THE UNIVERSITY OF CALGARY

THE PELL EQUATION AND POWERFUL NUMBERS

BY

PETER GARTH WALSH

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE

DEPARTMENT OF MATHEMATICS AND STATISTICS

CALGARY, ALBERTA

JUNE, 1988

© PETER GARTH WALSH 1988

Permission has been granted to the National Library of Canada to microfilm this thesis and to lend or sell copies of the film.

The author (copyright owner) has reserved other publication rights, and neither the thesis nor extensive extracts from it may be printed or otherwise reproduced without his/her written permission.

L'autorisation a été accordée à la Bibliothèque nationale du Canada de microfilmer cette thèse et de prêter ou de vendre des exemplaires du film.

L'auteur (titulaire du droit d'auteur) se réserve les autres droits de publication; ni la thèse ni de longs extraits de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation écrite.

ISBN 0-315-46680-4

THE UNIVERSITY OF CALGARY

FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled, "*The Pell Equation and Powerful Numbers*" submitted by Peter Garth Walsh in partial fulfillment of the requirements for the degree of Master of Science.

R.A. Mollin, Chairman
Department of Mathematics & Statistics

R.K. Guy
Department of Mathematics & Statistics

H.C. Williams
Department of Computer Science
University of Manitoba

DATE: June 10/88

ABSTRACT

This thesis constitutes a study of the Pell Equation, Powerful Numbers, and their relation to Fermat's Last Theorem. The first chapter is a study of the Pell equations $x^2 - dy^2 = \pm 1$, and a description of their solutions. In particular, the solvability of $x^2 - dy^2 = -1$ is considered, as well as a study of certain divisibility properties of the integers (x,y) which are solutions to these Pell equations. Chapter 2 is a study of the more general Pell equation $x^2 - dy^2 = n$ where n is any non-zero integer. A link between the factorization of the fundamental unit and ambiguous classes of solutions to $x^2 - dy^2 = n$ is also discussed. Chapter 3 is a study of differences of powerful numbers. It is shown that every integer is the proper difference of non-square powerful numbers in infinitely many ways. The fourth and last chapter is a survey style essay on many results involving powerful numbers. In particular, new results are obtained giving connections between powerful numbers and Fermat's Last Theorem. As well, formulae for the distribution of powerful numbers, powerful numbers in arithmetic progression, and sums of powerful numbers are discussed.

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my supervisor, Dr. Richard A. Mollin, for his never-ending support and guidance during the five years that I have studied under him, both as a graduate and undergraduate student.

As well, I would like to offer thanks to the University of Calgary for giving me the opportunity to pursue Graduate Studies, and in particular, the Department of Mathematics and Statistics for all the moral and financial support which has enabled me to complete this programme.

TABLE OF CONTENTS

LIST OF SYMBOLS

Symbol	Meaning	c.f. page
$\mathcal{A}$	the set of algebraic integers over Q	4
Q	field of rational numbers	4
$Q(\sqrt{d})$	quadratic extension of Q by $\sqrt{d}$	4
θ_d	the ring of integers of $Q(\sqrt{d})$	4
$\mathbb{Z}$	ring of integers	4
$\mathbb{Z}[\sqrt{d}]$	ring of elements of the form $a + b\sqrt{d}$, $a,b \in \mathbb{Z}$	4
$N(\alpha)$	norm of the quadratic number α	5
$\overline{\alpha}$	the conjugate of the quadratic number α	5
$\mathcal{U}_d$	the group of units in θ_d	5
$\frac{T + U\sqrt{d}}{2}$, ϵ_d	the Fundamental unit of θ_d	7
$\frac{T_k + U_k\sqrt{d}}{2}$	the k^{th} power of ϵ_d	8
$\left[\frac{d}{p}\right]$	the Legendre symbol	12
$a \mid b$	a divides b	5, 8
$p^k \parallel b$	$p^k \mid b$ but p^{k+1} does not divide b	21
$p \nmid b$	p does not divide b	103
$GCD(a,b)$, (a,b)	the greatest common divisor of a and b	13
$[x]$	the integer part of x	96
$\mu(n)$	the Möbius function of n	96
$\zeta(s)$	the Riemann zeta function at s	97
$R_{a,b}$	the set of a-b generalized squareful numbers	99
$R_{a,b}(x)$	the distribution of $R_{a,b}$	99
$U_i^{(k)}$	a k-full integer	78
$\phi(m)$	the Euler function of m	80

C H A P T E R O N E

Section 1 The Pell Equation -- A Brief History

The indeterminate equation $x^2 - Ay^2 = 1$, where A is not a perfect square, is known as Pell's Equation, or the Pell Equation, named after the seventeenth century mathematician John Pell. There has been a long-standing controversy concerning the title of the equation, as many feel that John Pell had little to do with the equation. The consensus, as documented in Whitford's "The Pell Equation" [76], is that Euler must have confused the contributions of Pell and those of Lord Brouncker, in his reading of Wallis's algebra; and hence misnamed the equation.

Nevertheless, mathematicians have not failed to recognize the contributions in this regard of Fermat, Brouncker, Wallis, Gauss, Lagrange, and many others.

The history of the equation goes as far back as the ancient Egyptian and Babylonian eras. Solutions to the Pell Equation are closely related to primitive methods of approximating a square root, and it is this connection which dates the equation to as far back as four thousand years ago.

According to Whitford, the first traces of this connection are found in the dimensions of ancient structures, such as the Pyramids. For example, in the King's Chamber, in the pyramid of Cheops, the ratio of the height to its breadth is about 1.117, or about $\sqrt{5}/2$, which is very close to half the ratio x/y of solutions to $x^2 - 5y^2 = 1$. A better example is found in the temple of Acropolis, where the ratio 17/12 occurs quite often in the architectural structure. It is more than a

curiosity that $x = 17$, $y = 12$ is a solution to $x^2 - 2y^2 = 1$.

The Ancient Greeks also had a hand in the history of the Pell Equation. In particular, Pythagoras had an affection for approximations of square roots. As well, Diophantus showed how to obtain infinitely many solutions to a Pell Equation from a given one.

It is also known that the Hindus had also contributed to the subject, although many feel their work depended greatly on the work of the Greeks.

Along with the Hindus, during the time period 650 A.D. to 1200 A.D., the Arabs made some contributions to the history of the equation. However it wasn't until the early modern era, about 1600 A.D., that the equation was studied algebraically. Also, some associated equations were studied, such as $x^2 - Ay^2 = -1$, $x^2 - Ay^2 = \pm 4$, $x^2 - Ay^2 = c$, and $mx^2 - ny^2 = \pm 1$.

Lord Brouncker was the first known to give an algorithm yielding the fundamental solution to $x^2 - Ay^2 = 1$; i.e., the solution from which all others are derived. His procedure may have been the beginnings of what is now known as the continued fraction algorithm.

Euler showed how square values of quadratic polynomials are directly related to Pell's equation via linear transformations, generalizing the work of Brouncker. At this point though, no general proof had been given to show that there are always solutions to $x^2 - Ay^2 = 1$ for every non-square positive integer A.

Finally in 1766, Lagrange solved the problem, and Gauss [18] was quick to proclaim, "The treatise of Lagrange grasps the problem in its entire generality and in this connection leaves nothing to be desired."

Lagrange also gave necessary conditions for the solvability of $x^2 - Ay^2 = -1$, and generalized his existence proof to the equation $x^2 - Ay^2 = B$.

Gauss transformed the problem by a method of substitutions, thereby avoiding the use of continued fractions. Dirichlet extended Gauss's work on the method of substitutions, now known as the theory of Quadratic Forms. He also studied the solvability of $x^2 - MNy^2 = -1$ in terms of solvability of the related equations $Mx^2 - Ny^2 = 1,2$. Dirichlet also showed that integer powers of the fundamental solution yield all solutions to $x^2 - Ay^2 = \pm 1$.

Euler calculated the fundamental solutions of $x^2 - Ay^2 = 1$ for A between 2 and 99 in 1770. Many tables have been calculated since then, and our supercomputers now can calculate the fundamental solution to $x^2 - Ay^2 = \pm 1$ for astronomically large A.

Although it is known that $x^2 - Ay^2 = 1$ always has a solution for non-square positive integers A, the equation $x^2 - Ay^2 = -1$ remains somewhat of a mystery. The problem of classifying all such integers A in terms of the arithmetic of the quadratic field $Q(\sqrt{A})$ remains an unsolved problem to this day. Many necessary, and many sufficient conditions have been given. For example, A cannot be divisible by any prime of the form $4k + 3$. But the unsolvability of $x^2 - 34y^2 = -1$ shows that this condition is not sufficient. Trotter [68], has given necessary and sufficient conditions in terms of the solvability of a related diophantine equation, cited earlier in our discussion of Dirichlet.

There are other related diophantine equations. For example, Cohn

[10] has studied $x^4 - Ay^2 = \pm 1, \pm 4$ and $x^2 - Ay^4 = \pm 1, \pm 4$. The solvability of these two equations is related to certain divisibility properties of solutions (x,y) to $x^2 - Ay^2 = \pm 1$. Lucas [32] and Lehmer [29] developed the well known "Lucas-Lehmer Theory", which laid the groundwork for any further study in this direction.

Recently, the equation has taken on some new directions. Cohn [7] has studied the equation $\epsilon^2 - \delta\eta^2 = 4i$ with ϵ, δ, η being Gaussian integers.

For a more complete history of the subject, the reader can refer to either Whitford [76] or Dickson [14, Ch. 17].

Section 2 Units in Quadratic Fields

Let d be a square-free integer. The field $Q(\sqrt{d})$ is called a quadratic extension of the rational field Q, or simply a Quadratic Field over Q, and consists of elements of the form $a + b\sqrt{d}$ where a and b are rational numbers. If d is positive, $Q(\sqrt{d})$ is a real quadratic field, otherwise it is a complex quadratic field.

Let α be any complex number. If there exists a monic polynomial, $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, with $a_i \in \mathbb{Z}$ for $i = 0,\ldots,n-1$, such that $p(\alpha) = 0$, then α is called an algebraic integer. The set of all algebraic integers is denoted by $\mathcal{A}$.

Let $\theta_d = \mathcal{A} \cap Q(\sqrt{d})$, then it is easy to see that θ_d is a ring, called the ring of integers of $Q(\sqrt{d})$.

Theorem I.1. If d is a square-free integer then

$$\theta_d = \mathbb{Z}[\sqrt{d}] \qquad \text{if } d \equiv 2, 3 \pmod 4$$

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \quad \text{if } d \equiv 1 \pmod 4.$$

Proof. See Samuel [55, Theorem 1, p. 35].

The ring θ_d will generally be the setting for our study.

By Theorem I.1, any element $\alpha \in \theta_d$ will be of the form $\alpha = \frac{a + b\sqrt{d}}{2}$ for some $a,b \in \mathbb{Z}$ satisfying $a \equiv b \pmod 2$. When $d \equiv 2,3 \pmod 4$, a and b are always even, by Theorem I.1.

Given $\alpha = \frac{a + b\sqrt{d}}{2} \in \theta_d$, let $\overline{\alpha} = \frac{a - b\sqrt{d}}{2}$. $\overline{\alpha}$ is called the algebraic conjugate of α. It is easily verified that for any $\alpha,\beta \in \theta_d$, $\overline{\alpha\cdot\beta} = \overline{\alpha}\cdot\overline{\beta}$. Now define a function $N: \theta_d \to \mathbb{Z}$ by $N(\alpha) = \alpha\cdot\overline{\alpha}$. N is called the Norm function, and $N(\alpha)$ is called the Norm of α. For $\alpha = \frac{a + b\sqrt{d}}{2}$, then $N(\alpha) = \frac{a^2 - b^2 d}{4}$. It can be checked that for any $\alpha,\beta \in \theta_d$, $N(\alpha\cdot\beta) = N(\alpha)\cdot N(\beta)$.

Given $\alpha,\beta \in \theta_d$, we say α divides β if $\frac{\beta}{\alpha} \in \theta_d$. An element $\alpha \in \theta_d$ is a unit if α divides 1.

Proposition I.1. For $\alpha \in \theta_d$, α is a unit if and only if $N(\alpha) = \pm 1$.

Proof. See Samuel [55, Prop. 1., p. 60]. □

The set of units in θ_d is denoted by $\mathcal{U}_d$, and clearly forms a group. For negative d we have:

Theorem I.2. Let d be a square-free negative integer, then

$$\mathcal{U}_d = \begin{cases} \{\pm 1\} & \text{if } d \neq -1, -3 \\ \{\pm 1, \pm i\} & \text{if } d = -1 \\ \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\} & \text{if } d = -3 \end{cases}$$

Proof. See Samuel [55, Prop. 1, p. 62] □

Theorem I.2 tells us that for complex quadratic fields, the group of units is uninteresting. Therefore we consider only square-free positive d henceforth.

Let $\alpha = \frac{a + b\sqrt{d}}{2}$ be a unit other than ± 1. Then $-\alpha$, α^{-1}, $-\alpha^{-1}$ are also units, and these four elements are precisely $\frac{\pm a \pm b\sqrt{d}}{2}$. It is easy to see that exactly one of these four elements is greater than one, namely the element $\frac{|a| + |b|\sqrt{d}}{2}$. We have proved:

Proposition I.2. A unit $\alpha = \frac{a + b\sqrt{d}}{2}$ satisfies $\alpha > 1$ if and only if $a > 0$ and $b > 0$. □

Units of this type will be called completely positive units, and throughout this chapter, we will be primarily concerned with these. Another important fact about units is given in the following result.

Proposition I.3. Let $\alpha = \frac{a + b\sqrt{d}}{2}$ and $\beta = \frac{x + y\sqrt{d}}{2}$ be completely positive units, then $\alpha < \beta$ if and only if $a < x$.

Proof. Since α and β are units, we have that $a^2 - db^2 = \pm 4$ and $x^2 - dy^2 = \pm 4$. It follows that one of the three equations

$$\text{(i)} \quad x^2 - a^2 = d(y^2 - b^2)$$

(ii) $x^2 - a^2 = d(y^2 - b^2) - 8$

(iii) $x^2 - a^2 = d(y^2 - b^2) + 8$ must hold.

Assume $\alpha < \beta$ and $a \geq x$, then $b < y$ must hold. In this case (i) implies $y \leq b$, a contradiction. (ii) implies $0 < d(y^2 - b^2) \leq 8$, hence $d = y = 2$ and $b = 1$, and so $x^2 - a^2 = -2$ which is not possible. (iii) implies $0 \geq x^2 - a^2 = d(y^2 - b^2) + 8 > 0$, again a contradiction. Conversely assume $a < x$ and $\alpha \geq \beta$, then $b \geq y$ must hold. In this case (i) implies $y > b$, a contradiction. (ii) implies $y > b$ also, which is a contradiction. (iii) implies $0 < d(b^2 - y^2) < 8$, hence $d = b = 2$ and $y = 1$, forcing $x^2 - a^2 = 2$, which is not possible. □

From Proposition I.3, it follows that the completely positive units are linearly ordered by their rational parts. Given a square-free positive integer d, let $\epsilon_d = \frac{T + U\sqrt{d}}{2}$ be the completely positive unit in θ_d with smallest possible T. Then ϵ_d is called the Fundamental Unit of θ_d, and by an abuse of language, is sometimes called the Fundamental Unit of $Q(\sqrt{d})$.

We still haven't proved the existence of units other than ± 1 in θ_d for $d > 0$, but it is worth noting that the existence of units other than ± 1 in θ_d is tantamount to the existence of completely positive units in θ_d, (and hence the existence of ϵ_d). We pursue this in the next section.

Section 3 Solution to Pell's Equation -- The Fundamental Unit

When considering the Pell equations

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

$$x^2 - dy^2 = \pm 4 \tag{2}$$

for positive non-square integers d, it suffices to consider those d which are square-free, since we can pull all square factors of d into y.

The solutions $(\pm 1, 0)$ to equation (1) and $(\pm 2, 0)$ to equation (2) will be considered trivial solutions. The existence of non-trivial solutions to (1) and (2) is equivalent to the existence of ϵ_d. We state the following theorem, first proved by Lagrange (e.g. see [42, p. 53]).

Theorem I.3. For any positive square-free integer d, ϵ_d exists. Moreover $\mathcal{U}_d = \{\pm \epsilon_d^{\,n} ; n \in \mathbb{Z}\}$, and all completely positive units are of the form $\epsilon_d^{\,k}$ with $k \geq 1$.

In general, ϵ_d will be of the form $\epsilon_d = \frac{T + U\sqrt{d}}{2}$ for some positive integers T and U. When $d \not\equiv 5 \pmod 8$, T and U are even (see [47, Theorem 3.10]), so that ϵ_d takes on the form $a + b\sqrt{d}$ with a and b positive integers. When $d \equiv 5 \pmod 8$, T and U may or may not be even.

Proposition I.4. Let $\epsilon_d = \frac{T + U\sqrt{d}}{2}$. If T and U are odd, then $d \equiv 5 \pmod 8$. Let $\epsilon_d^{\,k} = \frac{T_k + U_k\sqrt{d}}{2}$, then if T and U are odd, T_k

and U_k are even if and only if $3|k$.

Proof. See Samuel [55, p. 64]. □

Proposition I.4 will be useful in later sections since it shows that the subgroup $\mathcal{V}_d = \{\pm\epsilon_d^{3k} ; k \in \mathbb{Z}\}$ of $\mathcal{U}_d$ contains all the units of θ_d which are of the form $a + b\sqrt{d}$ with $a,b \in \mathbb{Z}$, when T and U are odd. For example, $\epsilon_5 = \frac{1 + \sqrt{5}}{2}$, while $\epsilon_5^3 = 2 + \sqrt{5}$. For $d = 37$, $\epsilon_d = 6 + \sqrt{37}$ showing that T and U may be even when $d \equiv 5 \pmod 8$.

In general, units are of the form $\pm\left(\frac{T_k + U_k\sqrt{d}}{2}\right)$ as described in Proposition I.4, and (T_k,U_k) is a solution to equation (2). When T_k and U_k are even, then $\left[\frac{T_k}{2}, \frac{U_k}{2}\right]$ is a solution to equation (1).

By the multiplicativity of the norm function, it can be seen that if $N(\epsilon_d) = 1$, then all units in $\mathcal{U}_d$ have norm 1. Therefore the equations $x^2 - dy^2 = -1,-4$ are not solvable. It is a long-standing problem to classify those d for which $N(\epsilon_d) = -1$ in terms of the arithmetic of the underlying field, $Q(\sqrt{d})$. We shall study this in more detail in the next section. For now we state the following easy result.

Theorem I.5. If $N(\epsilon_d) = 1$, then all units in $\mathcal{U}_d$ have norm one, hence the equations $x^2 - dy^2 = -1, -4$ are not solvable. If $N(\epsilon_d) = -1$, then all solutions to the equations $x^2 - dy^2 = -1, -4$ come from the set of units $\{\pm\epsilon_d^{2k+1} ; k \in \mathbb{Z}\}$, and all solutions to the equations $x^2 - dy^2 = 1,4$ come from the set of units

$\{\pm\epsilon_d^{2k} ; k \in \mathbb{Z}\}$. □

For example, $N(\epsilon_3) = N(2 + \sqrt{3}) = 2^2 - 1^2 \cdot 3 = 4 - 3 = 1$, so that $x^2 - 3y^2 = -1$ is not solvable. But $N(\epsilon_2) = N(1 + \sqrt{2}) = 1^2 - 1^2 \cdot 2 = 1 - 2 = -1$ so that the equation $x^2 - 2y^2 = -1$ is solvable and has in fact infinitely many solutions, all coming from the units $\pm(1 + \sqrt{2})^{2k+1}$ with $k \in \mathbb{Z}$. Theorem I.5 and Proposition I.4 give some insight into the problem of finding solutions to the equation $x^2 - dy^2 = 1$. For example, if $d = 13$, we may have to search quite a while to find integers x and y that satisfy $x^2 - 13y^2 = 1$. Instead, we merely apply these two theorems in the following way. Since $3^2 - 13 = -4$, we have that $\alpha = \frac{3 + \sqrt{13}}{2}$ is a unit in θ_{13} and $N(\alpha) = -1$. By Proposition I.4, α^3 is of the form $\alpha^3 = a + b\sqrt{13}$ with $a,b \in \mathbb{Z}$. In fact $\alpha^3 = 18 + 5\sqrt{13}$. By Theorem I.5, $N(\alpha^{2k}) = 1$ for $k \in \mathbb{Z}$, so that $N(\alpha^6) = 1$. Since $\alpha^6 = (\alpha^3)^2 = (18 + 5\sqrt{13})^2 = 649 + 180\sqrt{13}$, it follows that $(649)^2 - (180)^2 \cdot 13 = 1$. So we have found integer solutions to $x^2 - 13y^2 = 1$ with a minimal amount of work. Trying to find this solution by trial and error may have been exhausting.

There are algorithms to find the fundamental unit of a quadratic field. The most elementary of these is to write the numbers dy^2 for $y \geq 1$. Letting y_1 be the first number for which dy_1^2 differs from a square, x_1^2, by 1 or 4 yields the fundamental unit $x_1 + y_1\sqrt{d}$ or $\frac{x_1 + y_1\sqrt{d}}{2}$ respectively. For example, if $d = 7$ we obtain $7 \cdot 1^2$, $7 \cdot 2^2$, $7 \cdot 3^2$, and $7 \cdot 3^2$ differs from 8^2 by 1, so that $8 + 3\sqrt{7}$ is the fundamental unit of $\mathbb{Q}(\sqrt{7})$. Using the theory of continued fractions, there are much faster techniques for finding the fundamental unit. It

is not our intention to include this in the scope of our discussion. We merely mention it as a point of interest.

Before proceeding to the next section, we prove the following proposition which will be used later.

Proposition I.5. Let $n \geq 1$ and $\epsilon_d^n = \frac{T_n + U_n\sqrt{d}}{2}$. Assume that $(n,d) \neq (1,2)$, $(1,5)$, or $(2,5)$. Then

1. $T_n > U_n$
2. $T_n > T_1$ for $n > 1$.
3. $U_n > U_1$ for $n > 1$.

Proof. 1. If $N(\epsilon_d) = 1$, then $T_n^2 = U_n^2 d + 4 > U_n^2$, so the result holds. Assume $N(\epsilon_d) = -1$ and that $U_n \geq T_n$. Then $U_n^2 \geq T_n^2 = dU_n^2 - 4 > U_n^2 - 4$ forcing $0 \leq U_n^2 - T_n^2 < 4$. Since T_n and U_n are of the same parity, it follows that $T_n = U_n$. In this case, it follows that $-4 = T_n^2 - T_n^2 d = T_n^2[1-d]$, or equivalently, $4 - T_n^2[d-1]$. This gives $T_n = 2$, $d = 2$ or $T_n = 1$, $d = 5$, hence $(n,d) = (1,2)$ or $(n,d) = (1,5)$ contrary to our hypothesis.

2. This is precisely the result of Proposition I.3.

3. From the relation $\frac{T_2 + U_2\sqrt{d}}{2} = \left[\frac{T_1 + U_1\sqrt{d}}{2}\right]^2 = \frac{T_2 + T_1U_1\sqrt{d}}{2}$, we have that $U_2 = T_1U_1 > U_1$ unless $T_1 = 1$, in which case $d = 5$ and $(n,d) = (2,5)$. In this case, $U_3 = 2 > U_1 = 1$. Proceeding by induction, assume $U_n > U_1$. From the relation $\frac{T_{n+1} + U_{n+1}\sqrt{d}}{2} =$

$$\left[\frac{T + U\sqrt{d}}{2}\right]\left[\frac{T_n + U_n\sqrt{d}}{2}\right] = \frac{2T_{n+1} + (T_1U_n + T_nU_1)\sqrt{d}}{4}, \quad \text{it follows that}$$

$$U_{n+1} = \frac{T_1U_n + T_nU_1}{2} \geq \frac{T_1U_n + U_nU_1}{2} \geq \frac{U_1U_n + U_nU_1}{2} = U_nU_1 \geq U_n > U_1. \qquad \square$$

Section 4 Criteria for the Solvability of $x^2 - dy^2 = -1, -4$

As seen in Section 3, the equations

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

$$x^2 - dy^2 = -4 \tag{2}$$

may not have solutions for a given square-free positive integer d, while the equations

$$x^2 - dy^2 = 1 \tag{3}$$

$$x^2 - dy^2 = 4 \tag{4}$$

always have solutions.

The solvability of equations (1) and (2) is equivalent to $N(\epsilon_d) = -1$. In this section we will give some necessary and some sufficient conditions for $N(\epsilon_d) = -1$, the first of which is given in the following result.

Theorem I.6. If $N(\epsilon_d) = -1$, then d has no prime factor of the form $4k + 3$.

Proof. Let $\epsilon_d = \frac{T + U\sqrt{d}}{2}$ with $N(\epsilon_d) = -1$. Then $T^2 - U^2d = -4$ so that, for any odd prime divisor p of d, $T^2 \equiv -4 \pmod{p}$. This congruence shows $1 = \left[\frac{-4}{p}\right] = \left[\frac{4}{p}\right]\left[\frac{-1}{p}\right] = \left[\frac{-1}{p}\right]$, hence

$p \equiv 1 \pmod 4$. □

Note that the converse of Theorem I.6 is false. A counterexample is $d = 34$; 34 has no prime factor of the form $4k + 3$, but $N(\epsilon_{34}) = N(35 + 6\sqrt{34}) = 1$.

Trotter [68] has given necessary and sufficient conditions for $N(\epsilon_d) = -1$ in terms of solvability of another closely related diophantine equation. We generalize Trotter's result and give an arithmetical proof of his result as a corollary in what follows.

Theorem I.7. Let $d = 2^{\delta}d'$ with $\delta \in \{0,1\}$ and d' an odd positive square-free integer. Then $N(\epsilon_d) = 1$ if and only if one of the two following conditions hold;

1. $\epsilon_d = \tau^2$ where $\tau = \frac{a\sqrt{r} + b\sqrt{s}}{2}$ for some integers $a,b > 0$ and $r,s > 1$ such that $|a^2r - b^2s| = 4$ and $d = rs$.

2. $\epsilon_d = \tau^2/2$ where $\tau = a\sqrt{r} + b\sqrt{s}$ for some positive integers a,b,r,s such that $|a^2r - b^2s| = 2$ and $d = rs$.

Proof. It is easy to verify that if conditions (1) or (2) hold, then $N(\epsilon_d) = 1$. For the converse we have several cases. First note that $N(\epsilon_d) = 1$ implies $T > 2$ where $\epsilon_d = \frac{T + U\sqrt{d}}{2}$, for if $T = 1$, then $1 = N(\epsilon_d) = N\left[\frac{1 + U\sqrt{d}}{2}\right] = \frac{1 - U^2d}{4}$, i.e., $d = -3$, a contradiction; whereas if $T = 2$ then $1 = N(\epsilon_d) = N\left[\frac{2 + U\sqrt{d}}{4}\right] = \frac{4 - U^2d}{4}$; i.e., $d = 0$, a contradiction. Henceforth assume $T > 2$.

Case 1. $\delta = 0$, T odd.

Since $T^2 - 4 = U^2d = (T-2)(T+2)$ and $GCD(T-2,T+2) = 1$, it

follows that $T - 2 = A^2r$ and $T + 2 = B^2s$ for some positive integers A,B,r,s, with $AB = U$ and $d = rs$. If $r = 1$, then $d = s$ and so $A^2 - B^2d = -4$ contradicting $N(\epsilon_d) = 1$. If $s = 1$, then $d = r$ so that $B^2 - A^2d = 4$ and $\frac{B + A\sqrt{d}}{2}$ is a completely positive unit satisfying $B \leq U \leq T$. Since $\frac{T + U\sqrt{d}}{2}$ is the completely positive unit with T minimal, it follows that $T = B$ and $U = A$. Since $U = AB$ from above, it follows that $T = B = 1$ contradicting $T > 2$. Thus $s > 1$ holds and $\tau = \frac{A\sqrt{r} + B\sqrt{s}}{2}$ can be seen to satisfy condition (1).

Case 2. $\delta = 0$, $T \equiv 0 \pmod 4$.

In this case $GCD(T-2,T+2) = 2$ and so from $(T-2)(T+2) = U^2d$ we obtain positive integers A,B,r,s such that $T - 2 = 2A^2r$ and $T + 2 = 2B^2s$ with $U = 2AB$ and $d = rs$. So $2B^2s - 2A^2r = 4$ holds, and hence $B^2s - A^2r = 2$. Setting $\tau = A\sqrt{r} + B\sqrt{s}$, τ satisfies condition (2).

Case 3. $\delta = 0$, $T \equiv 2 \pmod 4$.

In this case, $GCD(T-2,T+2) = 4$ and from $(T-2)(T+2) = U^2d$ we obtain positive integers A,B,r,s such that $T - 2 = (2A)^2r$ and $T + 2 = (2B)^2s$ with $U = 4AB$ and $d = rs$. Therefore, $(2B)^2s - (2A)^2r = 4$ and by the same reasoning as case (1), $\tau = \frac{2A\sqrt{r} + 2B\sqrt{s}}{2} = A\sqrt{r} + B\sqrt{s}$ can be seen to satisfy condition (1).

Case 4. $\delta = 1$.

In this case $T^2 - 4 = U^2d$ with d even, forcing both T and U to be even. Thus $T^2 \equiv 4 \pmod 8$, forcing $T \equiv 2 \pmod 4$. So

GCD(T-2,T+2) = 4 and from $(T-2)(T+2) = U^2d$, we have positive integers A,B,r,s such that $T - 2 = (2A)^2 2^{\epsilon} r$ and $(T + 2) = (2B)^2 2^{1-\epsilon} s$ where $U = 4AB$, $d = 2rs$, and $\epsilon = 0$ or 1. This gives $(2B)^2 2^{1-\epsilon} s - (2A)^2 s^{\epsilon} r = 4$, and again by the same reasoning as case 1, $\tau = \frac{2A\sqrt{2^{\epsilon} r} + 2B\sqrt{2^{1-\epsilon} s}}{2}$ satisfies condition (1). □

From Theorem I.7 we obtain a useful set of corollaries. Among them is the following theorem proved by Trotter.

Corollary I.1. Let $d = 2^{\delta} d'$ with $\delta \in \{0,1\}$ and $d' \equiv 1 \pmod 4$ positive and square-free. Then $N(\epsilon_d) = 1$ if and only if d admits a non-trivial factorization, $d = rs$, such that $|a^2 r - b^2 s| = 4$ is solvable.

Proof. If d admits such a factorization, it can be seen that $N(\epsilon_d) = 1$. Now assume $N(\epsilon_d) = 1$ with d as above. Note that we are trying to prove that condition (1) of Theorem I.7 holds. The only case for which condition (2) held in the proof of Theorem I.7 was the case $\delta = 0$ and $T \equiv 0 \pmod 4$. In this case, $\frac{T}{2}$ and U are even, and $d = d'$ is odd. Thus $\left[\frac{T}{2}\right]^2 - \left[\frac{U}{2}\right]^2 d' = 1$, and hence $\left[\frac{U}{2}\right]^2 d' = \left[\frac{T}{2}\right]^2 - 1 \equiv 0 - 1 \equiv 3 \pmod 4$. It follows at once that $d' \equiv 3 \pmod 4$, contradicting our assumption that $d' \equiv 1 \pmod 4$. □

By Theorem I.6, classifying positive square-free integers d for which $N(\epsilon_d) = -1$, requires only considering those d for which the odd prime factors are all of the form $4k + 1$. Therefore in Corollary

I.1 we could have replaced the condition $d' \equiv 1 \pmod 4$ by the condition that d' is a product of primes of the form $4k + 1$. For those d' which are divisible by primes of the form $4k + 3$ we actually have the following result.

Corollary I.2. Let $d = 2^{\delta}d'$ with $\delta \in \{0,1\}$ and $d' \equiv 1 \pmod 4$ positive, square-free, and divisible by a prime $p \equiv 3 \pmod 4$. Then d admits a non-trivial factorization $d = rs$ such that the equation $rx^2 - sy^2 = \pm 4$ is solvable.

Proof. By Theorem I.6, $N(\epsilon_d) = 1$, and by Corollary I.1 the result follows. □

A special case of Corollary I.2 is given in the following result, which we isolate as a motivating result.

Corollary I.3. Let $p \equiv q \equiv 3 \pmod 4$ be distinct primes. Then $px^2 - qy^2 = \pm 4$ is solvable. □

This corollary sparks an interest in the more general equations $mx^2 - ny^2 = \pm 4, \pm 1$ with m and n square-free positive integers. We study this in more detail in the next chapter.

Another immediate consequence of Corollary I.1 is the following well-known theorem.

Theorem I.8. If $p \equiv 1 \pmod 4$ is prime, then $N(\epsilon_p) = -1$.

Proof. Since p admits no non-trivial factorization $p = rs$, condition (1) of Theorem I.7 can't hold, and hence $N(\epsilon_p) = -1$. □

Another consequence of Corollary I.1 is the following result which is a sufficient condition for $N(\epsilon_d) = -1$.

Theorem I.9. Let $d = 2^{\delta}d'$ with $\delta \in \{0,1\}$ and d' a product of primes of the form $4k + 1$. If d has no non-trivial factorization $d = rs$ such that r and s are quadratic residues of each other, then $N(\epsilon_d) = -1$.

Proof. If $N(\epsilon_d) = 1$, then by Corollary I.1, $d = rs$ with $r > 1$, $s > 1$ for some r and s such that $a^2r - b^2s = \pm 4$ is solvable. If a and b are odd, it follows at once that they are quadratic residues of each other. If a and b are even, then $\left[\frac{a}{2}\right]^2 r - \left[\frac{b}{2}\right]^2 s = \pm 1$ is solvable. From the form of the prime factors of r and s, it follows immediately that r and s are quadratic residues of each other. □

As a special case of the above we have the following result.

Corollary I.4. If $p \equiv 5 \pmod 8$ is prime, then $N(\epsilon_{2p}) = -1$.

Proof. Since $\left[\frac{2}{5}\right] = -1$, $d = 2p$ has no factorization as described in Theorem I.9. Thus $N(\epsilon_{2p}) = -1$. □

For example $d = 10 = 2 \cdot 5$ satisfies $N(\epsilon_d) = N(3 + \sqrt{10}) = -1$. However if $d = 82 = 41 \cdot 2$, then $\left[\frac{41}{2}\right] = \left[\frac{2}{41}\right] = 1$, whereas $N(\epsilon_{82}) = N(9 + \sqrt{82}) = -1$. This shows that Theorem I.9 gives only sufficient but not necessary conditions for $N(\epsilon_d) = -1$.

Section 5 Divisibility Properties of Solutions to Pell's Equation

Let $\epsilon_d = \frac{T + U\sqrt{d}}{2}$, and $\epsilon_d^n = \frac{T_n + U_n\sqrt{d}}{2}$ for $n \in \mathbb{Z}$. Consider the sequences $\{T_n\}_{n\in\mathbb{Z}}$ and $\{U_n\}_{n\in\mathbb{Z}}$. For $n = 0$ we have $T_n = 2$ and $U_n = 0$. Also, $T_{-n} = \pm T_n$ and $U_{-n} = \pm U_n$ holds for $n \geq 1$. Thus, consider instead the sequences $\{T_n\}_{n\geq 1}$ and $\{U_n\}_{n\geq 1}$, which we will denote by $\{T_n\}$ and $\{U_n\}$. These two sequences have been studied in great detail, e.g. see [23], [29], and the theory of these two sequences has been generalized to the theory of second order linearly recurrent sequences, and Lucas-Lehmer Theory.

A second order linearly recurrent sequence is a sequence $\{W_n\}_{n\geq 1}$ which satisfies the linearly recurrence relation $W_{n+2} = aW_{n+1} + bW_n$ for some $a,b \in \mathbb{Z}$, such that no integer c exists for which $W_{n+1} = cW_n$ for all $n \geq 1$. We will see that the sequences $\{T_n\}$ and $\{U_n\}$ satisfy these criteria.

In Lucas-Lehmer Theory, a polynomial $x^2 - Px + Q$ is considered, with P and Q relatively prime integers, and $P^2 - 4Q$ a non-square positive integer. If a and b are the roots, then the sequences $X_n = \frac{a^n - b^n}{a - b}$ and $Y_n = a^n + b^n$ are considered. Given $\epsilon_d = \frac{T + U\sqrt{d}}{2}$, then the polynomial $x^2 - Tx = N(\epsilon_d)$ yields $a = \frac{T + U\sqrt{d}}{2}$ and $b = \frac{T - U\sqrt{d}}{2}$, and hence the sequences $\{X_n\}_{n\geq 1}$ and $\{Y_n\}_{n\geq 1}$ defined above correspond to the sequences $\left\{\frac{U_n}{U_1}\right\}_{n\geq 1}$ and $\{T_n\}_{n\geq 1}$ respectively. Many of the theorems developed in this section hold for sequences obtained via the Lucas-Lehmer theory. We will not go into any

more detail with respect to the Lucas-Lehmer Theory. We mentioned the above to show the connection with our sequences $\{T_n\}$ and $\{U_n\}$.

The most widely studied sequence of this type is the Fibonacci sequence defined by $f_1 = f_2 = 1$ and $f_{n+2} = f_{n+1} + f_n$ for $n \geq 1$. It turns out that $\{f_n\}_{n\geq 1}$ corresponds to the sequence $\{U_n\}$ for $d = 5$. The corresponding sequence $\{T_n\}$ is the Lucas sequence $\{L_n\}$ which is defined by $L_1 = 1$, $L_2 = 3$, and $L_{n+2} = L_{n+1} + L_n$ for $n \geq 1$.

We first give a list of some elementary yet important properties of $\{T_n\}$ and $\{U_n\}$.

Theorem I.13. Let $\epsilon_d = \frac{T + U\sqrt{d}}{2}$ and $\epsilon_d^n = \frac{T_n + U_n\sqrt{d}}{2}$ for $n \geq 1$, and $N = N(\epsilon_d)$. Then the following properties hold.

(a) $T_{2n} = T_n^2 - 2N^n$, $U_{2n} = T_n U_n$

(b) $T_k = T_{k-n}T_n - N^n T_{k-2n}$, $U_k = U_{k-n}T_n - N^n U_{k-2n}$ for $k \geq 2n$

(c) $T_{kn} \equiv (-N^n)^{\frac{k-1}{2}} kT_n \pmod{T_n^2}$ for $k \geq 1$, k odd

(d) $U_{kn} \equiv (N^n)^{\frac{k-1}{2}} kU_n \pmod{U_n^2}$ for $k \geq 1$, k odd

(e) $T_n | T_{nk}$ for $k \geq 1$, k odd

(f) $U_n | U_{kn}$ for $k \geq 1$. □

We omit the proof of Theorem I.13 as it amounts to several tedious calculations.

With these elementary properties established, we can obtain some more properties which are quite interesting. First we note the significance of property (b). If we put $n = 1$, we get the recurrence

formulae

$$T_n = T_1 T_{n-1} - N(\epsilon_d) T_{n-2} \tag{1}$$

$$U_n = T_1 U_{n-1} - N(\epsilon_d) U_{n-2} \tag{2}$$

From properties (a) and (b) with $n = 1$, we get $T_2 = T_1^2 - 2N(\epsilon_d)$ and $U_2 = T_1 U_1$. It is easy to see that no constant c exists for which $T_{n+1} = cT_n$ or $U_{n+1} = cU_n$ holds for all n. Thus $\{T_n\}$ and $\{U_n\}$ are shown to be second order linearly recurrent sequences.

Before proceeding to the divisibility properties of $\{T_n\}$ and $\{U_n\}$, we first state a lemma. We know that

$$\frac{T_{kn} + U_{kn}\sqrt{d}}{2} = \left[\frac{T_k + U_k\sqrt{d}}{2}\right]^n \quad \text{for } k,n \geq 1, \text{ and it is easy to see that}$$

$$\frac{T_{kn} - U_{kn}\sqrt{d}}{2} = \left[\frac{T_k - U_k\sqrt{d}}{2}\right]^n \quad \text{for } k,n \geq 1.$$

Combining these two equations we obtain

$$T_{nk} = \left[\frac{T_k + U_k\sqrt{d}}{2}\right]^n + \left[\frac{T_k - U_k\sqrt{d}}{2}\right]^n$$

and

$$U_{nk}\sqrt{d} = \left[\frac{T_k + U_k\sqrt{d}}{2}\right]^n - \left[\frac{T_k - U_k\sqrt{d}}{2}\right]^n$$

for $k,n \geq 1$. From the binomial theorem we obtain the following result.

Lemma I.3. For $t,n \geq 1$ the following relations hold;

$$T_{nt} = 2^{1-n} \sum_{k=0}^{\left[\frac{n}{2}\right]} \binom{n}{2k} T_t^{n-2k} U_t^{2k} d^k$$

$$U_{nt} = 2^{1-n} \sum_{k=0}^{\left[\frac{n+1}{2}\right]} \binom{n}{2k+1} T_t^{n-2k-1} U_t^{k+1} d^k . \qquad \square$$

See Nagell [46, Theorem 104] for a similar result.

For the rest of this section, we are primarily concerned with the divisibility properties of the sequences $\{T_n\}$ and $\{U_n\}$. The first problem we tackle is how a prime behaves in these sequences. We begin our study with the oddest prime, $p = 2$.

Theorem I.14. (Divisibility of T_n by 2).

If T_1 is odd then $2 | T_n$ if and only if $3 | n$. In this case; if $2^a \| T_3$, then $2^a \| T_{6n+3}$ for $n \geq 0$ and $2 \| T_{6n}$ for $n \geq 1$.

If T_1 is even and $2^a \| T_1$, then $2^a \| T_n$ for n odd and $2 \| T_n$ for n even.

Proof. The first part of the theorem is a restatement of Proposition I.4. Assume T_1 is odd and $2^a \| T_3$, with $a \geq 1$. We first show $2 \| T_{6K}$ for $k \geq 1$. If $k = 1$, then because $T_6 = T_3^2 \pm 2$, it follows that $2 \| T_6$. Also $T_{12} = T_6^2 \pm 2$, which forces $2 \| T_{12}$, and so the result holds for $k = 2$. By the relation $T_{6(k+2)} = T_{6(k+1)} T_6 \pm T_{6k}$ it follows that $2 \| T_{6(k+2)}$ when $2 \| T_{6(k+1)}$ and $2 \| T_{6k}$. The result now follows by induction on k. Now assuming $2^a \| T_3$ and $2^a \| T_{6k-3}$, from the relation $T_{6k+3} = T_{6k} T_3 \pm T_{6k-3}$ it follows that $2^a \| T_{6k+3}$. Thus the result follows by induction on k. The second part of the theorem is proved exactly in the same manner, with the exception that all subcripts are divided by 3. $\square$

The same theorem for the sequence $\{U_n\}$ is similar but has more cases.

Theorem I.15. (Divisibility of U_n by 2).

If U_1 is odd then $2|U_n$ if and only if $3|n$. We now have four cases.

1. If U_1 is odd, $2\|U_3$, and $2^a\|T_3$, then $2\|U_{6k+3}$ for $k \geq 0$ and $2^{a+r+1}\|U_{6k2^r}$ k odd, $r \geq 0$.

2. If U_1 is odd and $2^a\|U_3$, then $2^a\|U_{6k+3}$ for $k \geq 0$, and $2^{a+r+1}\|U_{6k2^r}$ k odd, $r \geq 0$.

3. If U_1 is even, $2\|U_1$, and $2^a\|T_1$, then $2\|U_{2K+1}$ for $k \geq 0$ and $2^{a+r+1}\|U_{k2^{r+1}}$ k odd, $r \geq 0$.

4. If U_1 is even and $2^a\|U_1$, then $2^a\|U_{2k+1}$ for $k \geq 0$ and $2^{a+r+1}\|U_{k2^{r+1}}$ k odd, $r \geq 0$.

Proof. It suffices to prove (1) and (2) since the proofs of (3) and (4) differ only by the fact that all subscripts are divisible by 3.

(1). Assume U_1 is odd, $2^a\|T_3$ where $a \geq 1$. First we show that $2^{a+r+1}\|U_{6k2^r}$ with k odd and $r \geq 0$. Since $U_6 = U_3T_3$, it follows that $2^{a+1}\|U_6$. For odd k, the congruence $U_{6k} \equiv \pm kU_6 \pmod{U_6^2}$ shows that $2^{a+1}\|U_{6k}$. So the result holds for $r = 0$. Assume now that the result holds for $r = t$, i.e. $2^{a+1+t}\|U_{6k2^t}$. By Theorem I.14,

$2\|T_{6k2^t}$, and since $U_{6k2^{t+1}} = T_{6k2^t}U_{6k2^t}$, it follows that $2^{a+1+t+1}\|U_{6k2^{t+1}}$. Thus the result holds for $r = t + 1$, and hence for all $r \geq 0$ by induction. To show $2\|U_{6k+3}$ for $k \geq 0$ we use the relation $U_{6k+3} = U_{6k}T_3 \pm U_{6k-3}$. If $2\|U_{6k-3}$ then it follows that $2\|U_{6k+3}$. The result follows inductively.

(2). Now assume $2^a\|U_3$ with $a \geq 1$ and $2\|T_3$. By the same reasoning as (1), $2^{a+r+1}\|U_{6k2^r}$ for $r \geq 0$ and k odd. Also by the same reasoning as (1), $2^a\|U_{6k+3}$ for all $k \geq 0$. □

Thus we have completely determined how the prime $p = 2$ behaves in the sequences $\{T_n\}$ and $\{U_n\}$ (given that we know how it appears in the first or third terms). We will describe how the odd primes behave, but first we prove the following well-known result of Lehmer [29].

Theorem I.16. If m and n are odd positive integers, then $GCD(T_m,T_n) = T_{GCD(m,n)}$. If m and n are any positive integers, then $GCD(U_m,U_n) = U_{GCD(m,n)}$.

Proof. Let $g = GCD(T_m,T_n)$ and $h = GCD(m,n)$. By Theorem I.3, T_h divides both T_m and T_n, hence T_h divides g. By the Euclidean algorithm write $h = xm + yn$ for some integers x and y, and assume without loss of generality that x is odd and y is even. Since $\frac{T_h + U_h\sqrt{d}}{2} = \left[\frac{T_{mx} + U_{mx}\sqrt{d}}{2}\right]\left[\frac{T_{ny} + U_{ny}\sqrt{d}}{2}\right]$, we have $2T_h = T_{mx}T_{ny} + U_{mx}U_{ny}d$. Since x is odd, $T_m|T_{mx}$, and so $g|T_{mx}$. Since y is even, $U_{2n}|U_{ny}$. Thus $g|T_n|T_nU_n|U_{2n}|U_{ny}$, and so it follows that $g|2T_h$. It follows that $g = T_h$ or $g = 2T_h$, and so we will show that the

latter cannot hold. Referring to Theorem I.14, we have two cases; when T_1 is even and when T_1 is odd. If T_1 is even and $2^a \| T_1$, then because m, n, and h are odd, $2^a \| T_m$, $2^a \| T_n$, and $2^a \| T_h$. It follows that $2^a \| g$ so that $g = 2T_h$ cannot hold. Now assume T_1 is odd, $2^a \| T_3$, and $g = 2T_h$ for a contradiction. It follows that T_m and T_n are even, hence m and n are both odd and divisible by 3. From Theorem I.14, we have $2^a \| T_m$ and $2^a \| T_n$, so that $2^a \| g$. With m and n divisible by 3, h is odd and divisible by 3, hence $2^a \| T_h$ also. This contradicts $g = 2T_h$. In any case $g = T_h$ must hold as desired. For the second part of the theorem we follow the same line of argument as the first part of the proof to obtain $GCD(U_m, U_n) = U_{GCD(m,n)}$ or $GCD(U_m, U_n) = 2U_{GCD(m,n)}$. Referring to each case of Theorem I.15 shows that $GCD(U_m, U_n) = 2U_{GCD(m,n)}$ is not possible, and hence $GCD(U_m, U_n) = U_{GCD(m,n)}$ holds as desired. □

These two facts are used to prove the law of repetition of odd primes, which completely describes how an odd prime behaves in the sequences $\{T_n\}$ and $\{U_n\}$. Lehmer [29, Theorem I.6] proves the law of repetition for the sequence $\{U_n\}$, but here we prove the result for both sequences using the facts obtained so far. We first need two preliminary results.

Lemma I.4. Let $a \geq 1$ and p an odd prime. If $p^a \| T_k$ then $p^{a+1} \| T_{pk}$ for any $k \geq 1$. Similarly if $p^a \| U_k$ then $p^{a+1} \| U_{pk}$ for any $k \geq 1$.

Proof. We invoke Lemma I.3. Since $T_k | T_{pk}$ and $U_k | U_{pk}$ we obtain the identities

$$2^{p-1}\frac{T_{pk}}{T_k} = \sum_{t=0}^{\frac{p-1}{2}} \binom{p}{2t} T_k^{p-2t-1} U_k^{2t} d^t$$

$$2^{p-1}\frac{U_{pk}}{U_k} = \sum_{t=0}^{\frac{p-1}{2}} \binom{p}{2t+t} T_k^{p-2t-1} U_k^{2t} d^t .$$

Since $p \geq 3$ is an odd prime, p^2 divides all terms in the first summation except the last term which is $\binom{p}{p-1} U_k^{p-1} d^{\frac{p-1}{2}} = pU_k^{p-1} d^{\frac{p-1}{2}}$. Since $p|T_k$ and p is an odd prime, p does not divide $U_k^{p-1} d^{\frac{p-1}{2}}$, and so this last term is properly divisible by p, hence so is the sum. It follows that $p^{a+1} \| T_{pK}$. Similarly, if $p^a \| U_K$, then p^2 divides all terms of the second summation except the first term, which is $\binom{p}{1} T_k^{p-1} = pT_k^{p-1}$. Since $p|U_k$, p does not divide T_k, and so this last term is properly divisible by p, hence so is the second summation. It follows that $p^{a+1} \| U_{pk}$. □

Lemma I.5. Let p be an odd prime and $a \geq 1$. If $p^a \| T_k$ and ℓ is odd such that $GCD(p,\ell) = 1$, then $p^a \| T_{k\ell}$. Similarly if $p^a \| U_k$ and ℓ is odd such that $GCD(p,\ell) = 1$, then $p^a \| U_{k\ell 2^r}$ for all $r \geq 0$.

Proof. By the congruence $T_{k\ell} \equiv \pm \ell T_k \pmod{T_k^2}$, it follows that if $p^a \| T_k$ and $GCD(p,\ell) = 1$ then $p^a \| T_{k\ell}$. By the congruence $U_{k\ell} \equiv \pm \ell U_k \pmod{U_k^2}$, it follows that if $p^a \| U_k$ and $GCD(p,\ell) = 1$ then $p^a \| U_{k\ell}$. We proceed by induction on $r \geq 0$. The result holds for $r = 0$. Now assume the result holds for $r = t$, i.e. $p^a \| U_{k\ell 2^t}$. Since $U_{k\ell 2^{t+1}} = U_{k\ell 2^t} T_{k\ell 2^t}$ and p does not divide $T_{k\ell 2^t}$, we have

$p^a \| U_{k\ell 2^{t+1}}$. Thus $p^a \| U_{k\ell 2^r}$ for all $r \geq 0$. □

We can now prove the following result.

Theorem I.17. (The Law of Repetition for odd primes).

Let p be an odd prime and assume $p^a \| T_k$ with $a \geq 1$. Then for all $t \geq 0$ and ℓ odd such that $GCD(p,\ell) = 1$, $p^{a+t} \| T_{k\ell p^t}$. Similarly if $p^a \| U_k$ with $a \geq 1$, then for all $t \geq 0$ and positive integers ℓ with $GCD(p,\ell) = 1$, $p^{a+t} \| U_{k\ell p^t}$.

Proof. We will prove the result for the sequence $\{T_n\}$ only. By Lemma I.5, we have $p^a \| T_{k\ell}$ for all odd ℓ such that $GCD(p,\ell) = 1$. By repeated applications of Lemma I.4, we get $p^{a+t} \| T_{k\ell p^t}$ for any $t \geq 0$. The proof for $\{U_n\}$ is similar. □

Theorem I.17. completely describes how an odd prime behaves in the sequences $\{T_n\}$ and $\{U_n\}$ once it has occurred already. The natural question to now ask is whether or not an odd prime p does occur, and when it does occur, where does it appear first as a divisor of some element in the sequence. Lehmer [29], in his discussion of Lucas functions, completely solves this problem for the sequence $\{U_n\}$, and gives some partial results for the sequence $\{T_n\}$. Before proceeding we need the following result.

Lemma I.6. Let d be a positive square-free integer, and p an odd prime. Let $\epsilon = \left[\frac{d}{p}\right]$ be the Legendre symbol, where $\epsilon = 0$ if $p \mid d$. Then $T_p \equiv T_1 \pmod{p}$ and $U_p \equiv U_1 \epsilon \pmod{p}$.

Proof. From Fermat's little theorem we have $2^p \equiv 2 \pmod{p}$. Thus, by Lemma I.3 we have the sequence of congruences, $2T_p \equiv 2^p T_p \equiv (T_1 + U_1\sqrt{d})^p + (T_1 - U_1\sqrt{d})^p \equiv T_1^p + T_1^p \equiv 2T_1^p \pmod{p}$. Hence it follows that $T_p \equiv T_1^p \pmod{p}$. If $p \mid T_1$ then because $T_1 \mid T_p$ we have $T_p \equiv T_1 \equiv 0 \pmod{p}$. If p does not divide T_1, then again by Fermat's little theorem $T_p \equiv T_1^p \equiv T_1 \pmod{p}$. Similarly, $2U_p \equiv 2^p U_p$

$\equiv \frac{1}{\sqrt{d}} [(T_1 + U_1\sqrt{d})^p - (T_1 - U_1\sqrt{d})^p] \equiv 2U_1^p d^{\frac{p-1}{2}} \pmod{p}$, forcing

$U_p \equiv U_1^p d^{\frac{p-1}{2}} \pmod{p}$. If $p \mid U_1$, then because $U_1 \mid U_p$ we have $U_p \equiv U_1 \epsilon \equiv 0 \pmod{p}$. If p does not divide U_1, then

$U_1^p \equiv U_1 \pmod{p}$ so that $U_p \equiv U_1 d^{\frac{p-1}{2}} \pmod{p}$. If p does not divide

d, then $d^{\frac{p-1}{2}} \equiv \left[\frac{d}{p}\right] \pmod{p}$, and so $U_p \equiv U_1 \epsilon \pmod{p}$. If $p \mid d$, then it can be seen by Lemma I.3 that $p \mid U_p$, and hence $U_p \equiv U_1 \epsilon \equiv 0 \pmod{p}$. □

Using Lemma I.6 we get the next result.

Theorem I.18. For ϵ, d and p as in Lemma I.6, $p \mid U_{p-\epsilon}$.

Proof. It is easy to see that $2U_{p-\epsilon} = \pm(T_\epsilon U_p - T_p U_\epsilon) \equiv \pm(T_\epsilon U_1 \epsilon - T_1 U_\epsilon) \pmod{p}$. If $\epsilon = 1$, then $2U_{p-1} = \pm(T_1 U_1 - T_1 U_1) \equiv 0 \pmod{p}$. If $\epsilon = -1$, then because $T_{-1} = N(\epsilon_d) T_1$ and $U_{-1} = -N(\epsilon_d) T_1$, we have $2U_{p+1} \equiv \pm(T_{-1} U_1 (-1) - T_1 U_{-1}) \equiv \pm(-N(\epsilon_d) T_1 U_1 - T_1(-N(\epsilon_d) U_1)) \equiv \pm(-N(\epsilon_d) T_1 U_1 + N(\epsilon_d)(T_1 U_1) \equiv 0 \pmod{p}$. If $p \mid d$ then

from $U_p \equiv U_1\epsilon \equiv 0 \pmod{p}$ we have $U_{p-\epsilon} \equiv U_p \equiv 0 \pmod{p}$. □

Theorem I.18 is important from two perspectives. First of all, it tells us that every prime divides some term in the sequence $\{U_n\}$, and hence infinitely many terms by Theorem I.13(f). Secondly, Theorem I.18 tells us where we can find a term divisible by p. For example, let $d = 2$ and $p = 5$. In this case, $\left[\frac{d}{p}\right] = -1$, and so 5 divides the term $U_6 = 140$. Unfortunately, 5 also divides $U_3 = 10$ so that our subscript $p-\epsilon$ in Theorem I.18 may not be the smallest subscript α for which $p \mid U_\alpha$. The first subscript $\alpha(p)$ for which $p \mid U_{\alpha(p)}$ is called the rank of apparition of p in the sequence $\{U_k\}$. By Theorem I.18, $\alpha(p)$ always exists. The corresponding rank of apparition of p in the sequence $\{T_n\}$ is denoted by $\beta(p)$, when it exists. We will see that for a given d, infinitely many primes p exist for which $\beta(p)$ does not exist. By Theorem I.18 we have the following result.

Theorem I.19. $\alpha(p)$ divides $p-\epsilon$.

Proof. By Theorem I.16 $GCD(U_{\alpha(p)}, U_{p-\epsilon}) = U_{GCD(\alpha(p),p-\epsilon)}$. Since p divides both $U_{\alpha(p)}$ and $U_{p-\epsilon}$, it follows that p divides $U_{GCD(\alpha(p),p-\epsilon)}$. By the definition of $\alpha(p)$, we have $\alpha(p) \leq GCD(\alpha(p),p-\epsilon)$. But clearly we have $GCD(\alpha(p),p-\epsilon) \leq \alpha(p)$, so that equality holds. It follows that $\alpha(p) \mid p-\epsilon$. □

So $\alpha(p)$ is a divisor of $p-\epsilon$, and although we don't know which one, we have certainly reduced the possible choices for $\alpha(p)$ considerably. When $N(\epsilon_d) = 1$ we can strengthen our result.

Theorem I.20. If $N(\epsilon_d) = 1$, then $\alpha(p)$ divides $\frac{p-\epsilon}{2}$ for p not dividing d. If $p|d$ then $\alpha(p) = 1$ or $\alpha(p) = p$.

Proof. The second statement clearly holds in general. Now assume p does not divide d. From Theorem I.13(a), we have $U_{p-\epsilon} = U_{\frac{p-\epsilon}{2}} T_{\frac{p-\epsilon}{2}} \equiv 0 \pmod{p}$, so it suffices to show $T_{\frac{p-\epsilon}{2}} \not\equiv 0 \pmod{p}$. It is easy to see that $2T_{p-\epsilon} = T_p T_\epsilon - U_p U_\epsilon d$ and hence $2T_{p-\epsilon} \equiv T_1^2 - U_1^2 d \equiv 4 \pmod{p}$, or equivalently, $T_{p-\epsilon} \equiv 2 \pmod{p}$. If $T_{\frac{p-\epsilon}{2}} \equiv 0 \pmod{p}$, then by Theorem I.13(a), $T_{p-\epsilon} = T^2_{\frac{p-\epsilon}{2}} - 2N(\epsilon_d) \equiv 0 - 2 \equiv -2 \pmod{p}$, a contradiction. □

Recall in Theorem I.3, it was stated that Pell's equation $x^2 - dy^2 = 1$ is solvable for any positive square-free integer d. This, together with Theorem I.18 allows us to prove that $x^2 - Ay^2 = 1$ is solvable for any non-square positive integer A.

Proposition I.9. The equation $x^2 - Ay^2 = 1$ is solvable for every non-square positive integer A, and has infinitely many solutions.

Proof. Write $A = 2^a p_1 \ldots p_r\, p_{r+1}^{e_{r+1}} \ldots p_k^{e_k}$ as the prime decomposition of A, with $p_1, \ldots, p_r$ distinct primes, $a \geq 0$, e_i even for $r+1 \leq i \leq k$, and $p_{r+1}, \ldots, p_k$ distinct primes, but not necessarily distinct from $p_1, \ldots, p_r$. Let $\delta = 0$ if a is even and $\delta = 1$ if a is odd. Set $d = 2^\delta p_1 \ldots p_r$, then Theorem I.3 states that ϵ_d exists, and hence $x^2 - dy^2 = 1$ is solvable. Let δ_d be the

fundamental solution to $x^2 - dy^2 = 1$, and write δ_d as $\delta_d = \frac{T + U\sqrt{d}}{2}$, i.e. treat δ_d as the fundamental unit. For $r+1 \leq i \leq k$ set $\epsilon_i = \left[\frac{d}{p_i}\right]$ if p_i does not divide d, and $\epsilon_i = 0$ if $p_i | d$. Put $m = \prod_{r+1}^{k} (p_i - \epsilon_i) p_i^{\frac{e_i}{2} - 1}$. By Theorems I.18 and I.17, $p_{r+1}^{\frac{e_{r+1}}{2}} \ldots p_k^{\frac{e_k}{2}}$ divides U_{km} for all $k \geq 1$. Choose $k_o \geq 1$ divisible by a high enough power of 2 so that $2^{\frac{a-\delta}{2}} | Uk_om$. This can be accomplished by Theorem I.15. Then $U_{k_om} = 2^{\frac{a-\delta}{2}} p_{r+1}^{\frac{e_{r+1}}{2}} \ldots p_k^{\frac{e_k}{2}} \cdot t$ for some $t \geq 1$, and so $T_{k_om}^2 - U_{k_omd}^2 = T_{k_om}^2 - At^2 = 1$, showing that the equation $x^2 - Ay^2 = 1$ is solvable. The last part is trivial. □

Another way to describe the above phenomena is as follows. Let $\{U_n\}$ be any sequence derived from some positive square-free integer d. Let m be any other positive integer. Then $m | U_n$ for some n. This will be useful in the next chapter. Recall that the Fibonacci sequence corresponds to $\{U_n\}$ for $d = 5$. Thus every integer divides some Fibonacci number, and hence divides infinitely many Fibonacci numbers.

It was mentioned earlier that for a given positive square-free integer d, $\beta(p)$, the first appearance of p as a divisor of some term in the sequence $\{T_n\}$, does not exist for infinitely many primes p. We have the following result, which is not found in the literature to the best of our knowledge.

Proposition I.10. Given an odd prime p such that p does not divide the positive square-free integer d, then $\beta(p)$ does not exist if and only if $p|U_k$ for some odd integer k. Hence infinitely many primes exist for which $\beta(p)$ does not exist.

Proof. Suppose $\beta(p)$ does not exist. A simple induction shows $U_{p-\epsilon} = T_{\frac{p-\epsilon}{2}} T_{\frac{p-\epsilon}{4}} \cdots T_{\frac{p-\epsilon}{2^r}} U_{\frac{p-\epsilon}{2^r}}$ where $2^r \| p-\epsilon$. Since $p|U_{p-\epsilon}$ and $\beta(p)$ does not exist, it follows that $p|U_{\frac{p-\epsilon}{2^r}}$, and $\frac{p-\epsilon}{2^r}$ is odd.

Conversely, assume $p|U_k$ for some odd k and that $\beta(p)$ exists. Then $p|T_n$ for some n, and hence $p|U_{2n} = T_n U_n$. Thus $p|GCD(U_k, U_{2n}) = U_{GCD(k,2n)}$. Since k is odd, it can be seen that $GCD(k,2n)$ divides n, and so $p|U_n$. But then $p|GCD(T_n, U_n)|4$, contradicting the fact that p is an odd prime. To prove the last part, let $P = \{p$ is an odd prime such that p does not divide $U_1 d\}$. For $p,q \in P$, $p \neq q$, $GCD(U_p, U_q) = U_1$, so that $GCD\left[\frac{U_p}{U_1}, \frac{U_q}{U_1}\right] = 1$.

Also for $p \in P$ we have $GCD\left[\frac{U_p}{U_1}, U_1\right] = 1$ by Theorem I.17. So for each $p \in P$, there exists an odd prime, p', such that $p' | \frac{U_p}{U_1}$ and p' does not divide U_1, and p' does not divide $\frac{U_q}{U_1}$ for any other $q \in P$. Let $P' = \{p';\ p \in P\}$, then we have a bijection $f: P \to P'$ by $f(p) = p'$. Since P is infinite, so is P'. Since for each $p' \in P'$ we have $p'|U_p$ with p an odd subscript, it follows that $\beta(p')$ does not exist for any $p' \in P'$. □

Recall that the Lucas sequence corresponds to $\{T_n\}$ for $d = 5$. Hence infinitely many primes do not divide any Lucas number.

Theorem I.21. Let d be a positive square-free integer. Then $N(\epsilon_d) = 1$ if and only if a prime $p \equiv 3 \pmod 4$ divides U_k for some odd subscript k.

Proof. Assume $N(\epsilon_d) = 1$. If d is divisible by a prime $p \equiv 3 \pmod 4$ then $p \mid U_p$. Assume that $d = 2^{\delta} p_1 \ldots p_k$ with $\delta \in \{0,1\}$ and $p_i \equiv 1 \pmod 4$ for $1 \leq i \leq k$. Choose a prime q such that $q \equiv 1 \pmod{p_i}$ for $1 \leq i \leq k$ and $q \equiv 7 \pmod 8$. Then $\left[\frac{2}{q}\right] = \left[\frac{p_i}{q}\right] = 1$ for $1 \leq i \leq k$, and so $\epsilon = \left[\frac{d}{q}\right] = 1$. From our assumption that $N(\epsilon_d) = 1$, $q \mid U_{\frac{q-\epsilon}{2}}$ by Theorem I.20, and in fact $q \mid U_{\frac{q-1}{2}}$ since $\epsilon = 1$. Since $\frac{q-1}{2} \equiv 3 \pmod 4$ is odd, we have found our subscript k.

For the converse, assume that $N(\epsilon_d) = -1$. Then for k odd we have $T_k^2 + 4 = U_k^2 d$. Following the proof of Theorem I.6, it follows that U_k is divisible only by primes $p \equiv 1 \pmod 4$, contrary to our assumption. □

As a corollary, we can prove the following generalization of Theorem I.20 which was proved by Lehmer [29] and Motada [44].

Corollary I.5. Let $\epsilon = \left[\frac{d}{p}\right]$ where d is a positive square-free integer and p is an odd prime not dividing $2TUd$ with $\epsilon_d = \frac{T + U\sqrt{d}}{2}$.

If $\left[\frac{N(\epsilon_d)}{p}\right] = -1$ then p divides $T_{\frac{p-\epsilon}{2}}$, otherwise p divides $U_{\frac{p-\epsilon}{2}}$.

Proof. By Theorem I.18 $p \mid U_{p-\epsilon} = U_{\frac{p-\epsilon}{2}} T_{\frac{p-\epsilon}{2}}$. Assume $\left[\frac{N(\epsilon_d)}{p}\right] = -1$, then it follows that $N(\epsilon_d) = -1$ and $p \equiv 3 \pmod 4$. If $\epsilon = 1$, then $U_{\frac{p-\epsilon}{2}}$ has odd subscript, and so, because $N(\epsilon_d) = -1$, Theorem I.21 shows that p must divide $T_{\frac{p-\epsilon}{2}}$. Now assume $\epsilon = -1$, and suppose p divides $U_{\frac{p-\epsilon}{2}} = U_{\frac{p+1}{2}}$. It follows that $T_{\frac{p+1}{2}} \equiv \pm 2 \pmod p$ and furthermore that $T_{p+1} \equiv 2 \pmod p$, by Theorem I.13(a). By Lemma I.6 we obtain the sequence of congruences $4 \equiv 2T_{p+1} \equiv T_p T_1 + U_p U_1 d \equiv T_1^2 + U_1^2 d\epsilon \equiv T_1^2 - U_1^2 d \equiv -4 \pmod p$. This contradicts the fact that p is an odd prime. Thus p divides $T_{\frac{p-\epsilon}{2}}$. If $\left[\frac{N(\epsilon_d)}{p}\right] = 1$ then there are two possibilities. The first is that $N(\epsilon_d) = 1$, in which case Theorem I.20 shows p divides $U_{\frac{p-\epsilon}{2}}$. The other case is $N(\epsilon_d) = -1$ and $p \equiv 1 \pmod 4$. By way of contradiction, assume $T_{\frac{p-\epsilon}{2}} \equiv 0 \pmod p$. If $\epsilon = 1$, then $p \mid T_{\frac{p-1}{2}}$ and it follows by Theorem I.13(a) that $T_{p-1} \equiv -2 \pmod p$. It is easy to see that $2T_{p-1} = U_p U_1 d - T_p T_1$ and so $-4 \equiv U_p U_1 d - T_p T_1 \equiv \epsilon U_1^2 d - T_1^2 \equiv -(T_1^2 - U_1^2 d) \equiv 4 \pmod p$ by Lemma I.6, contradicting the fact that p is an odd prime. If $\epsilon = -1$ then $p \mid T_{\frac{p+1}{2}}$ and so $T_{p+1} \equiv 2 \pmod p$.

Thus $4 \equiv 2T_{p+1} \equiv T_p T_1 + U_p U_1 d\epsilon \equiv T_1^2 - U_1^2 d \equiv -4 \pmod{p}$, yielding the same contradiction. In either case we see that $p \mid U_{\frac{p-\epsilon}{2}}$. □

In [44], Motada also discusses whether p divides $T_{\frac{p-\epsilon}{2^k}}$ or $U_{\frac{p-\epsilon}{2^k}}$ in terms of power residues. It is not within the scope of our discussion to do this. E. Lehmer [30] has studied criteria for p to divide $T_{\frac{p-\epsilon}{3}}$ or $U_{\frac{p-\epsilon}{3}}$.

C H A P T E R T W O

Section 1 The Diophantine Equations $mx^2 - ny^2 = \pm 1, \pm 4$

The equations of the title are closely related to the Pell equations $x^2 - mny^2 = \pm 1, \pm 4$, as was seen in Section 4 of Chapter I. In our discussion we will assume m and n are positive square-free integers with no common factor. D.T. Walker [73] has given an overview of these equations, and most of the results of this section can be found therein. We will be discussing integer solutions to these equations when they exist, and how they are related to solutions of the Pell Equations $x^2 - mny^2 = \pm 1, \pm 4$. For reference purposes, we will label the equations as

(1)	$mx^2 - ny^2 = 4$	(1a)	$mx^2 - ny^2 = -4$
(2)	$mx^2 - ny^2 = 1$	(2a)	$mx^2 - ny^2 = -1$
(3)	$x^2 - mny^2 = 4$	(3a)	$x^2 - mny^2 = -4$
(4)	$x^2 - mny^2 = 1$	(4a)	$x^2 - mny^2 = -1$.

Definition II.1. An element $\frac{x\sqrt{m} + y\sqrt{n}}{2}$ is a solution to (1), resp. (1a), if $x^2m - y^2n = 4$, resp. -4.

Definition II.2. An element $\alpha = \frac{x\sqrt{m} + y\sqrt{n}}{2}$ is a solution to (2), resp. (2a), if α is a solution to (1), resp. (1a), and both x and y are even.

From these definitions, we see that any solution to (2), resp. (2a), is also a solution to (1), resp. (1a). Without loss of generality we will henceforth concentrate mainly on the solvability of (1)

and (1a).

Definition II.3. A solution $\alpha = \frac{x\sqrt{m} + y\sqrt{n}}{2}$ to (1), resp. (1a), is called a completely positive solution to (1), resp. (1a), if $x > 0$ and $y > 0$.

The following two results are similar to Propositions I.2 and I.3, hence the proofs are omitted.

Proposition II.1. An element α is a completely positive solution to (1) or (1a) if and only if $\alpha > 1$. □

Proposition II.2. Let $\alpha = \frac{x\sqrt{m} + y\sqrt{n}}{2}$ and $\beta = \frac{a\sqrt{m} + b\sqrt{n}}{2}$ both be completely positive solutions to one of the equations (1) or (1a). Then the following three conditions are equivalent;

1. $\alpha < \beta$
2. $x < a$
3. $y < b$. □

Clearly when solutions to (1), resp. (1a), exist, then so do completely positive solutions to (1), resp. (1a). To see this, if $\frac{x\sqrt{m} + y\sqrt{n}}{2}$ is a solution to (1), resp. (1a), then $\frac{|x|\sqrt{m} + |y|\sqrt{n}}{2}$ is a completely positive solution to (1), resp. (1a). The completely positive solution $\frac{x\sqrt{m} + y\sqrt{n}}{2}$ to (1), resp. (1a), with x minimal will be called the fundamental solution to (1), resp. (1a), and will be denoted by $\tau_{m,n}$. It turns out that at most one of the two equations (1) and (1a) is solvable, so that no confusion will arise.

Our main result of this section is to prove that $\tau_{m,n}^2 = \epsilon_{mn}$ when $\tau_{m,n}$ exists, and so $\tau_{m,n}$ satisfies the τ of condition (1) of Theorem I.7. To prove this result, we need some preliminary results whose proofs amount to tedious calculations, and so are omitted. First note that if (1) or (1a) is solvable, then $N(\epsilon_{mn}) = 1$ by Theorem I.7, and so equation (3a) is not solvable.

Lemma II.1. If α is a (completely positive) solution to (1), resp. (1a), and β is a (completely positive) solution to (3), then $\alpha \bullet \beta$ is a (completely positive) solution to (1), resp. (1a). □

Lemma II.2. If α and β are (completely positive) solutions to (1), resp. (1a), then $\alpha \bullet \beta$ is a (completely positive) solution to (3). □

Before proceeding, we note that an element α of the form $\alpha = \frac{x\sqrt{m} + y\sqrt{n}}{2}$ with $x \neq 0$ and $y \neq 0$ can't be written in the form $\frac{a + b\sqrt{mn}}{2}$, and hence is not an element of $\theta(\sqrt{mn})$. See Nagell [45].

Theorem II.1. If $\tau_{m,n}$ exists, then $\tau_{m,n}^2 = \epsilon_{mn}$.

Proof. Assume $\tau_{m,n}$ exists. From Lemma II.2, $\tau_{m,n}^2$ is a completely positive solution to (3), and so $\tau_{m,n}^2 = \epsilon_{mn}^k$ for some $k \geq 1$. If k is even, then $\tau_{m,n} = \epsilon_{mn}^{k/2} \in Q(\sqrt{mn})$ which contradicts our discussion above. Thus k is odd, say $k = 2\ell + 1$ for some $\ell \geq 0$. We have $\tau_{m,n}^2 = (\epsilon_{m,n}^{\ell})^2 \epsilon_{mn}$, and so $(\tau_{m;n}\epsilon_{mn}^{-\ell})^2 = \epsilon_{mn}$. It follows that $\tau_{m,n}\epsilon_{mn}^{-\ell} > 1$ and is a solution to (1) or (1a) by Lemma II.1. From Proposition II.1 $\tau_{m,n}\epsilon_{mn}^{-\ell}$ is a completely positive solution to (1) or (1a). From our definition of $\tau_{m,n}$ and Proposition II.2, it follows

that $\tau_{m,n} \leq \tau_{m,n}\epsilon_{mn}^{-\ell}$, and hence $1 \leq \epsilon_{mn}^{-\ell}$. Since $\epsilon_{mn} > 1$ we know $\epsilon_{mn}^{-\ell} \leq 1$, and so $\epsilon_{mn}^{-\ell} = 1$ must hold. This shows that $\ell = 0$ and $k = 1$. □

Theorem II.2. One of equations (1) or (1a) is not solvable.

Proof. If $\tau_{m,n}$ does not exist, then neither (1) nor (1a) is solvable. Assume now that $\tau_{m,n}$ exists and without loss of generality is a solution to (1). For contradiction assume α is a solution to (1a). A calculation shows $\tau_{m,n} \bullet \alpha$ is a solution to (3a), and hence $N(\epsilon_{mn}) = -1$. Since $\tau_{m,n}^2 = \epsilon_{mn}$, $\tau_{m,n}$ satisfies the τ of condition (I) of Theorem I.7, and hence $N(\epsilon_{mn}) = 1$, a contradiction. Thus no such α exists, and hence (1a) is not solvable. □

The following result is a structure theorem for all solutions to (1), resp. (1a), when they exist.

Theorem II.3. Assume $\tau_{m,n}$ exists and is a solution to (1), resp. (1a). Then (1), resp. (1a), has infinitely many solutions which correspond to the set $\{\pm\tau_{m,n}^{2k+1} ; k \in \mathbb{Z}\}$. The set of completely positive solutions is $\{\tau_{m,n}^{2k+1} ; k \geq 0\}$. We also have $\mathcal{U}_{mn} = \{\pm\tau_{m,n}^{2k} ; k \in \mathbb{Z}\}$.

Proof. It is clear that any element of the form $\pm\tau_{m,n}^{2k+1}$ with $k \in \mathbb{Z}$ is a solution to (1), resp. (1a). Conversely, by the argument used in the proof of Theorem II.1, any solution to (1), resp. (1a), will be of the form $\pm\tau_{m,n}^{2k+1}$. This proves the first part of the theorem. The second part of the theorem follows directly from Proposition II.1. The

last part of the theorem follows from Theorem I.3. □

We are often interested in the situation where a solution $\alpha = \frac{x\sqrt{m} + y\sqrt{n}}{2}$ of (1), resp. (1a), is also a solution to (2), resp. (2a); i.e. when x and y are even. The following result is similar to Proposition I.4, so we omit the proof.

Proposition II.3. Assume $\tau_{m,n} = \frac{A_1\sqrt{m} + B_1\sqrt{n}}{2}$ exists. For $k \in \mathbb{Z}$, k odd, set $\tau_{m,n}^{k} = \frac{A_k\sqrt{m} + B_k\sqrt{n}}{2}$. If A_1 and B_1 are even, then A_k and B_k are even for every k. If A_1 and B_1 are odd, then $mn \equiv 5 \pmod 8$ and A_k and B_k are even if and only if $k \equiv 0 \pmod 3$. □

For example, $\tau_{3,7} = \frac{\sqrt{3} + \sqrt{7}}{2}$, while $\tau_{3,7}^{3} = 3\sqrt{3} + 2\sqrt{7}$. If $\tau_{m,n} = \frac{x\sqrt{m} + y\sqrt{n}}{2}$ with x and y even, then $\tau_{m,n}$ will be called the fundamental solution to (2), resp. (2a). If x and y are odd, $\tau_{m,n}^{3}$ will be the fundamental solution to (2), resp. (2a). In the example above, $\tau_{3,7}^{3} = 3\sqrt{3} + 2\sqrt{7}$ is the fundamental solution to $3x^2 - 7y^2 = -1$, while $\tau_{3,7} = \frac{\sqrt{3} + \sqrt{7}}{2}$ is the fundamental solution to $3x^2 - 7y^2 = -4$. In our discussion of differences of non-square powerful numbers in Chapter III, we will be mainly concerned with solutions to (2) or (2a).

Heretofore we have needed to use the notation $\tau_{m,n}$ as opposed to τ_{mn} for $d = mn$ might admit another factorization $d = rs$ such that $rx^2 - sy^2 = \pm 1, \pm 4$ might be solvable. In this instance we show that

this is not possible, and hence the notation τ_{mn} can replace $\tau_{m,n}$.

Theorem II.4. For any positive square-free integer d, there is at most one non-trivial factorization $d = mn$ such that $\tau_{m,n}$ exists.

Proof. Suppose there exists two non-trivial factorizations $d = mn$ and $d = rs$ such that $\tau_{m,n}$ and $\tau_{r,s}$ exist. Then $\epsilon_d = \tau_{m,n}^2 = \tau_{r,s}^2$, and since both $\tau_{m,n}$ and $\tau_{r,s}$ are positive, $\tau_{m,n} = \tau_{r,s}$. Set $\tau_{m,n} = \frac{x\sqrt{m} + y\sqrt{n}}{2}$ and $\tau_{r,s} = \frac{a\sqrt{r} + b\sqrt{s}}{2}$, then $x\sqrt{m} + y\sqrt{n} = a\sqrt{r} + b\sqrt{s}$. Multiplying this equality through by $\sqrt{m}$ yields $xm + y\sqrt{d} = a\sqrt{rm} + b\sqrt{sm}$. Again by Nagell [44] it follows that $r = m$ or $r = n$, and so $d = rs$ is the same factorization as $d = mn$. □

For example $\tau_{6,5} = \sqrt{6} + \sqrt{5}$, and so neither of $\tau_{2,15}$ or $\tau_{10,3}$ exist, and we may simply write $\tau_{30} = \sqrt{6} + \sqrt{5}$.

Section 2 Special Types of Fundamental Units

A real quadratic field, $Q(\sqrt{d})$, with d square-free, is said to be of Richaud-Degert type if $d = \ell^2 + r$ for some integers $\ell > 0$ and $r \neq 0$ such that $-\ell < r \leq \ell$ and $4\ell \equiv 0 \pmod{r}$. Refer to [11] and [52]. These quadratic fields have been studied in great detail because of certain special characteristics they possess. In terms of the continued fraction expansion of $\sqrt{d}$, which was briefly mentioned in the introductory section of Chapter I, $\sqrt{d}$ has a very short period. Because of this fact, the fundamental unit, ϵ_d can be written explicitly in terms of ℓ and r.

When $Q(\sqrt{d})$ is of Richaud-Degert type, we simply say that d is

of R.D. type. If $|r| = 1$ or 4, d is said to be of narrow R.D. type, otherwise if $|r| \neq 1$ or 4, d is of wide R.D. type.

The purpose of this section is to give formulae for the fundamental units of all quadratic fields of R.D. type. It turns out that we may drop the condition $-\ell < r \leq 4\ell$ upon making the following definitions. Henceforth d is understood to be square-free.

Definition II.4. If $d = \ell^2 + r$ for some integers $\ell > 0$ and $r \neq 0$ such that $4\ell \equiv 0 \pmod{r}$ and $d \neq 5$, d is said to be of extended R.D. type.

Definition II.5. If d is of E.R.D. type with $|r| = 1$ or 4 then d will be said to be of extended narrow R.D. type. Otherwise, when $|r| \neq 1$ or 4 then d is of extended wide R.D. type.

We will see at the end of this section that when d is of extended R.D. type and $N(\epsilon_d) = 1$, then ϵ_d satisfies an interesting criterion which is related to the decomposition of ϵ_d given in Theorem I.7.

To write down explicit formulae for the fundamental units of extended R.D. type quadratic fields, we need two lemmas, the first of which is proved by Nagell [46, Theorem 105].

Lemma II.3. Suppose $\epsilon_d = \frac{T + U\sqrt{d}}{2}$ with T and U even and $N(\epsilon_d) = 1$. If x and y are positive integers satisfying $x^2 - dy^2 = 1$ and $x > \frac{1}{2}y^2 - 1$, then $x + y\sqrt{d} = \epsilon_d$.

Lemma II.4. Suppose $N(\epsilon_d) = 1$. If x and y are positive integers satisfying $x^2 - dy^2 = 4$ and $x \geq 2y^2 - 2$, then $\epsilon_d = \frac{x + y\sqrt{d}}{2}$.

Proof. Clearly if $y = 1$, then $\epsilon_d = \frac{x + y\sqrt{d}}{2}$. Assume $y > 1$. Let $\epsilon_d = \frac{a + b\sqrt{d}}{2}$, and assume by way of contradiction that $y > b \geq 1$, i.e. $\epsilon_d \neq \frac{x + y\sqrt{d}}{2}$. Then $d = \frac{a^2 - 4}{b^2} = \frac{x^2 - 4}{y^2}$ so that $a^2y^2 - b^2x^2 = 4(y^2 - b^2) = f > 0$. Let $ay - bx = f_1$ and $ay + bx = f_2$. Then f_1 and f_2 are positive integers satisfying $f_1f_2 = f$. Thus $x = \frac{f_2 - f_1}{2b} \leq \frac{f - 1}{2b} = \frac{4y^2 - 4b^2 - 1}{2b} < \frac{4y^2 - 4b^2}{2b} = \frac{2y^2 - 2b^2}{b} \leq 2y^2 - 2b^2 \leq 2y^2 - 2$, contradicting our assumption on x and y. □

We can now write down the fundamental units of all extended R.D. types in terms of ℓ and r.

Theorem II.5. Assume d is of extended R.D. type.

1. If d is of extended narrow R.D. type, then
$$\epsilon_d = |r|^{-1/2}(\ell + \sqrt{\ell^2+r}).$$
2. If d is of extended wide R.D. type, then
$$\epsilon_d = |r|^{-1}(2\ell^2 + r + 2\ell\sqrt{\ell^2+r}).$$

Proof. 1. In this case, $|r|^{-1/2}(\ell + \sqrt{\ell^2+r})$ is certainly a completely positive unit in θ_d, and of the form $\frac{T + U\sqrt{d}}{2}$ with $U = 1$ or 2. Since $d \neq 5$ it follows that $|r|^{-1/2}(\ell + \sqrt{\ell^2+r})$ is in fact the fundamental unit of $Q(\sqrt{d})$.

2. Assume now that d is of extended wide R.D. type. A calculation shows that the completely positive unit given is not the square of another unit in $Q(\sqrt{d})$, and so $N(\epsilon_d) = 1$. We now have two

separate cases.

Case 1. r divides 2ℓ.

Set $x = \frac{2\ell^2 + r}{|r|}$ and $y = \frac{2\ell}{|r|}$. Then $x^2 - dy^2 = 1$, and so by Lemma II.3, it suffices to show $x > \frac{1}{2} y^2 - 1$, or equivalently, $\frac{2\ell^2 + r}{|r|} > \frac{1}{2}\left[\frac{2\ell}{|r|}\right]^2 - 1$. Rearranging terms, we see that this is the same as showing $2\ell^2|r| - r|r| > 2\ell^2 - |r|^2$, which clearly holds.

Case 2. r divides 4ℓ but r does not divide 2ℓ.

In this case set $x = \frac{2}{|r|}(2\ell^2 + r)$ and $y = \frac{4\ell}{|r|}$, then x and y are odd positive integers satisfying $x^2 - dy^2 = 4$. Since r divides 4ℓ and r does not divide 2ℓ, it follows that 4 divides r, and since $|r| \neq 4$, we have $|r| \geq 8$. Thus the inequality $4\ell^2|r| + 2r|r| \geq 32\ell^2 - 2|r|^2$ holds. Rearranging this inequality shows that $\frac{2}{|r|}(2\ell^2 + r) \geq 2\left[\frac{4\ell}{|r|}\right]^2 - 2$ holds, hence $x \geq 2y^2 - 2$. By Lemma II.4, $\frac{x + y\sqrt{d}}{2} = \epsilon_d$ as desired. □

It can be seen that the set of extended narrow R.D. type quadratic fields is just the set of narrow R.D. type quadratic fields with $Q(\sqrt{13})$ included. However, the set of wide R.D. type quadratic field is much smaller than the set of extended wide R.D. type quadratic fields.

Example II.1. If $q = 9p + 4$, where p and q are square-free then $d = pq$ is of extended wide R.D. type, but not of wide R.D. type. To see this, we see that $d = (3p)^2 + 4p$ so that $\ell = 3p < 4p = r$. In this case we have $\epsilon_d = \frac{1}{2}(9p + 2 + 3\sqrt{d})$.

The following theorem gives necessary and sufficient conditions for a fundamental unit to be of extended R.D. type with $N(\epsilon_d) = 1$ in terms of the factorization of ϵ_d given in Theorem I.7.

Theorem II.6. Assume $N(\epsilon_d) = 1$, and let $\epsilon_d = \frac{1}{4}(a\sqrt{m} + b\sqrt{n})^2$ or $\epsilon_d = \frac{1}{2}(a\sqrt{m} + b\sqrt{n})^2$ be the factorization of ϵ_d as given in Theorem I.7.

Then d is of extended narrow R.D. type if and only if $a = b = 1$ and d is of extended wide R.D. type if and only if exactly one of a or b is 1 or at least one of a or b is 2.

Proof. ϵ_d will be of one of the following forms, either $\frac{a^2m - 2 + ab\sqrt{mn}}{2}$ or $a^2m - 1 + ab\sqrt{mn}$. Since $a \equiv b \pmod 2$, and $d = mn$ is of extended narrow R.D. type if and only if the coefficient of $\sqrt{d}$ is 1, we see that d is of extended narrow R.D. type if and only if $ab = 1$. This is equivalent to $a = b = 1$. If exactly one of a or b is 1 or at least one of a or b is 2, a trivial calculation yields $d = mn$ to be of extended wide R.D. type. Without loss of generality, assume $a^2m > b^2n$ and $r > 0$. Similar arguments hold for the other possible cases. In this case, we have $\frac{2\ell^2 + r}{r} + \frac{2\ell}{r}\sqrt{\ell^2+r} = \frac{b^2n + 2 + ab\sqrt{mn}}{2}$ or $b^2n + 1 + ab\sqrt{mn}$. In the first case $\frac{4\ell^2 + 2r}{r} = b^2n + 2$, and so $\frac{4\ell^2}{2} = b^2n$, while $\frac{4\ell}{r} = ab$. Thus $b^2n = \frac{4\ell^2}{r} = ab\ell$, and so $bn = a\ell$. Clearly $GCD(bn,a)$ divides 2, so that $a = 1$ or $a = 2$. This shows that exactly one of a or b is 1 or at least one of a or b is 2, for if $b = 1$ and $a = 1$ then d would be of extended narrow R.D. type contradicting the fact that d is already

assumed to be of extended wide R.D. type. Under the different cases of $r < 0$ and $a^2m < b^2n$, we would obtain $b = 1$ or $b = 2$ in exactly the same way. □

Section 3 The Diophantine Equations $x^2 - dy^2 = N, 4N$

Nagell [46, p. 204] and Stolt [61], [62], [63] have studied the diophantine equations

$$x^2 - dy^2 = N \qquad \text{and} \qquad x^2 - dy^2 = 4N$$

respectively, where d is a square-free integer, and N is any non-zero integer. In this section we give an overview of their results as a precursor to the next section, wherein we similarly study the analogous diophantine equations

$$mx^2 - ny^2 = N, 4N.$$

Henceforth d is a square-free positive integer, N is a non-zero integer, and δ is either 0 or 1. We will consider the diophantine equation

$$(5) \quad x^2 - dy^2 = 2^{2\delta}N$$

such that if $\delta = 1$ then $d \equiv 1 \pmod 4$ and a solution $(x,y) = (a,b)$ exists with both a and b being odd integers when any solution exists at all.

If a and b are integers satisfying (5), the element $\dfrac{a + b\sqrt{d}}{2^{\delta}}$ is called a solution of (5).

If $\dfrac{T + U\sqrt{d}}{2^{\delta}}$ is a solution to the Pell equation

(6) $x^2 - dy^2 = 2^{2\delta}$

then $\frac{a_1 + b_1\sqrt{d}}{2^\delta} = \left[\frac{a + b\sqrt{d}}{2^\delta}\right]\left[\frac{T + U\sqrt{d}}{2^\delta}\right]$ is also a solution of (5), and the two solutions, $\frac{a_1 + b_1\sqrt{d}}{2^\delta}$ and $\frac{a + b\sqrt{d}}{2^\delta}$, are called <u>associated</u> solutions of (5). The set of all associated solutions of (5) is called the <u>class</u> of solutions of (5). It can be seen that the class of solutions corresponding to a particular solution $\frac{a + b\sqrt{d}}{2^\delta}$ is the set $\left\{\pm\left[\frac{a + b\sqrt{d}}{2^\delta}\right]\left[\frac{T + U\sqrt{d}}{2^\delta}\right]^k ; k \in \mathbb{Z}\right\}$ where $\frac{T + U\sqrt{d}}{2^\delta}$ is the fundamental solution to (6). It is also easily checked that two solutions, $\frac{a + b\sqrt{d}}{2^\delta}$ and $\frac{a_1 + b_1\sqrt{d}}{2^\delta}$, are associated with each other if and only if the numbers $\frac{aa_1 - bb_1d}{2^\delta N}$ and $\frac{ab_1 - a_1b}{2^\delta N}$ are integers.

Let L be a class of solutions of (5) consisting of the elements $\left\{\frac{a_i + b_i\sqrt{d}}{2^\delta} \text{ for } i \in \mathbb{Z}\right\}$. Then the set of elements $\left\{\frac{a_i - b_i\sqrt{d}}{2^\delta} ; i \in \mathbb{Z}\right\}$ is also a class of solutions of (5), called the <u>conjugate class</u> of L, and denoted $\bar{L}$. In general L and $\bar{L}$ are distinct classes, but when $L = \bar{L}$, L is called an <u>ambiguous class</u>. These will be studied in further detail in Section 5 of this chapter.

Among all solutions $\frac{a + b\sqrt{d}}{2^\delta}$ in a class L, let $\frac{a^* + b^*\sqrt{d}}{2^\delta}$ be the solution in L in which b^* takes on the least non-negative value for b. Furthermore, if L is ambiguous, impose the condition that a^* is non-negative. Then $\frac{a^* + b^*\sqrt{d}}{2^\delta}$ is uniquely determined, and called

the fundamental solution of the class L. It can be seen that $|a^*|$ is the least non-negative value possible for $|a|$ among all solutions $\frac{a + b\sqrt{d}}{2^\delta}$ in L. It is also easy to see that if $a^* = 0$ or $b^* = 0$ or $N = 1$ then the class is ambiguous.

The following theorem gives upper bounds for $|a^*|$ and b^*. For proof see Nagell [46, Theorem 108] and Stolt [61].

Theorem II.7. Let $\frac{a^* + b^*\sqrt{d}}{2^\delta}$ be the fundamental solution of a class L to (5) and $\frac{T + U\sqrt{d}}{2^\delta}$ be the fundamental solution to (6). Then

1. If $\delta = 0$, $N > 0$
$$0 \leq b^* \leq U\sqrt{\frac{N}{2(T+1)}}$$
$$|a^*| \leq \sqrt{\frac{1}{2}N(T+1)}$$

2. If $\delta = 0$, $N < 0$
$$0 \leq b^* \leq U\sqrt{\frac{N}{2(T-1)}}$$
$$|a^*| \leq \sqrt{\frac{1}{2}N(T-1)}$$

3. If $\delta = 1$, $N > 0$
$$0 \leq b^* \leq U\sqrt{\frac{N}{(T+2)}}$$
$$|a^*| \leq \sqrt{N(T+2)}$$

4. If $\delta = 1$, $N < 0$
$$0 \leq b^* \leq U\sqrt{\frac{N}{(T-2)}}$$
$$|a^*| \leq \sqrt{N(T-2)}$$ □

Corollary II.1. The Diophantine Equation (5) has a finite number of classes of solutions. □

Stolt goes on to give precise formulae for the number of classes of solutions of (5) for a given N. It is not our intention to pursue this.

M.J. De Leon [12] and [13] has given necessary and sufficient conditions for a solution of a class to be fundamental. We first note that a solution $\frac{a + b\sqrt{d}}{2^{\delta}}$ is the fundamental solution of a class L if and only if $\frac{-a + b\sqrt{d}}{2^{\delta}}$ is the fundamental solution of the class $\bar{L}$, when L is not ambiguous. Thus we can assume that a and b are non-negative integers.

Theorem II.8. Let $\frac{a + b\sqrt{d}}{2^{\delta}}$ be a solution to (5) with a and b non-negative integers. For $\frac{a + b\sqrt{d}}{2^{\delta}}$ to be a fundamental solution of a class of solutions to (5), it is necessary and sufficient that the following inequalities hold;

1. $a > kb$ with $k = \frac{T + 1}{U}$ when $\delta = 0$ and $N > 0$
2. $b > ka$ with $k = \frac{U}{T - 1}$ when $\delta = 0$ and $N < 0$
3. $a > kb$ with $k = \frac{T + 2}{U}$ when $\delta = 1$ and $N > 0$
4. $b > ka$ with $k = \frac{U}{T - 2}$ when $\delta = 1$ and $N < 0$. □

Example II.2. Let $d = 2$, $N = 7$, $\delta = 0$, then (5) becomes $x^2 - 2y^2 = 7$. This equation is solvable, and $3 + \sqrt{2}$ is a solution. In this case $3 + 2\sqrt{2}$ is the fundamental solution to (6), and so

$k = \frac{3 + 1}{2} = 2$. Now $a = 3$ and $b = 1$, and so $a > kb$ holds so that $3 + \sqrt{2}$ is the fundamental solution of its class. Note that $-3 + \sqrt{2}$ is the fundamental solution of the conjugate class.

Section 4 The Diophantine Equations $mx^2 - ny^2 = N, 4N$.

In this section we let m and n be positive square-free integers, as in Section 1 of this chapter, and N a non-zero integer. Also, δ will be 0 or 1. We will consider the diophantine equation

$$mx^2 - ny^2 = 2^{2\delta}N \tag{7}$$

with $\delta = 1$ only when $mn \equiv 1 \pmod 4$ and x and y are odd integers. Results analogous to those from the previous section will be given here.

If a and b are integers satisfying (7), then the number $\frac{a\sqrt{m} + b\sqrt{n}}{2^{\delta}}$ is called a solution to (7). If $\frac{T + U\sqrt{mn}}{2^{\delta}}$ is a solution to

$$x^2 - mny^2 = 2^{2\delta} \tag{8}$$

then the number $\frac{a_1\sqrt{m} + b_1\sqrt{n}}{2^{\delta}} = \left[\frac{a\sqrt{m} + b\sqrt{n}}{2^{\delta}}\right]\left[\frac{T + U\sqrt{mn}}{2^{\delta}}\right]$ is also a solution to (7), and is called a solution of (7) associated with the solution $\frac{a\sqrt{m} + b\sqrt{n}}{2^{\delta}}$. The set of all associated solutions is called a class of solutions of (7), and it is easily seen that the class of solutions of (7) in which $\frac{a\sqrt{m} + b\sqrt{n}}{2^{\delta}}$ lies is the set

$$\left\{ \pm\left[\frac{a\sqrt{m} + b\sqrt{n}}{2^{\delta}}\right]\left[\frac{T + U\sqrt{mn}}{2^{\delta}}\right]^k : k \in \mathbb{Z} \right\}$$ where $\frac{T + U\sqrt{mn}}{2^{\delta}}$ is the fundamental solution to (8). It can also be seen that two solutions,

$\frac{a\sqrt{m} + b\sqrt{n}}{2^{\delta}}$ and $\frac{a_1\sqrt{m} + b_1\sqrt{n}}{2^{\delta}}$, are associated if and only if the numbers $\frac{aa'm - bb'n}{2^{\delta}N}$ and $\frac{b'a - a'b}{2^{\delta}N}$ are integers.

Let L be a class of solutions of (7) generated by $\frac{a\sqrt{m} + b\sqrt{n}}{2^{\delta}}$. Then the class of solutions of (7) generated by $\frac{a\sqrt{m} - b\sqrt{n}}{2^{\delta}}$ is called the conjugate class of L, and is denoted by $\bar{L}$. In general, L and $\bar{L}$ are distinct, but when they are equal, L is said to be an ambiguous class.

Among all solutions $\frac{a\sqrt{m} + b\sqrt{n}}{2^{\delta}}$ in a class L, let $\frac{a^*\sqrt{m} + b^*\sqrt{n}}{2^{\delta}}$ be the solution in L in which b^* takes on the least possible non-negative value. If the class is ambiguous, impose the condition that a^* is also non-negative. Then $\frac{a^*\sqrt{m} + b^*\sqrt{n}}{2^{\delta}}$ is uniquely determined, and called the fundamental solution of the class L. As before, it can be seen that $a^* = 0$, $b^* = 0$, or $N = \pm 1$ can only occur when the class is ambiguous. It can be seen that $|a^*|$ is the least non-negative value $|a|$ among all solutions $\frac{a\sqrt{m} + b\sqrt{n}}{2^{\delta}}$ in a class. As in Theorem II.7, we can obtain upper bounds for $|a^*|$ and b^*.

Theorem II.9. Let $\frac{a\sqrt{m} + b\sqrt{n}}{2^{\delta}}$ be the fundamental solution to (7) and $\frac{T + U\sqrt{mn}}{2^{\delta}}$ the fundamental solution to (8). Then we have the following inequalities;

1. $|a^*| \leq \sqrt{\frac{(T+1)N}{2m}}$

$0 \leq b^* \leq U\sqrt{\frac{Nm}{2(T+1)}}$ when $N > 0$ and $\delta = 0$.

2. $|a^*| \leq \sqrt{\frac{-(T-1)N}{2m}}$

$0 \leq b^* \leq U\sqrt{\frac{-Nm}{2(T-1)}}$ when $N < 0$ and $\delta = 0$.

3. $|a^*| \leq \sqrt{\frac{(T+2)N}{m}}$

$0 \leq b^* \leq U\sqrt{\frac{Nm}{(T+2)}}$ when $N > 0$ and $\delta = 1$.

4. $|a^*| \leq \sqrt{\frac{-(T-2)N}{m}}$

$0 \leq b^* \leq U\sqrt{\frac{-Nm}{(T-2)}}$ when $N < 0$ and $\delta = 1$.

Proof. As the others are proved in a similar fashion, we will only prove 1. here. Thus $a\sqrt{m} + b\sqrt{n}$ is the fundamental solution of its class, and $a\sqrt{m} + b\sqrt{n})(T - U\sqrt{mn}) = (aT - Ubn)\sqrt{m} + (bT - Uam)\sqrt{n}$ is an associated solution of $a\sqrt{m} + b\sqrt{n}$. If $a \leq 0$ then it is easily checked that $-a\sqrt{m} + b\sqrt{n}$ is the fundamental solution of the class $\bar{L}$. Thus we will assume $a \geq 0$. Now $a^2T^2 = \left[\frac{b^2n + N}{m}\right](1 + U^2mn) = (b^2n + N)\left[\frac{1}{m} + U^2n\right] \geq (b^2n)(U^2n)$, hence $aT \geq bUn$, and so $aT - bUn \geq 0$. Since $a\sqrt{m} + b\sqrt{n}$ is the fundamental solution of its class, it follows that $a \leq aT - bUn$ and so $b^2U^2n^2 \leq a^2(T-1)^2$. From this inequality we obtain $(a^2m - N)\left[\frac{T^2 - 1}{m}\right] \leq a^2(T-1)^2$, and so

$1 - \frac{N}{a^2m} \leq \frac{T-1}{T+1}$. Multiplying through by $T+1$, and rearranging yields $\frac{(T+1)N}{2m} \geq a^2$, and hence $a^* \leq \sqrt{\frac{(T+1)N}{2m}}$. The inequality $b^* \leq U\sqrt{\frac{Nm}{2(T+1)}}$ follows from the above inequality. □

Corollary II.2. The Diophantine equation (7) has a finite number of classes of solutions.

As in Theorem II.8, necessary and sufficient conditions can be given to determine whether a solution of (7) is fundamental or not. We first need the following result.

Lemma II.5. Let $B = \frac{a_o\sqrt{m} + b_o\sqrt{n}}{2^\delta}$ be the fundamental solution of a class L of solutions to (1) such that both $a_o \geq 0$ and $b_o \geq 0$. Let B_k denote $B\epsilon^k$ for $k \in \mathbb{Z}$, where $\epsilon = \frac{T + U\sqrt{mn}}{2^\delta}$ is the fundamental solution to (8). Then the set $\{B_k : k \geq 0\} = \left\{ \frac{a_k\sqrt{m} + b_k\sqrt{n}}{2^\delta} : k \geq 0 \right\}$ is the set of all solutions of (7) in L for which $a_k \geq 0$ and $b_k \geq 0$ for each $k \geq 0$. Moreover $a_{k+1} > a_k$ for each $k \geq 0$.

Proof. It is clear that $a_k \geq 0$ and $b_k \geq 0$ for each $k \geq 0$, and that $a_{k+1} > a_k$ since $2^\delta a_{k+1} = a_kT + b_kUn$ and $T \geq 2$. The class L is precisely the set $\{\pm B\epsilon^k : k \in \mathbb{Z}\}$. Any element of the form $-B\epsilon^k$ with $k \geq 0$ is of the form $\frac{-a_k\sqrt{m} - b_k\sqrt{n}}{2^\delta}$ and hence has negative coefficients. Now consider elements of L of the form $B\epsilon^{-k}$ with $k > 0$. Then this element has the form

$$\left[\frac{a_o\sqrt{m} + b_o\sqrt{n}}{2^\delta}\right]\left[\frac{T_k - U_k\sqrt{mn}}{2^\delta}\right] = \frac{1}{2^{2\delta}}(a_oT_k - b_oU_kn)\sqrt{m} + (b_oT_k - a_oU_km)\sqrt{n}.$$

We will show that one of these coefficients is negative. Suppose that they are both non-negative, $a_oT_k \geq b_oU_kn$ and $b_oT_k \geq a_oU_km$. Because a_o and b_o are the smallest possible non-negative coefficients of a solution in L, it follows that $a_oT_k - b_oU_kn \geq 2^\delta a_o$ and $b_oT_k - a_oU_km \geq 2^\delta b_o$. From these inequalities we obtain $a_o \geq \frac{b_oU_kn}{T_k - 2^\delta}$ and $b_o \geq \frac{a_oU_km}{T_k - 2^\delta}$, and so $b_o \geq \frac{a_oU_km}{T_k - 2^\delta} \geq \frac{b_oU_k^2mn}{(T_k - 2^\delta)^2} > \frac{b_oU_k^2mn}{T_k^2 - 2^{2\delta}} = b_o$, a contradiction. Thus at least one of $a_oT_k - b_oU_kn$ or $b_oT_k - a_oU_km$ is negative, so that $B\epsilon^{-k}$, $k > 0$, has a negative coefficient. Similarly one can show any element of the form $-B\epsilon^k$ with $k \geq 0$ has a negative coefficient, and so the result holds. □

Theorem II.11. Let $\beta = \frac{a\sqrt{m} + b\sqrt{n}}{2^\delta}$ be a solution of (7) in a class L such that $b \geq 0$. Then β is the fundamental solution of the class L if and only if

1. $|a| \geq kb$ with $k = \frac{Un}{T - 1}$ when $\delta = 0$, $N > 0$.
2. $|a| \geq kb$ with $k = \frac{Un}{T - 2}$ when $\delta = 1$, $N > 0$.
3. $b \geq k|a|$ with $k = \frac{Un}{T - 1}$ when $\delta = 0$, $N < 0$.
4. $b \geq k|a|$ with $k = \frac{Un}{T - 2}$ when $\delta = 1$, $N < 0$.

Proof. As the others are proved in a similar fashion, we will only prove 1. here. Also, we will assume that $a \geq 0$ since a solution $\frac{a\sqrt{m} + b\sqrt{n}}{2^{\delta}}$ is a fundamental solution of a class L if and only if $\frac{-a\sqrt{m} + b\sqrt{n}}{2^{\delta}}$ is a fundamental solution of $\bar{L}$, and the inequalities above are identical for a or $-a$. First, assume β is fundamental, and for contradiction, assume $a < kb$.

Thus $N = a^2m - b^2n < k^2b^2m - b^2n = b^2[k^2m-n] = b^2\left[\frac{U^2n^2}{(T-1)^2} - n\right]$.

By Theorem II.9, $\frac{2b^2(T+1)}{U^2m} \leq N < b^2\left[\frac{U^2n^2}{(T-1)^2} - n\right]$. A trivial calculation shows $\frac{2b^2(T+1)}{U^2m} = b^2\left[\frac{U^2n^2}{(T-1)^2} - n\right]$, and hence a contradiction is established.

Now assume $a \geq kb$ and for contradiction assume $a\sqrt{m} + b\sqrt{n}$ is not the fundamental solution of its class. Since $a \geq 0$ and $b \geq 0$, $a\sqrt{m} + b\sqrt{n}$ has the form $(a^*\sqrt{m} + b^*\sqrt{n})(T + U\sqrt{mn})^i$ for some $i \geq 1$. Thus $(a\sqrt{m} + b\sqrt{n})(T - U\sqrt{mn}) = (aT - bUn)\sqrt{m} + (bT - Uam)\sqrt{n}$ is of the form $(a^*\sqrt{m} + b^*\sqrt{n})(T + U\sqrt{mn})^{i-1}$ where $i-1 \geq 0$. By Lemma II.5, it follows that $0 \leq aT - bUn < a$, and so $a < kb$, a contradiction. □

The remarkable aspect of Theorem II.11 is that the constant k never depends on N, but only on the fundamental solution $\frac{T + U\sqrt{mn}}{2^{\delta}}$ to (8).

Example II.3. Let $m = 5$, $n = 3$. Then $U = 1$ and $T = 4$. Assuming

$N > 0$, the coefficient from Theorem II.11 obtained is $k = 1$. Thus a solution (a,b) to $5x^2 - 3y^2 = N$ is fundamental if and only if $a \geq b$. In other words, a solution to $5x^2 - 3y^2 = N$ exists if and only if a solution (a,b) exists with $a \geq b$. For $N = 98$, $5\sqrt{5} + 3\sqrt{3}$ is the fundamental solution, since $a = 5 > 3 = b$.

Section 5 Ambiguous Classes of Solutions to $x^2 - dy^2 = N$

In this section we will find, for a positive square-free integer d, all integers N for which the equation $x^2 - dy^2 = 2^{2\delta}N$ has an ambiguous class of solutions. It turns out that this problem is closely related to the factorization of the fundamental unit, ϵ_d, given in Theorem I.7.

The following result shows that we need only consider those N which are square-free.

Lemma II.6. Let $N = m^2n$ where n is square-free. The equation $x^2 - dy^2 = 2^{2\delta}N$ has an ambiguous class of solution if and only if the equation $x^2 - dy^2 = 2^{2\delta}n$ has one also.

Proof. Let $\alpha = \frac{a + b\sqrt{d}}{2^{\delta}}$ be a solution to $x^2 - dy^2 = 2^{2\delta}N$ and $\epsilon = \frac{T + U\sqrt{d}}{2^{\delta}}$ a unit such that $\alpha\epsilon = \overline{\alpha}$. Then $\alpha^2\epsilon = \alpha(\alpha\epsilon) = \alpha\overline{\alpha} = N = m^2n$, or equivalently, $\alpha^2 = \overline{\epsilon}m^2n$. Thus $\alpha = \sqrt{\overline{\epsilon}}\sqrt{n}m$, and it follows that both a and b are divisible by m. Let $a_1 = \frac{a}{m}$ and $b_1 = \frac{b}{m}$, then $\alpha_1 = \frac{a_1 + b_1\sqrt{d}}{2^{\delta}}$ is a solution to $x^2 - dy^2 = 2^{2\delta}n$ and $\alpha_1\epsilon = \overline{\alpha}_1$. Thus $x^2 - dy^2 = 2^{2\delta}n$ has an ambiguous class of solutions. The

converse is clear, as one simply multiplies solutions of $x^2 - dy^2 = 2^{2\delta}n$ by m to obtain solutions of $x^2 - dy^2 = 2^{2\delta}N$. □

Henceforth we will assume that N is square-free. The following result, due to Nagell [45], gives a sufficient condition for $x^2 - dy^2 = 2^{2\delta}N$ to have an ambiguous class of solutions.

Theorem II.12. Let d be a square-free positive integer and N an integer which divides $2d$. Then $x^2 - dy^2 = 2^{2\delta}N$ has at most one class of solutions, and if this class exists, it is ambiguous. □

We will derive a converse to this theorem, and find all square-free integers N for which the equation $x^2 - dy^2 = 2^{2\delta}N$ has an ambiguous class of solutions. Note that we do not consider $N = \pm d$, since solutions of this type are derived by multiplying the units of $Q(\sqrt{d})$ by $\sqrt{d}$.

Lemma II.7. Suppose $x^2 - dy^2 = 2^{2\delta}N$ has a solution (x_0,y_0) where N is square-free. Then $GCD(y_0,N) = 1$ or 2.

Proof. Let p divide $GCD(y_0,N)$. Then $p|x_0$ and hence p^2 divides both x_0^2 and dy_0^2. It follows that p^2 divides $2^{2\delta}N$, and since N is square-free, $p = 2$. Also, since N is square-free, 2^2 does not divide $GCD(y_0,N)$, forcing $GCD(y_0,N) = 1$ or 2. □

We now prove a converse of Theorem II.12.

Theorem II.13. If $x^2 - dy^2 = 2^{2\delta}N$ has an ambiguous class of solutions, then N divides $2d$.

Proof. Let $\alpha = \frac{a + b\sqrt{d}}{2^{\delta}}$ be a solution to $x^2 - dy^2 = 2^{\delta}N$ and $\epsilon = \frac{T + U\sqrt{d}}{2^{\delta}}$ a unit such that $\alpha = \overline{\alpha}\epsilon$. Then $\alpha^2 = N\epsilon$, and so $\frac{a^2 + b^2d + 2ab\sqrt{d}}{2^{2\delta}} = \frac{NT + NU\sqrt{d}}{2^{\delta}}$. Thus

(1) $a^2 + b^2d = 2^{\delta}NT$

and

(2) $2ab = 2^{\delta}NU$.

Multiplying (1) by $4b^2$ and subtracting (2) squared yields $4b^4d \equiv 0 \pmod{N}$. By Lemma II.7, $GCD(N,4b^4) = 1$ or 2, and so N divides $2d$. □

Thus, to find all square-free integers N for which the equation $x^2 - dy^2 = 2^{2\delta}N$ has an ambiguous class of solutions, it suffices to consider those N which are divisors of $2d$. The following result, proved by Nagell [45], gives a more precise description of the possible values for N and in fact leads us to a nice result connecting ambiguous classes of solutions and the factorization of the fundamental unit discussed earlier.

Theorem II.14. Let d be a positive square-free integer and N a square-free divisor of $2d$ such that $N \neq 1$ and $N \neq \pm d$. Furthermore, if $d \equiv 1 \pmod{4}$, let N be odd.

1. If $x^2 - dy^2 = 2^{2\delta}N$ is solvable for $N = -1$, then it is not solvable for any other possible value N.

2. If $x^2 - dy^2 = 2^{2\delta}N$ is not solvable for $N = -1$, then it is

solvable for exactly two different values for N, say r and s.

In the latter case, the product of these two values is $-d$ unless d is odd and one of r or s is even, in which case the product of these two values is $-4d$. □

This result of Nagell can be restated the following way; in terms of the factorization of the fundamental unit given in Theorem I.7. Again, we make the same assumptions on N as above.

Theorem II.15. Let d be a positive square-free integer, and assume that $N(\epsilon_d) = 1$. Then

1. $\epsilon_d = \tau^2$ where $\tau = \frac{a\sqrt{r} + b\sqrt{s}}{2}$ for some positive integers a,b and $r,s > 1$ such that $a^2r - b^2s = 4$ and $d = rs$ if and only if the equation $x^2 - dy^2 = 2^{2\delta}N$ has an ambiguous class of solutions for precisely the values $N = r$ and $N = -s$ with $GCD(r,s) = 1$ and $r,s > 1$.

2. $\epsilon_d = \frac{1}{2}\tau^2$ where $\tau = a\sqrt{r} + b\sqrt{s}$ for some positive integers a,b,r,s such that $a^2r - b^2s = 2$ and $d = rs$ if and only if the equation $x^2 - dy^2 = 2^{2\delta}N$ has an ambiguous class of solutions for precisely the values $N = 2r$ and $N = -2s$ with $GCD(r,s) = 1$ and $r,s > 1$.

Proof. We only prove (1), as (2) is similar. Let τ^k, k odd, be any solution to $x^2r - y^2s = 4$. Then one can verify that $\tau^k\epsilon_d^{-k} = \tau^{-k}$, hence $(\sqrt{r}\tau^k)\epsilon_d^{-k} = \sqrt{r}\,\tau^{-k}$. It is easy to see that $\sqrt{r}\,\tau^k$ is of the

form $\frac{a_o + b_o\sqrt{rs}}{2^\delta}$ and that $a_o^2 - b_o^2 rs = 2^{2\delta}r$. Thus $x^2 - dy^2 = 2^{2\delta}r$ has an ambiguous class of solutions. Similarly, by multiplying solutions of $x^2r - y^2s = 4$ by $\sqrt{s}$ we see that $x^2 - dy^2 = -2^{2\delta}s$ has an ambiguous class of solutions. By Theorem II.14 we know that these are the only possible values. Clearly $GCD(r,s) = 1$.

Now assume that $x^2 - dy^2 = 2^{2\delta}N$ has an ambiguous class of solutions for precisely the values $N = r$ and $N = -s$. It follows from Theorem II.13 that r divides $2d$ and s divides $2d$. Since $GCD(r,s) = 1$, we further have that r divides d or s divides d. Without loss of generality, assume that r divides d. Thus a solution $\frac{x_o + y_o\sqrt{d}}{2}$ exists to the equation $x^2 - dy^2 = -2^{2\delta}r$ with r dividing d. It follows that r divides x_o, and hence the equation $rx^2 - \left[\frac{d}{r}\right]y^2 = 4$ is solvable. Multiplying a solution of this equation by $\left[\frac{d}{r}\right]$, we see that the equation $x^2 - dy^2 = -2^{2\delta}\left[\frac{d}{r}\right]$ has an ambiguous class of solutions, forcing $\frac{d}{r} = s$, or equivalently, $d = rs$. So the equation $rx^2 - sy^2 = 4$ is solvable with $d = rs$ and $r,s > 1$. Letting τ be the fundamental solution to this equation, we see by Theorem II.1 that $\epsilon_d = \tau^2$. □

We illustrate this theorem by two examples.

Example II.4. Let $d = 15$. Since $\epsilon_d = 4 + \sqrt{15} = \frac{1}{2}(\sqrt{3} + \sqrt{5})^2$, we refer to part (2) of Theorem II.15. It follows that $N = 10$ and $N = -6$ are the only square-free integers, other than $N = 1$ and $N = -15$ of course, which have an ambiguous class of solutions to the

equation $x^2 - 15y^2 = N$. By Lemma II.6, all integers N for which $x^2 - 15y^2 = N$ has an ambiguous class of solutions are of the form m^2, $10m^2$, $-6m^2$ and $15m^2$.

Example II.5. Let $d = 6$. Since $\epsilon_d = 5 + 2\sqrt{6} = (\sqrt{3} + \sqrt{2})^2$, we refer to part (1) of Theorem II.15. It follows that $N = 3$ and $N = -2$ are the only square-free integers, other than $N = 1$ and $N = -6$, for which $x^2 - 6y^2 = N$ has an ambiguous class of solutions.

We have seen in sections 1, 2 and 5 of this chapter how the factorization of the fundamental unit is related to several aspects of the different Pell equations. As to how much more information can be obtained about these and other related equations from this factorization has yet to be determined, and is probably limited. Yet, this information obtained has been informative and leads one to believe that there is more to discover.

CHAPTER THREE

Section 1 Powerful Numbers

In [17], Erdös and Szekeres studied positive integers n satisfying the property that p^i divides n whenever the prime p divides n, where i is a fixed positive integer. Golomb [19], considered the case $i = 2$ and called these numbers Powerful Numbers. Golomb asked many questions concerning the gaps between powerful numbers, and in particular he asked which integers can be written as the difference of two relatively prime powerful numbers. He conjectured that 6 is not the difference of two relatively prime powerful numbers, and that there are infinitely many such numbers.

It turns out that Golomb was wrong. In fact, this chapter will be devoted to showing that every integer is the difference of two relatively prime powerful numbers in infinitely many ways.

An elementary but useful result is the following:

Proposition III.1. The following statements are equivalent.

1. n is a powerful number.
2. $n = x^2y^3$ for some positive integers x,y with y square-free.
3. $n = md^2$ for some positive integers m,d such that $m|d$ and m is square-free.

Proof. (1) $\Rightarrow$ (2).

Let $n = p_1^{e_1} \cdots p_r^{e_r} p_{r+1}^{e_{r+1}} \cdots p_k^{e_k}$ where $e_i \geq 2$ for

$1 \le i \le k$, e_i is even for $1 \le i \le r$, and e_i is odd for $r+1 \le i \le k$. Then $e_i \ge 3$ for $r+1 \le i \le k$, and so let $x = (p_1^{e_1} \cdots p_r^{e_r} p_{r+1}^{e_{r+1}-3} \cdots p_k^{e_{k-3}})^{1/2}$ and $y = p_{r+1} \cdots p_k$. Then y is square-free and $n = x^2y^3$.

(2) $\Rightarrow$ (3). Put $m = y$ and $d = xy$, then the result is trivial.

(3) $\Rightarrow$ (1). Assume p is any prime divisor of $n = md^2$. Certainly if $p|d$, Then $p^2|d^2$, and so $p^2|n$. If $p|m$ then because $m|d$, it follows that $p|d$ also, forcing $p^2|n$. □

By Proposition III.1, we can see that if k is the difference of two powerful numbers, then we have a solution to the diophantine equation $rx^2 - sy^2 = k$ with $r|x$ and $s|y$, and both r and s square-free.

If neither r nor s is 1, then k is said to be the difference of non-square powerful numbers. If exactly one of r or s is 1, k is said to be the difference of a square and a non-square powerful number. If both $r = s = 1$, k is a difference of squares. Since every integer is the difference of squares in only finitely many ways, we do not pursue these types of differences. We will only be considering the first two types of differences described above.

Section 2 Consecutive Powerful Numbers

In finding consecutive powerful numbers, we are looking for solutions to the equations

(1) $rx^2 - sy^2 = \pm 1$ with $r|x$ and $s|y$ and r,s being positive square-free integers, and

(2) $x^2 - dy^2 = \pm 1$ with $d|y$ and d is positive a square-free integer.

Both of these equations have been studied in great detail thus far, and we can easily prove the following result.

Theorem III.1. There exist infinitely many pairs of consecutive powerful numbers.

Proof. Consider the Pell Equation $x^2 - dy^2 = 1$ where d is any non-square powerful number. By Proposition I.9, this equation has infinitely many solutions (x,y). For any such solution, dy^2 is a powerful number so that x^2 and dy^2 are consecutive powerful numbers. □

Example III.1. Let $d = 27 = 3^3$. The fundamental solution of $x^2 - 27y^2 = 1$ is the element $\epsilon_3^3 = 26 + 15\sqrt{3} = 26 + 5\sqrt{27}$. Letting $A_k + B_k\sqrt{27} = (26 + 5\sqrt{27})^k$ for $k \geq 1$, it follows that $A_k^2 - 3^3B_k^2 = 1$ for each such k.

Although we now know that infinitely many pairs of consecutive powerful numbers exist, it is of interest to see how these pairs can be generated from the fundamental solution of $x^2 - dy^2 = \pm 1$ of any quadratic field $Q(\sqrt{d})$.

Theorem III.2. Let d be any positive square-free integer and $T + U\sqrt{d}$ the fundamental solution to $x^2 - dy^2 = \pm 1$. Letting $T_n + U_n\sqrt{d} = (T + U\sqrt{d})^n$ for $n \geq 1$, we have $d|U_n$ if and only if $n \equiv 0 \pmod{d_1}$ where $d_1 = \frac{d}{GCD(U,d)}$.

Proof. A modified form of Lemma I.3 shows that for each $n \geq 1$, $U_n = \sum_{k=0}^{\left[\frac{n+1}{2}\right]} \binom{n}{2k+1} T^{n-2k-1} U^{2k+1} d^k$. Thus $d \mid U_n$ if and only if $nT^{n-1}U \equiv 0 \pmod{d}$. Since $\gcd(T^{n-1}, d) = 1$, this is equivalent to $nU \equiv 0 \pmod{d}$. This is equivalent to $n \equiv 0 \pmod{d_1}$ where d_1 is as defined above. □

Example III.2. Let $d = 5$. The fundamental solution to $x^2 - 5y^2 = \pm 1$ is $2 + \sqrt{5}$. Since $d_1 = d = 5$, we take $k \equiv 0 \pmod 5$. When $k = 5$, $(2 + \sqrt{5})^5 = 682 + 305\sqrt{5}$, and hence $1 = 61^2 \cdot 5^3 - (682)^2$.

Example III.3. Let $d = 46$. The fundamental solution to $x^2 - 46y^2 = \pm 1$ is $24335 + 3588\sqrt{46}$, and in this case $d_1 = \frac{46}{\gcd(46, 3588)} = 1$, so that we merely choose $k \equiv 0 \pmod 1$ to obtain consecutive powerful numbers. When $k = 1$ we have $1 = (24335)^2 - (46)^3 \cdot (78)^2$.

Corollary III.1. There exist infinitely many pairs of consecutive powerful numbers, one of which is a perfect square. Moreover, these types of consecutive powerful numbers can be generated from any given real quadratic field. □

Notice that the pairs of consecutive powerful numbers generated so far are a square and a non-square powerful number. Now we will consider pairs of consecutive non-square powerful numbers. We have the following result which is similar to Theorem III.2.

Theorem III.3. Let r and s be square-free positive integers such that $rx^2 - sy^2 = 1$ is solvable. Let $a\sqrt{r} + b\sqrt{s}$ be the fundamental solution to this equation and $a_k\sqrt{r} + b_k\sqrt{s} = (a\sqrt{r} + b\sqrt{s})^k$ for k odd and $k \geq 1$. Then $a_k \equiv 0 \pmod{r}$ and $b_k \equiv 0 \pmod{s}$ if and only if $k \equiv 0 \pmod{r_1}$ and $k \equiv 0 \pmod{s_1}$ where $r_1 = \frac{r}{GCD(a,r)}$ and $s_1 = \frac{s}{GCD(a,s)}$.

Proof. We will show $a_k \equiv 0 \pmod{r}$ if and only if $k \equiv 0 \pmod{r_1}$. As in the case of Lemma I.3 we have that for k odd, $k \geq 1$,

$$a_k\sqrt{r} = \sum_{i=0} \left[\begin{matrix} k \\ 2i \end{matrix} \right] (a\sqrt{r})^{k-2i} (b\sqrt{s})^{2i} = \left[\sum_{i=0} \left[\begin{matrix} k \\ 2i \end{matrix} \right] a^{k-2i} r^{\frac{k-2i-1}{2}} b^{2i} s^i \right] \sqrt{r}.$$

Thus $a_k \equiv 0 \pmod{r}$ if and only if $kab^{k-1}s^{\frac{k-1}{2}} \equiv 0 \pmod{r}$. Since $GCD(bs,r) = 1$, this is equivalent to $ka \equiv 0 \pmod{r}$. This is equivalent to $k \equiv 0 \pmod{r_1}$ where r_1 is as defined above. The other congruence is proved in exactly the same fashion. □

Example III.4. The fundamental solution to $7x^2 - 3y^2 = 1$ is $2\sqrt{7} + 3\sqrt{3}$. In this case $r_1 = 7$ and $s_1 = 1$ so that we choose $k \equiv 0 \pmod{7}$ to obtain our consecutive non-square powerful numbers. When $k = 7$ we have $(2\sqrt{7} + 3\sqrt{3})^7 = 2637362\sqrt{7} + 4028637\sqrt{3}$ and so $(376766)^2 \cdot 7^3 - (1342879)^2 \cdot 3^3 = 1$.

The following was proved by Walker in [74].

Corollary III.2. There exist infinitely many pairs of consecutive non-square powerful numbers. □

Although there is an abundance of pairs of consecutive powerful

numbers, it is not known whether or not three consecutive powerful numbers exist. This problem is very difficult and even has connections with Fermat's Last Theorem, as will be seen in Chapter IV. At this point we merely give necessary and sufficient conditions in terms of the existence of a special unit in a real quadratic field. Note that four consecutive powerful numbers cannot exist since one of the four consecutive integers will be properly divisible by the prime $p = 2$.

Theorem III.4. (Mollin and Walsh [36]). The following are equivalent statements.

1. There exist three consecutive powerful numbers.
2. There exists a positive square-free integer $d \equiv 7 \pmod 8$ whose fundamental unit is $T + U\sqrt{d}$ with $T \equiv 0 \pmod 4$, and an odd positive integer $k \equiv 0 \bmod \left[\frac{d}{GCD(U,d)} \right]$ such that T_k is a powerful number.

Proof. (1) $\Rightarrow$ (2). Let $x-1$, x, $x+1$ be the three consecutive powerful numbers. Then clearly $x \equiv 0 \pmod 4$. Let $x^2 - 1 = dy^2$ where d is square-free. Since $dy^2 \equiv 15 \pmod{16}$, it follows that $d \equiv 7 \pmod 8$ and that $x + y\sqrt{d} = T_k + U_k\sqrt{d} = (T + U\sqrt{d})^k$ for some $k \geq 1$, where $T + U\sqrt{d}$ is the fundamental unit of $Q(\sqrt{d})$. Since U_K is odd, k must be odd. Since $x^2 - 1 = dy^2 = dU_k^2$ is powerful, it follows from the fact that d is square-free, that $U_k \equiv 0 \pmod d$. Thus $k \equiv 0 \bmod \left[\frac{d}{GCD(U,d)} \right]$ by Theorem III.2. Also $x = T_K$ is a powerful number and since $T_k \equiv 0 \pmod 4$ and k is odd, it follows from Theorem I.14 that $T \equiv 0 \pmod 4$. The converse is clear. □

It seems, for various reasons to be studied in Chapter IV, that the condition (2) of Theorem III.4 can never be satisfied. Thus Mollin and Walsh [36] made the following conjecture.

Conjecture III.1. Three consecutive powerful numbers do not exist.

In a paper by Erdös and Selfridge [16] concerning products of consecutive integers, a conjecture was made which contains Conjecture III.1. Similarly, Schinzel and Tijdeman [56] made a conjecture on powerful values of higher order polynomials which is closely connected with Conjecture III.1. Thus from several different perspectives, the conjecture is believed to be true. The following example illustrates how large a counter-example would be.

Example III.5. Let us suppose a counter-example could be derived from $Q(\sqrt{7})$. Then it would be a unit of the form $(8 + 3\sqrt{7})^{7k}$ where $k \geq 1$. Since $T_7 = 2^3 \cdot 29 \cdot 197 \cdot 2857$, the first possible value of k for which T_{7K} is powerful is $k = 29 \cdot 197 \cdot 2857$. This follows from Theorem I.13(b). So we would have to calculate $(8 + 3\sqrt{7})^{114254287}$.

In sections 3 and 4, we generalize Corollaries III.1 and III.2 respectively. In each of these two sections we will show that the corresponding result on differences of relatively prime powerful numbers exist for every non-zero integer n, instead of just $n = 1$.

Section 3 Differences of Square and Non-Square Powerful Numbers

In this section we will generalize Corollary III.1 and show that every non-zero integer is the difference of two relatively prime powerful numbers in infinitely many ways. Note that it suffices to show that the result holds for either one of n or $-n$.

If P_1 and P_2 are powerful numbers such that $GCD(P_1,P_2) = 1$, then $n = P_1 - P_2$ is said to be the proper difference of P_1 and P_2.

We are primarily concerned with proper differences as the following example illustrates.

Example III.6. $1 = 9 - 8 = 3^2 - 2^2$ is a difference of powerful numbers. By multiplying through by 3^2, we obtain $3^2 = 9 = 3^4 - 2^3 \cdot 3^2$ as a difference of powerful numbers. This way of obtaining 9 as a difference of powerful numbers is uninteresting, and so we will require our differences to be proper from now on.

McDaniel [33] was the first to show that every non-zero integer is the proper difference of two powerful numbers in infinitely many ways. In his proof, all the differences obtained, except for those $n \equiv 2 \pmod 4$, are differences of a square and a non-square powerful number. Vanden Eynden [70] extended the work of McDaniel by considering the case of $n \equiv 2 \pmod 4$, hence showing that every non-zero integer is the proper difference of a square and a non-square powerful number in infinitely many ways. Before proceeding we state a useful result used in [39], which is easily proved by induction on k.

Lemma III.1. Let $T + U\sqrt{d}$ be a solution to $x^2 - dy^2 = \pm 1$ and $T_k + U_k\sqrt{d} = (T + U\sqrt{d})^k$ for $k \geq 1$. Then $T_k \equiv T^k \pmod d$ and

$U_k \equiv kT^{k-1}U \pmod{d}$. □

Lemma III.1 allows us to give sufficient conditions for a non-zero integer n to be a proper difference of a square and a non-square powerful number in infinitely many ways. We prove the following result similar to one found in Mollin and Walsh [39].

Theorem III.5. Let n be a positive integer and suppose there exists a non-square positive integer d such that the following conditions are satisfied.

1. There exist positive integers a and b with $GCD(a,n) = 1$ and $a^2 - b^2d = \pm n$.
2. There exist positive integers T and U such that $T^2 - U^2d = \pm 1$ and $r = GCD(U,d)$ divides b.

Then $a_k + b_k\sqrt{d} = (a + b\sqrt{d})(T + U\sqrt{d})^k$ with $k \equiv -\left[\frac{b}{r}\right] T \left[\frac{aU}{r}\right]^{-1} \left[\bmod \left[\frac{d}{r}\right]\right]$ satisfies $a_k^2 - b_k^2 d = n$, $d \mid b_k$, and $GCD(a_k^2, b_k^2 d) = 1$. In other words, n is the proper difference of the powerful numbers a_k^2 and $b_k^2 d$ for each k in the congruence class given.

Proof. Because of the GCD conditions given, the congruence shown is solvable, and so infinitely many integers k satisfy the congruence. Clearly $a_k^2 - b_k^2 d = \pm n$ holds by the multiplicativity of the Norm function defined in Section 1 of Chapter I. By the definition of a_k and b_k, we have

(1) $a_k = aT_k + bU_kd$

and

(2) $b_k = bT_k + aU_k$.

Thus by Lemma III.1 we have $b_k = bT^k + aT^{k-1}kU \equiv T^{k-1}[bT + akU] \pmod{d}$. Rearranging the congruence shows $bT + akU \equiv 0 \pmod{d}$, thus $b_k \equiv 0 \pmod{d}$ as desired. For the last part, it suffices to show $GCD(a_k,b_kd) = 1$. Multiplying (1) by T_k and (2) by U_kd and then subtracting yields

(3) $\pm a = T_ka_k - U_kdb_k$.

Multiplying (1) by U_k and (2) by T_k and subtracting yields

(4) $\pm b = U_ka_k - T_kb_k$.

If a prime p divides $GCD(a_k,b_k)$, then by (3) and (4), it follows that p divides $GCD(a,b)$, and hence p divides $GCD(a,n) = 1$. Thus $GCD(a_k,b_k) = 1$. From (1) it is clear that $GCD(a_k,d) = 1$, hence $GCD(a_k,b_kd) = 1$. □

For each positive integer n we must now find integers d,a,b,T and U which satisfy conditions (1) and (2) of Theorem III.5. The following table gives the desired integers. We omit the special cases of $n = 2$, 5 and 10 as they are represented by $(d,a,b,T,U) = (7,3,1,8,3)$, $(11,4,1,8,3)$ and $(39,7,1,25,4)$ respectively.

Table III.1.

n	d	a	b	T	U
$4k-1$	$16k^2-8k+5$	$8k^2-6k+2$	$2k-1$	$32k^3-24k^2+12k-2$	$8k^2-4k+1$
$4k+1$ $k>1$	$4k^2-4k-1$	$2k$	1	$4k^2-4k$	$2k-1$
$4k$	$4k^2+1$	$2k+1$	1	$2k$	1
$8k+2$ or $8K-2$ with $3 \mid n$ $k>1$	$(2k-1)^2 \pm 2$	$2k+1$	1	$d \pm 1$	$2k-1$
$8k-2$ and $3 \mid n$	$36k^2-20k+3$	$6k-1$	1	$9d-1$	$3(18k-5)$

We must show that in each case, the conditions (1) and (2) of Theorem III.5 are satisfied. A calculation shows in each case that $a^2 - db^2 = \pm n$ and that $T^2 - U^2 d = \pm 1$. Thus in each case we merely show that $GCD(a,n) = 1 = GCD(U,d)$, and that d is a non-square integer.

Case 1. $n = 4k - 1$.

$d = (4k-1)^2 + 4$, hence a non-square integer. If $p \mid GCD(a,n)$, then $p \mid a - (2k-1)n = 1$. Thus $GCD(a,n) = 1$. Also $d - 2U = 3$ and 3 does not divide d, thus $GCD(U,d) = 1$.

Case 2. $n = 4k + 1$.

$d = (2k-1)^2 - 2$, so d is a non-square integer. $GCD(a,n) = GCD(4k+1,2k) = 1$. Lastly, $d - U^2 = -2$ and d is odd so that $GCD(U,d) = 1$.

Case 3. $n = 4k$.

$d = (2k)^2 + 1$, hence not a square. $GCD(a,n) = GCD(4k,2k+1) = 1$.

Also, $GCD(d,U) = GCD(d,1) = 1$.

Case 4. $n = 8k + 2$ or $n = 8k - 2$ with $k \equiv 1 \pmod 3$.

$d = (2k-1)^2 \pm 2$ is not a square integer. $n - 4a = -2$ and a is odd so that $GCD(a,n) = 1$. Lastly, $d - U^2 = \pm 2$ and U is odd so that $GCD(U,d) = 1$.

Case 5. $n = 8k - 2$ and $k \not\equiv 1 \pmod 3$.

It can be seen that $(6k-2)^2 < d < (6k-1)^2$, so that d is a non-square integer. Since $3n - 4a = -2$ and a is odd, it follows that $GCD(a,n) = 1$. Lastly, it can be seen that $a^2 - 81d = -18$. Since $GCD(d,6) = 1$, it follows that $GCD(U,d) = 1$.

For each positive n, using the values given in Table III.1 and the algorithm of Theorem III.5, we can find infinitely many pairs of relatively prime powerful numbers differing by n, with one of the powerful numbers being a perfect square and the other a non-square powerful number. We state the following result.

Theorem III.6. Every non-zero integer is the proper difference of powerful numbers, one of the powerful numbers being a perfect square, in infinitely many ways. □

We illustrate the procedure by the following two examples.

Example III.7. Let $n = 3$. We refer to the first row of Table III.1 to obtain the values $(d,a,b,T.U) = (13,4,1,18,5)$. So we form the product $(4 + \sqrt{13})(18 + 5\sqrt{13})^k$ with $k \equiv 3 \pmod{13}$. When $k = 3$ we get the element $177823 + 49322\sqrt{13} = 177823 + 3794 \cdot 13\sqrt{13}$. Thus

$3 = 13^3 \cdot (3794)^2 - (177823)^2$.

Example III.8. Let $n = 6$. We refer to the last row of the table. We obtain the values $(d,a,b,T,U) = (19,5,1,170,39)$. So we form the product $(5 + \sqrt{19})(170 + 39\sqrt{19})^k$ with $k \equiv 4 \pmod{19}$. When $k = 4$ we obtain the element $62531004125 + 14344596201\sqrt{19}$ and hence $6 = (62531004125)^2 - 19^3 \cdot (755031379)^2$.

This last example is a counter-example to the conjecture of Golomb mentioned earlier in Section 1 of this chapter.

Section 4 Differences of Non-Square Powerful Numbers

In this section we will generalize Corollary III.2 and show that every non-zero integer is the proper difference of non-square powerful numbers in infinitely many ways.

Mollin and Walsh [38] and McDaniel [34] independently showed the result for all odd integers, while in the same paper McDaniel showed the result for integers $n \equiv 2 \pmod{4}$. McDaniel also showed that for $n \equiv 0 \pmod{4}$, n is a difference of non-square powerful numbers in infinitely many ways, but the differences given are never proper. In [37], Mollin and Walsh attempted to show the result for all even integers, but the result rested upon the existence of a unit $T + U\sqrt{d}$ in $Q(\sqrt{d})$ with $GCD(U,d) = 1$. They incorrectly invoked a theorem of Slavutsky [59], leaving the problem unsolved. In [39], Mollin and Walsh resolved the aforementioned gap in their proof, and thus the result was finally shown to be true for all non-zero integers.

This section follows very much the same format as the previous

section. We first give sufficient conditions for a non-zero integer n to be the proper difference of two non-square powerful numbers in infinitely many ways. This result can be found in [39].

Theorem III.7. Let n be a positive integer and suppose there exist non-square positive integers r and s such that the following conditions hold.

1. There exist positive integers a and b with $GCD(ar,bs) = 1$ and $a^2r - b^2s = \pm n$.

2. There exist positive integers T and U with $GCD(U,rs) = 1$ and $T^2 - U^2rs = \pm 1$.

If $(a_k\sqrt{r} + b_k\sqrt{s}) = (a\sqrt{r} + b\sqrt{s})(T + U\sqrt{rs})^k$ with $k \equiv -(Ta)(Ubs)^{-1} \pmod{r}$ and $k \equiv -Tb(aUr)^{-1} \pmod{s}$, then $a_k \equiv 0 \pmod{r}$, $b_k \equiv 0 \pmod{r}$, $\left[\frac{a_k}{r}\right]^2 r^3 - \left[\frac{b_k}{s}\right]^2 s^3 = \pm n$, and $GCD(a_k^2r, b_k^2s) = 1$. In other words n is the proper difference of two non-square powerful numbers in infinitely many ways.

Proof. Let $T_k + U_k\sqrt{d} = (T + U\sqrt{d})^k$ with k chosen by the congruences given. By the GCD conditions, the congruences are both solvable. Then

$$(1) \quad a_k = aT_k + bsU_k$$

and

$$(2) \quad b_k = bT_k + arU_k .$$

By Lemma III.1, $a_k \equiv aT^k + bskT^{k-1}U \equiv T^{k-1}[aT + bskU] \equiv 0 \pmod{r}$. Similary $b_k \equiv 0 \pmod{s}$. Now suppose a prime p divides

$GCD(a_k^2 r, b_k^2 s)$. Then p divides $GCD(a_k r, b_k s)$. Thus by (1) we obtain

(3) $arT_k + brsU_k = pc_1$

and by (2) we obtain

(4) $bsT_k + arsU_k = pc_2$

for some integers c_1 and c_2. Multiplying (3) by T_K and (4) by rU_K and subtracting yields $p[c_2T_k - c_1rU_k] = \pm ar$. Multiplying (4) by T_k and (3) by sU_k and subtracting yields $p[c_2T_k - c_1sU_k] = \pm bs$. Thus p divides $GCD(ar,bs)$ contradicting our assumption. Thus $GCD(a_k^2 r, b_k^2 s) = 1$ for each k. Lastly $\left[\frac{a_k}{r}\right]^2 r^3 - \left[\frac{b_k}{s}\right]^2 s^3 = a_k^2 r - b_k^2 s = (aT_k + bU_k)^2 r - (bT_k + arU_k)^2 s =$
$(a^2 r - b^2 s)(T_k^2 - rsU_k^2) = \pm n.$ □

Thus by Theorem III.7, it suffices for each non-zero n to find integers (r,s,a,b,T,U) satisfying the conditions given.

We give a table of values as in the previous section. The special cases $n = 1$, 2 or 4 are not listed in the table as they are represented by $(r,s,a,b,T,U) = (11,7,4,5,351,40)$, $(5,3,1,1,4,1)$ and $(11,7,1,1,351,40)$ respectively. Also note that several choices in each class of n modulo 4 are given to ensure that both r and s are non-square integers in at least one choice. In each row, $t \geq 1$ unless otherwise stated.

Table III.2.

n	r	s	a	b	T	U
$2t+1$ $t\not\equiv 2 \pmod 5$	t^2+2t+2	t^2+1	1	1	t^2+t+1	1
$2t+1$ $t\equiv 2 \pmod 5$	2	$2t^2+2t+1$	$t+1$	1	$2t+1$	1
$4t+2$	$2t^2+4t+1$	$2t^2-1$	1	1	$(2t^2+2t-1)^2-1$	$2t^2+2t-1$
$4t+2$ $t\not\equiv 1 \pmod 3$	$2t^2+4t+3$	$2t^2+1$	1	1	$(2t^2+2t+1)^2+1$	$2t^2+2t+1$
$4t+2$ $t\equiv 1 \pmod 3$	$6t^2+8t+3$	$6t^2+4t+1$	1	1	$(18t^2+18t+5)^2+1$	$3(18t^2+18t+5)$
$4t$ t odd	t^2+2t+2	t^2-2t+2	1	1	$\frac{1}{2}(t^6+3t^2)$	$\frac{1}{2}(t^4+1)$
$4t$ t even	$2t^2+2t+1$	$2t^2-2t+1$	1	1	$2t^2$	1
$4t$ t even	$2t^2+3t+1$	$2t^2-t+1$	1	1	$4t^3+2t^2+1$	$2t$
$4t$ t even	$2t^2+t+1$	$2t^2-3t+1$	1	1	$4t^3-2t^2-1$	$2t$

We must show that for each class modulo 4, there is at least one row which satisfies all the conditions of Theorem III.7. Trivial calculations show that $a^2r - b^2s = \pm n$ and $T^2 - U^2rs = \pm 1$ hold in each case. We omit the proofs of all the GCD conditions, as these proofs follow very closely the same type of reasoning as given in the previous section concerning the GCD conditions. It suffices now to show that at least one row, in each class modulo 4, contains both r and s as non-square integers.

Case 1. $n = 2t + 1$, $r = t^2 + 2t + 2$, $s = t^2 + 1$.

In this case, both r and s are squares plus one, hence neither are squares.

Case 2. $n = 2t + 1$, $r = 2$, $s = 2t^2 + 2t + 1$, $t \equiv 2 \pmod 5$.

In this case $s \equiv 8 + 4 + 1 \equiv 3 \pmod 5$, hence r and s are not squares.

Case 3. $n = 4t + 2$, $t \not\equiv 1 \pmod 3$.

In this case either $r = 2(t+1)^2 - 1$ and $s = 2t^2 - 1$, or $r = 2(t+1)^2 + 1$ and $s = 2t^2 + 1$. By considering the Pell equations $x^2 - 2y^2 = \pm 1$, it can be seen that for any given t value, one of the two choices for r and s produces non-square integers.

Case 4. $n = 4t + 2$, $t \equiv 1 \pmod 3$.

By considering r and s modulo 3, it can be seen that both r and s produces non-square integers.

Case 5. $n = 4t$, t odd.

Since $r = (t+1)^2 + 1$ and $s = (t-1)^2 + 1$, r and s are both non-square integers.

Case 6. $n = 4t$, t even.

We consider the last three lines of the table simultaneously. We will show that for a given t value, no two of the s values can be squares. Similarly no two of the r values can be squares for a given t value. Thus at least one of the three rows contains both r and s as non-square integers. Suppose that $2t^2 - k_1 t + 1 = x^2$ and $2t^2 - k_2 t + 1 = y^2$, where $k_1, k_2 \in \{1,2,3\}$ and $k_1 < k_2$. Then $x^2 - y^2 = ct$ where $c = 1$ or 2. It follows that $x + y < 2t$. If $t = 2$, then $r = 2t^2 + 2t + 1 = 13$ and $s = 2t^2 - 2t + 1 = 5$ are non-squares. Now assume that $t \geq 4$. Then it can be seen that $2t^2 - kt + 1 > t^2$ for $k \in \{1,2,3\}$ so that $x > t$ and $y > t$. Thus

$x + y > 2t$ contradicting $x + y < 2t$ obtained earlier. Thus no two s values can simultaneously be squares, and hence at least one of the three lines has both r and s as non-square integers for any given t value.

Using the values of Table III.2 and the algorithm of Theorem III.7, we have proved the following result, which is the main result of [39].

Theorem III.8. Every non-zero integer is the proper difference of two non-square powerful numbers in infinitely many ways. □

We illustrate the procedure in the following two examples.

Example III.9. $n = 3$. We refer to the first row. In this case $(r,s,a,b,T,U) = (5,2,1,1,3,1)$ and so we form the product $(\sqrt{5} + \sqrt{2})(3 + \sqrt{10})^k$ with $k \equiv 1 \pmod{10}$. When $k = 1$, we obtain the element $5\sqrt{5} + 8\sqrt{2}$, and so $3 = 2^7 - 5^3$.

Example III.10. $n = 16$. We refer to the last line of the table. In this case $(r,s,a,b,T,U) = (37,21,1,1,223,8)$ and so we form the product $(\sqrt{37} + \sqrt{21})(223 + 8\sqrt{777})^k$ with $k \equiv 24 \pmod{37}$ and $k \equiv 4 \pmod{21}$ to obtain our desired differences.

CHAPTER FOUR

Section 1 Introduction

Erdös and Szekeres [17] studied positive integers n satisfying the property that $p^k | n$ whenever the prime $p | n$. These are called k-full numbers. Since then, many papers have been published on the special case of 2-full numbers. These are also referred to as squareful numbers, and more recently powerful numbers.

Authors have studied many different properties of powerful numbers. In Chapter III we considered differences of powerful numbers. Other topics on powerful numbers include the distribution of powerful numbers, powerful numbers in arithmetic progression, sums of powerful numbers, and the connection between powerful numbers and the first case of Fermat's Last Theorem.

In this chapter we give an overview of these topics and include some conjectures and open questions on powerful numbers.

We first consider the connection between powerful numbers and Fermat's Last Theorem.

In or about 1637, Pierre de Fermat stated that if n is an integer ≥ 3, then the diophantine equation

$$x^n + y^n = z^n$$

has no solutions in integers x, y, z with $xyz \neq 0$.

It is clear that it suffices to show the result whenever n is a prime p. We denote this by $(FLT)_p$. The problem has been split into two cases;

I. p does not divide xyz.

II. p divides xyz.

We denote these by $(FLTI)_p$ and $(FLTII)_p$ respectively. We will see that the truth of certain conjectures on powerful numbers would imply $(FLTI)_p$ for infinitely many primes p.

We note at this point that Adleman and Heath-Brown [1] have shown that $(FLTI)_p$ does in fact hold for infinitely many primes p.

We then turn our attention to the existence of certain units in quadratic fields possessing special properties. We will see that the non-existence of powerful numbers in certain linearly recurrent sequences has some bearing on $(FLTI)_p$ as shown in Theorem IV.12.

In the last section we discuss some of the aforementioned literature on powerful numbers, in particular, the distribution of, arithmetic progressions of, and sums of powerful numbers.

Section 2. Powerful Numbers and Fermat's Last Theorem

From a result of Granville [20], it is known that the first case of Fermat's Last Theorem, $(FLTI)_p$, is related to the existence of certain powerful numbers in a very strong way. In this section we investigate some of these connections to give sufficient conditions for $(FLTI)_p$ to hold for infinitely many prime exponents.

In 1909 Wieferich [75] proved the following remarkable result.

Theorem IV.1. If $(FLTI)_p$ fails for an odd prime p, then $2^p \equiv 2 \pmod{p^2}$. □

Using Theorem IV.1 and the following Lemma, Granville [20] gave the first connection between powerful numbers and (FLTI).

Lemma IV.1. If $2^p \equiv 2 \pmod{p^2}$ and $p \mid 2^m-1$ for some $m \geq 1$, then $p^2 \mid 2^m-1$.

Proof. Let $2^m-1 = kp$. From $2^p \equiv 2 \pmod{p^2}$, it follows that $2^m \equiv 2^{mp} \equiv (1 + kp)^p \equiv 1 \pmod{p^2}$ by the binomial theorem. □

Lemma IV.2. If $(a,m) = 1$ then $a^{k\phi(m)} \equiv 1 \pmod{m}$ for all $m > 1$, $k \geq 1$. If $a \not\equiv 1 \pmod{m}$ and $a^k \equiv 1 \pmod{m}$, then $GCD(k,\phi(m)) > 1$.

Proof. See [69, p. 74].

Theorem IV.2. (Granville [20]). If three consecutive powerful numbers do not exist, then (FLTI) holds for infinitely many primes.

Proof. Assume that (FLTI) fails for all primes $p > p_o$.

Put $t = \prod_{p \leq p_o} p(p-1)$. We will show that $2^{nt} - 1$ is powerful for all $n \geq 1$. Fix n and assume that q is a prime such that $q \mid 2^{nt}-1$. If $q \leq p_o$, then since $nt \equiv 0 \pmod{\phi(q^2)}$ it follows from Lemma IV.2 that $q^2 \mid 2^{nt}-1$. If $q > p_o$, then by assumption (FLTI) fails for the prime q. Thus $2^q \equiv 2 \pmod{q^2}$ and $q^2 \mid 2^{nt}-1$ by Lemma IV.1. This shows that $2^{nt}-1$ is powerful. Similarly $2^{2nt}-1$ is powerful. Since $2^{2nt}-1 = (2^{nt}-1)(2^{nt}+1)$ and $GCD(2^{nt}-1,2^{nt}+1) = 1$, both $2^{nt} - 1$ and $2^{nt} + 1$ are powerful. So for every $n \geq 1$, $2^{nt}-1$, 2^{nt}, $2^{nt}+1$ are three consecutive powerful numbers. □

In the statement of his theorem, Granville [20] wrote that "if the

conjecture of Mollin and Walsh is true, then there exists an infinite sequence of primes p for which the First Case of Fermat's Last Theorem is true." It should be noted that Erdös [15] had earlier conjectured the non-existence of three consecutive powerful numbers.

Corollary IV.1. If only finitely many triples of three consecutive powerful numbers of the form 2^k-1, 2^k, 2^k+1 exist, then $(FLTI)_p$ holds for infinitely many primes p. □

Under the hypothesis that $(FLTI)_p$ fails for all sufficiently large primes p, we have shown the existence of a large class of powerful integers of the form $2^k - 1$. Under the same hypothesis, we can show that another class of integers of the form $2^k - 1$ is made up of powerful numbers.

Theorem IV.3. Assume that $(FLTI)_p$ fails for all primes $p > p_o$. If k is a positive integer not divisible by any prime $p \leq p_o$, then $2^k - 1$ is powerful.

Proof. Assume k is divisible only by primes $p > p_o$, and let q be a prime such that $q \mid 2^k-1$. By Lemma IV.2, $GCD(q-1,k) > 1$, and we have that $q > p_o$. Thus $(FLTI)_p$ fails for $p = q$, and so $2^q \equiv 2 \pmod{q^2}$. Lemma IV.1 shows that $q^2 \mid 2^k-1$, and hence $2^k - 1$ is powerful. □

Summarizing Theorems IV.2 and IV.3, we have;

Corollary IV.2. If $(FLTI)$ fails for all prime $p > p_o$ and

$t = \prod_{p \le p_0} p(p-1)$, then 2^k-1 is powerful if either $t \mid k$ or $GCD(t,k) = 1$. □

One could conjecture that numbers of the form 2^n-1 are never powerful, and if this were the case, the result of Adleman and Heath-Brown would follow immediately. In fact, A. Schinzel conjectured that infinitely many Mersenne numbers (numbers of the form 2^p-1 with p a prime) are square-free. Rotkiewicz [54] showed that if Schinzel's conjecture is true then $(FLTI)_p$ holds for infinitely many primes p. As a result of Theorem IV.3 we can prove the following similar result.

Corollary IV.3. If infinitely many Mersenne numbers are not powerful, then $(FLTI)_p$ holds for infinitely many primes p.

Proof. Let k be a prime $p > p_0$ in Theorem IV.3. □

Although it is weaker to conjecture that infinitely many Mersenne numbers are not powerful, as opposed to square-free, it is probably no easier to prove the statement.

As another corollary to Theorem IV.3, we can prove the following result of Puccioni [50].

Corollary IV.4. If $(FLTI)_p$ fails for all sufficiently large primes p then there is an infinite sequence of primes $\{q_i\}$ s.t. $2^{q_i} \equiv 2 \pmod{q_i^3}$.

Proof. Let p_0 be a prime such that $p > p_0$ implies that (FLTI) fails for p, and $\{p_i\}_{i \ge 1}$ be the set of primes $p_0 < p_1 < \ldots$. By

Corollary IV.3, $2^{p_i} - 1 = M_i$ is powerful for each i. By the result of Lebesgue [27], none of the M_i are squares, and so there exist primes $q_i | M_i$ such that $q_i^3 | 2^{p_i}-1$. It follows that $p_i | q_i - 1$ and that $2^{q_i - 1} \equiv 1 \pmod{q_i^3}$. Clearly for $i \neq j$, $GCD(M_i, M_j) = 1$ so that each q_i is distinct, and hence the set $\{q_i\}_{i \geq 1}$ is infinite. □

Mirimanoff [35] gave a result similar to that of Wieferich: if $(FLTI)_p$ fails for the prime p, then $3^p \equiv 3 \pmod{p^2}$. By the work of Vandiver [71], Pollaczek [49], Morishima [43], Granville and Monagan [21], it is now known that if $(FLTI)_p$ fails for the prime p, then $q^p \equiv q \pmod{p^2}$ for all primes $q \leq 89$. Because of these results, much of the earlier work in this section can be generalized. To do this we first need to generalize Lemma IV.1.

Lemma IV.3. Let p and q be primes such that $q^p \equiv q \pmod{p^2}$. If m is an integer such that $p | q^m - 1$, then $p^2 | q^m - 1$.

Proof. Proceed exactly as in the proof of Lemma IV.1. □

Similar to Theorem IV.1 we have;

Theorem IV.4. If $(FLTI)_p$ fails for all primes $p > p_o$ and $t = \prod_{p \leq p_o} p(p-1)$ then $q^{nt} - 1$ is powerful for all primes $q \leq 89$ and integers $n \geq 1$.

Proof. Let p be a prime dividing $q^{nt}-1$. If $p \leq p_o$, then since $nt \equiv 0 \pmod{\phi(p^2)}$, it follows by Lemma IV.2 that $p^2 | q^{nt}-1$. If

$p > p_o$ then $(FLTI)_p$ fails for p, and so $q^p \equiv q \pmod{p^2}$. By Lemma IV.3 it follows that $p^2 | q^{nt}-1$. Thus $q^{nt} - 1$ is powerful. □

Note that the proof of Theorem IV.4 rests upon the fact that $(FLTI)_p$ holds for all primes $p \leq 89$. In fact Granville and Monagan [21] have shown that $(FLTI)_p$ holds for all primes $p \leq 7 \times 10^{14}$.

We can similarly generalize Theorem IV.3. We first need the following result.

Lemma IV.4. If p, q are primes and k is a product of primes greater than q, then $p | q-1$ implies that p does not divide $\frac{q^k - 1}{q - 1}$.

Proof. Suppose $p | \frac{q^k-1}{q-1}$ and assume $p^a \| q-1$. Then $p^{a+1} | q^k-1$, and so $GCD(k, p^a(p-1)) > 1$ by Lemma IV.2. But k is a product of primes greater than q, and $p^a(p-1)$ is a product of primes less than q since $p < q$. □

Theorem IV.5. Assume $(FLTI)_p$ fails for all primes $p > p_o$. If k is an integer not divisible by any primes $p \leq p_o$, then $\frac{q^k - 1}{q - 1}$ is powerful for all primes $q \leq 89$.

Proof. Fix a prime $q \leq 89$. By the result of Granville and Monagan mentioned above, k is not divisible by any prime $p \leq 89$. Let p be a prime such that $p | \frac{q^k-1}{q-1}$. By Lemma IV.4 it follows that $q \not\equiv 1 \pmod{p}$. By Lemma IV.2 it follows that $GCD(k, p-1) > 1$. Thus $p > p_o$, and so $q^p \equiv q \pmod{p^2}$. Lemma III.3 shows $p^2 | q^k-1$, and

since p does not divide $q - 1$, $p^2 \mid \frac{q^k-1}{q-1}$. Thus $\frac{q^k - 1}{q - 1}$ is powerful. □

The following corollary is a special case of Theorem IV.5.

Corollary IV.5. If $(FLTI)_p$ fails for all primes $p > p_0$ then $\frac{q^p - 1}{q - 1}$ is powerful for all primes $p > p_0$ and $q \leq 89$. □

The result of Puccioni, Corollary IV.4, can similarly be generalized. The proof is a bit more complicated. We use a result of Walker [73, Theorem 10] to prove the following well known result.

Lemma IV.5. Let p and q be odd primes such that $q - 1$ is not a square. If $\frac{q^p - 1}{q - 1} = n^2$ then $q = 3$, $p = 5$, and $n = 11$.

Proof. From $\frac{q^p - 1}{q - 1} = n^2$ we have that $\gamma = q^{\frac{p-1}{2}}\sqrt{q} + n\sqrt{q - 1}$ is a solution to $x^2q - y^2(q-1) = 1$. By Walker [73, Theorem 10], γ is the fundamental solution, or its third power, to the equation $x^2q - y^2(q - 1) = 1$. Clearly the fundamental solution to $x^2q - y^2(q - 1) = 1$ is the element $\sqrt{q} + \sqrt{q - 1}$, and the third power is $(4q - 3)\sqrt{q} + (4q - 1)\sqrt{q - 1}$. Thus $q^{\frac{p-1}{2}} = 4q - 3$ and this forces $q = 3$, $p = 5$, $n = 11$. □

Lemma III.6. If q is a prime and p_1, p_2 are primes such that $p_2 > p_1 > q$, then $GCD\left[\frac{q^{p_1}-1}{q-1}, \frac{q^{p_2}-1}{q-1}\right] = 1$.

Proof. Let r be a prime dividing $GCD\left[\frac{q^{p_1}-1}{q-1}, \frac{q^{p_2}-1}{q-1}\right]$. Then

$q^{p_1} \equiv 1 \pmod{r}$ and $q^{p_1} \equiv 1 \pmod{r}$. By the Euclidean Algorithm, there are integers a,b such that $1 = ap_1 - bp_2$. Then $q \equiv q^{1+bp_1} \equiv q^{ap_2} \equiv 1 \pmod{r}$. Thus r divides $q - 1$. By Lemma IV.4 it follows that r does not divide either of $\frac{q^{p_1} - 1}{q - 1}$ or $\frac{q^{p_2} - 1}{q - 1}$, a contradiction. □

Theorem IV.6. If $(FLTI)_p$ fails for all sufficiently large primes, then for each prime $q \leq 89$ there is an infinite sequence of primes $\{p_i\}_{i \geq 1}$ such that $q^{p_i} \equiv q \pmod{p_i^3}$.

Proof. Fix q a prime, $q \leq 89$. Assume $(FLTI)_p$ fails for all primes $r > r_0$, and denote these primes $r_1 < r_2 < \ldots$. By Corollary III.5, $\frac{q^{r_i} - 1}{q - 1} = M_i$ is powerful for $i \geq 1$. If $q - 1$ is a square, then by the result of Lebesgue [27], each M_i is not a square. If $q - 1$ is not a square, then by Lemma IV.5 each M_i is again not a square. Thus we can choose for each $i \geq 1$ a prime p_i such that $p_i^3 | M_i$. By Lemma IV.6, $GCD(M_i, M_j) = 1$ for $i \neq j$, and so the set of primes $\{p_i\}_{i \geq 1}$ is infinite. Moreover, $q^{r_i} \equiv 1 \pmod{p_i^3}$. It is easy to see that $r_i | p_i - 1$ for each $i \geq 1$, and so $q^{p_i - 1} \equiv 1 \pmod{p_i^3}$. Equivalently $q^{p_i} \equiv q \pmod{p_i^3}$ for each $i \geq 1$. □

Corollary IV.5 can be restated as follows.

Theorem IV.7. If $(FLTI)_p$ fails for all primes $p > p_0$, then for $p > p_0$, p a prime, the p^{th} cyclotomic polynomial

$1 + x + x^2 + \ldots + x^{p-1}$ is a powerful number whenever $x = q$ a prime and $q \leq 89$. □

This leads us to consider certain polynomials and when they can have values which are powerful numbers. The following is a conjecture of Schinzel and Tijdeman [56].

Conjecture IV.1. If a polynomial $P(x)$ with rational coefficients has at least three simple zeros, then the equation $P(x) = y^2z^3$ has only finitely many solutions in integers x,y,z with $yz \neq 0$. □

In the same paper, Schinzel and Tijdeman proved

Theorem III.8. If a polynomial $P(x)$ with rational coefficients has at least two distinct zeros, then the equation $P(x) = y^m$ with x,y integers and $|y| > 1$ implies $m < c(P)$ where $c(P)$ is an effectively computable constant. □

Conjecture IV.1 is very deep, and perhaps intractable.

Proposition IV.1. If any of the following polynomials yield powerful numbers as values for only finitely many integers x, then (FLTI) holds for infinitely primes.

1. $f_1(x) = x^n - 1 \quad n \geq 3$
2. $f_2(x) = x^n + 1 \quad n \geq 3$
3. $f_3(x) = x^3 - x$.

Proof. Assume $(FLTI)_p$ fails for all primes $p > p_0$. If

$t = \prod_{p \le p_0} p(p-1)$, then $2^{ntk} \pm 1$ is a powerful number for all integers $n \ge 1$, $k \ge 1$. By putting $x = 2^{tk}$ in $f_1(x)$ or $f_2(x)$ for $k \ge 1$, we see that both $f_1(x)$ and $f_2(x)$ have powerful numbers as values for infinitely many integers x. By putting $x = 2^{kt}$ with $k \ge 1$ in $f_1(x)$, we see that $f_3(x)$ has powerful numbers as values for infinitely many integers x. □

Proposition IV.1 leads one to consider Catalan's equation. In [6] Catalan conjectured that the only solution to the equation

$$x^n - y^m = 1 \quad \text{with} \quad x > 1,\ y > 1,\ n > 1,\ m > 1$$

is $x = 3 = m$, $y = n = 2$. In fact Tijdeman [66] proved;

Theorem IV.9. The equation $x^p - y^q = 1$, $x > 1$, $y > 1$, $p > 1$, $q > 1$ has only finitely many solutions in integers. Effective bounds for the solutions p,q,x,y can be given. □

One can generalize Catalan's problem by considering the difference of a proper power of degree at least 3, and powerful numbers. We make the following conjecture similar to that of Catalan.

Conjecture III.2. The equation $x^n - m^3y^2 = \pm 1$ is solvable in integers $x > 1$, $m \ge 1$, $y > 1$, $n > 2$ if and only if $(x,m,y,n) = (2,1,3,3)$ or $(x,m,y,n) = (23,2,39,3)$. □

We note that $f_3(x) = x^3 - x$ is the product of the three consecutive integers $x - 1$, x and $x + 1$. Erdös and Selfridge [16] proved that the product of $k \ge 2$ consecutive positive integers is never a square or higher power. In fact Erdös [15] conjectured that the

product of three or more consecutive positive integers is always properly divisible by some prime. Note that this conjecture is slightly stronger than the conjecture that three consecutive powerful numbers do not exist.

It would be of great interest if these problems, the Catalan problem, the problem of Schinzel and Tijdeman, and the problem of Erdös and Selfridge, which have been solved for proper powers, could be solved for the more general case of powerful numbers.

Although proofs of these conjectures for powerful numbers are nowhere in sight, it is of interest to see how these problems are related to $(FLTI)_p$. We hope that some of these connections can inspire new approaches to $(FLTI)_p$ and perhaps that a more elementary proof of the result of Adleman and Heath-Brown might be obtained.

Section 3. Certain Quadratic Units and Powerful Numbers in Recurrence Sequences

It was shown in Theorem III.4 (Mollin and Walsh [36]) that the existence of three consecutive powerful numbers is equivalent to the existence of a unit $a + b\sqrt{m}$ in a real quadratic field $Q(\sqrt{m})$, $m \equiv 7 \pmod 8$, satisfying the conditions;

1. $b \equiv 0 \pmod m$

2. $a = x^2y^3$ for some integers x, y and a even.

In this section we take a closer look at these two conditions independently.

The condition $b \equiv 0 \pmod m$ is of particular interest when

$a + b\sqrt{m}$ is the fundamental unit ϵ_m of $Q(\sqrt{m})$.

When m is a prime $p \equiv 1 \pmod 4$, Ankeny, Artin and Chowla [2] made the following conjecture.

Conjecture IV.3. Let p be a prime $p \equiv 1 \pmod 4$ and $\epsilon_p = \frac{1}{2}(T + U\sqrt{p})$ be the fundamental unit of $Q(\sqrt{p})$. Then $U \not\equiv 0 \pmod p$. □

Mordell [40] was able to prove;

Theorem IV.10. If p is a prime $p \equiv 5 \pmod 8$, then the fundamental unit $\epsilon_p = \frac{1}{2}(T + U\sqrt{p})$ satisfies $U \equiv 0 \pmod p$ if and only if $B_{\frac{p-1}{4}} \equiv 0 \pmod p$ where B_n is the Bernoulli number defined by $\frac{t}{e^t - 1} = 1 - \frac{t}{2} + \sum_{n=1}^{\infty} (-1)^{n-1} \frac{B_n t^{2n}}{(2n)}$. Moreover, this is equivalent to the congruence $1^{\frac{p-1}{2}} + \ldots + (p-1)^{\frac{p-1}{2}} \equiv 0 \pmod{p^2}$. □

In [41], Mordell conjectured the similar result for primes $p \equiv 3 \pmod 4$. That is, if $T + U\sqrt{p} = \epsilon_p$ is the fundamental unit, then $U \not\equiv 0 \pmod p$. He was able to prove;

Theorem IV.11. If p is a prime $p \equiv 3 \pmod 4$ and $T + U\sqrt{p}$ is the fundamental unit of $Q(\sqrt{p})$ then $U \equiv 0 \pmod p$ if and only if $E_{\frac{p-3}{4}} \equiv 0 \pmod p$ where E_n is the n^{th} Euler number defined by $\sec t = \sum_{n=0}^{\infty} \frac{E_n t^{2n}}{(2n)!}$. □

Chowla was then able to show that Theorem IV.10 holds for primes $p \equiv 1 \pmod 8$.

Slavutski [59] was able to generalize these results slightly by considering square-free positive integers of the form $d = np$ with p a prime $p > 3$ and n a positive integer $1 \leq n < p$.

It would be of great interest if these techniques could be generalized to all square-free positive integers m, that is give necessary and sufficient conditions for the fundamental unit $\epsilon_m = \frac{1}{2}(T + U\sqrt{m})$ to satisfy $U \equiv 0 \pmod m$.

Stephens and Williams [60] have recently shown that for $m < 10^8$, the condition $U \equiv 0 \pmod m$ holds only if $m \in \{46, 430, 1817, 58254, 209991, 1752299, 3124318, 4099215\}$. In all of these cases, it can be shown that $N(\epsilon_m) = 1$. This raises two questions:

1. Are there infinitely many square-free positive integers m such that $\epsilon_m = \frac{1}{2}(T + U\sqrt{m})$ satisfies $U \equiv 0 \pmod m$?
2. Does there exist square-free positive m such that $\epsilon_m = \frac{1}{2}(T + U\sqrt{m})$ satisfies $N(\epsilon_m) = -1$ and $U \equiv 0 \pmod m$?

These questions are very pertinent to $(FLTI)_p$. After proving the following lemma, the connection between these types of fundamental unit and $(FLTI)_p$ will be shown.

Lemma IV.7. If $a + b\sqrt{m}$ is a unit in a real quadratic field $Q(\sqrt{m})$ and $a = 2^k$ for some $k \geq 2$, then $a + b\sqrt{m} = \epsilon_m$, the fundamental unit.

Proof. Since $k > 1$, it can be seen that $m \equiv \pm 1 \pmod 8$, and so ϵ_m is of the form $\epsilon_m = T + U\sqrt{m}$. Thus $a + b\sqrt{m} = (T + U\sqrt{m})^{\ell} = T_{\ell} + U_{\ell}\sqrt{m}$ for some integer $\ell \geq 1$. By Theorem I.14, ℓ is odd and $2^k \| T$. This shows $a = T_{\ell} \leq T$. But certainly $T \leq T_{\ell}$ since $\ell \geq 1$, hence $a = T$ and $a + b\sqrt{m} = \epsilon_m$. □

Theorem IV.12. If only finitely many real quadratic fields $Q(\sqrt{m})$ have fundamental units ϵ_m of the form $2^k + U\sqrt{m}$ with $U \equiv 0 \pmod m$, then $(FLTI)_p$ holds for infinitely many primes p.

Proof. As in the proof of Theorem IV.1, suppose $(FLTI)_p$ fails for all primes $p > p_o$ and set $t = \prod_{p \leq p_o} p(p-1)$. Then for each $n \geq 1$ there exist integers m_n and y_n with m_n square-free such that $2^{nt} - 1 = m_n{}^3 y_n{}^2$. Clearly t is even so that $\delta_n = 2^{\frac{nt}{2}} + m_n y_n \sqrt{m_n}$ is a unit in $Q(\sqrt{m_n})$. By the lemma, $\delta_n = \epsilon_{m_n}$ and each m_n is a distinct positive square-free integer. □

It should be noted that in the list of fundamental units given by Stephens and Williams with $U \equiv 0 \pmod m$, none of the rational parts, T, is of the form 2^k. Thus there is no known example of a fundamental unit of the form $2^k + U\sqrt{m}$ with $U \equiv 0 \pmod m$.

The second condition mentioned at the outset of this section is of great interest. Given that $\frac{1}{2}(T + U\sqrt{m}) = \epsilon_m$ and $\frac{1}{2}(T_n + U_n\sqrt{m}) = \epsilon_m{}^n$, then when can T_n or $\frac{1}{2}T_n$ be a powerful number. The question of when T_n or U_n can be a proper power has long been

studied. The most widely studied sequences in this regard are the Fibonacci and Lucas sequences $\{F_n\}_{n\geq 1}$ and $\{L_n\}_{n\geq 1}$ defined by $\frac{1}{2}(L_n + F_n\sqrt{5}) = \left[\frac{1}{2}(1+\sqrt{5})\right]^n$.

Cohn [8], [9] proved that the only perfect squares in the Fibonacci sequence are $F_1 = F_2 = 1$ and $F_{12} = 144$. Also he showed that the only perfect squares in the Lucas sequence are $L_1 = 1$ and $L_3 = 4$.

London and Finkelstein [31] and Lagarias and Weisser [26] independently showed that $F_1 = F_2 = 1$ and $F_6 = 8$ are the only cubes in the Fibonacci sequence, and that $L_1 = 1$ is the only cube in the Lucas sequence.

It is natural to ask whether $F_1 = F_2 = 1$, $F_6 = 8$, and $F_{12} = 144$ are the only Fibonacci numbers which are powerful numbers. Pethö [48] was able to prove the following result. Let $r(p)$ be the smallest positive k such that $p|F_k$.

Theorem IV.13. Suppose p is a prime and at least one of the following conditions hold;

1. $r(p)$ is not a prime power.
2. $F_{r(p)} = q_1^{\alpha_1} \cdots q_n^{\alpha_n}$ with $q_1,\ldots,q_n$ distinct prime $n \geq 2$ and $3\nmid\alpha_1$, $3\nmid\alpha_2$.
3. $r(p)$ is a power of 2, 3, 7, 13 or 17.

Then the equation $F_n = p^2x^3$ is not solvable for any positive integers n or x. □

In regard to this problem it should be noted that Carmichael [5] proved that if $N \neq 1, 2, 6, 12$ then $N = r(p)$ for some prime p.

This can be found in [23] also. Moreover, if $r(p^2)$ is the smallest positive integer k such that $p^2 | F_k$, Williams [78] has shown that $r(p) \neq r(p^2)$ for all primes $p < 10^9$. If one could prove that $r(p) \neq r(p^2)$ for all primes p, then it follows immediately that F_n is never powerful unless $n = 1, 2, 6$ or 12.

The more general question that one can raise here is: given a non-degenerate second order linear sequence, are there only finitely many powerful numbers in the sequence? In other words, given x_0 and x_1 and $x_{n+1} = ax_n + bx_{n-1}$ for some given a,b is there a constant c depending on x_0, x_1, a, b such that if x_n is powerful then $n < c$?

Shorey and Stewart [58] have shown that given such a sequence, the diophantine equation $x_n = ed^q$ with $|d| > 1$ and $q \geq 2$ must satisfy $\max\{n, |d|, q\} < c$ for some effectively computable constant c.

In the special case of Pell's equation, wherein we study the sequences $\{T_n\}$ and $\{U_n\}$, Cohn [10] has proved the following result on squares in these sequences.

Theorem IV.14. Assume that d is a positive square-free integer such that the Pell equation $x^2 - dy^2 = -4$ is solvable in positive odd integers x and y. Then

1. The equation $x^2 - dy^4 = 1$ has only the solutions $x = 9$, $d = 5$.

2. The equation $x^4 - dy^2 = 1$ is solvable for a finite number of values d, and for these values of d, only one solution exists.

3. The equation $y^2 - 4dx^4 = 1$ has only the solution $x = 6$, $d = 5$.

4. The equation $y^2 - dx^4 = -1$ has at most one solution for any d.

5. The equation $4x^4 - dy^2 = -1$ has only the solutions $x = 1$, $d = 5$ and $x = 3$, $d = 13$.

6. The equation $y^2 - dx^4 = 4$ has only the solutions $x = 1, 12$ for $d = 5$ and at most one solution for $d \neq 5$.

7. The equation $y^2 - dx^4 = -4$ has at most one solution for any d.

8. The equation $x^4 - dy^2 = -4$ has at most one solution for $d \neq 5$ and only the solutions $x = 1,2$ for $d = 5$. □

The assumptions of the above theorem are very restrictive. Firstly, d must be $\equiv 5 \pmod 8$, and this is not sufficient for $x^2 - dy^2 = -4$ to have solutions in odd integers, as the examples $d = 37, 101$ and 197 show.

Zhenfu [77] proved the following analogue of Cohn's result.

Theorem IV.15. If the Pell equation $x^2 - dy^2 = -1$ is solvable then for $n > 2$, the diophantine equation $x^{2n} - dy^2 = 1$ is not solvable. □

Thus Cohn and Zhenfu have shown that if $N(\epsilon_d) = -1$ and $\epsilon_d^n = \frac{1}{2}(T_n + U_n\sqrt{d})$, then only a certain class of the numbers $\{T_n\}$ or $\{U_n\}$ can be squares or perfect powers. It would be of great interest

if similar results for powerful numbers could be obtained. More precisely, let x be any even powerful number. Write $x^2 - 1 = dy^2$ with d square-free. Then $x + y\sqrt{d}$ is a unit in $Q(\sqrt{d})$, and in all known cases, $x + y\sqrt{d} = \epsilon_d$. Is there an even powerful number x such that $x + y\sqrt{d}$, as obtained above, is not the fundamental unit?

If one can prove that $x + y\sqrt{d}$ is always the fundamental unit, then three consecutive powerful numbers always come from the fundamental unit $T + U\sqrt{m}$ in Theorem III.4. Then if one can show that only finitely many square-free positive m exist for which $U \equiv 0 \pmod{m}$, the problem of three consecutive powerful numbers would essentially be solved. Of course both of the steps seem very difficult at this point, but they are practically the only known avenues for solving this problem.

Section 4. Results and Problems on Powerful Numbers

Since Erdös and Szekeres [17] studied k-full numbers, there has been an extensive amount of study on this topic.

Another topic of study has been the asymptotic density of powerful numbers. More precisely, the number of powerful numbers up to a given $x > 0$. For $x > 0$ it is clear that the number of squares up to x is $[x^{1/2}]$ where $[x]$ represents the integer part of x. To obtain formulae for the asymptotic density of powerful numbers we first need to make some definitions. We refer to [19].

Definition. Let n be a positive integer and $n = p_1^{e_1},\ldots,p_k^{e_k}$ its canonical prime factorization. The Möbius function $\mu(n)$ is defined by

$$\mu(n) = 0 \qquad \text{if} \quad e_i > 1 \quad \text{for some} \quad 1 \le i \le k$$

$$= (-1)^k \qquad \text{if} \quad e_i = 1 \quad \text{for some} \quad 1 \le i \le k$$

$$= 1 \qquad \text{if} \quad n = 1.$$

The purpose of defining the Möbius function for the study of powerful numbers is given in the following discussion.

It was proved in Proposition III.1 that every powerful number can be uniquely written in the form n^2m^3 with m square-free. Thus every powerful number is uniquely determined by the form n^2m^3 with $\mu(m) \neq 0$.

Definition. The Riemann zeta-function is defined by $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$.

It is well known that $\zeta(s)$ converges for $1 < s < \infty$, and that $\zeta(s) = \prod_p \left(\sum_{k=0}^{\infty} p^{ks} \right) = \prod_p (1 - p^{-s})^{-1}$ where the products extend over all primes p.

We will prove that $k(x) = (\#\text{ of } n^2m^3 \le x \quad \mu(m) \neq 0)$ is approximated by $cx^{1/2}$ with $c = \frac{\zeta(3/2)}{\zeta(3)}$. To show this, we first prove the following result, which can be found in [67, Theorem 1.2.7, p. 5].

Lemma IV.8. $\sum_{m=1}^{\infty} \frac{\mu^2(m)}{m^s} = \frac{\zeta(s)}{\zeta(2s)}$.

Proof. An easy check shows $\sum_{m=1}^{\infty} \frac{\mu^2(m)}{m^s} = \prod_p \left[1 + \frac{1}{p^s} \right]$ where the product extends over all primes p. Thus we obtain

$$\sum_{m=1}^{\infty} \frac{\mu^2(m)}{m^s} = \prod_p (1 + p^{-s}) = \prod_p \left[\frac{1 - p^{-2s}}{1 - p^{-s}} \right] = \frac{\prod_p (1 - p^{-s})^{-1}}{\prod_p (1 - p^{-2s})^{-1}} = \frac{\zeta(s)}{\zeta(2s)} . \qquad \square$$

We now give a simple formula for $k(x)$, as proved in [18].

Proposition IV.2. $k(x) = \sum_{m=1}^{\infty} \mu^2(m) \left[\left[\frac{x}{m^3} \right]^{1/2} \right]$ where $[x]$ denotes the integer part of x. $\square$

By Proposition IV.2, we see that $k(x)$ can be approximated by $\left[\sum_{m=1}^{\infty} \frac{\mu^2(m)}{m^{3/2}} \right] x^{1/2}$.

Theorem IV.16. The number of powerful numbers up to $x > 0$ is approximately $\frac{\zeta(3/2)}{\zeta(3)} x^{1/2}$.

Proof. By Lemma IV. $\sum_{m=1}^{\infty} \frac{\mu^2(m)}{m^{3/2}} = \frac{\zeta(3/2)}{\zeta(3)}$ and so

$$k(x) = \sum_{m=1}^{\infty} \mu^2(m) \left[\left[\frac{x}{m^3} \right]^{1/2} \right] \sim \sum_{m=1}^{\infty} \frac{\mu^2(m)}{m^{3/2}} x^{1/2} = \frac{\zeta(3/2)}{\zeta(3)} x^{1/2} . \qquad \square$$

The value of $\frac{\zeta(3/2)}{\zeta(3)}$ is approximately 2.1732, and so one concludes that the number of non-square powerful numbers up to x will be greater than the number of squares, provided that x is large enough.

Sharper estimates of $k(x)$ have been given by Erdös and Szekeres [17], who showed that

$$k(x) = \frac{\zeta(3/2)}{\zeta(3)} x^{1/2} + O(x^{1/3}) .$$

Later, Bateman [3] showed that

$$k(x) = \frac{\zeta(3/2)}{\zeta(3)} x^{1/2} + \frac{\zeta(3/2)}{\zeta(2)} x^{1/3} + O(x^{1/5}) .$$

Furthermore, it is known that if
$k(x) = \frac{\zeta(3/2)}{\zeta(3)} x^{1/2} + \frac{\zeta(3/2)}{\zeta(2)} x^{1/3} + O(x^{\theta})$ then θ satisfies
$\frac{1}{10} \leq \theta \leq \frac{2}{15}$. We refer to [25] and [53] for this.

Improvements have been made on
$\Delta(x) = k(x) - \frac{\zeta(3/2)}{\zeta(3)} x^{1/2} - \frac{\zeta(3/2)}{\zeta(2)} x^{1/3}$ by Bateman and Grosswald [4], and Suryanarayana and Sitaramachandra Rao [65], but the proofs are too complicated for our discussion.

Suryanarayana [64] has introduced the idea of generalized powerful numbers. He defines $R_{a,b}$ to be the set of positive integers $n = p_1^{e_1} \ldots p_k^{e_k}$ satisfying $e_i \equiv 0$ or $a \pmod b$. Clearly $R_{2,3}$ is the set of powerful numbers. He has shown that $R_{a,b}(x)$, the number of integers in $R_{a,b}$ up to x satisfies the approximation

$$R_{a,b}(x) = \frac{\zeta(b/a)}{\zeta(2b/a)} x^{1/a} + \frac{\zeta(a/b)}{\zeta(2)} x^{1/b} + \Delta(x)$$

where $\Delta(x)$ is an error term depending on a and b.

Again it is beyond the scope of our discussion to include any of his proofs here.

Golomb [19] defined a function similar to the Riemann zeta-function, defined by $F(s) = \prod_p \left(\sum_{\substack{k=0 \\ k \neq 1}}^{\infty} p^{-ks} \right) = \prod_p \left[1 + \frac{1}{p^s(p^s-1)} \right]$.
Note that in the product-sum formula for $F(s)$, we have the Riemann zeta-function without the second term in each sum. A trivial check

shows that $F(s) = \sum_{r \in k} r^{-s}$ where k is the set of powerful numbers.

Although $\zeta(s)$ is defined for $1 < s < \infty$, it is easy to see that $F(1)$ is defined and moreover $F(s)$ converges for $\frac{1}{2} < s < \infty$.

Proposition IV.3. $F(s)$ converges for $\frac{1}{2} < s < \infty$.

Proof. $F(s)$ can be written as $\left[\sum_{n=1}^{\infty} n^{-2s} \right] \left[\sum_{m=1}^{\infty} \mu^2(m)\, m^{-3s} \right]$.

$F_1(s) = \sum_{n=1}^{\infty} n^{-2s}$ converges for $\frac{1}{2} < s < \infty$ and $F_2(s) = \sum_{n=1}^{\infty} n^{-3s}$ converges for $\frac{1}{3} < s < \infty$. Thus their product $F_1 \cdot F_2(s)$ converges for $\frac{1}{2} < s < \infty$. Clearly $F(s) < F_1 \cdot F_2(s)$, and so $F(s)$ converges for $\frac{1}{2} < s < \infty$. It is clear that $F\left[\frac{1}{2}\right]$ diverges since $F\left[\frac{1}{2}\right] =$

$$\sum_{r \in k} r^{-1/2} > \sum_{r=n^2} r^{-1/2} = \sum_{n=1}^{\infty} \frac{1}{n} = \infty. \qquad \square$$

$F(1)$ can be calculated exactly since

$$F(1) = \left[\sum_{n=1}^{\infty} n^{-2} \right] \left[\sum_{m=1}^{\infty} \mu^2(m) m^{-3} \right] = \zeta(2) \cdot \frac{\zeta(3)}{\zeta(6)}$$ by Lemma IV.8. It is well known that $\zeta(2) = \frac{\pi^2}{6}$ and $\zeta(6) = \frac{\pi^6}{945}$, thus $F(1) = \frac{315}{2\pi^4} \zeta(3) \cong 1.9435$ is the sum of the reciprocals of the powerful numbers.

Shiu [57] has studied the number of powerful numbers between successive squares. Let $f(n)$ be the number of powerful numbers strictly between n^2 and $(n+1)^2$. Let $F_m = \{n : f(n) = m\}$. Let d_m be the asymptotic density of F_m, more precisely

$d_m = \lim_{x\to\infty} \frac{|n \leq x \; ; \; f(n) = m\}|}{x}$. Shiu was able to give the following formulae for d_m.

<u>Theorem IV.17</u>. $d_m = \sum_{\ell=0}^{\infty} (-1)^{\ell} \frac{(m+\ell)!}{m!\ell!} C_{m+\ell}$ where $C_0 = 1$ and $C_r = \sum_{1<b_0<\ldots<b_r} \frac{\mu^2(b_0)\ldots\mu^2(b_r)}{(b_0\ldots b_r)^{3/2}}$ and $b_0 < b_1 \ldots$ are the square-free positive integers. □

Shiu gives approximate values for d_m for $m \leq 5$. They are $d_0 = 0.2759 \ldots$ $d_1 = 0.3955 \ldots$ $d_2 = 0.2312 \ldots$ $d_3 = 0.0770 \ldots$ $d_4 = 0.0170 \ldots$ $d_5 = 0.0027 \ldots$.

As an application, since $d_0 > 0$ one can conclude that infinitely many integers n exist for which no powerful numbers lie strictly between n^2 and $(n+1)^2$. In a sense this contradicts the fact obtained earlier, that the number of non-square powerful numbers up to x will exceed the number of squares, for large x.

Another topic of inquiry concerning powerful numbers has been powerful numbers in arithmetic progression. This topic has been less studied and there are still many unsolved problems in the area. Most of the unsolved problems were first given by Erdös and then restated by Guy in [22].

In particular, Erdös first asked what is the largest integer r such that r powerful numbers are in arithmetic progression? If no GCD conditions are imposed, then it is easy to see that r is unbounded. Erdös tacitly assumed that consecutive powerful numbers in the

progression are relatively prime.

It is easy to show that infinitely many triples of powerful numbers in arithmetic progression exist. In fact if $n = 4(m^3\ell - \ell^3 m)$ for some integers $m > \ell$ $GCD(m,\ell) = 1$, then $((2m\ell + m^2 - \ell^2)^2, (m^2 + \ell^2)^2, (2m\ell + \ell^2 - m^2)^2)$ are squares differing by n.

The question one raises at this point is for which n do there exist three powerful numbers in arithmetic progression differing by n. The following theorem is similar to Theorem III.4.

Theorem IV.18. There exist three powerful numbers in arithmetic progression differing by n if and only if the equation $x^2 - dy^2 = n^2$ is solvable in positive integers x,y,d with d square-free, x a powerful number, $GCD(x,n) = 1$, $x \not\equiv n \pmod 2$, and $y \equiv 0 \pmod d$.

Proof. Suppose P_1,P_2,P_3 are powerful numbers satisfying $P_i - P_{i-1} = n$ and $GCD(P_i,P_{i-1}) = 1$ for $i = 2,3$. Let $x = P_2$ and $P_1P_3 = y^2d$ with d square-free. Then clearly $x^2 - dy^2 = n^2$, $GCD(x,n) = 1$, $y \equiv 0 \pmod d$, and x is a powerful number.

If $x - n$ is even, then so is $x + n$. Since $x - n$ and $x + n$ are powerful, they are both divisible by 4, so that their sum $2x$ is divisible by 4. Thus x is even contradicting $GCD(P_i,P_{i-1}) = 1$ for $i = 2,3$.

Conversely, if $x^2 - dy^2 = n^2$ is solvable with all those conditions listed, then $(x - n)(x + n) = y^2d = \left[\frac{y}{d}\right]^2 d^3$ is powerful. Since $GCD(x,n) = 1$ and $x \not\equiv n \pmod 2$, it follows that $GCD(x - n, x + n) = 1$ so that both $x - n$ and $x + n$ are powerful.

Thus $x - n$, x, $x + n$ are three powerful numbers in arithmetic progression. □

It was conjectured that no triples of powerful numbers in arithmetic progression exist for $n = 1$. We further conjecture that infinitely many n do not have solutions, and for those n which have solutions, only finitely many exist. There are no known examples of four powerful numbers in arithmetic progression, although this certainly does not preclude the non-existence of such quadruples.

It is of interest to consider when powerful numbers exist in an arbitrary arithmetic progression. That is, when is the congruence $x^2y^3 \equiv a \pmod{b}$ solvable. This is completely solved in the following result.

Theorem III.19. The congruence $x^2y^3 \equiv a \pmod{b}$ has either no solutions or infinitely many. It is solvable if and only if for every prime p such that $p \| a$, we have $p^2 \nmid b$.

Proof. Suppose $x^2y^3 \equiv a \pmod{b}$ and a prime p exists for which $p \| a$ and $p^2 | b$. Write $a = k_1 p$ with $GCD(k_1, p) = 1$ and $b = k_2 p^2$. Then $x^2y^3 = p[k_1 + ck_2 p]$, and $GCD(k_1 + ck_2 p, p) = 1$. Thus $p \| x^2y^3$, which is a contradiction.

Conversely, write $a = A_1A_2A_3$ where $GCD(A_1, b) = 1$, if $p | A_2$ then $p \| a$ and $p \| b$, and $p | A_3$ implies $p^2 | GCD(a,b)$. By our assumption, a can be written this way. Note that A_3 is powerful and A_2 is square-free. Since $GCD(A_1, b) = 1$, there exists a solution to $A_1X \equiv 1 \pmod{b}$. Write $A_2 = p_1 \ldots p_k$ with p_i distinct primes. Let

$b_i = \frac{b}{p_i}$ for $1 \le i \le k$. By the definition of A_2, $GCD(b_i,p_i) = 1$ for $1 \le i \le k$, so let Q_i be a solution to $Q_i p_i \equiv 1 \pmod{b_i}$. It follows that $(Q_i p_i)^2 p_i \equiv p_i \pmod{b}$, and so $P = (\prod_{i=1}^{k} Q_i^2 p_i^3)(A_1X)^2 A_1 A_3 \equiv p_1 \cdots p_X A_1 A_3 \equiv A_2 A_1 A_3 \equiv a \pmod{b}$, and P is powerful. Infinitely many solutions exist since infinitely many choices exist for X and the Q_i, $1 \le i \le k$. □

Erdös considered k-full numbers $U_1^{(K)} < U_2^{(K)} < \cdots$, and made the following conjectures.

Conjecture IV.4.

1. There exist infinitely many triples of $U_i^{(3)}$ in arithmetic progression.
2. There do not exist triples of $U_i^{(4)}$ in arithmetic progression.
3. There are no consecutive $U_i^{(3)}$ numbers, i.e. $U_i^{(3)} - U_j^{(3)} = 1$ is not solvable.

We remark that no example of a triple of $U_i^{(3)}$ in arithmetic progression is known. Furthermore, Conjecture IV.4.3 can be strengthened.

Conjecture IV.5. The only solutions to the equation $U_i^{(3)} - U_j^{(2)} = \pm 1$ are $2^3, 3^2$ and $23^3, 39^2 \cdot 2^3$.

The last topic of study on powerful numbers is sums of powerful numbers. It is well known that every integer is the sum of four

squares, and hence the sum of four powerful numbers. It was conjectured by Erdös that every sufficiently large integer is the sum of three powerful numbers. In fact, Mollin and Walsh [36] conjectured that only 7, 15, 23, 87, 111, 119 are not representable as a sum of three powerful numbers. Subbarao (unpublished) has produced a table for integers n, up to 10^5, giving the number of ways that n can be written as a sum of three powerful numbers. From the table, one could conjecture that the number of representations of n as a sum of three powerful numbers tends to infinity as n gets large.

Heath-Brown [24] has recently proved the following unpublished result, and we thank him for allowing us to give an outline of his proof.

Theorem IV.20. There is an effectively computable constant n_0 such that $n \geq n_0$ is a sum of at most 3 squareful numbers.

Outline of Proof. It is well-known, see Mordell [42, p. 175, p. 178] that if $n \neq 4^t(8k + 7)$, then n is expressible as a sum of three squares. Furthermore, if $n = 4^t(8k + 7)$ with $t \geq 1$, then n is expressible as $n = x^2 + y^2 + 2z^2$ with $2 \mid z$. Thus it is left only to consider those positive integers $n \equiv 7 \pmod 8$. It is then shown that for sufficiently large n, the equation $pn = x^2 + y^2 + p^4z^2$ is solvable in integers x, y and z with p a prime and $p \equiv 5 \pmod 8$. It follows that $p \mid x^2+y^2$ and so from Gaussian arithmetic $p^{-1}(x^2 + y^2)$ is a sum of two squares, $z^2 + w^2$. It follows that $n = z^2 + w^2 + p^3z^2$. □

Heath-Brown conjectures that every sufficiently large integer is expressible as $n = x^2 + y^2 + 5^3z^2$, and more generally, it would seem that for a given prime $p \equiv 5 \pmod 8$ there is an $n(p)$ such that if $n > n(p)$ then $n = x^2 + y^2 + p^3z^2$ for some integers x, y and z. This would show that the number of representations of n as a sum of three powerful numbers tends to infinity as n gets large.

It is also of interest to find out which integers are the sum of two powerful numbers. It is known that if n has no prime factor $p \equiv 3 \pmod 4$ to an odd exponent in its canonical prime factorization, then n is a sum of two squares, hence the sum of two powerful numbers. For other n, the problem seems very difficult.

Even when considering which primes $p \equiv 3 \pmod 4$ are the sum of two powerful numbers, there is no known method. The only known result in this direction comes from Gauss. If p is a prime, $p \equiv 1 \pmod 3$, and the congruence $x^3 \equiv 2 \pmod p$ is solvable, then $p = x^2 + 27y^2$ for some integers x and y. There is more discussion on sums of powerful numbers in Mollin and Walsh [36].

We conclude this section with some more conjectures of Erdös.

Conjecture IV.6.

1. The equation $U_i^{(3)} + U_j^{(3)} = U_K^{(3)}$ has infinitely many solutions.
2. The equation $U_i^{(4)} + U_j^{(4)} = U_K^{(4)}$ has only finitely many solutions.

3. For $k \geq 4$ the equation $U_{i_1}^{(k)} + U_{i_2}^{(k)} + \ldots + U_{i_{k-2}}^{(k)} = U_{i_{k-1}}^{(k)}$ has only finitely many solutions.

B I B L I O G R A P H Y

[1] L.M. Adleman and D.R. Heath-Brown, The first case of Fermat's Last Theorem, Invent. Math. 79 (1986), 801-806.

[2] N.S. Ankeny, E. Artin, S. Chowla, The class-number of real quadratic fields, Ann. of Math. 56 (1952), 479-493.

[3] P.T. Bateman, Square-Full Integers, Amer. Math. Monthly 61 (1954), 477-479.

[4] P.T. Bateman and E. Grosswald, On a theorem of Erdös and Szekeres, Illinois J. Math. 2 (1958), 88-98.

[5] R.D. Carmichael, On the numerical factors of the arithmetic form $\alpha^n \pm \beta^n$, Ann. Math. 15 (1913-14), 30-70.

[6] E. Catalan, Note extrait d'une lettre adressée à l'éditeur, J. Reine Angew. Math. 27 (1844), 192.

[7] H. Cohn, The next Pellian equation, Lecture Notes in Math, 899, Springer-Verlag, Berlin, (1981), 221-230.

[8] J.H.E. Cohn, On square Fibonacci numbers, J. London Math. Soc. 39 (1964), 537-540.

[9] J.H.E. Cohn, Lucas and Fibonacci numbers and some Diophantine equations, Proc. Glasgow Math. Assoc. 7 (1965), 24-28.

[10] J.H.E. Cohn, Eight Diophantine equations, Proc. London Math. Soc. (3)16 (1966), 153-166.

[11] G. Degert, Über die Bestimmung der Grundeinheit gewisser

reell-quadratischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg 22 (1958), 92-97.

[12] M.J. De Leon, Pell's equation and Pell number triples, Fib. Quart. 14 (Dec. 1976), 456-460.

[13] M.J. De Leon, A characterization of the fundamental solutions to Pell's equation $u^2 - Dv^2 = C$, Fibonacci Quart. 19 (Feb. 1981), 4-6.

[14] L.E. Dickson, History of the Theory of Numbers Vol. I, Carnegie Institution, (1919).

[15] P. Erdös, Consecutive integers, Eureka 38 (1975-76), 3-8.

[16] P. Erdös and J.L. Selfridge, The product of consecutive integers is never a power, Illinois J. Math. 19 (1975), 292-301.

[17] P.Erdös and G. Szekeres, Über die Anzahl der Abelschen Gruppen gegenbener Ordnung und über ein verwandtes zahlentheoretisches Problem, Acta. Litt. Sci. Szeged. (1934), 95-102.

[18] C.F. Gauss "Disquisitiones arithmeticae," f 222, p. 309, Leipzig, 1801.

[19] S.W. Golomb, Powerful numbers, Amer. Math. Monthly 77 (1970), 848-852.

[20] A. Granville, Powerful numbers and Fermat's Last Theorem, C.R. Math. Rep.Acad.Canada 8 no. 3 (1986), 215-218.

[21] A. Granville and M.B. Monagan, The First Case of Fermat's Last Theorem is true for all prime exponents up to 714,591,416,091,389. (preprint).

[22] R.K. Guy, Unsolved Problems in Number Theory, Springer-Verlag, New York (1981).

[23] J.H. Halton, On the divisibility properties of Fibonacci numbers, Fibonacci Quart. 4 (1966), 217-240.

[24] D.R. Heath-Brown, Ternary Quadratic Forms and Sums of Three Square-Full integers, (preprint).

[25] E. Krätzel, Ein Teilerproblem, J. Reine Angew. Math. 235 (1969), 150-174.

[26] J.C. Lagarias and D.P. Weisser, Fibonacci and Lucas cubes, Fibonacci Quart. 19, no. 1 (1981), 39-43.

[27] V.A. Lebesgue, Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$, Nouv. Ann. Math. 1, no. 9 (1850), 178-181.

[28] D.H. Lehmer, On the indeterminate equation $t^2 - p^2Du^2 = 1$, Ann. Math. 27 (1926), 471-476.

[29] D.H. Lehmer, An extended theory of Lucas functions, Ann. Math. 31 (1930), 419-448.

[30] E. Lehmer, On the cubic character of quadratic units, J. Number Theory 5 (1973), 385-389.

[31] H. London and R. Finkelstein, On Fibonacci and Lucas numbers

which are perfect powers, Fib. Quart. 7 (1969), 476-481.

[32] E. Lucas, Theorie des fonctions numériques simplement périodiques, Amer. J. Math. 1 (1878), 184-240.

[33] W.L. McDaniel, Representations of every integer as the difference of powerful numbers, Fibonacci Quart. 20, no. 1 (1982), 85-87.

[34] W.L. McDaniel, Représentations comme la différence des nombres puissants non-carrés, C.R. Math.Rep. Sci. Canada 8 (1986), 53-57.

[35] D. Mirimanoff, Sur le dernier théorème de Fermat, J. Reine Angew. Math. 139 (1911), 309-324.

[36] R.A. Mollin and P.G. Walsh, A note on powerful numbers, quadratic fields, and the Pellian, C.R. Math. Rep. Sci. Canada 8, no. 2 (1986), 109-114.

[37] R.A. Mollin and P.G. Walsh, On powerful numbers, Internat. J. Math. and Math. Sci. 9 (1986), 801-806.

[38] R.A. Mollin and P.G. Walsh, On non-square powerful numbers, Fibonacci Quart. 25 (1987), 34-37.

[39] R.A. Mollin and P.G. Walsh, Proper differences of non-square powerful numbers (to appear C.R. Math. Rep. Acad. Sci. Canada).

[40] L.J. Mordell, On a Pellian equation conjecture, Acta Arith. 6 (1960), 137-144.

[41] L.J. Mordell, On a Pellian equation conjecture II, J. London Math. Soc. 36 (1961), 282-288.

[42] L.J. Mordell, Diophantine Equations, Academic Press, London, (1970).

[43] T. Morishima, Über den Fermatschen Quotienten, Japan. J. Math. 8 (1931), 159-173.

[44] Y. Motada, On units of a real quadratic field, Mem. Fac. Gen. Ed. Kumamoto Univ. Ser. Nat. Sci. 13 (1977), 9-13.

[45] T. Nagell, On a special class of Diophantine equations of the second degree, Ark. Math. 3 (1954), 51-65.

[46] T. Nagell, Introduction to Number Theory, 2nd ed., Chelsea, New York (1964).

[47] W. Narkiewicz, Algebraic Numbers, Polish Scientific Publishers, Warsaw, (1970).

[48] A. Pethö, Full cubes in the Fibonacci sequence, Publ. Math. Debrecen 30 (1983), no. 1-2, 117-127.

[49] F. Pollaczek, Über die irregulären Kreiskörper der ℓ-ten und ℓ^2-ten Einheitswürzeln, Math. Ann. 21 (1924), 1-37.

[50] S. Puccioni, Un teorema per una resoluzione parziale del famoso problema di Fermat, Archimede 20 (1968), 219-220.

[51] P. Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer-Verlag, New York (1979).

[52] C. Richaud, Sur la résolution des équations $x^2 - Ay^2 = \pm 1$,

Alti. Acad. Pontif. Nuovi Lincei (1866), 177-182.

[53] H.E. Richert, Über die Anzahl Abelscher Gruppen gegebener Ordnung, Math.Z. 56 (1952), 21-32.

[54] A. Rotkiewicz, Sur les nombres de Mersenne dépourvus de diviseurs carrés et sur les nombres naturels n, tels que $n^2 | 2^n-2$, Mat. Vesnik 2(17) (1965), 78-80.

[55] P.Samuel, Algebraic Theory of Numbers, Houghton Mifflin, Boston, 1970. (English translation by A.J. Silberger).

[56] A. Schinzel and R. Tijdeman, On the equation $y^m = P(x)$, Acta Arith. 31 (1976), 199-204.

[57] P. Shiu, On the number of square-full integers between successive squares, Mathematika 27 (1980), 171-178.

[58] T.N. Shorey and C.L. Stewart, On the diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences, Math. Scand. 52, no. 1 (1983), 24-36.

[59] I. Slavutski, On Mordell's theorem, Acta Arith. 11 (1965), 57-66.

[60] A.J. Stephens and H.C. Williams, Some computational results on a problem concerning powerful numbers, Math. Comp. 50 (1988), 619-632.

[61] B. Stolt, On the Diophantine equation $u^2 - Dv^2 = \pm 4N$, Ark. Mat. 2 (1952), 1-23.

[62] B. Stolt, On the Diophantine equation $u^2 - Dv^2 = \pm 4N$ II,

Ark. Mat. 2 (1952), 251-268.

[63] B. Stolt, On the Diophantine equation $u^2 - Dv^2 = \pm 4N$ III, Ark. Mat. 3 (1955), 117-132.

[64] D. Suryanarayana, On the distribution of some generalized square-full integers, Pacific J. Math. 72, no. 2 (1977), 547-555.

[65] D. Suryanarayana and R. Sitaramachandra Rao, The distribution of square-full integers, Ark. Mat. 11 (1973), 195-201.

[66] R. Tijdeman, On the equation of Catalan, Acta Arith. 29 (1976), 197-209.

[67] E.C. Titchmarsh, The theory of the Riemann zeta function, Clarendon Press, Oxford, England, 1951

[68] H.F. Trotter, On the norms of units in quadratic fields, Proc. Amer. Math. Soc. 22 (1969), 198-201.

[69] D. Underwood, Elementary Number Theory 2nd ed., W.H. Freeman, San Francisco (1978).

[70] C. Vanden Eynden, Differences between squares and powerful numbers, Fibonacci Quart. 24, no. 4 (1986), 347-348.

[71] H.S. Vandiver, On Fermat's Last Theorem, Trans. Amer. Math. Soc. 31 (1929), 613-642.

[72] N.N. Vorob'ev, Fibonacci Numbers, Blaisdell, New York (1961). (English translation by H. Moss).

[73] D.T. Walker, On the diophantine equation $mX^2 - nY^2 = \pm 1$, Amer. Math. Monthly 74 (1967), 504-513.

[74] D.T. Walker, Consecutive integer pairs of powerful numbers and related diophantine equations, Fibonnaci Quart. 14, no. 2 (1976), 111-116.

[75] A. Wieferich, Zum letzten Fermatschen Theorem, J. Reine Angew. Math. 136 (1909), 293-302.

[76] E.E. Whitford, The Pell Equation, Ph.D. Thesis, Columbia University, New York (1912).

[77] C. Zhenfu, On the diophantine equation $x^{2n} - Dy^2 = 1$, Proc. Amer. Math. Soc. 98, no. 1 (1986), 11-16.

[78] H.C. Williams, A note on the Fibonacci quotient $\frac{F_{p-\epsilon}}{p}$, Canad. Math. Bull. 25, no. 3 (1982), 366-370.

[79] B.D. Beach and H.C. Williams, A numerical investigation of the Diophantine equation $x^2 - dy^2 = -1$, Proc. 3rd S-E Conf. Combinatorics, Graph Theory and Computing (1972), 37-52.

[80] J.C. Lagarias, On the computational complexity of determining the solvability of the equation $X^2 - DY^2 = -1$, Trans. Amer. Math. Soc. 260 (1980), 485-508.

[81] J.C. Lagarias, The set of primes dividing the Lucas numbers has density 2/3, Pac. Journal Math. 118 (1985), 449-461.

[82] D.H. Lehmer, On the multiple solutions of the Pell equation, Annals of Math. 30 (1928), 66-72.

[83] P. Morton, On Rédei's Theory of the Pell equation, J. Reine Angew. Math. 307/308 (1979), 373-398 .