 - x^{10})$ and so $z^5 \equiv x^{10} \pmod 5$. Since $\gcd(x, z) = 1$, we have $5 \nmid xz$. So, $z \equiv z^5 \equiv x^{10} \equiv (x^2)^5 \equiv x^2 \pmod 5$. Since $5 \nmid x$, $x^2 \equiv \pm 1 \pmod 5$. Consequently, $z \equiv x^2 \equiv \pm 1 \pmod 5$ implying that $z^4+z^3x^2+z^2x^4+zx^6+x^8 \equiv 0 \pmod 5$. Thus, $\gcd(z-x^2, z^4+z^3x^2+z^2x^4+zx^6+x^8) = 5$.

Writing $z = 5q_1 \pm 1$ and $x^2 = 5q_2 \pm 1$, for some $q_1, q_2 \in \mathbb{Z}$, the expression $z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8$ is equal to

$$(5q_1 \pm 1)^4 + (5q_1 \pm 1)^3(5q_2 \pm 1) + (5q_1 \pm 1)^2(5q_2 \pm 1)^2 + (5q_1 \pm 1)(5q_2 \pm 1)^3 + (5q_2 \pm 1)^4.$$

Note that since $z \equiv x^2 \pmod 5$, the positive and negative signs agree. Reducing each term in the above expression modulo 25 yields

$$\begin{aligned}
&(\pm 20q_1 + 1) + (15q_1 \pm 1)(5q_2 \pm 1) + (\pm 10q_1 + 1)(\pm 10q_2 + 1) + (5q_1 \pm 1)(15q_2 \pm 1) \\
&\qquad + (\pm 20q_2 + 1) \\
&\equiv (\pm 20q_1 + 1) + (\pm 15q_1 \pm 5q_2 + 1) + (\pm 10q_1 \pm 10q_2 + 1) + (\pm 5q_1 \pm 15q_2 + 1) \\
&\qquad + (\pm 20q_2 + 1) \\
&\equiv \pm 50q_1 \pm 50q_2 + 5 \\
&\equiv 5 \pmod{25}.
\end{aligned}$$

Therefore, $5 \mid\mid (z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8)$. Then, from equation (5.25), we have that $5^{2\beta-1} \mid\mid (z - x^2)$.

Since $\gcd(z - x^2, z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8) = 5$, $p^{2\gamma}$ divides either $z - x^2$ or $z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8$. Suppose for a contradiction that $p^{2\gamma} \mid (z - x^2)$. Then, $2^{2\alpha}5^{2\beta-1} \mid (z - x^2)$ and equation (5.25) implies that $z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8 = 5$. Since $x$, $z \in \mathbb{Z}^+$, it must be that $x = z = 1$. By equation (5.24), this is impossible. Thus, when $\beta \neq 0$,

$$z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8 = 5p^{2\gamma}$$

and

$$z - x^2 = 2^{2\alpha}5^{2\beta-1}.$$

Let $j = 0$ if $\beta = 0$, and let $j = 2\beta - 1$ if $\beta \neq 0$. Then, the above equation implies that

$$z - x^2 = 2^{2\alpha}5^j. \tag{5.27}$$

Combining this with equation (5.24) yields

$$2^{2\alpha}5^{2\beta}p^{2\gamma} = \left(2^{2\alpha}5^j + x^2\right)^5 - x^{10}.$$

Expanding and simplifying, we find that

$$5^{2\beta}p^{2\gamma} = 2^{8\alpha}5^{5j} + 2^{6\alpha}5^{4j+1}x^2 + 2^{4\alpha+1}5^{3j+1}x^4 + 2^{2\alpha+1}5^{2j+1}x^6 + 5^{j+1}x^8. \tag{5.28}$$

If $\beta = 0$, then $j = 0$, and so this equation yields

$$5^{2\beta}p^{2\gamma} = 2^{8\alpha} + 2^{6\alpha}5x^2 + 2^{4\alpha+1}5x^4 + 2^{2\alpha+1}5x^6 + 5x^8.$$

Since $\alpha \geq 1$, reducing modulo 8 yields $5^{2\beta}p^{2\gamma} \equiv 5x^8 \pmod 8$. Since $2 \nmid x$, this implies that $1 \equiv 5 \pmod 8$, which is a contradiction.

Finally, if $\beta \neq 0$, then $j = 2\beta - 1$, and so equation (5.28) implies that

$$5^{2\beta}p^{2\gamma} = 2^{8\alpha}5^{10\beta-5} + 2^{6\alpha}5^{8\beta-3}x^2 + 2^{4\alpha+1}5^{6\beta-2}x^4 + 2^{2\alpha+1}5^{4\beta-1}x^6 + 5^{2\beta}x^8.$$

Reducing this equation modulo 3 yields

$$p^{2\gamma} \equiv 2 + 2x^2 + 2x^4 + x^6 + x^8 \pmod 3.$$

It is easy to see that, regardless of whether $3 \mid x$ or not, $2 + 2x^2 + 2x^4 + x^6 + x^8 \equiv 2 \pmod 3$. Thus, $n \neq 5$, completing the proof of the theorem. □

# Bibliography


[1] S. A. Arif and F. S. Abu Muriefah, "On the Diophantine equation $x^2+2^k = y^n$", *Internat. J. Math. Math. Sci.* **20** (1997), 299–304.

[2] S. A. Arif and F. S. Abu Muriefah, "On the Diophantine equation $x^2 + 2^k = y^n$, II", *Arab J. Math. Sci.*, **7** (2001), no. 1, 67–71.

[3] F. S. Abu Muriefah and Y. Bugeaud, "The Diophantine equation $x^2 + c = y^n$: A brief overview", *Rev. Colombiana Mat.* **40** (2006), no. 1. 31–37.

[4] A. Baker, "Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers", *Quart. J. Math. Oxford*, **15** (1964), no. 2, 375–383.

[5] A. Baker, "Linear forms in the logarithms of algebraic numbers", *Mathematika* **13** (1966) 204–216.

[6] A. Baker, "Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms", *Philos. Trans. Roy. Soc. London Ser. A* **263** (1967/1968) 173–191.

[7] M. A. Bennett, "Explicit lower bounds for rational approximation to algebraic numbers", *Proc. London Math. Soc. (3)*, **75**, (1997), no. 1, 63–78.

[8] M. A. Bennett, "The equation $x^{2n} + y^{2n} = z^5$", *J. Thèor. Nombres Bordeaux* **18** (2006), no. 2, 315–321.

[9] M. A. Bennett, "The Diophantine equation $(x^k - 1)(y^k - 1) = (z^k - 1)^t$", *Indag. Math. (N.S.)*, **18** (2007), no. 4, 507–525.

[10] M. A. Bennett and I. Chen, "Multi-Frey $\mathbb{Q}$-curves and the Diophantine equation $a^2 + b^6 = c^n$", *Algebra Number Theory* **6** (2012), no. 4, 707–730.

[11] M. A. Bennett, I. Chen, S. R. Dahmen, and S. Yazdani, "Generalized Fermat equations: a miscellany". *Int. J. Number Theory* **11** (2015), no. 1, 1–28.

[12] M. A. Bennett and C. M. Skinner, "Ternary Diophantine equations via Galois representations and modular forms", *Canad. J. Math.* **56** (2004), no. 1, 23–54.

[13] F. Beukers, "The Diophantine equation $Ax^p + By^q = Cz^r$", *Duke Math. J.* **91** (1998), no. 1, 61–88.

[14] Y. Bilu and G. Hanrot, "Solving Thue equations of high degree", *J. Number Theory* **60** (1996), no. 2, 373–392.

[15] Y. Bilu, G. Hanrot, and P. M. Voutier, "Existence of primitive divisors of Lucas and Lehmer numbers, with appendix by M. Mignotte", *J. Reine Angew. Math.* **539** (2001), 75–122.

[16] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, "On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises". *J. Amer. Math. Soc.* **14** (2001), no. 4, 843–939.

[17] E. Bombieri, "On the Thue-Siegel-Dyson theorem", *Acta Math.* **148** (1982), 255–296.

[18] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[19] N. Bruin, "Chabauty methods using elliptic curves", *J. reine angew. Math.* **562** (2003), 27–49.

[20] Y. Bugeaud, "On the Diophantine equation $(x^k-1)(y^k-1) = (z^k-1)$", *Indag. Math. (N.S.)*, **15** (2004), no. 1, 21–28.

[21] Y. Bugeaud and A. Dujella,"On a problem of Diophantus for higher powers", *Math. Proc. Cambridge Philos. Soc.*, **135** (2003), no. 1, 1–10.

[22] D. M. Burton, *Elementary Number Theory, 4th ed.*, McGraw-Hill Companies, Inc., New York, 1998.

[23] D. M. Burton, *The History of Mathematics: An Introduction, 4th ed.*, McGraw-Hill Companies, Inc., New York, 1998.

[24] R. D. Carmichael, "On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$", *Ann. of Math.* **15** (1913), no. 2, 30–70.

[25] J. W. S. Cassels, *Rational Quadratic Forms*, Dover Publications, New York, 1968.

[26] I. Chen, "On the equation $a^2+b^{2p} = c^5$", *Acta Arith.* **143** (2010), no. 4, 345–375.

[27] H. Cohen, *A Course in Computational Algebraic Number Theory, 2nd ed.*, Springer, New York, 1995.

[28] H. Cohen, *Number Theory, Vol. II: Analytic and Modern Tools*, Springer, New York, 2007.

[29] J. H. E. Cohn, "The Diophantine equation $x^2 + 2^k = y^n$", *Arch. Math. (Basel)* **59** (1992), no. 4, 341–344.

[30] J. H. E. Cohn, "The Diophantine equation $x^2 + C = y^n$", *Act Arith.* **65** (1993), no. 4, 367–381.

[31] H. Darmon and A. Granville, "On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$", *Bull. London Math. Soc.* **27** (1995), no. 6, 513–544.

[32] B. M. M. de Weger, "Algorithms for Diophantine Equations", Stichting Mathematisch Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[33] F. Diamond and J. Shurman *A First Course in Modular Forms*, Springer, New York, 2005.

[34] F. J. Dyson, "The approximation to algebraic numbers by rationals", *Acta Math.* **79** (1947), 225–240.

[35] A. O. Gel'fond, *Transcendental and algebraic numbers*. Translated from the first Russian edition (1952) by Leo F. Boron, Dover Publications, Inc., New York, 1960.

[36] E. G. Goedhart and H. G. Grundman, "On the Diophantine equation $NX^2 + 2^L 3^M = Y^N$", *J. Number Theory* **141** (2014), 214–224.

[37] E. G. Goedhart and H. G. Grundman, "Diophantine approximation and the equation $(a^2cx^k - 1)(b^2cy^k - 1) = (abcz^k - 1)^2$", *J. Number Theory* **154** (2015), 74–81.

[38] E. G. Goedhart and H. G. Grundman, "On the Diophantine equation $X^{2N} + 2^{2\alpha}5^{2\beta}p^{2\gamma} = Z^5$", preprint.

[39] C. Heuberger and M. H. Le, "On the generalized Ramanujan-Nagell equation $x^2 + D = p^z$", *J. Number Theory* **78** (1999), no. 3, 312–331.

[40] L. K. Hua, *Introduction to Number Theory*, Springer-Verlag, Berlin, 1982.

[41] M. Laurent, M. Mignotte, and Y. Nesterenko, "Formes linéaires en deux logarithmes et déterminants d'interpolation", *J. Number Theory* **55** (1995), no. 2, 285–321.

[42] M. H. Le, "Some exponential Diophantine equations. I, the equation $D_1x^2 - D_2y^2 = \lambda k^z$", *J. Number Theory* **55** (1995), 209–221.

[43] D. H. Lehmer, "An extended theory of Lucas' functions". *Ann. of Math. (2)* **31** (1930), no. 3, 419–448.

[44] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász,"Factoring polynomials with rational coefficients". *Math. Ann.* **261** (1982), no. 4, 515–534.

[45] W. LeVeque, *Topics in Number Theory, Vol. 1*, Addison-Wesley, Reading, Mass., 1956.

[46] J. Liouville, "Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques", *Comptes rendus* **18** (1844), 883–885, 910–911; *J. Math, pures et appl.* **16** (1851), 133–142.

[47] F. Luca, "On the equation $x^2 + 2^a3^b = y^n$", *Int. J. Math. Math. Sci.* **29** (2002), no. 4, 239–244.

[48] F. Luca and G. Soydan, "On the Diophantine equation $2^m + nx^2 = y^n$", *Journal of Number Theory* **132** (2012), 2604–2609.

[49] F. Luca and A. Togbé, "On the Diophantine equation $x^2+7^{2k}=y^n$", *Fibonacci Quart.* **45** (2007), no. 4, 322–326.

[50] F. Luca and A. Togbé, "On the Diophantine equation $x^2+2^a5^b=y^n$", *Int. J. Number Theory* **4** (2008), no. 6, 973–979.

[51] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, New York, 1984.

[52] D. A. Marcus, *Number Fields*, Springer, New York, 1977.

[53] M. Mignotte, "A corollary to a theorem of Lauren-Mignotte-Nesterenko", *Acta Arith.* **86** (1998), no. 2, 101–111.

[54] R. A. Mollin, *Quadratics*, CRC Press, New York, 1996.

[55] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers, 3rd ed.*, Springer, New York, 2004.

[56] C. L. Olds, *Continued Fractions*, Random House, New York, 1963.

[57] I. Pink, "On the Diophantine equation $x^2+2^\alpha 3^\delta 5^\gamma 7^\delta=y^n$", *Publ. Math. Debrecen* **70** (2007) 149–166.

[58] B. Poonen, "Some Diophantine equations of the form $x^n+y^n=z^m$", *Acta Arith.* **86** (1998), no. 3, 193–205.

[59] K. A. Ribet, "On modular representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms", *Invent. Math.* **100** (1990), no. 2, 431–476.

[60] P. Ribenboim, "The Fibonacci numbers and the Arctic Ocean", *Proceedings of the 2nd Gauss Symposium. Conference A: Mathematics and Theoretical Physics (Munich, 1993)*, 41–83, Sympos. Gaussiana, de Gruyter, Berlin, 1995.

[61] J. H. Rickert, "Simultaneous rational approximations and related Diophantine equations", *Math. Proc. Cambridge Philos. Soc.* **113** (1993), no. 3, 461–472.

[62] K. F. Roth, "Rational approximations to algebraic numbers", *Mathematika* **2** (1955), 1–20; corrigendum, 168.

[63] A. Schnizel, "Primitive divisors of the expression $A^n - B^n$ in algebraic number fields," *J. Reine Angew. Math.* **268/269** (1974), 27–33.

[64] C.L. Siegel, "Die Gleichung $ax^n - by^n = c$", *Math. Annalen* **114** (1937), 57–68.

[65] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

[66] W. A. Stein et al., *Sage Mathematics Software (Version 6.2)*, The Sage Development Team, 2015, `http://www.sagemath.org`.

[67] C. L. Stewart, "On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers", *Proc. London Math. Soc.* **35** (1977), no. 3, 425–447.

[68] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem, 3rd ed.*, A. K. Peters, Massachusetts, 2002.

[69] G. Soydan, M. Ulas, and H. L. Zhu, "On the Diophantine equation $x^2+2^a \cdot 19^b = y^n$", *Indian Journal of Pure and Applied Mathematics*, **43** (2012), 251–261.

[70] L. Tao, "On the Diophantine equation $x^2+3^m = y^n$", *Electr. J. Comm. Number Theory* **8** (2008), 1–7.

[71] R. Taylor and A. Wiles, "Ring-theoretic properties of certain Hecke algebras", *Ann. of Math. (2)* **141** (1995), no. 3, 553–572.

[72] A. Thue, "Über Annäherungswerte algebraischer Zahlen", *J. reine angew. Math.* **135**, (1909), 284–305.

[73] A. Thue, "Berechnung aller Lösungen gewisser Gleichungen von der Form $ax^r - by^r = f$" , *Vid. selskap. Skrifter (Kristiania)* **I** (1918), no. 4, 1–9.

[74] N. Tzanakis and B. M. M. de Weger, "On the practical solution of the Thue equation", *J. Number Theory* **31** (1989), 99–132.

[75] P. M. Voutier, "Primitive divisors of Lucas and Lehmer sequences", *Math. Comp.* **64** (1995), 869–888.

[76] M. Waldschmidt, "A lower bound for linear forms in logarithms", *Acta Arith.* **37** (1980), 257–283.

[77] Y. Wang and T. Wang, "On the Diophantine equation $nx^2 + 2^{2m} = y^n$", *J. Number Theory* **131** (2011), no. 8, 1486–1491.

[78] M. Ward, "The intrinsic divisors of Lehmer numbers", *Ann. of Math.* **62** (1955), no. 2, 230–236.

[79] L. Washington, *Elliptic Curves. Number Theory and Cryptography, 2nd ed.*, Chapman & Hall/CRC, Boca Raton, FL, 2008.

[80] H. Wu, "The Diophantine equation $nx^2 + 2^m = y^n$", *Adv. Math. (China)* **40** (2011), no. 3, 365–369.

[81] A. Wiles, "Modular elliptic curves and Fermat's last theorem", *Ann. of Math. (2)* **141** (1995), no. 3, 443–551.

[82] Z. Zhang, "The Diophantine equation $(ax^k - 1)(by^k - 1) = abz^k - 1$", *J. Number Theory*, **136** (2014), 252–260.

[83] K. Zsigmondy, "Zur Theorie der Potenzreste", (German) *Monatsh. Math. Phys.* **3** (1892), no. 1, 265–284.

# VITA

Eva Goedhart was born in the Netherlands, but lived most of her early life in various parts of Virginia. Prior to completing a Doctorate of Philosophy degree in mathematics from Bryn Mawr College in 2015, she received a Bachelor of Science degree from James Madison University in 2003. She then moved to North Carolina to attend Wake Forest University for graduate school, where she wrote a thesis under the supervision of Kenneth Berenhaut. She completed the Master of Arts degree in 2005.

After graduating from Bryn Mawr College, she hopes to teach the next generation of mathematicians and to share her research interests in algebraic number theory and Diophantine analysis.