SOLVABILITY CHARACTERIZATIONS OF PELL LIKE EQUATIONS

by

Jason Smith

A thesis

submitted in partial fulfillment

of the requirements for the degree of

Master of Science in Mathematics

Boise State University

August 2009

BOISE STATE UNIVERSITY GRADUATE COLLEGE

DEFENSE COMMITTEE AND FINAL READING APPROVALS

of the thesis submitted by

Jason Michael Smith

Thesis Title: Solvability Characterizations of Pell Like Equations

Date of Final Oral Examination: 03 June 2009

The following individuals read and discussed the thesis submitted by student Jason Michael Smith, and they also evaluated his presentation and response to questions during the final oral examination. They found that the student passed the final oral examination, and that the thesis was satisfactory for a master's degree and ready for any final modifications that they explicitly required.

Marion Scheepers, Ph.D. Chair, Supervisory Committee

Liljana Babinkostova, Ph.D. Member, Supervisory Committee

Uwe Kaiser, Ph.D. Member, Supervisory Committee

The final reading approval of the thesis was granted by Marion Scheepers, Ph.D., Chair of the Supervisory Committee. The thesis was approved for the Graduate College by John R. Pelton, Ph.D., Dean of the Graduate College.

To the power, beauty, and existence of Christopher Chaloupka

ACKNOWLEDGEMENTS

Thank you to my father, Mike, for his analytical mind.

ABSTRACT

Pell's equation has intrigued mathematicians for centuries. First stated as Archimedes' Cattle Problem, Pell's equation, in its most general form, $X^2 - P \cdot Y^2 = 1$, where P is any square free positive integer and solutions are pairs of integers, has seen many approaches but few general solutions. The eleventh century Indian mathematician Bhaskara solved $X^2 - 61 \cdot Y^2 = 1$ and, in response to Fermat's challenge, Wallis and Brouncker gave solutions to $X^2 - 151 \cdot Y^2 = 1$ and $X^2 - 313 \cdot Y^2 = 1$. Fermat claimed to posses a general solution, but it wasn't until 1759 that Leonard Euler published the first general solution to Pell's Equation. In fact, it was Euler who, mistakenly, first called the equation Pell's Equation after the 16th century mathematician John Pell. Pell had little to do with the problem and, though Pell made huge contributions to other fields of mathematics, his name is inexplicably linked to this equation.

One natural generalization of the problem is to allow for 1 to be any integer k. This yields the Pell-Like equation $X^2 - P \cdot Y^2 = k$, where P is any prime and k is any integer. In fact, on his way to the solution of $X^2 - 61 \cdot Y^2 = 1$, Bhaskara solved many Pell-Like equations; although at the time this was not his goal.

Neglecting any time considerations, it is possible, using current methods, to determine the solvablility of all Pell-Like equations. Whereas some have claimed that these methods solve the problem, we shall illustrate that a decision as to the solvability of many Pell-Like equations is computationally unfeasible.

From a computational standpoint, there are two fundamental questions associated with Pell-Like equations. First, is there an efficient means to decide if solutions exist? Second, if a particular Pell-Like equation is solvable, is there an efficient means to find all solutions? These are, respectively, the Pell-Like decision and search problems.

The problem of finding an *efficient* solution to the Pell-Like decision and search problems, for *all* Pell-Like equations, remains unsolved. In what lies ahead we hope to shed some illuminating light on these problems and give a partial solution. Our tools are Modular Arithmetic, Gauss' Quadratic Reciprocity Law, and the theory of Continued Fractions. We review these as well as historical efforts on these problems in Chapter 1.

Once we have developed the necessary theory for the Quadratic Reciprocity law and the theory of Continued Fractions, we will use these ideas in Chapter 2 to further develop a partial criterion for the solvability of Pell-Like equations. Using the Quadratic Reciprocity law we will develop a series of tests that efficiently decide the unsolvability of many Pell-Like equations. Using the Theory of Continued Fractions, we will develop in Chapter 3 the necessary tools to solve the Pell Like search problem for a specific subset of all Pell-Like equations. We show that all solutions taken on by convergents in the continued fraction expansion of $\sqrt{P}$ are taken on within the first two iterations of the period.

Chapter 4 presents cryptographic applications of Pell-Like equations. We will define and prove the existence of a cryptographic group and then discuss its applications

to many types of cryptosystems. We conclude with a discussion of a cryptographic attack that uses the Theory of Continued Fractions.

For all results from classical Number Theory which we do not prove we refer the reader to [2]. For those results from the Theory of Continued Fractions that we do not prove, we refer the reader to [8], [2], and [9].

TABLE OF CONTENTS

LIST OF TABLES

Chapter 1

INTRODUCTION

1.1 Preliminaries

1.1.1 Elementary Number Theory

Pure Mathematics on the whole is steeped in abstraction and uses highly complex structures to discuss difficult topics. However, we will be working in the field of mathematics known as Elementary Number Theory. Unbeknowest, one should not be led into a false sense of security. The word "elementary" merely indicates that the techniques employed use no more than basic logic and the mathematics that is familiar to an outstanding high school student.

Some topics that should be familiar are integer factorization, modular arithmetic, divisibility, and basic proof strategies. For a good introduction to these topics please see [2]. The most essential Number Theoretic topics, Quadratic Reciprocity and Continued Fractions, will be discussed in the next three subsections.

1.1.2 Quadratic Reciprocity

We now introduce the celebrated Law of Quadratic Reciprocity. First proved by Gauss in 1795, the Law of Quadratic Reciprocity allows one to quickly decide whether or not an integer is a square modulo an odd prime. Its proof, which we will state but not prove, is difficult. According to Gauss, "[The proof] tortured me for the whole year and eluded my most strenuous efforts before, finally, I got the proof..." [2].

We will first consider the notion of a square modulo an odd prime. Let p be an odd prime, $a \in \mathbb{Z}$ and $gcd(a, p) = 1$. If $X^2 \equiv a \bmod p$ admits a solution, then *a is a quadratic residue modulo p.* Otherwise, *a is a quadratic non residue modulo p.*

For example consider $p = 7$ and $a = 2$. Since $X^2 \equiv 2 \bmod 7$ admits a solution, namely 3 and 4, 2 is a quadratic residue modulo 7. The fact that there are two solutions is no coincidence. Indeed, this follows from the fact that the integers, modulo 7, form a field, namely $\mathbb{Z}_7$.

Now, consider $p = 29$ and $a = 10$. Since there is no integer, modulo 29 , that solves $X^2 \equiv 10 \bmod 29$ (as the reader may check), we say that 10 is a quadratic non residue modulo 29.

There is a convenient way to denote that an integer is a quadratic (non)residue modulo p, attributed to Adrien Marie Legendre (1752-1833). Let p be an odd prime and $gcd(a, p) = 1$. The Legendre symbol (a/p) is a function (defined over $\mathbb{Z}_p^x$) given

by the rule

$$(a/p) = \begin{cases} 1 & \text{if a is a quadratic residue modulo p} \\ -1 & \text{if a is a quadratic non residue modulo p} \end{cases}$$

Above, we took note of the fact that $X^2 \equiv 2 \bmod 7$ admits a solution and $X^2 \equiv 10 \bmod 29$ admits no solution. Using the Legendre symbol, this may be expressed as $(2/7) = 1$ and $(10/29) = -1$. The most striking feature of this function is that there is an efficient (*polynomial time*) algorithm for computing its values for each odd prime P. This algorithm is summarized in Theorems 1.1, 1.3, and 1.4.

That the Legendre function may be computed in polynomial time follows from Jacobi's generalization of both the Legendre function and the Law of Quadratic Reciprocity to the case where P is any integer. Indeed, for it is the Jacobi function that can be computed in polynomial time using Jacobi's generalized Quadratic Reciprocity Law.

Theorem 1.1 *Let P be an odd prime and $a, b \in \mathbb{Z}$. Further assume $gcd(a, P) = gcd(b, P) = 1$. Then,*

(a) If $a \equiv b$ mod P, then $(a/P) = (b/P)$.

(b) $(a^2/P) = 1$.

(c) $(a \cdot b/P) = (a/P) \cdot (b/P)$.

(d) $(1/P) = 1$ and $(-1/P) = (-1)^{\frac{p-1}{2}}$.

Proof: If $a \equiv b$ mod P, then $X^2 \equiv a$ mod P is solvable $\Leftrightarrow$X$^2 \equiv b$ mod P is solvable.

Thus, $(a/P) = 1 \Leftrightarrow (b/P) = 1$. This proves (a).

a solves $X^2 \equiv a^2$ mod P. Thus, $(a^2/P) = 1$, which proves (b).

To prove (c) we need Euler's Criterion: For an odd prime P and a such that $gcd(a, P) = 1$ we have $a^{\frac{p-1}{2}} \equiv (a/P)$ mod P. For a proof see [2].

By Euler's Criterion, $(a \cdot b/P) \equiv (a \cdot b)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv (a/P) \cdot (b/P)$ mod P. If $(a \cdot b/P) \neq (a/P) \cdot (b/P)$ then since the Legendre symbol only takes on $1, -1$ we must have $1 \equiv -1 \equiv P - 1$ mod P. But then, $P|(2 - P) \Rightarrow P|2$, a contradiction. This proves (c).

1 solves $X^2 \equiv 1$ mod P and by Euler's criterion we have $(-1/P) \equiv (-1)^{\frac{p-1}{2}}$ mod P. This proves (d). □

Now, with the above theorem at our disposal, we can decide whether or not a particular integer is a quadratic residue modulo an odd prime P. For example consider $a = 18$ and $P = 7$. Since $18 = 3^2 \cdot 2$, we have $(18/7) = (3^2 \cdot 2/7) = (3^2/7) \cdot (2/7) = 1 \cdot (2/7) = (2/7)$. We established above that $(2/7) = 1$. Thus, $(18/7) = 1$. That is, $X^2 \equiv 18$ mod 7 admits a solution.

Theorem 1.2 *We have*

$$(-1/P) = \begin{cases} 1 & , \textit{ if } P \equiv 1 \textit{ mod } 4 \\ -1 & , \textit{ if } P \equiv 3 \textit{ mod } 4 \end{cases}$$

Proof: If $P \equiv 1$ mod 4, then for some integer k, $P = 4k + 1$. Thus, by Theorem 1.1(d) we have $(-1/P) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+1-1}{2}} = (-1)^{\frac{4k}{2}} = 1$. If $P \equiv 3$ mod 4,

then for some integer k, $P = 4k + 3$. Thus, by Theorem 1.1(d) we have $(-1/P) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+3-1}{2}} = (-1)^{\frac{2(k+1)}{2}} = (-1)^{k+1} = -1$. $\square$

We will not prove the next two important results, the second of which is the Law of Quadratic Reciprocity.

Theorem 1.3 *We have*

$$(2/P) = \begin{cases} 1 & , \textit{ if } P \equiv \pm 1 \textit{ mod } 8 \\ -1 & , \textit{ if } P \equiv \pm 5 \textit{ mod } 8 \end{cases}$$

Theorem 1.4 (Gauss) *Let P and q be distinct odd primes. We have*

$$(P/q) = \begin{cases} (q/P) & , \textit{ if } P \equiv 1 \textit{ mod } 4 \textit{ or } q \equiv 1 \textit{ mod } 4 \\ -(q/P) & , \textit{ if } P \equiv q \equiv 3 \textit{ mod } 4 \end{cases}$$

We now have the ability to efficiently decide, given any odd prime P and integer a such that $gcd(a, P) = 1$, whether or not the congruence $X^2 \equiv a$ mod P admits a solution. In effect, the Law of Quadratic Reciprocity is the final piece necessary to solve the quadratic residue *decision problem*.

For example, consider the congruence $X^2 \equiv 29$ mod 103. Since $29 \equiv 1$ mod 4, $(29/103) = (103/29)$. But, since $103 \equiv 16$ mod 29, we have $(103/29) = (16/29) = (4^2/29) = 1$. Thus, $(29/103) = 1$.

This ends our preliminary discussion of Quadratic Reciprocity. In what lies ahead we will see that Quadratic Reciprocity allows us to formulate a good first test for the

solvability of any Pell-Like equation.

1.1.3 Continued Fractions

In 1759 Leonard Euler, using the theory of continued fractions, gave the first published solution to Pell's equation $X^2 - PY^2 = 1$, where P is any prime. With this achievement Euler highlighted the importance of continued fractions and their connection to Pell equations. We now develop the necessary theory.

A *finite simple continued fraction* is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ldots + \cfrac{1}{a_n}}}}},$$

where for $1 \leq i \leq n$, $a_i \in \mathbb{N}$ and $a_0 \in \mathbb{Z}$. For example, $\frac{170}{53} = 3 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{2}}}}$.

We use the notation $[a_0, a_1, a_2, a_3, ..., a_n]$ to stand for $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ldots + \cfrac{1}{a_n}}}}}$. We call the a_i *partial quotients*. For $m < n$, the number whose continued fraction expansion is $[a_m, a_{m+1}, ..., a_n]$ is known as a *complete quotient* in the continued fraction expansion of $[a_0, a_1, a_2, a_3, ..., a_n]$. We may write $[a_0, a_1, a_2, a_3, ..., a_n] = [a_0, a_1, ..., a_{m-1}, X]$, where $X = [a_m, a_{m+1}, ..., a_n]$.

The continued fraction made from cutting off the expansion after the mth partial quotient is called the *mth convergent* and is denoted C_m. We will often refer to the numerators and denominators of convergents and denote them as $C_k = \frac{p_k}{q_k}$.

Thus, the continued fraction for $\frac{170}{53}$ may be written as $[3, 4, 1, 4, 2]$. The conver-

gents of $\frac{170}{53}$ are $C_0 = 3$, $C_1 = \frac{13}{4}$, $C_2 = \frac{16}{5}$, $C_3 = \frac{68}{21}$, $C_4 = \frac{170}{53}$ while the numerator of C_3 is $p_3 = 68$ and the denominator of C_2 is $q_2 = 5$.

Clearly, all convergents are rational. Thus, every finite simple continued fraction represents a rational number. Moreover, every rational can be expressed as a finite simple continued fraction.

Theorem 1.5 *Let $X = [a_0, a_1, a_2, a_3, ...a_n]$ be a finite simple continued fraction. Then, the numerators and denominators of X are given by the following formulas:*

(a) $p_0 = a_0$, $p_1 = a_1 a_0 + 1$, and $p_k = a_k p_{k-1} + p_{k-2}$

(b) $q_0 = 1$, $q_1 = a_1$, and $q_k = a_k q_{k-1} + q_{k-2}$.

Induction arguments allow one to prove the following three theorems.

Theorem 1.6 *Let $C_k = \frac{p_k}{q_k}$ be the kth convergent of $[a_0, a_1, a_2, a_3, ...a_n]$.*

Then, $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$ for $1 \leq k \leq n$.

Theorem 1.7 *$(q_k : k > 1)$ forms a strictly increasing sequence.*

Theorem 1.8 *For all $k \in \mathbb{N}$ we have*

(a) $C_0 < C_2 < C_4 < ...$

(b) $C_1 > C_3 > C_5 > ...$

(c) If k is odd and l is even, then $C_l < C_k$.

A *infinite simple continued fraction* is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cdots}}}},$$

where for $i \geq 1$, $a_i \in \mathbb{N}$ and $a_0 \in \mathbb{Z}$.

To define the value of an infinite simple continued fraction we need a little elementary calculus. Let $a_0, a_1, a_2, a_3, ...$ be an infinite sequence of integers. Then, the *infinite simple continued fraction* $[a_0, a_1, a_2, a_3, ...]$ has the value $lim_{n\to\infty}[a_0, a_1, a_2, ..., a_n]$.

Why does the limit exist? From Theorem 1.8 we know that $\{C_{2n}\}$ is strictly increasing and $\{C_{2n+1}\}$ is strictly decreasing. Since both of these sequences are bounded, by C_1 and C_0 respectively, the Bolzano Weierstrass Theorem implies that their limits exist. Let α, α' be these respective limits. Then, for every $n \in \mathbb{N}$ we have $|\alpha - \alpha'| \leq |C_{2n+1} - C_{2n}| = |\frac{p_{2n+1}}{q_{2n}} - \frac{p_{2n}}{q_{2n}}| = |\frac{1}{q_{2n+1}q_{2n}}| < \frac{1}{q_{2n}^2}$. By Theorem 1.7, $\{q_n\}_{n\in\mathbb{N}}^{n>1}$ is strictly increasing. As n becomes large $\frac{1}{q_{2n}^2}$ becomes arbitrarily small. Thus, $\alpha = \alpha'$.

Analogous to the fact that every rational has a finite simple continued fraction representation, every irrational has an infinite simple continued fraction representation.

Theorem 1.9 *Let* $[a_0, a_1, a_2, a_3, ...]$ *be an infinite simple continued fraction. Then,* $[a_0, a_1, a_2, a_3, ...]$ *represents an irrational number.*

Proof: Let $\alpha = [a_0, a_1, a_2, a_3, ...]$, $C_n = \frac{p_n}{q_n}$, $C_{n+1} = \frac{p_{n+1}}{q_{n+1}}$. Suppose that $\alpha = \frac{r}{s} \in \mathbb{Q}$. By Theorem 1.8, we know that $C_n < \alpha < C_{n+1}$ or $C_{n+1} < \alpha < C_n$. Thus, $0 <$

$|\alpha - C_n| < |C_{n+1} - C_n| = |\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}| = \frac{1}{q_n q_{n+1}}$. So, $0 < |\frac{r}{s} - \frac{p_n}{q_n}| < \frac{1}{q_n q_{n+1}}$. Thus, when we multiply this inequality by $s \cdot q_n$ we obtain $0 < |r \cdot q_n - s \cdot p_n| < \frac{s}{q_{n+1}}$. We know $\{q_n\}$ is strictly increasing. Thus, for n large, we have $\frac{s}{q_{n+1}} < 1$. That is, for n large, $0 < |r \cdot q_n - s \cdot p_n| < 1$. So, there is an integer between 0 and 1, a clear contradiction. □

These results imply the following theorem.

Theorem 1.10 *Every irrational number has a unique infinite simple continued fraction representation.*

Above, we defined the notion of a complete quotient for a finite simple continued fraction. This notion can be extended to infinite simple continued fractions. Let $[a_0, a_1, a_2, a_3, ...]$ be an infinite simple continued fraction and $m \in \mathbb{N}$. Then, the number whose continued fraction expansion is $[a_m, a_{m+1}, a_{m+2}, ...]$ is known as a *complete quotient* in the continued fraction expansion of $[a_0, a_1, a_2, a_3, ...]$. We may write $[a_0, a_1, a_2, a_3, ..., a_{m-1}, X]$, where $X = [a_m, a_{m+1}, a_{m+2}, ...]$.

1.1.4 Periodic Continued Fractions

Now that we have developed the general theory, we talk about some specific continued fractions that will greatly aid us in solving Pell-Like equations. These are periodic continued fractions. Before we study the definition, we look at a concrete example.

We will now begin to expand $\sqrt{13}$ into an infinite simple continued fraction using the *continued fraction algorithm*. For any $x \in \mathbb{R}$, let $[x]$ denote the greatest integer

less than or equal to x.

Let $a_0 = [\sqrt{13}] = 3$. Then, $\sqrt{13} = a_0 + \frac{1}{X_1} = 3 + \frac{1}{X_1}$. Thus, $X_1 = \frac{1}{\sqrt{13}-3} \cdot \frac{\sqrt{13}+3}{\sqrt{13}+3} = \frac{3+\sqrt{13}}{4}$.

Let $a_1 = [\frac{3+\sqrt{13}}{4}] = 1$. Then, $\frac{3+\sqrt{13}}{4} = a_1 + \frac{1}{X_2} = 1 + \frac{1}{X_2}$. Thus, $X_2 = \frac{4}{\sqrt{13}-1} \cdot \frac{\sqrt{13}+1}{\sqrt{13}+1} = \frac{1+\sqrt{13}}{3}$.

Continuing this process we create Table 1.1, given below.

TABLE 1.1 Expansion of $\sqrt{13}$

n	a_n	X_{n+1}
0	3	$\frac{3+\sqrt{13}}{4}$
1	1	$\frac{1+\sqrt{13}}{3}$
2	1	$\frac{2+\sqrt{13}}{3}$
3	1	$\frac{1+\sqrt{13}}{4}$
4	1	$\frac{3+\sqrt{13}}{1}$
5	6	$\frac{3+\sqrt{13}}{4}$
6	1	$\frac{1+\sqrt{13}}{3}$
7	1	$\frac{2+\sqrt{13}}{3}$

Notice that $X_1 = X_6$, $X_2 = X_7$, and $X_3 = X_8$. This is no coincidence. Indeed, as we shall see, the continued fraction expansion of $\sqrt{13}$ is periodic.

From our work above, we may write $\sqrt{13} = [3, 1, 1, 1, 1, 6, 1, 1, ...]$. If we were to continue the continued fraction algorithm to expand $\sqrt{13}$ into a continued fraction we would see that $\sqrt{13} = [3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, 1, ...]$ (as the reader may check). We will often write $[3, \overline{1, 1, 1, 1, 6}]$ to stand for $[3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, 1, ...]$ and refer to the number of terms in the repeating block as the *period*.

A *periodic* simple continued fraction is one in which a sequential block of partial

quotients repeats indefinitely. For example, $[1,2,2,2,2,...] = [1,\overline{2}]$, $\sqrt{7} = [2,\overline{1,1,1,4}]$, and $\frac{2+\sqrt{13}}{3} = [\overline{1,1,6,1,1}]$ are all periodic. The first two are periodic after an initial stage and the third is *purely periodic*. The period of $[1,\overline{2}]$ is 1 and the period of $[\overline{1,1,6,1,1}]$ is 5.

Let us return to the expansion of $\sqrt{13}$. Notice that the real numbers $X_1 = \frac{3+\sqrt{13}}{4}$, $X_2 = \frac{1+\sqrt{13}}{3}$, $X_3 = \frac{2+\sqrt{13}}{3}$, $X_4 = \frac{1+\sqrt{13}}{4}$, $X_5 = 3+\sqrt{13}$ all have purely periodic continued fractions; namely $X_1 = [\overline{1,1,1,1,6}]$, $X_2 = [\overline{1,1,1,6,1}]$, $X_3 = [\overline{1,1,6,1,1}]$, $X_4 = [\overline{1,6,1,1,1}]$,$X_5 = [\overline{6,1,1,1,1}]$. This, as well, is no coincidence. In fact, given the periodic nature of the continued fraction expansion for $\sqrt{13}$ it is essential that X_1,...,X_5 have purely periodic continued fraction expansions.

The numbers X_1,...,X_5 are known as reduced quadratic irrationals. A *quadratic irrational* is a number that solves a quadratic equation with integer coefficients and whose discriminant is positive but not a perfect square. All quadratic irrationals have the form $A + B \cdot \sqrt{D}$, where $A, B \in \mathbb{Q}$ and $D \in \mathbb{Z}$ is not a perfect square. If $\alpha = A + B\sqrt{D}$ is a quadratic irrational, then so is $\alpha' = A - B\sqrt{D}$. In fact, α and α' both satisfy the same quadratic equation. The number α' is the *conjugate* root of α. The properties of conjugates are summarized in the following theorem.

Theorem 1.11 *Let α and β be quadratic irrationals. Then the following hold:*

(a) $(\alpha \pm \beta)' = \alpha' \pm \beta'$.

(b) $(\alpha \cdot \beta)' = \alpha' \cdot \beta'$.

(c) $(\frac{\alpha}{\beta})' = \frac{\alpha'}{\beta'}$.

If α is a quadratic irrational such that $1 < \alpha$ and $-1 < \alpha' < 0$ then α is said to be a *reduced quadratic irrational*. The next theorem relates reduced quadratic irrationals and numbers that have purely periodic continued fraction expansions. We will refer to it as Galois' Theorem.

Theorem 1.12 (Galois' Theorem) *α is a reduced quadratic irrational if and only if the continued fraction for α is purely periodic. Moreover, if β is the continued fraction for α but with the period reversed, then $\alpha' = \frac{-1}{\beta}$.*

We will mainly be concerned with the continued fraction expansions of $\sqrt{P}$, where P is a prime. In fact, these continued fractions have a very interesting form, which is summarized in the next theorem.

Theorem 1.13 *Let P be a prime. Then, $\sqrt{P} = [a_0, \overline{a_1, a_2, a_3, ..., a_3, a_2, a_1, 2a_0}]$.*

Proof: Let $\sqrt{P} = [a_0, a_1, a_2, a_3, ...]$. Note that $\sqrt{P}$ is not a reduced quadratic irrational, as $\sqrt{P} > 1 \Rightarrow -\sqrt{P} < -1$. However, since $a_0 = [\sqrt{P}]$, $a_0 + \sqrt{P}$ is reduced (since $a_0 + \sqrt{P} > 1$ and $-1 < a_0 - \sqrt{P} < 0$). Thus, by Galois' Theorem, the continued fraction for $a_0 + \sqrt{P}$ is purely periodic. Hence, fix an n so that $a_0 + \sqrt{P} = [\overline{2a_0, a_1, a_2, a_3, ..., a_n}]$. So, $\sqrt{P} = [a_0, \overline{a_1, a_2, a_3, ..., a_n, 2a_0}]$. This yields $\sqrt{P} - a_0 = [0, \overline{a_1, a_2, a_3, ..., a_n, 2a_0}]$. So, $\frac{1}{\sqrt{P}-a_0} = [\overline{a_1, a_2, a_3, ..., a_n, 2a_0}]$.

Let β be the continued fraction for $a_0+\sqrt{P}$, but with the repeating block reversed. Then, by Galois' Theorem, we have $\beta = \frac{-1}{\alpha'} = \frac{1}{\sqrt{P}-a_0} = [\overline{a_n, a_{n-1}, ..., a_2, a_1, 2a_0}]$.

So, $[\overline{a_1, a_2, a_3, ..., a_n, 2a_0}] = [\overline{a_n, a_{n-1}, ..., a_2, a_1, 2a_0}]$. Thus, $a_1 = a_n$, $a_2 = a_{n-1}$,..., $a_{n-1} = a_2$, $a_n = a_1$. $\square$

Once again returning to the partial quotients in the continued fraction for $\sqrt{13}$, consider $X_2 = [\overline{1, 1, 1, 6, 1}]$ and $X_4 = [\overline{1, 6, 1, 1, 1}]$. For illustrative purposes, let $\alpha = X_2$. Then, the continued fraction for α with the repeating block reversed is $\beta = X_4$. Then, by Galois' Theorem, $\alpha' = \frac{-1}{\beta}$. So, $\alpha' \cdot \beta = -1$. Taking conjugates, we obtain $\alpha \cdot \beta' = -1$. This illustrates the following observation.

Observation 1.14 *Let α be a complete quotient in the continued fraction expansion of $\sqrt{P}$, where P is prime. Then, β, the continued fraction for α with the repeating block reversed, is also a complete quotient in the continued fraction expansion of $\sqrt{P}$, and moreover, $\alpha \cdot \beta' = -1$.*

To prove the statement in italics, notice that if β is not a complete quotient in the continued fraction expansion of $\sqrt{P}$, then this contradicts the symmetric nature of $\sqrt{P}$ that was established in Theorem 1.13. By Galois' Theorem, $\alpha' \cdot \beta = -1$. Then, taking conjugates, we have $\alpha \cdot \beta' = -1$.

1.2 Historical Solutions

1.2.1 The methods of Brahmagumpta and Bhaskara

The Indian mathematicians Brahmagumpta (ca. 600 AD) and Bhaskara (1114-1185) developed methods for solving Pell equations [1]. In fact, Brahmagumpta challenged

that "Any person who can within a year solve $X^2 - 92 \cdot Y^2 = 1$ is a mathematician". By this criterion, both Bhaskara and the eleventh century Indian mathematician A. D. Jayadeva were mathematicians. Indeed, both Bhaskara and Jayadeva gave general solutions to Pell's equation.

The following identity, attributed to Brahmagumpta, is extremely useful for creating solutions to Pell-Like equations. We will refer to it as Brahmagumpta's Identity and use it often.

Theorem 1.15 (Brahmagumpta) *If $u^2 - Pv^2 = k$ and $r^2 - Ps^2 = l$ then $(ur \pm Pvs)^2 - P(us \pm vr)^2 = kl$.*

Proof: Notice that $(ur + Pvs)^2 = u^2r^2 + 2Puvrs + P^2v^2s^2$ and $(us + vr)^2 = u^2s^2 + 2uvrs + v^2r^2$. So, $-P(us + vr)^2 = -Pu^2s^2 - 2Puvrs - Pv^2r^2$. So, $kl = (u^2 - Pv^2)(r^2 - Ps^2) = r^2(u^2 - Pv^2) - Ps^2(u^2 - Pv^2) = (u^2r^2 - Pv^2r^2) + (P^2v^2s^2 - Pu^2s^2) = (u^2r^2 - Pv^2r^2) + (P^2v^2s^2 - Pu^2s^2) + 2Puvrs - 2Puvrs = (u^2r^2 + 2Puvrs + P^2v^2s^2) + (-Pu^2s^2 - 2Puvrs - Pv^2r^2) = (ur + Pvs)^2 - P(us + vr)^2$ $\square$

We now describe Bhaskara's method for solving Pell equations. The following lemma, attributed to Bhaskara, will simplify our work.

Theorem 1.16 (Bhaskara) *Let N be square free and k a nonzero integer. If (x_0, y_0) solves $X^2 - NY^2 = k$, then for every integer m, $(mx_0 + Ny_0, y_0m + x_0)$ solves $X^2 - NY^2 = k(m^2 - N)$. Moreover, if $gcd(k, y_0) = 1$ and $k \cdot l = (my_0 + x_0)$ for some $l \in \mathbb{Z}$ then $k|(m^2 - N)$ and $k|(mx_0 + Ny_0)$.*

Proof: We have $(mx_0 + Ny_0)^2 = m^2x_0^2 + 2mNx_0y_0 + N^2y_0^2$ and $(y_0m + x_0)^2 = y_0^2m^2 + 2x_0y_0m + x_0^2$. Thus, $-N(y_0 + m + x_0)^2 = -Ny_0^2m^2 - 2Nx_0y_0m - Nx_0^2$. So, $(mx_0+Ny_0)^2-N(y_0m+x_0)^2 = m^2x_0^2+2mNx_0y_0+N^2y_0^2-Ny_0^2m^2-2Nx_0y_0m-Nx_0^2 = m^2x_0^2+N^2y_0^2-Ny_0^2m^2-Nx_0^2 = (x_0^2-Ny_0)m^2-(x_0^2-Ny_0^2)N = km^2-kN = k(m^2-N)$.

Now assume that $gcd(k, y_0) = 1$ and $k \cdot l = (my_0 + x_0)$ for some $l \in \mathbb{Z}$. Then, $k(1-l(x_0-my_0)) = k-(x_0-my_0)k\cdot l = k-(x_0-my_0)(x_0+my_0) = k-x_0^2+m^2y_0^2 = m^2y_0^2-Ny_0^2 = (m^2-N)y_0^2$. Thus, $k|(m^2-N)y_0^2$. But, $gcd(k, y_0) = 1$. So, $k|(m^2-N)$. So, there is $r \in \mathbb{Z}$ such that $kr = (m^2 - N)$. As for $k|(mx_0 + Ny_0)$, $k(ml - ry_0) = mkl - kry_0 = m(x_0 + my_0) - (m^2 - N)y = mx_0 + m^2y_0 - m^2y_0 + Ny_0 = mx_0 + Ny_0$.

□

We now describe *Bhaskara's Algorithm* for solving Pell equations. Let P be any prime. We wish to solve $X^2 - PY^2 = 1$. Choose integers a, b, k such that $a^2 - Pb^2 = k$, and $gcd(k, b) = 1$. Thus, by Bhaskara's Lemma, for any integer m, we have $(ma + Pb)^2 - P(mb + a)^2 = k(m^2 - P)$. Multiplying this equation by $\frac{1}{k^2}$ yields the equation $(\frac{ma+Pb}{k})^2 - P(\frac{bm+a}{k})^2 = \frac{m^2-P}{k}$.

We choose m such that $k|mb + a$ and $|\frac{m^2-P}{k}|$ is as small as possible. Thus, by Bhaskara's Lemma, $(\frac{ma+Pb}{k})^2-P(\frac{bm+a}{k})^2 = \frac{m^2-P}{k}$ is a Pell-like equation. If $\frac{m^2-P}{k} = 1$, then we are done. If $\frac{m^2-P}{k} \neq 1$ then we let $a' = \frac{ma+Pb}{k}$, $b' = \frac{bm+a}{k}$, and $k' = \frac{m^2-P}{k}$. Thus, we obtain $(a')^2 - P(b')^2 = k'$. Moreover, notice that $gcd(k', b') = 1$.

Once again using Bhaskara's Lemma and multiplying by $\frac{1}{(k')^2}$, we arrive at $(\frac{m'a'+Pb'}{k'})^2 - P(\frac{b'm'+a'}{k'})^2 = \frac{(m')^2-P}{k'}$ for any integer m'. We choose m' such that

$k'|m'b' + a'$ and $|\frac{(m')^2-P}{k'}|$ is as small as possible and conclude that $(\frac{m'a'+Pb'}{k'})^2 - P(\frac{b'm'+a'}{k'})^2 = \frac{(m')^2-P}{k'}$ is another Pell-like equation. If $\frac{(m')^2-P}{k'} = 1$, then we are done. If $\frac{(m')^2-P}{k'} \neq 1$, then we continue this process. We will not prove that this particular algorithm *always* produces a solution to $X^2 - PY^2 = 1$. In the next section we will give a systematic method for *always* finding solutions to Pell's equation. We now give an example to illustrate Bhaskara's Algorithm.

Example 1.17 Bhaskara's algorithm applied to $X^2 - 61Y^2 = 1$. Consider $8^2 - 61 \cdot 1^2 = 3$. For any $m \in \mathbb{Z}^+$, we have $(\frac{8m+61}{3})^2 - P(\frac{8+m}{3})^2 = \frac{m^2-61}{3}$. We now find m such that $3|m + 8$ with $|\frac{m^2-61}{3}|$ as small as possible. This yields $39^2 - 61 \cdot 5^2 = -4$ [1].

TABLE 1.2 Bhaskara's Method Applied to $X^2 - 61Y^2 = 1$

Step	a	b	k
1	8	1	3
2	39	5	-4
3	164	21	-5
4	453	58	5
5	1523	195	4
6	5639	722	-3
7	29718	3805	-1
8	469849	60158	-3
9	2319527	296985	4
10	9747957	1248098	5
11	26924344	3447309	-5
12	90520989	11590025	-4
13	335159612	42912791	3
14	1766319049	226153980	1

Continuing this process, noting that $gcd(-4, 5) = 1$ we arrive at $(\frac{39m+305}{-4})^2 -$

$P(\frac{5m+39}{-4})^2 = \frac{m^2-61}{-4}$. We now look for m such that $-4|5m+39$ and $|\frac{m^2-61}{-4}|$ is as small as possible. This yields $164^2 - 61 \cdot 21^2 = -5$ [1].

Continuing this process we yield a string of fourteen solved Pell-Like equations, as shown in Table 1.2. The fourteenth of these equations is $1766319049^2 - 61 \cdot 226153980^2 = 1$ [1]. That Bhaskara had the ability, sans calculator or modern algebraic notions, to solve Pell equations, is remarkable.

1.2.2 Wallis-Brounker Method

In 1657, Pierre de Fermat, arguably the best Number Theorist of his time, issued a challenge to the English Mathematician John Wallis. Fermat asked Wallis to, in general, find an integer y such that $dy^2 + 1$ is a square integer, where d is any non square integer [2]. In this subsection we will discuss the method devised by Wallis and his patron, Lord William Brounker.

We will now consider the solvability of $X^2 - 7Y^2 = 1$. Through trial and error one quickly arrives at $(8, 3)$ as the least positive solution to $X^2 - 7Y^2 = 1$. However, for explanatory purposes, this equation allows us to easily digest the Wallis-Brounker Method.

The smallest square bigger than 7 is $3^2 = 9$. So, $7 = 3^2 - 2$. Clearly, for any integer m, $7m^2 = (3m)^2 - 2m^2$. What we are looking for here is $m \in \mathbb{Z}$ such that $(3m)^2 - 2m^2 + 1$ is a square. Since $m = 1$ does not do the trick, we move on to $m = 2$. This yields $7 \cdot 2^2 = (3 \cdot 2)^2 - 2 \cdot 2^2 = 20$, which does not work either. We try $m = 3$.

This yields $7 \cdot 3^2 = (3 \cdot 3)^2 - 2 \cdot 3^2 = 63$. We write $63 = (3 \cdot 3)^2 - 2 \cdot 3^2 = 8^2 - 1$ and substitute this into $7 \cdot 3^2 = (3 \cdot 3)^2 - 2 \cdot 3^2 = 63$ to obtain $7 \cdot 3^2 = 8^2 - 1$ which yields $8^2 - 7 \cdot 3^2 = 1$.

In [2], Wallis and Brounker used this method to solve $X^2 - 151Y^2 = 1$ and $X^2 - 313Y^2 = 1$. However, the Wallis-Brounker Method for solving Pell equations does not work in general.

1.2.3 The Euler-Lagrange General Solution

While Wallis and Brounker were able to solve particular Pell equations, Leonard Euler gave the first published general solution in 1759 [2]. Although, it was Lagrange who gave the first proof of Theorem 1.21, which asserts that all solutions to Pell equations may be found among the convergents in the continued fraction expansion of $\sqrt{P}$ where P is prime and $X^2 - PY^2 = 1$ [2]. Lagrange also proved that the continued fraction expansion of any quadratic irrational is periodic from some point onward. For a proof of this remarkable theorem, see [8].

To prove Theorem 1.19 we will need the following.

Theorem 1.18 *Let $X \in \mathbb{R} - \mathbb{Q}$ and $\frac{a}{b} \in \mathbb{Q}$ with $gcd(a, b) = 1$ and $b \geq 1$.*

If $|X - \frac{a}{b}| < \frac{1}{2b^2}$, then $\frac{a}{b}$ is a convergent in the continued fraction expansion of X.

As an aside, Hurwitz proved that for every irrational X there are infinitely many $\frac{p}{q} \in \mathbb{Q}$ such that $|X - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$. The 5 cannot be enlarged. Moreover, Thue, Siegel, and Roth proved that for algebraic irrationals, the exponent 2 cannot be enlarged.

This is the beginning of approximation theory. See [8].

Theorem 1.19 *If (p, q) is a solution to $X^2 - PY^2 = 1$, then $\frac{p}{q}$ is a convergent in the continued fraction expansion of $\sqrt{P}$.*

Proof: Since $p^2 - Pq^2 = 1$, we have $(p - q\sqrt{P})(p + q\sqrt{P}) = 1$. Thus, $\frac{p}{q} - \sqrt{P} = \frac{1}{q(p+q\sqrt{P})}$ and $p > q$ (since $p \leq q \Rightarrow p \leq q\sqrt{P} \Rightarrow p - q\sqrt{P} \leq 0 \Rightarrow 1 \leq 0$).

Thus, $0 < \frac{p}{q} - \sqrt{P} < \frac{\sqrt{P}}{q(q\sqrt{P}+q\sqrt{P})} = \frac{\sqrt{P}}{2q^2\sqrt{P}} = \frac{1}{2q^2}$. So, by Theorem 1.18, $\frac{p}{q}$ is a convergent in the continued fraction expansion of $\sqrt{P}$. $\square$

We now show that all Pell equations are solvable. To do this we need the following facts. First, *if $X = [a_0, a_1, a_2, ..., a_n, X_{n+1}]$, then we may write $X = \frac{X_{n+1}p_n + p_{n-1}}{X_{n+1}q_n + q_{n-1}}$* and *for all $n \in \mathbb{N}$, $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$* [8].

Theorem 1.20 *If r is the length of the period in the continued fraction expansion of $\sqrt{P}$, then $p_{kr-1}^2 - Pq_{kr-1}^2 = (-1)^{kr}$ where k runs through all natural numbers and $\frac{p_k}{q_k}$ is any convergent in the continued fraction expansion of $\sqrt{P}$.*

Proof: Let $k \in \mathbb{N}$. By Theorem 1.13, $\sqrt{P} = [a_0, \overline{a_1, a_2, a_3, ..., a_3, a_2, a_1, 2a_0}]$. So, $a_0 + \sqrt{P} = [\overline{2a_0, a_1, a_2, ..., a_2, a_1}]$. Thus, we may write $\sqrt{P} = [a_0, a_1, a_2, ..., a_{kr-1}, a_0 + \sqrt{P}]$. By the remark above, we have $a_0 + \sqrt{P} = \frac{a_0\sqrt{P}p_{kr-1}+p_{kr-2}}{a_0+\sqrt{P}q_{kr-1}+q_{kr-2}}$, which gives rise to the equation $Pq_{kr-1} + (a_0 q_{kr-1} + q_{kr-2})\sqrt{P} = (a_0 p_{kr-1} + p_{kr-2}) + p_{kr-1}\sqrt{P}$. Thus, $Pq_{kr-1} = (a_0 p_{kr-1} + p_{kr-2})$ and $(a_0 q_{kr-1} + q_{kr-2}) = p_{kr-1}$, which yields $p_{kr-2} = Pq_{kr-1} - a_0 p_{kr-1}$ and $q_{kr-2} = p_{kr-1} - a_0 q_{kr-1}$.

By the above we have $p_{kr-1}q_{kr-2} - q_{kr-1}p_{kr-2} = (-1)^{kr-2} = (-1)^{kr}$. So, $p_{kr-1}(p_{kr-1} -$

$a_0q_{kr-1}) - q_{kr-1}(Pq_{kr-1} - a_0p_{kr-1}) = p_{kr-1}^2 - Pq_{kr-1}^2$. Thus, $p_{kr-1}^2 - Pq_{kr-1}^2 = (-1)^{kr}$.

□

Consider $X^2 - 19 \cdot Y^2 = 1$. Using the continued fraction algorithm we find that $\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}]$, where the period is 6. Thus, by Theorem 1.20, $X^2 - 19 \cdot Y^2 = 1$ is solvable, and moreover, $\frac{p_5}{q_5} = \frac{170}{39}$, $\frac{p_{11}}{q_{11}} = \frac{57799}{13260}$, $\frac{p_{17}}{q_{17}} = \frac{19651490}{4508361}$, $\frac{p_{23}}{q_{23}} = \frac{6681448801}{1532829480}$ are particular solutions. Indeed, as the reader may check, $170^2 - 19 \cdot 39^2 = 1$, $57799^2 - 19 \cdot 13260^2 = 1$, $19651490^2 - 19 \cdot 4508361^2 = 1$, $6681448801^2 - 19 \cdot 1532829480^2 = 1$.

Theorem 1.20 may be used to prove the following. We will generalize Theorem 1.21 in section 3.2.

Theorem 1.21 *Let r be the length of the period in the continued fraction expansion of $\sqrt{P}$.*

(a) If r is even, then all positive solutions to $X^2 - PY^2 = 1$ are given by $X = p_{kr-1}$ and $Y = q_{kr-1}$, $k = 1, 2, 3, ...$

(b) If r is odd, then all positive solutions to $X^2 - PY^2 = 1$ are given by $X = p_{2kr-1}$ and $Y = q_{2kr-1}$, $k = 1, 2, 3, ...$

To implement Theorem 1.21, one must be able to determine if the length of the period, r, is even or odd. In fact, computing r is at the very heart of the matter, for, according to [10], for some constant A, we have $A \cdot \log(P) < r < 0.72\sqrt{P} \cdot \log(P)$ and it is anticipated that $A \cdot \sqrt{P} < r < 0.72\sqrt{P} \cdot \log(P)$. Thus, it is anticipated that the time it takes to compute r may not happen in polynomial time.

We will now give a criterion for recursively finding all positive solutions to Pell equations, but first, some terminology. We will often refer to the smallest positive solution to a Pell equation as the *fundamental solution.*

Theorem 1.22 *Let (x_1, y_1) be the fundamental solution to $X^2 - PY^2 = 1$. Then, all solutions to $X^2 - PY^2 = 1$ are given by (x_n, y_n) where $x_n + y_n\sqrt{P} = (x_1 + y_1\sqrt{P})^n$, where n runs through all Positive Integers.*

By Theorem 1.21, we know that all solutions to $X^2 - PY^2 = 1$ are among the convergents in the continued fraction expansion of $\sqrt{P}$. The next theorem generalizes this result.

Theorem 1.23 (Lagrange) *If (p, q) is a solution to $X^2 - PY^2 = k$ and $|k| < \sqrt{P}$, then $\frac{p}{q}$ is a convergent in the continued fraction expansion of $\sqrt{P}$.*

1.3 The Pell Class Approach

We now introduce a method for determining the solvability of Pell-Like equations. As we shall see, this approach is not efficient in any sense. However, the Pell Class approach does give us a good place to start.

Let P be any prime, k any integer, and (a, b), (r, s) be solutions to $X^2 - PY^2 = k$. Then, (a, b) and (r, s) are said to be *associated* if for some solution (u, v) to $X^2 - PY^2 = 1$ we have $(au \pm Pbv, av \pm bu) = (r, s)$. Notice that this is well defined by

Brahmagumpta's Identity. Observe that being "associated" is an equivalence relation. An equivalence class for this equivalence relation is said to be a *Pell Class*.

Let K be a Pell Class for $X^2 - PY^2 = k$ and $(x_0, y_0) \in K$. Suppose that y_0 is the smallest positive second coordinate appearing in a pair in K. Then, x_0 is a uniquely determined positive integer. We call (x_0, y_0) the *primitive solution* of the class K. If (u, v) is a solution to $X^2 - PY^2 = k$ and v is the smallest second coordinate among all positive second coordinates of solutions to $X^2 - PY^2 = k$ and u is positive, then we call (u, v) the *fundamental solution* to $X^2 - PY^2 = k$.

The theory of Pell Classes yields tight bounds that may be used to search for the fundamental solution of Pell-Like equations. The main theorem is the following.

Theorem 1.24 *Let P be prime and (x_1, y_1) be the fundamental solution of $X^2 - PY^2 = 1$. If (u,v) is the fundamental solution of $X^2 - PY^2 = k$, then $0 \leq |u| \leq \sqrt{k(x_1+1)/2}$ and $0 \leq v \leq y_1\sqrt{k/(2(x_1+1))}$.*

From a computational standpoint, the question as to the solvability of any equation may be formulated into two problems: a *decision problem*, and a *search problem*. The decision problem seeks an efficient algorithm with an output of solvable or not solvable when given any instance of an equation. The search problem seeks to find all solutions, provided solutions exist, in a reasonable amount of time.

Phrased in terms of the Pell Class approach, the Pell-Like decision and search problems for a prime P and integer k are (respectively): *Is there an efficient means to decide if there is a nonempty Pell Class* and *Is there an efficient method for finding*

the primitive solution in each Pell Class.

Moreover, by Theorem 1.23, when $|k| < \sqrt{P}$ and $X^2 - PY^2 = k$ is solvable, then all primitive solutions of the Pell Classes associated with k are to be found among the convergents of the continued fraction expansion of $\sqrt{P}$. These matters are examined further in section 3.2.

Chapter 2

A GENERAL CRITERION FOR SOLVABILITY

2.1 Introduction

Disregarding any time considerations, Theorem 1.24 may be used to determine whether any Pell-Like equation is solvable or not.

Example 2.1 The Pell-Like equation $X^2-53Y^2 = 28$. According to Theorem 1.24, if $X^2-53Y^2 = 28$ is solvable its fundamental solution (u,v) must lie within the following bounds: $0 \leq |u| \leq [\sqrt{28(66249+1)/2}] = 963$ and $0 \leq v \leq [9100\sqrt{28/(2(66249+1))}] = 132$, where $(66249, 9100)$ is the fundamental solution to $X^2 - 53Y^2 = 1$. With a little work, one may find that $u = 9$ and $v = 1$ is the fundamental solution to $X^2 - 53Y^2 = 28$.

Example 2.2 The Pell-Like equation $X^2-43Y^2 = 35$. According to Theorem 1.24, if $X^2-43Y^2 = 35$ is solvable its fundamental solution (u,v) must lie within the following bounds: $0 \leq |u| \leq [\sqrt{35(3482+1)/2}] = 246$ and $0 \leq v \leq [532\sqrt{35/(2(3482+1))}] = 37$, where $(3482, 532)$ is the fundamental solution to $X^2 - 43Y^2 = 1$. After checking all $9,102$ possible combinations of (u, v) we eventually see that $X^2 - 43Y^2 = 35$ is not solvable.

With regards to computational efficiency, the question of solvability for these particular Pell-Like equations are no match for modern computers. But, what happens when k gets large? It is not hard to see that, as $k \to \infty$, $[\sqrt{k(x_1+1)/2}]$ grows without bound. Thus, Theorem 1.24, though a nice tool, does not allow one to efficiently decide if a particular Pell-Like equation is solvable, especially when k gets big.

Example 2.3 $X^2 - 313Y^2 = 172635965$. If this equation is solvable, its fundamental solution (u, v) will lie within the following bounds: $0 \leq |u| \leq 94216351720$, $0 \leq v \leq 942163517200$, where $(32188120829134849, 1819380158564160)$ is the fundamental solution to $X^2 - 313Y^2 = 1$.

Using the methods of 2.4 we will be able to show that $X^2 - 313Y^2 = 172635965$ is not solvable. We use MAPLE to gain a rough estimate on the amount of time it would take, using the Pell Class approach, to determine that $X^2 - 313Y^2 = 172635965$ is not solvable. Using MAPLE on a *Pentium D* powered computer, with a processor speed of 3.0 GHz, it can be determined that it takes roughly 0.0000000062 seconds to perform an arithmetic operation. Thus, neglecting the time it takes to make comparisons, it takes $4 \cdot 0.0000000062 = 0.0000000248$ seconds to check if $X^2 - 313Y^2 = 172635965$ is solvable for a particular pair of integers chosen from their respective ranges is solvable or not. We have $94216351720 \cdot 942163517200 = 8.876720931 \times 10^{22}$ possible pairs to check. Thus, it would, roughly, take $0.0000000248 \cdot 8.876720931 \times 10^{22} = 2.201426791 \times 10^{15}$ seconds to decide the unsolvability of $X^2 - 313Y^2 = 172635965$. This is about $611,507,442,000$ hours which is about $69,806,785$ years.

Thus, in this particular example, with $k = 172635965$ relatively small, it is not hard to see that, using this approach, even with our modern high powered computing machines, a decision as to whether or not $X^2 - 313Y^2 = 172635965$ is solvable will take a considerable amount of time.

Recall, from section 1.3, that the question of solvability of any equation may be formulated into two problems: a *decision problem*, and a *search problem*. Using these classifications, we now define the Pell-Like decision and search problems. The Pell-Like decision problem is: *Given a prime P and an integer k, is there an efficient means to decide if $X^2 - PY^2 = k$ is solvable?* Assuming for a prime P and integer k, $X^2 - PY^2 = k$ is solvable, the Pell-Like search problem for P and k is: *Can we find all primitive solutions in the Pell classes of $X^2 - PY^2 = k$ in a reasonable amount of time*?

Notice that a general criterion for solvablilty is, in effect, a solution to a decision problem. Thus, to find a *general criterion for the solvability* of Pell-Like equations is the same as solving the Pell-Like equation decision problem for all instances of Pell-Like equations.

The Pell Class approach does not solve either of these problems for all Pell-Like equations. Indeed, for large k, as in example 2.3, the Pell Class approach does not yield an efficient algorithm to answer the decision problem. Moreover, if for some prime P and integer k, $X^2 - PY^2 = k$ is solvable, the Pell Class approach only guarantees that one will find the fundamental solution. Still, the Pell Class approach

is a step in the right direction and its power has been employed in the data collection for this Thesis (see Appendix A.1).

In the rest of this and the next chapter we address the problem of finding a general criterion for solvability of Pell-Like equations and give a partial solution. In effect, we solve the Pell-Like decision problem for many, but not all, Pell-Like equations.

Most of the tests that we will develop throughout this chapter do not rely on integer factorization. However, a few of the implementations based on the theorems of Section 2.4 will rely heavily on the efficiency of integer factorization, which is likely no more efficient than tests based on the Pell Class approach. Throughout this chapter, we will give special attention to these considerations.

The next section gives an equivalent formulation of the Pell-Like decision problem.

2.2 The Square Polynomial Problem

In this section we will show that the decision problem for Pell-Like equations is equivalent to the problem of deciding whether or not a particular second degree polynomial with integer coefficients has a square integer value. We start with an example.

Consider the question of solvability for $X^2 - 17 \cdot Y^2 = 47$. Since $(47/17) = 1$, we know there is $a \in \mathbb{Z}$ such that $a^2 \equiv 47 \bmod 17$. Equivalently, there is $m \in \mathbb{Z}$ such that $17m = a^2 - 47$. If $m = \frac{a^2-47}{17}$ is a square integer, then we are done. Indeed, for if $m = b^2$, then we have $17b^2 = a^2 - 47$. Thus, $a^2 - 17b^2 = 47$.

Recall that equivalence mod 17 is an equivalence relation and that a is a representative of the equivalence class $\{a + 17n : n \in \mathbb{Z}\}$. Thus, if m is not a square, we may use the fact that $(a+17\cdot 1)^2 \equiv a^2 \equiv 47 \bmod 17$ to form $17m' = (a+17\cdot 1)^2 - 47$. If $m' = \frac{(a+17\cdot 1)^2-47}{17}$ is a square, then once again we are done.

What if m' is not a square? Then, we may use the fact that $(a+17\cdot 2)^2 \equiv a^2 \equiv 47$ mod 17 to form $17m'' = (a + 17 \cdot 2)^2 - 47$ and check if $m'' = \frac{(a+17\cdot 2)^2-47}{17}$ is a square. If m'' is a square then we are done.

Continuing in this way we see that we have an infinitum of candidates for m becoming a square. In other words, is it possible that for some $n \in \mathbb{Z}$, $\frac{(a+17\cdot n)^2-47}{17} = 17n^2 + 2an + \frac{a^2-47}{17}$ is a square? This is the square polynomial decision problem for $P = 17$ and $k = 47$.

The general square polynomial decision problem is the following: *does there exist an algorithm that, for any odd prime P and $k \in \mathbb{Z}$ with $(k, P) = 1$ decides if there is for some a with $k \equiv a^2$ mod P an $n \in \mathbb{Z}$ such that $Pn^2 - 2an + \frac{a^2-k}{P}$ is a square*?

The square polynomial and Pell-Like equation solvability decision problems for specific P and k may be formulated in terms of *Arithmetic* functions.

Let P be prime, $k \in \mathbb{Z}$, with $(k/P) = 1$ and consider $X^2 - PY^2 = k$. Since $(k/P) = 1$ we have $(\exists a \in \mathbb{Z})$, $(a^2 \equiv k \bmod P)$. Note that the algorithm of Tonelli-Shanks, assuming the Generalized Riemann Hypothesis, efficiently finds an $a \in \mathbb{Z}$ such that $a^2 \equiv k \bmod P$.

Define

$$\Phi(P,k) = \begin{cases} 1 & \text{if } (\exists n \in \mathbb{Z})(\exists a \in \mathbb{Z}_P)(k^2 \bmod P \text{ and } Pn^2 - 2an + \frac{a^2-k}{P}) \text{ is a square} \\ -1 & \text{otherwise} \end{cases}$$

and

$$\Psi(P,k) = \begin{cases} 1 & \text{if } X^2 - PY^2 = k \text{ is solvable} \\ -1 & \text{otherwise} \end{cases}$$

We now have the proper terminology to prove the following.

Theorem 2.4 *Let P be an odd prime and $k \in \mathbb{Z}$, with $(k/P) = 1$.*

Then, $\Psi(P,k) = 1 \Leftrightarrow \Phi(P,k) = 1$.

Proof: Suppose $\Psi(P,k) = 1$. So, there are $u, m \in \mathbb{Z}$ such that $u^2 - Pm^2 = k$. Note that $u^2 \equiv k$ mod P. To prove $\Phi(P,k) = 1$ we must show that there is an integer n such that $Pn^2 - 2un + \frac{u^2-k}{P}$ is a square. We have $\frac{u^2-k}{P} = m^2$. Thus, we choose $n = 0$. So, $\Phi(P,k) = 1$.

Now, suppose $\Phi(P,k) = 1$. That is, there are integers n, m and $u \in \mathbb{Z}_P$ such that $u^2 \equiv k$ mod P and $Pn^2 - 2un + \frac{u^2-k}{P} = m^2$. So, $P^2n^2 + 2Pun + u^2 - k = pm^2 \Rightarrow (u+pn)^2 - k = Pm^2 \Rightarrow (u+pn)^2 - Pm^2 = k$. So, $((u+pn), m)$ furnishes a solution

to $X^2 - PY^2 = k$. Thus, $\Psi(P, k) = 1$. $\square$

This proves that the square polynomial decision problem is equivalent to the Pell-Like decision problem.

2.3 The Legendre Test

The Legendre function and the Law of Quadratic Reciprocity provide our first test for the solvability of Pell-Like equations. Consider the Pell-Like equation $X^2 - 17 \cdot Y^2 = -46$. Using theorems 1, 2, 3, and 4 we compute $(-46/17) = (-1/17) \cdot (46/17) = 1 \cdot (12/17) = (4/17) \cdot (3/17) = 1 \cdot (3/17) = (17/3) = (2/3) = -1$. Thus, $X^2 \equiv -46 \mod 17$ admits no solution. In other words, $X^2 - 17 \cdot Y^2 = -46$ is not solvable. For if $X^2 - 17 \cdot Y^2 = -46$ were solvable, then there would exist integers u, v such that $u^2 - 17 \cdot v^2 = -46$. But then, $u^2 - (-46) = 17 \cdot v^2$. So, $X^2 \equiv -46 \mod 17$ admits a solution and $(-46/17) = 1$, a clear contradiction. This illustrates the following theorem.

Theorem 2.5 *If* $(k/P) = -1$ *then* $\Psi(P, k) = -1$.

Proof: If $X^2 - PY^2 = k$ were solvable, then there are integers u, v such that $u^2 - P \cdot v^2 = k$. But then, $u^2 - k = P \cdot v^2$. So, $X^2 \equiv k \mod P$ admits a solution and $(k/P) = 1$, contradicting our assumption. $\square$

Corollary 2.6 *If* $(k/P) = 1$ *and* $(l/P) = -1$ *then* $X^2 - PY^2 = kl$ *is not solvable.*

The Legendre function and the Law of Quadratic Reciprocity open the door to many other tests for unsolvability. These are addressed in the next subsection.

2.4 Legendre Style Unsolvability Tests

As the title suggests, this section uses Quadratic Reciprocity and other properties of the Legendre function to characterize many tests for the unsolvability of Pell-Like equations. Our first theorem is motivated by the desire to understand the behavior of Pell-Like equations when k is negative.

Theorem 2.7 *If $P \equiv 3$ mod 4 and $(k/P) = 1$ then $x^2 - Py^2 = -k$ is not solvable.*

Proof: Let us suppose that $x^2 - Py^2 = -k$ is solvable. So, there are $r, s \in \mathbb{Z}$ such that $r^2 - Ps^2 = -k$. So, $r^2 - (-k) = Ps^2$. So, $X^2 \equiv -k$ mod P is solvable. So, $(-1/P) \cdot (k/P) = (-k/P) = 1$. So, $(-1/P) = (-1/P) \cdot 1 = (-1/P) \cdot (k/P) = (-k/P) = 1$. But, by the Law of Quadratic Reciprocity, this only happens when $P \equiv 1$ mod 4, contradicting our assumption. □

Example 2.8 *Consider $x^2 - 11y^2 = -5$. Since $(4, 1)$ solves $x^2 - 11y^2 = 5$, we have $(5/11) = 1$. Since $11 \equiv 3$ mod 4, we know, by Theorem 2.7, that $x^2 - 11y^2 = -5$ in not solvable.*

The next theorem yields a very general test for the unsolvability of a large class of Pell-Like equations. Although we assume the factorization of k we will not actually use factorization when implementing this theorem.

Theorem 2.9 *Let $P \equiv 3$ mod 4 and $k = m^2n$ with n square free. If $X^2 - PY^2 = k$ is solvable, then $n \equiv 1$ mod 4.*

Proof: Suppose that $n \equiv 3$ mod 4. Since $x^2 - Py^2 = k$ is solvable, there are $u, v \in \mathbb{Z}$ such that $u^2 - Pv^2 = m^2n$. We shall collect the following three facts:

(i) $(n/P) = 1$.

(ii) If q is a prime divisor of n with $q \equiv 3$ mod 4 , then $(q/P) = -1$.

(iii) Let $r = |\{q : q|n$ and q is an odd prime and $q \equiv 3$ mod $4\}|$. Then r is odd.

Since $u^2 - Pv^2 = m^2 \cdot n$, we have $u^2 - m^2 \cdot n = Pv^2$. So, $X^2 \equiv k$ mod P is solvable. Thus, $(n/P) = (m^2 \cdot n/P) = 1$. This proves (i).

Now suppose that q is a prime divisor of n. So, $n = q \cdot n_0$ for some $n_0 \in \mathbb{Z}$. Thus, $u^2 - Pv^2 = q \cdot n_0$ and so $X^2 \equiv Pv^2$ mod q is solvable. So, $(P/q) = (Pv^2/q) = 1$. By the Quadratic Reciprocity Law, we know that, since $P \equiv q \equiv 3$ mod 4, $(P/q) = -(q/P)$. So, $-(q/P) = 1$. This proves (ii).

Let $n = q_1 \cdot ... \cdot q_r \cdot q_{r+1} \cdot ... \cdot q_l$, where $q_1 \equiv ... \equiv q_r \equiv 3$ mod 4 and $q_{r+1} \equiv ... \equiv q_l \equiv 1$ mod 4. If r is even then we may arrange these first r primes in pairs as follows: $(q_1 \cdot q_2), (q_3 \cdot q_4), ..., (q_{r-1} \cdot q_r)$. Then, for i even with $1 \leq i \leq r$ $(q_{i-1} \cdot q_i) \equiv 9 \equiv 1$ mod 4. But, then $n = (q_1 \cdot q_2) \cdot (q_3 \cdot q_4) \cdot ... \cdot (q_{r-1} \cdot q_r) \cdot q_{r+1} \cdot ... \cdot q_l \equiv 1$ mod 4 contrary to assumption. This proves (iii).

Again let $n = q_1 \cdot ... \cdot q_r \cdot q_{r+1} \cdot ... \cdot q_l$ where $q_1 \equiv ... \equiv q_r \equiv 3$ mod 4 and $q_{r+1} \equiv ... \equiv q_l \equiv 1$ mod 4. By (ii), we have $(q_1/P) \cdot ... \cdot (q_r/P) = (-1) \cdot ... \cdot (-1) = (-1)^r = -1$, since r is odd, by (iii). Also, $(q_{r+1}/P) \cdot ... \cdot (q_l/P) = (1) \cdot ... \cdot (1) = (1)^{l-r}$. Thus, by (i)

$1 = (n/P) = (q_1 \cdot ... \cdot q_r \cdot q_{r+1} \cdot ... \cdot q_l/P) = (q_1/P) \cdot ... \cdot (q_r/P) \cdot (q_{r+1}/P) \cdot ... \cdot (q_l/P) = (-1)^r \cdot (1)^{l-r} = -1$, a clear contradiction. $\square$

Theorem 2.9, when expressed using the contrapositive, yields a nice test for unsolvability. We state this as the following corollary.

Corollary 2.10 *Let $k = m^2n$ with n square free. If $P \equiv n \equiv 3$ mod 4, then $x^2 - Py^2 = k$ is not solvable.*

The next corollary follows immediately.

Corollary 2.11 *If $P \equiv k \equiv 3$ mod 4 and $l \equiv 1$ mod 4 then $X^2 - PY^2 = kl$ is not solvable.*

With Corollary 2.9 at our disposal, we can lay to rest the question of solvability for many Pell-Like equations. For example, consider $X^2 - 31Y^2 = 1008$. Since $1008 = 12^2 \cdot 7$ and $7 \equiv 3 \bmod 4$, Corollary 2.10 allows us to conclude that $X^2 - 31Y^2 = 1008$ is not solvable.

In Example 2.2, we considered the solvability of the Pell-Like equation $X^2 - 43Y^2 = 35$. Using a quick application of Corollary 2.10, we see that $X^2 - 43Y^2 = 35$ is not solvable.

The next theorem requires that we know an odd prime factor of k.

Theorem 2.12 *Let q be an odd prime such that q divides k .*

If $x^2 - Py^2 = k$ is solvable, then $(P/q) = 1$.

Proof: Suppose that $x^2 - Py^2 = k$ is solvable. So, there are $u, v \in \mathbb{Z}$ such that $u^2 - Pv^2 = k$. Since q divides k, we have $k = q \cdot k_0$ for some $k_0 \in \mathbb{Z}$. So, $q|(u^2 - Pv^2)$ and thus $(P/q) = (Pv^2/q) = 1$. □

Assuming that we can find an odd prime factor of k, the contrapositive to Theorem 2.12 paves the way for a nice test for unsolvability.

Corollary 2.13 *Let q be an odd prime such that q divides k .*

If $(P/q) = -1$, then $x^2 - Py^2 = k$ is not solvable.

Example 2.14 In Example 2.3, we noted that we would have to check up to 94216351720 possible X values to see if $X^2 - 313Y^2 = 172635965$ is or is not solvable. We computed that this would take $69,806,785$ years. But since $5|172635965$ and $(313/5) = -1$, we may use Corollary 2.13 to conclude that $X^2 - 313Y^2 = 172635965$ is not solvable.

Corollary 2.15 *Let q be an odd prime such that q divides k.*

If P or $q \equiv 1$ mod 4 and $(q/P) = -1$, then $x^2 - Py^2 = k$ is not solvable.

Proof: Since P or $q \equiv 1$ mod 4, $(P/q) = (q/P) = -1$. By Corollary 2.13, $x^2 - Py^2 = k$ is not solvable. □

Regarding the next corollary, integer factorization is used to write $k = m^2 n$ where n is square free.

Corollary 2.16 *Let $k = m^2 n$ where n is square free. If $P \equiv 5$ mod 8, and n is even then $x^2 - Py^2 = k$ is not solvable.*

Proof: Suppose that there exists $u, v \in \mathbb{Z}$ such that $u^2 - Pv^2 = k$ (that is, $x^2 - Py^2 = k$ is solvable). So, $u^2 - k = Pv^2$ and thus, $(n/P) = (m^2 n/p) = 1$. Since $2|n$ there is $n_0 \in \mathbb{Z}$ such that $n = 2 \cdot n_0$. So, $(2 \cdot n_0/P) = (n/P) = 1$. But $P \equiv 5$ mod $8 \Rightarrow (2/P) = -1$ So, there must be another prime factor of n, say q such that $(q/P) = -1$ (otherwise $(n/P) = -1$). But, n is square free. So, q is odd. Moreover, $P \equiv 5$ mod $8 \Rightarrow P \equiv 1$ mod 4. Thus, we may apply Corollary 2.13 to obtain that $x^2 - Py^2 = k$ is not solvable, contradicting our assumption. □

Example 2.17 $X^2 - 181Y^2 = 1908360$. Then since $181 \equiv 5$ mod 8 and $1908360 = (18)^2 \cdot 5890$ with $5890 = 2 \cdot 5 \cdot 19 \cdot 31$ even and square free, we have, by Corollary 2.16, that $X^2 - 181Y^2 = 1908360$ is not solvable.

2.5 Modulo N Unsolvability Tests

We now develop a relatively simple way to test for the unsolvability of Pell-Like equations.

Theorem 2.18 (Mod N Test) *If $x^2 - Py^2 = k$ is not solvable in $\mathbb{Z}_n$ then $x^2 - Py^2 = k$ is not solvable in $\mathbb{Z}$.*

Proof: If $x^2 - Py^2 = k$ is solvable in $\mathbb{Z}$, then there are $u, v \in \mathbb{Z}$ such that $u^2 - Pv^2 = k$. The remainder upon dividing $u^2 - Pv^2$ by n will be the same as the remainder in the

division of k by n. Thus, $u^2 - Pv^2 = k$ in $\mathbb{Z}_n$. Thus, by the contrapositive, we have the result. $\square$

Note that if $x^2 - Py^2 = k$ is solvable in $\mathbb{Z}_n$ then it is not necessarily the case that $x^2 - Py^2 = k$ is solvable in $\mathbb{Z}$.

Remark 2.19 Using the Mod N Test, we can define a *probabilistic* algorithm that, when given a prime P and integer k as input, will yield an output of 'unsolvable' or 'probably solvable'. For primes $P_1, P_2, ..., P_g$, define $Q(P_1, P_2, ..., P_g, P, k)$ to be the probability that $X^2 - PY^2 = k$ is unsolvable but for all $1 \leq i \leq g$, $X^2 - PY^2 = k$ is solvable in $\mathbb{Z}_{Pi}$. We fix a base of primes $B = \{P_1, P_2, ..., P_g\}$ such that $Q(P_1, P_2, ..., P_g, P, k)$ is small. Then, if for each P_i, $X^2 - PY^2 = k$ is solvable in $\mathbb{Z}_{Pi}$ we may conclude that it is highly likely that $X^2 - PY^2 = k$ is solvable. Moreover, if there is at least one P_i for which $X^2 - PY^2 = k$ is not solvable in $\mathbb{Z}_{Pi}$, the Mod P_i Test allows us to conclude that $X^2 - PY^2 = k$ is not solvable.

That such a base of primes $B = \{P_1, P_2, ..., P_g\}$ such that $Q(P_1, P_2, ..., P_g, P)$ is small exists has yet be proven. Further research into the Pell-Like decision and search problems should address this issue.

We now give an alternate proof of the weaker version of Theorem 2.14 discussed in the previous section.

Theorem 2.20 *Let P be prime and k odd with $P \equiv 3$ mod 4. If $x^2 - Py^2 = k$ is solvable, then $k \equiv 1$ mod 4.*

Proof: Notice that $2^2 \equiv 4 \equiv 0$ and $3^2 \equiv 9 \equiv 1 \bmod 4$. So, $x^2 \equiv 0$ or 1 and $y^2 \equiv 0$ or 1 mod 4. By direct calculation, we see that $x^2 - Py^2 \equiv x^2 - 3y^2 \equiv 0$, 1, or 2 mod 4. Thus, if $k \equiv 3 \bmod 4$, $x^2 - Py^2 = k$ is not solvable in $\mathbb{Z}_4$. Thus, by the mod N test, $x^2 - Py^2 = k$ is not solvable in $\mathbb{Z}$. The result follows using the contrapositive. □

Using this exact same argument, but in $\mathbb{Z}_8$, allows one to prove the following.

Theorem 2.21 *Let P be an odd prime. If $P \equiv 1$, 3, or 5 mod 8, and $k \equiv 2$ mod 4, then $x^2 - Py^2 = k$ is not solvable.*

2.6 Solvability Tests

We now give some tests for the solvability of Pell-Like equations. The first was proved in section 1.2.1.

Theorem 2.22 (Brahmagumpta) *If $u^2 - Pv^2 = k$ and $r^2 - Ps^2 = l$ then $(ur \pm Pvs)^2 - P(us \pm vr)^2 = kl$.*

Let us now consider the question of solvability of $X^2 - 29Y^2 = 575$. Since $575 = 25 \cdot 23$ and $X^2 - 29Y^2 = 25$ and $X^2 - 29Y^2 = 23$ are both solvable, with solutions $(5, 0)$ and $(38, 7)$, $X^2 - 29Y^2 = 575$ is solvable by Theorem 2.22.

Suppose we wish to find a *purely* positive solution to $X^2 - PY^2 = a^2$. Clearly, $(a, 0)$ solves $X^2 - PY^2 = a^2$. Then, using Theorem 1.19, we obtain a solution, (x_0, y_0) to $X^2 - PY^2 = 1$. Thus, by Brahmagumpta's Identity (ax_0, ay_0) solves $X^2 - PY^2 = a^2$.

Theorem 2.7 allowed us to partially answer the question of solvability for $X^2 - PY^2 = k$ for $k < 0$ and $P \equiv 3 \bmod 4$. The following two theorems allow us to fully answer this question when $P \equiv 1 \bmod 4$.

Theorem 2.23 *Let P be prime. $P \equiv 1$ mod 4 if and only if $x^2 - Py^2 = -1$ is solvable.*

Proof: First suppose that $x^2 - Py^2 = -1$ is solvable. Then there are $u, v \in \mathbb{Z}$ such that $u^2 - Pv^2 = -1$. So, $u^2 - (-1) = Pv^2$. So, $(-1/P) = 1$ which, by Theorem 1.2, only happens when $P \equiv 1 \bmod 4$.

Now suppose that P is a prime with $P \equiv 1 \bmod 4$. Let (x_1, y_1) be the fundamental solution to $X^2 - PY^2 = 1$. So, $x_1^2 - 1 = Py_1^2$. If x_1 is even, then y_1 is odd and we have $-1 \equiv P \bmod 4$, contrary to assumption (since $(2m)^2 = 4m^2 \equiv 0 \bmod 4$ and $P(2m+1)^2 = 4Pm^2 + 4Pm + P \equiv P \bmod 4$). Thus, x_1 is odd. So, $\gcd(x_1+1, x_1-1) = 2$.

Thus, for some choice of sign we have $x_1 \pm 1 = 2a^2$ and $x_1 \mp 1 = 2Pb^2$. So, $Py_1^2 = (x_1 - 1)(x_1 + 1) = (2a^2)(2Pb^2) = 4Pa^2b^2$. So, $y_1 = 2ab$. Upon subtracting $x_1 \mp 1 = 2Pb^2$ from $x_1 \pm 1 = 2a^2$ we have $\pm 1 = a^2 - Pb^2$. But $b < y_1$ and (x_1, y_1) is the fundamental solution to $X^2 - PY^2 = 1$. So, we must have $a^2 - Pb^2 = -1$. $\square$

Theorem 2.23 yields an alternate approach to solving Pell equations when $P \equiv 1 \bmod 4$. Using Brahmagupta's identity, if (x_0, y_0) solves $X^2 - PY^2 = -1$, then $(x_0^2 + Py_0^2, 2x_0y_0)$ solves $X^2 - PY^2 = 1$.

Using Theorems 2.22 and 2.23, we are now able to describe the situation when $k < 0$ and $P \equiv 1 \bmod 4$.

Theorem 2.24 *If $P \equiv 1$ mod 4 then $x^2 - Py^2 = k$ is solvable if and only if $x^2 - Py^2 = -k$ is solvable.*

Proof: We assume $P \equiv 1 \bmod 4$. Thus, by Theorem 2.30 $x^2 - Py^2 = -1$ is solvable. If $x^2 - Py^2 = k$ is solvable then by Brahmagumpta's Identity $x^2 - Py^2 = -k$ is solvable. If we assume that $x^2 - Py^2 = -k$ is solvable, then by Brahmagumpta's Identity and the fact that $x^2 - Py^2 = -1$ is solvable, we have that $x^2 - Py^2 = (-1) \cdot (-k) = k$ is solvable. □

2.7 A Partial Criterion for Solvability

Using the results proven above, we now illustrate a partial criterion for the solvability of Pell-Like equations. We will show that, for many Pell-Like equations, the decision problem is solved. We begin by separating the problem into cases, proceed with tests for unsolvability, and then conclude with a discussion of methods used to show that Pell-Like equations are solvable.

Let P be any prime and k a positive integer. If $(k/P) = -1$, then by the Legendre Test, $X^2 - PY^2 = k$ is not solvable. Thus, assume $(k/P) = 1$.

We now separate the problem into two cases: k is a square and k is not a square. If $k = a^2$ for some integer a, then, $(a, 0)$ solves $X^2 - PY^2 = k$. If we wish to obtain a purely positive solution, we may use Brahmagumpta's Identity with $u, v \in \mathbb{Z}^+$ such that $u^2 - Pv^2 = 1$ to obtain (au, av) as a solution to $X^2 - PY^2 = a^2 = k$. That there exists $u, v \in \mathbb{Z}^+$ with these properties follows from 1.2.3. With respect to computational efficiency, the *Intermediate Value Theorem* provides an efficient test to decide if a given integer is a square. See Appendix B.1 for a discussion of this test.

Having dealt with the cases when $(k/P) = -1$ and k is a square, we now assume that k is a quadratic residue modulo P and k is not a square. We now consider unsolvability tests in the cases that k is odd and k is even.

Suppose that k is odd. If $P \equiv k \equiv 3 \bmod 4$, then by Corollary 2.10, $X^2 - PY^2 = k$ is not solvable (since k odd and $k \equiv 3 \bmod 4 \Rightarrow n \equiv 3 \bmod 4$). If this test fails to be conclusive, we turn to the Mod N Test over a Pell Solvability Base as discussed in Remark 2.19. If the Mod N Test yields that $X^2 - PY^2 = k$ is likely solvable, we may try to find an odd prime factor of k and use Corollary 2.13 to further convince ourselves of solvability. If, having tried these unsolvability tests, we have not found conclusive evidence as to the unsolvability of $X^2 - PY^2 = k$, we try to show that $X^2 - PY^2 = k$ is solvable.

Example 2.25 $X^2 - 41 \cdot Y^2 = 17325$. Since $(17325/41) = 1$, the Legendre test is inconclusive. After a little work, we see that 17325 is not a square. Integer factorization yields $17325 = 3^2 \cdot 5^2 \cdot 7 \cdot 11$. We check $(3/41)$, $(5/41)$, $(7/41)$, $(11/41)$ and find

that $(7/41) = (11/41) = -1$. Thus, by Corollary 2.13, $X^2 - 41 \cdot Y^2 = 17325$ is not solvable.

Now suppose that k is even and write $k = 2^s t$, where t is odd. If s is even, then we deal with the solvability of $X^2 - PY^2 = k$ by dealing with the solvability of $X^2 - PY^2 = t$ as we did in the case when k is odd, with one exception. We must, for reasons to be discussed in 2.8, perform the Mod N Test on $X^2 - PY^2 = k$ and not on $X^2 - PY^2 = t$. Note that corollary 2.10 allows us to conclude that $X^2 - PY^2 = k$ is not solvable if $X^2 - PY^2 = t$ is not solvable, provided $P \equiv t \equiv 3 \bmod 4$.

If s is odd, then we first test if $P \equiv 1$ or 3 or 5 mod 8 and $k \equiv 2 \bmod 4$. If so, then we may conclude, by Theorem 2.21, that $X^2 - PY^2 = k$ is not solvable. As a second test (if necessary) we apply the Mod N Test.

If s is odd and both Theorem 2.21 and the Mod N Test are inconclusive, we resort to integer factorization and write $k = m^2 n$, where n is square free. So, $n = 2 \cdot n_0$ where n_0 is odd. If $P \equiv 5 \bmod 8$, then by Corollary 2.16, $X^2 - PY^2 = k$ is not solvable. If $P \equiv 1$ or 3 or 7 mod 8, we test using Corollary 2.13. If, at this point, all of our tests for unsolvability have failed, we try to show that $X^2 - PY^2 = k$ is solvable.

We now consider methods that may be employed to show the solvability of Pell-Like equations.

Remark 2.26 Notice that if we can factor k, say $k = k_1 \cdot ... \cdot k_i$ and show, for all $1 \leq j \leq i$, that $X^2 - PY^2 = k_j$ is solvable, then using Brahmagumpta's Identity i

times we have that $X^2 - PY^2 = k$ is solvable. Observe that k_j does not have to be a prime. Moreover, the converse need not hold, as the next example illustrates.

Example 2.27 Consider $X^2 - 37 \cdot Y^2 = 192$. We may write $192 = 4^2 \cdot 12$ and $192 = 8^2 \cdot 3$. $(7, 1)$ furnishes a solution to $X^2 - 37 \cdot Y^2 = 12$ and $X^2 - 37 \cdot Y^2 = 4^2$ is clearly solvable. Thus, by Brahmagumpta's Identity, $X^2 - 37 \cdot Y^2 = 192$ is solvable. Using an implementation of the Pell Class approach, we see that $X^2 - 37 \cdot Y^2 = 3$ is not solvable. Thus, we may not conclude that the unsolvability of $X^2 - 37 \cdot Y^2 = 3$ yields the unsolvability of $X^2 - 37 \cdot Y^2 = 8^2 \cdot 3 = 192$.

Using methods to be discussed in Chapter three, it is computationally feasible to check for the solvablility of $X^2 - PY^2 = 2$, provided $P > 3$. Moreover, $(2, 1)$ solves $X^2 - 2Y^2 = 2$ and $X^2 - 3Y^2 = 2$ is unsolvable by the Legendre test. Thus, if $X^2 - PY^2 = 2$ and $X^2 - PY^2 = n_0$ are solvable, we can use Brahmagumpta's Identity to establish the solvablility of $X^2 - PY^2 = k$, where $k = m^2 \cdot n_0 \cdot 2$. Moreover, $(2, 1)$ solves $X^2 - 2Y^2 = 2$ and $X^2 - 3Y^2 = 2$ is unsolvable by the Legendre test.

Example 2.28 Consider $X^2 - 31Y^2 = 1650 = 2 \cdot 33 \cdot 25$. $(39, 7)$ solves $X^2 - 31Y^2 = 2$, $(67, 12)$ solves $X^2 - 31Y^2 = 25$, and $(8, 1)$ solves $X^2 - 31Y^2 = 33$. Thus, by Brahmagumpta's Identity, $X^2 - 31Y^2 = 1650$ is solvable.

We now consider the case when $k < 0$. If $P \equiv 1 \bmod 4$ then we consider the solvability of $X^2 - PY^2 = -k$. Using Theorem 2.24, we know that $X^2 - PY^2 = k$ is solvable if and only if $X^2 - PY^2 = -k$ is solvable. Thus, when $k < 0$ and $P \equiv 1 \bmod$

4 we may deal with the solvability of $X^2 - PY^2 = k$ by dealing with the solvability of $X^2 - PY^2 = -k$.

By Theorem 2.7, if $P \equiv 3 \bmod 4$ and $X^2 - PY^2 = -k$ is solvable, then $X^2 - PY^2 = k$ is not solvable. But when $P \equiv 3 \bmod 4$ and $X^2 - PY^2 = -k$ is not solvable Theorem 2.7 is inconclusive. Using methods discussed in the next chapter, we will be able to deal with many more solvability questions for $X^2 - PY^2 = k$, provided $|k| < 1 + 2\sqrt{P}$.

Further research into the case when $k < 0$ and $P \equiv 3 \bmod 4$, may include work similar to the following theorem. The proof requires a simple modification of the proof of Theorem 2.10.

Theorem 2.29 *Let $P \equiv 3$ mod 4 and $k = -1 \cdot m^2 \cdot n$ with n square free. If $n \equiv 1$ mod 4, then $X^2 - PY^2 = k$ is not solvable.*

2.8 An Arithmetic of Solvability

In this section we will discuss the difficulty of obtaining an answer to the full decision problem and address a possible strategy for a solution.

Example 2.30 Refer to Table 2.1. In line 6, we see that $X^2 - 11Y^2 = 2$ and $X^2 - 11Y^2 = 7$ are not solvable but $X^2 - 11Y^2 = 14$ is solvable. In line 11 we see that $X^2 - 17Y^2 = 19$ is solvable but $X^2 - 17Y^2 = 2$ and $X^2 - 17Y^2 = 38$ are not solvable. Additionally, line 27 illustrates that $X^2 - 37Y^2 = 9$ is solvable and $X^2 - 37Y^2 = 11$ is not solvable and $X^2 - 37Y^2 = 99$ is solvable. Moreover, line 16 illustrates that

$X^2 - 37Y^2 = 5$ and $X^2 - 37Y^2 = 2$ are not solvable and $X^2 - 37Y^2 = 10$ is not as well.

These examples illustrate a seemingly pathological phenomenon. Fix a prime P. Then, sometimes, two Pell-Like equations (in terms of P), one solvable and the other unsolvable may be combined to form a solvable Pell-Like equation. In other instances these equations combine to form an unsolvable Pell-Like equation. Moreover, sometimes two unsolvable Pell-Like equations (in terms of a fixed prime P) combine to yield a solvable Pell-Like equation.

Some of this behavior is easily understood using Corollaries 2.6 and 2.11. However, a large portion of this phenomenon is not understood.

If we were able to decide, given a fixed prime, P and integers k, l, if $X^2 - PY^2 = k \cdot l$ were solvable based on the solvability of $X^2 - PY^2 = k$ and $X^2 - PY^2 = l$ then we would, in effect, be able to form an ***arithmetic of solvability*** in which, for a fixed prime P, and an initial base of integers, say $k_1, k_2, ..., k_j$, we could, by direct computation, form the following infinite sets: $S = \{(P, k) : k = (k_1)^{e_1} \cdot ... \cdot (k_j)^{e_j}$ and $X^2 - PY^2 = k$ is solvable$\}$ and $U = \{(P, k) : k = (k_1)^{e_1} \cdot ... \cdot (k_j)^{e_j}$ and $X^2 - PY^2 = k$ is not solvable$\}$.

Using the theorems of this chapter, we already have a partial arithmetic of solvability. For a fixed prime P, and $k_1, k_2, ..., k_j$ with $X^2 - PY^2 = k_i$ solvable for each $1 \leq i \leq j$ we can, using Brahmagumpta's Identity, form the set $A = \{(P, k) : k = (k_1)^{e_1} \cdot ... \cdot (k_j)^{e_j}$ and $X^2 - PY^2 = k$ is solvable$\}$. Clearly $A \subseteq S$.

The major difference between this partial arithmetic of solvability and a full arithmetic of solvability is that we assume that, for each $1 \leq i \leq j$, $X^2 - PY^2 = k_i$ is solvable. In a full arithmetic of solvability we would be able to decide the solvability of $X^2 - PY^2 = k \cdot l$ from the solvability of $X^2 - PY^2 = k$ and $X^2 - PY^2 = l$. Thus, we would be able to decide if $(P, k \cdot l) \in S_P$ or if $(P, k \cdot l) \in U_P$.

Example 2.31 *Referring to table 2.1, we see that for* $P = 37$ *and base* $\{2, 3, 7\}$ *we have* $(37, 4), (37, 9) \in S_{37}$ *while* $(37, 2), (37, 3), (37, 7) \in U_{37}$. *However,* $(37, 12) \in S_{37}$. *Moreover,* $(37, 84) \in S_{37}$.

One pitfall of an arithmetic of solvability is its reliance on integer factorization. Still, an arithmetic of solvability would be a nice tool for deciding the solvability of many Pell-Like equations. Even if this approach is not employed in an eventual solution to the Pell-Like decision problem, the phenomenon described in Example 2.30 is, in the author's opinion, the major crux of the issue. Further study of the Pell-Like decision problem should address this issue.

2.9 Conclusion

We have developed many efficient methods for determining the solvability and unsolvability of a large subset of the set of all Pell-Like equations. Using the Law of Quadratic Reciprocity we have been able to use the notion of quadratic residue to develop many solid tests for unsolvability. Using the methods of Brahmagumpta we

know how to combine solvable Pell-Like equations into solvable Pell-Like equations. In Chapter 3 we will develop new ways to discuss the solvability of Pell-Like equations.

As mentioned above, the phenomenon illustrated in Example 2.30 is at the heart of the issue. It is the author's opinion that when this phenomenon is understood a solution to the decision problem for Pell-Like equations will soon follow.

Another necessary consideration is the eventual meshing of the techniques presented in Chapter 2 with those we are about to present in Chapter 3. The work in these chapters is, in a sense, disjoint. The author believes that when the notions of Quadratic Reciprocity and Convergent Solutions are put together, a vast amount of new understanding will result.

Additionally, we have only scratched the surface of what Time Complexity theory has to offer to the problem. There is a great body of work waiting to be done on the Pell-Like decision and search problems in this direction.

It is exciting, in the author's opinion, to see where these considerations will take us in our knowledge of Pell-Like equations.

TABLE 2.1 $X^2 - P \cdot Y^2 = k \cdot l$

Line	P	k	Solvable?	l	Solvable?	$k \cdot l$	Solvable?
1	3	3	not	2	not	6	is
2	3	11	not	2	not	22	is
3	3	11	not	3	not	33	is
4	3	23	not	2	not	46	is
5	7	7	not	2	is	14	not
6	11	2	not	7	not	14	is
7	11	2	not	11	not	22	is
8	11	2	not	19	not	38	is
9	17	4	is	2	not	8	is
10	17	17	is	2	not	34	not
11	17	19	is	2	not	38	not
12	19	3	not	2	not	6	is
13	19	19	not	2	not	38	is
14	23	2	is	23	not	46	not
15	31	3	not	11	not	33	is
16	37	5	not	2	not	10	not
17	37	4	is	3	not	12	is
18	37	3	not	7	not	21	is
19	37	3	not	9	is	27	is
20	37	4	is	7	not	28	is
21	37	11	not	3	not	33	is
22	37	11	not	4	is	44	is
23	37	3	not	16	is	48	is
24	37	9	is	7	not	63	is
25	37	11	not	7	not	77	is
26	37	12	is	7	not	84	is
27	37	11	not	9	is	99	is
28	41	4	is	2	not	8	is
29	41	9	is	2	not	18	is
30	41	16	is	2	not	32	is
31	43	3	not	2	not	6	is
32	43	2	not	7	not	14	is
33	43	7	not	3	not	21	is
34	43	19	not	2	not	38	is

Chapter 3

CONTINUED FRACTIONS

3.1 The Middle Term Theorem

The Middle Term Theorem arose in conjunction with the solvability of $X^2 - PY^2 = -1$ for a prime P. Below we give a discussion of the problem and a solution.

The Middle Term Theorem is intimately connected to our next theorem. We will refer to it as Fermat's Great Theorem since it was Fermat who gave the first statement of the theorem. In fact, Fermat claimed to have a proof of the theorem, but never published the result. Over a hundred years later, Euler published a proof.

Theorem 3.1 (Fermat's Great Theorem) *Let P be an odd prime.*

Then, $P \equiv 1$ mod 4 if and only if there exists unique positive integers a, b with $a < b$ such that $P = a^2 + b^2$.

By Theorem 1.14, $\sqrt{P} = [a_0, \overline{a_1, a_2, a_3, ..., a_3, a_2, a_1, 2a_0}]$. We call the sequence of terms $a_1, a_2, a_3, ..., a_3, a_2, a_1$ the *symmetric part* of the continued fraction for $\sqrt{P}$. For example, consider $\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}]$ and $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$. Notice that for the former the symmetric part has no middle term and that the latter does (namely 1).

The Middle Term Theorem is the assertion that $P \equiv 1$ *mod 4 if and only if the continued fraction expansion for* $\sqrt{P}$ *has no middle term.* The following takes care of the "only if" part.

Theorem 3.2 *Let* P *be an odd prime. If the continued fraction expansion for* $\sqrt{P}$ *has no middle term then* $P \equiv 1$ *mod 4.*

Proof: We assume that the continued fraction expansion for $\sqrt{P}$ has no middle term. That is, $\sqrt{P} = [a_0, \overline{a_1, a_2, a_3, ...a_m, a_m, ..., a_3, a_2, a_1, 2a_0}]$ or equivalently $\sqrt{P} = [a_0, a_1, a_2, a_3, ...a_m, \alpha]$, where $\alpha = [\overline{a_m, ..., a_3, a_2, a_1, 2a_0, a_1, a_2, a_3, ..., a_m}]$. Thus, the continued fraction for α is symmetrical. So, $\beta = \alpha$, where β is the continued fraction obtained from α by reversing the periodic part. Using Galois' Theorem, we have $\alpha' = \frac{-1}{\beta}$. Thus, $\alpha \cdot \alpha' = \alpha' \cdot \beta = -1$. But α is a quadratic irrational associated with P and hence has the form $\alpha = \frac{u+\sqrt{P}}{v}$ for $u, v \in \mathbb{Z}$. Therefore, we have $-1 = \alpha \cdot \alpha' = \frac{u+\sqrt{P}}{v} \cdot \frac{u-\sqrt{P}}{v}$ which is equivalent to $P = u^2 + v^2$. Thus, by Fermat's Great Theorem, $P \equiv 1 \bmod 4$. $\square$

The "if" part is the crux of the issue. Recall that, by Theorem 2.23, we have $P \equiv 1$ *mod* $4 \Leftrightarrow X^2 - PY^2 = -1$ *is solvable.* We show that $X^2 - PY^2 = -1$ *solvable* $\Rightarrow$ *the continued fraction for* $\sqrt{P}$ *has no middle term.* To do so, we require a theorem and a lemma.

Recall that the complete quotients in the continued fraction expansion of $\sqrt{P}$ are expressions of the form $\frac{k+\sqrt{P}}{h}$. Moreover, given the symmetric nature of the continued fraction expansion of $\sqrt{P}$ established in Theorem 1.13, it is clear that their are finitely

many complete quotients for a prime P. We let $u_i = \frac{k_i+\sqrt{P}}{h_i}$ denote the ith complete quotient to appear in the continued fraction for $\sqrt{P}$.

Theorem 3.3 *Let $\frac{p_n}{q_n}$ be the nth convergent in the continued fraction expansion of $\sqrt{P}$. Then, $p_n^2 - P \cdot q_n^2 = (-1)^{n-1} \cdot h_{n+1}$.*

Proof: We may write $\sqrt{P} = [a_0, a_1, a_2, ..., a_n, u_{n+1}]$, where u_{n+1} denotes the $(n+1)$st complete quotient in the continued fraction expansion for $\sqrt{P}$. As in the proof of Theorem 1.20 we have $\sqrt{P} = \frac{u_{n+1}p_n+p_{n-1}}{u_{n+1}q_n+q_{n-1}}$. But, $u_{n+1} = \frac{k_{n+1}+\sqrt{P}}{h_{n+1}}$. So, $\sqrt{P} = \frac{(k_{n+1}+\sqrt{P})p_n+p_{n-1}}{(k_{n+1}+\sqrt{P})q_n+q_{n-1}}$. Multiplying by $(k_{n+1}+\sqrt{P})q_n+q_{n-1}$ and simplifying yields $(Pq_n)+(q_nk_{n+1}+h_{n+1}q_{n-1})\sqrt{P} = (p_nk_{n+1}+h_{n+1}p_{n-1})+p_n\sqrt{P}$. So, $Pq_n^2 = p_nk_{n+1}q_n + h_{n+1}p_{n-1}q_n$ and $p_n^2 = q_nk_{n+1}p_n + h_{n+1}q_{n-1}p_n$ which yields $p_n^2 - Pq_n^2 = q_nk_{n+1}p_n + h_{n+1}q_{n-1}p_n - p_nk_{n+1}q_n - h_{n+1}p_{n-1}q_n$. Since $q_nk_{n+1}p_n + h_{n+1}q_{n-1}p_n - p_nk_{n+1}q_n - h_{n+1}p_{n-1}q_n = h_{n+1}q_{n-1}p_n - h_{n+1}p_{n-1}q_n = h_{n+1}(q_{n-1}p_n - p_{n-1}q_n)$, we have $p_n^2 - Pq_n^2 = h_{n+1}(q_{n-1}p_n - p_{n-1}q_n)$. But, $q_{n-1}p_n - p_{n-1}q_n = (-1)^{n-1}$. So, $p_n^2 - Pq_n^2 = (-1)^{n-1}h_{n+1}$, as desired.

Notice that Theorem 1.20 is a special case. For a proof of the following see [5].

Lemma 3.4 (Euler) *$h_m = 1 \Leftrightarrow m = rk$ for some $k \in \mathbb{N}$.*

Theorem 3.5 *If $X^2 - PY^2 = -1$ is solvable then the continued fraction expansion of $\sqrt{P}$ has no middle term.*

Proof: We prove the contrapositive. That is, suppose that the continued fraction

for $\sqrt{P}$ has a middle term. So, $\sqrt{P} = [a_0, \overline{a_1, a_2, a_3, ...a_m, a_{m+1}, a_m, ..., a_3, a_2, a_1, 2a_0}]$. Thus the length of the period, r, is even.

Let $l \in \mathbb{N}$ and suppose that $p_l^2 - Pq_l^2 = -1$. By Theorem 3.3, we must have $-1 = (-1)^{l-1}h_{l+1}$. So, $h_{l+1} = 1$. So, by Lemma 3.4, $l + 1 = rt$ for some $t \in \mathbb{N}$. That is, $l = rt - 1$. But then, by Theorem 1.20, we have $-1 = p_l^2 - Pq_l^2 = p_{tr-1}^2 - P \cdot q_{tr-1}^2 = (-1)^{tr} = 1$, since r is even. This clear contradiction shows that, $X^2 - PY^2 = -1$ is not solvable by the convergents in the continued fraction expansion of $\sqrt{P}$.

But, $|-1| < \sqrt{P}$. Thus, by Theorem 1.23, the only solutions to $X^2 - PY^2 = -1$ are among the convergents in the continued fraction expansion of $\sqrt{P}$. Thus, applying the contrapositive, the result follows. □

Using Theorem 3.5 and Theorem 2.23, we now have the following.

Theorem 3.6 *If $P \equiv 1$ mod 4, then the continued fraction expansion for $\sqrt{P}$ has no middle term.*

The Middle Term Theorem gives one of many equivalent characterizations of prime numbers P with $P \equiv 1$ mod 4. These are summarized in the following theorem.

Theorem 3.7 *Let P be an odd prime. Then the following are equivalent:*

(a) $P \equiv 1$ mod 4.

(b) There are unique positive integers $a < b$ such that $P = a^2 + b^2$.

(c) The continued fraction expansion for $\sqrt{P}$ has no middle term.

(d) The period of the continued fraction expansion of $\sqrt{P}$ is odd.

Proof: The equivalence of (a), (b), and (c) has been established above. We use (c) to establish (d). Suppose that (c) holds. So, $\sqrt{P} = [a_0, \overline{a_1, a_2, ..., a_m, a_m, ..., a_2, a_1, 2a_0}]$. So, $r = 2 \cdot |\{a_1, a_2, ..., a_m\}| + |\{2a_0\}|$, which is clearly odd.

Now suppose that (d) holds. If the continued fraction expansion for $\sqrt{P}$ had a middle term, then $\sqrt{P} = [a_0, \overline{a_1, a_2, ..., a_m, a_n, a_m, ..., a_2, a_1, 2a_0}]$. So, $r = 2 \cdot |\{a_1, a_2, ..., a_m\}| + |\{2a_0\}| + |\{a_n\}|$, which is clearly even, contradicting our assumption. Thus, we have (c).

We will now apply the Middle Term Theorem to prove an interesting result about the continued fraction expansions of primes congruent to 1 mod 4. First, an example.

Consider $\sqrt{29} = [5, \overline{2, 1, 1, 2, 10}]$. By Fermat's Great Theorem, 29 may be written as a sum of squares, namely $29 = 5^2 + 2^2$. This equation gives rise to the equation $\frac{2+\sqrt{29}}{5} \cdot \frac{2-\sqrt{29}}{5} = -1$, which allows one to show that $\frac{2+\sqrt{29}}{5}$ is a reduced quadratic irrational. Moreover, applying the continued fraction algorithm we obtain $\frac{2+\sqrt{29}}{5} = [\overline{1, 2, 10, 2, 1}]$. Thus, $\frac{2+\sqrt{29}}{5}$ is a complete quotient in the continued fraction expansion of $\sqrt{29}$.

We will now prove the general case. We begin with two preliminary theorems.

Theorem 3.8 *(a) Let P be an odd prime with $P \equiv 1$ mod 4 and $P = a^2 + b^2$ be the unique sums of squares representation of P. Then, $\frac{a+\sqrt{P}}{b}$ and $\frac{b+\sqrt{P}}{a}$ are reduced quadratic irrationals. Moreover, $\frac{a+\sqrt{P}}{b}$ and $\frac{b+\sqrt{P}}{a}$ are the only reduced quadratic irrationals associated with $\sqrt{P}$ that have a symmetrical continued fraction expansion.*

(b) If $P \equiv 3$ mod 4 then no reduced quadratic irrationals associated with $\sqrt{P}$ have a

symmetrical continued fraction expansion.

Proof: The equation $P = a^2 + b^2$ gives rise to the equations $\frac{a+\sqrt{P}}{b} \cdot \frac{a-\sqrt{P}}{b} = -1$ and $\frac{b+\sqrt{P}}{a} \cdot \frac{b-\sqrt{P}}{a} = -1$. Clearly, $\frac{a+\sqrt{P}}{b} > 1$. Thus, $\frac{a-\sqrt{P}}{b} < 0$. Moreover, $|\frac{a-\sqrt{P}}{b}| = \frac{1}{\frac{a+\sqrt{P}}{b}}$. So, $0 < |\frac{a-\sqrt{P}}{b}| < 1$. Thus, $-1 < \frac{a-\sqrt{P}}{b} < 0$ and $\frac{a+\sqrt{P}}{b}$ is reduced. A similar argument shows that $\frac{b+\sqrt{P}}{a}$ is reduced.

Let $\alpha = \frac{a+\sqrt{P}}{b}$ and β be obtained from the continued fraction expansion for α with the period reversed. So, $\alpha' = \frac{a-\sqrt{P}}{b}$. By Galois' Theorem, $\alpha' = \frac{-1}{\beta}$. So, $\alpha' \cdot \beta = -1$. But, $\alpha \cdot \alpha' = -1$. So, $\alpha \cdot \alpha' = \alpha' \cdot \beta$. Thus, $\alpha = \beta$ and the continued fraction for α is symmetrical. A similar argument shows that the continued fraction for $\frac{b+\sqrt{P}}{a}$ is symmetrical. This establishes that there are at least two reduced quadratic irrationals associated with $\sqrt{P}$ that have a symmetrical continued fraction expansion.

Let $r, s \in \mathbb{Z}^+$ with $\{r, s\} \neq \{a, b\}$. Suppose that $\gamma = \frac{r+\sqrt{P}}{s}$ is a reduced quadratic irrational that has a symmetrical continued fraction expansion. So, $\gamma = \beta_\gamma$, where β_γ denotes the continued fraction obtained from the continued fraction expansion for γ with the period reversed. Then, by Galois' Theorem $\gamma \cdot \gamma' = \gamma' \cdot \beta_\gamma = -1 \Leftrightarrow P = r^2 + s^2$, contradicting the uniqueness of the sums of squares representation. This proves (a).

Suppose that $P \equiv 3 \bmod 4$ and for $h, k \in \mathbb{Z}$, $\varphi = \frac{h+\sqrt{P}}{k}$ is a reduced quadratic irrational with a symmetrical continued fraction expansion. So, $\varphi = \beta_\varphi$. Then, by Galois' Theorem $\varphi \cdot \varphi' = \varphi' \cdot \beta_\varphi = -1 \Leftrightarrow P = h^2 + k^2 \Leftrightarrow P \equiv 1 \bmod 4$, a clear contradiction. This proves (b). □

Lemma 3.9 *All complete quotients that appear in the continued fraction for* $\sqrt{P}$ *are*

reduced quadratic irrationals.

Proof: Let α be a complete quotient in the continued fraction for $\sqrt{P}$. The continued fraction algorithm may be used to show that α is a quadratic irrational. We show that α us reduced. Clearly, $\alpha > 1$. By the Observation 1.14 we know that there is a complete quotient, γ with $\gamma > 1$ such that $\alpha \cdot \gamma' = -1$. Taking conjugates we obtain $\alpha' \cdot \gamma = -1$. So, $|\alpha'| \cdot \gamma = 1 \Rightarrow |\alpha'| = \frac{1}{\gamma}$. That is, $0 < |\alpha'| < 1$. So, $-1 < \alpha' < 0$. Thus, α is reduced. $\square$

Theorem 3.10 establishes the general case.

Theorem 3.10 *Let P be an odd prime with $P \equiv 1$ mod 4 and $P = a^2 + b^2$ be the unique sums of squares representation of P. Then, $\frac{a+\sqrt{P}}{b}$ or $\frac{b+\sqrt{P}}{a}$ is a complete quotient in the continued fraction expansion of $\sqrt{P}$.*

Proof: Since $P \equiv 1 \bmod 4$, the Middle Term Theorem establishes that the continued fraction for $\sqrt{P}$ has no middle term. Thus, as in the proof of Theorem 3.2, there is a complete quotient in the continued fraction for $\sqrt{P}$, say α that has a symmetrical continued fraction expansion. By Lemma 3.9, α is a reduced quadratic irrational associated with $\sqrt{P}$. But, by Theorem 3.8, the only reduced quadratic irrationals associated with $\sqrt{P}$ that have symmetrical continued fraction expansions are $\frac{a+\sqrt{P}}{b}$, $\frac{b+\sqrt{P}}{a}$. Thus, $\alpha = \frac{a+\sqrt{P}}{b}$ or $\alpha = \frac{b+\sqrt{P}}{a}$. $\square$

3.2 Convergents as Solutions

In 1.2.3 we found that all solutions to $X^2 - PY^2 = 1$ are among the convergents in the continued fraction expansion of $\sqrt{P}$. Indeed, as Theorem 1.19 asserts, if (x_0, y_0) is a solution to $X^2 - PY^2 = 1$ then $\frac{x_0}{y_0}$ is a convergent in the continued fraction expansion of $\sqrt{P}$. But not all convergents in the continued fraction expansion of $\sqrt{P}$ solve Pell's equation. In fact, many do not. However, all convergents for $\sqrt{P}$ solve some Pell-Like equation. The work of this section can be considered a generalization of Theorems 1.20 through 1.22.

Recall the two problems associated with finding solutions to Pell-Like equations: the decision problem and the search problem. We will now formulate similar problems for convergent solutions.

Let P be prime. The convergent solutions decision problem for P and integer k is the question: *Does there exist an efficient means to decide if there exists a convergent,* $C_m = \frac{p_m}{q_m}$ *in the continued fraction expansion of* $\sqrt{P}$ *such that* $p_m^2 - Pq_m^2 = k$? The convergent solutions search problem for P is the following: *Can we find all integers* k *such that there exist a convergent,* $C_m = \frac{p_m}{q_m}$ *in the continued fraction expansion of* $\sqrt{P}$ *such that* $p_m^2 - Pq_m^2 = k$ *in a reasonable amount of time*?

We will now give a systematic method for finding all Pell-Like equations solved by convergents in the continued fraction expansion of $\sqrt{P}$.

Our first theorem narrows our view of the possible Pell-Like equations solved by convergents.

Theorem 3.11 *If $\frac{p}{q}$ is a convergent in the continued fraction expansion of $\sqrt{P}$, then $|p^2 - P \cdot q^2| < 1 + 2\sqrt{P}$.*

We now introduce some notation. Let $C_n = \frac{p_n}{q_n}$. If $p_n^2 - Pq_n^2 = N$ then we write $C_n \to N$ and say "C_n takes on N". Rephrasing Theorem 3.3 in terms of this new notation , we have $C_m \to (-1)^{m-1}h_{m+1}$ for all convergents C_m in the continued fraction expansion of $\sqrt{P}$.

Now, suppose $C_n \to N$, where C_n is a convergent in the continued fraction expansion of $\sqrt{P}$. If $P \equiv 3 \bmod 4$, we know, by Theorem 2.7, that $X^2 - PY^2 = -N$ is not solvable and thus no convergents take on $-N$. If $P \equiv 1 \bmod 4$, then we know, by Theorem 2.23, that $X^2 - PY^2 = -N$ is solvable. However, we do not yet know, in general, that $C_m \to -N$ for some integer m. But if we add the assumption that $|-N| < \sqrt{P}$ then, by Theorem 1.23, the only solutions to $X^2 - PY^2 = -N$ are among the convergents in the continued fraction expansion of $\sqrt{P}$. So, there is an integer m such that $C_m \to -N$.

We can tell a lot about what values are taken on by convergents by considering their subscripts as the next theorem illustrates.

Theorem 3.12 *Let $C_k = \frac{p_k}{q_k}$.*

(a) k is even $\Leftrightarrow p_k^2 - P \cdot q_k^2 < 0$.

(b) k is odd $\Leftrightarrow p_k^2 - P \cdot q_k^2 > 0$.

Proof: We have $C_0 < C_2 < C_4 < ... < \sqrt{P} < ... < C_5 < C_3 < C_1$. Thus, k even

$\Leftrightarrow C_k = \frac{p_k}{q_k} < \sqrt{P} \Leftrightarrow p_k < \sqrt{P} \cdot q_k \Leftrightarrow p_k^2 < P \cdot q_k^2 \Leftrightarrow p_k^2 - P \cdot q_k^2 < 0$. This proves (a) and the contrapositive proves (b). $\square$

Now consider $\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}]$ and recall that a reduced quadratic irrational associated with $\sqrt{13}$ is an expression of the form $\frac{k+\sqrt{13}}{h}$, where $k, h \in \mathbb{Z}$ and $0 < h$. There are five reduced quadratic irrationals (complete quotients) that show up in the continued fraction expansion of $\sqrt{13}$, namely $u_1 = [\overline{1, 1, 1, 1, 6}] = \frac{3+\sqrt{13}}{4}$, $u_2 = [\overline{1, 1, 1, 6, 1}] = \frac{1+\sqrt{13}}{3}$, $u_3 = [\overline{1, 1, 6, 1, 1}] = \frac{2+\sqrt{13}}{3}$, $u_4 = [\overline{1, 6, 1, 1, 1}] = \frac{1+\sqrt{13}}{4}$, and $u_5 = [\overline{6, 1, 1, 1, 1}] = \frac{3+\sqrt{13}}{1}$. Recall that we denote by h_i the denominator of u_i.

After a considerable amount of computations we arrive at $C_0 \to -4 = -h_1$, $C_1 \to 3 = h_2$, $C_2 \to -3 = -h_3$, $C_3 \to 4 = h_4$, $C_4 \to -1 = -h_5$, $C_5 \to 4 = h_6 = h_1$, ..., $C_9 \to 1 = h_{10} = h_5$.

Before establishing the general case we exercise a word of caution. We must have a specific order on the set $\{h_i : i \in \mathbb{N}\}$. To do so we first consider the set of complete quotients $\{u_i : i \in \mathbb{N}\}$ and order these in the natural way. That is, u_1 is the first complete quotient in the continued fraction expansion of $\sqrt{P}$, u_2 is the second complete quotient in the continued fraction expansion of $\sqrt{P}$,...,u_r is the rth complete quotient in the continued fraction expansion of $\sqrt{P}$, where r is the length of the period. Then, $h_i < h_j \Leftrightarrow u_i < u_j \Leftrightarrow i < j$ is the correct way to order the sequence $\{h_i\}$. Moreover, since there are only finitely many u_i there are finitely many h_i. So, for $i, j \in \mathbb{Z}^+$, $i \equiv j \bmod r \Rightarrow h_i = h_j$. *From this point onward, when we refer to the sequence $\{h_i\}$ we assume that it is ordered in the above mentioned way.*

Theorem 3.13 *Let P be an odd prime, $k \in \mathbb{N}$, and r be the length of the period in the continued fraction expansion of $\sqrt{P}$.*

(a) If $P \equiv 1$ mod 4 then $C_k \to N \Leftrightarrow C_{k+r} \to -N$.

(b) If $P \equiv 3$ mod 4 then $C_k \to N \Leftrightarrow C_{k+r} \to N$.

Proof: Clearly, $k+1 \equiv k+r+1$ mod r. So, $h_{k+1} = h_{k+r+1}$. Also, $h_i > 0$ for all i.

Suppose $P \equiv 1$ mod 4. Then, by the Middle Term Theorem, r is odd. Thus, by Theorem 3.3 we have $N = (-1)^{k-1}h_{k+1} > 0 \Leftrightarrow k-1$ is even $\Leftrightarrow k+r-1$ is odd $\Leftrightarrow (-1)^{k+r-1}h_k = (-1)^{k+r-1}h_{k+r-1} = -N < 0$. This proves (a).

Now suppose $P \equiv 3$ mod 4. Then, by the Middle Term Theorem, r is even. Thus, we have $N = (-1)^{k-1}h_{k+1} > 0 \Leftrightarrow k-1$ is even $\Leftrightarrow k+r-1$ is even $\Leftrightarrow (-1)^{k+r-1}h_{k+1} = (-1)^{k+r-1}h_{k+r+1} > 0$. This proves (b). $\square$

Theorem 3.14 *Let P be an odd prime, $k \in \mathbb{N}$, and r the length of the period in the continued fraction expansion of $\sqrt{P}$.*

(a) If $P \equiv 1$ mod 4 and $C_m \to N$, then $C_i \to N$ for some $0 \leq i \leq 2r-1$.

(b) If $P \equiv 3$ mod 4 and $C_m \to N$, then $C_i \to N$ for some $0 \leq i \leq r-1$.

Proof: Let $m \in \mathbb{N}$. By the Division Algorithm, we have $m = r \cdot Q + l$ with $0 \leq l < r$ for some unique $Q, l \in \mathbb{Z}$. Thus, $l < r \leq l+r < 2r$ and $l \equiv r+l \equiv 2r+l$ mod r. So, $h_m = h_l = h_{l+r}$. So, $h_{m+1} = h_{l+1} = h_{l+r+1}$. By Theorem 3.3, $C_m \to (-1)^{m-1}h_{m+1}$.

Suppose $P \equiv 1$ mod 4 and $2r \leq m$. Then r is odd. Thus, $(-1)^{m-1}h_{m+1} \neq (-1)^{l-1}h_{l+1} \Leftrightarrow (-1)^{m-1} \neq (-1)^{l-1} \Leftrightarrow (-1)^{m-1} = (-1)^{l+r-1} \Leftrightarrow (-1)^{m-1}h_{m+1} = (-1)^{l+r-1}h_{l+r+1}$, since $(-1)^{m-1} \neq (-1)^{l-1} \Rightarrow m-1$ even and $l-1$ odd or vice versa.

This proves (a).

Suppose that $P \equiv 3 \bmod 4$ and $r \leq m$. Then r is even. So, $(-1)^{m-1} = (-1)^{m+r-1}$. We have $h_m = h_l$. So, $(-1)^{m-1}h_l = (-1)^{m+r-1}h_{l+r}$. This proves (b). $\square$

We now have an efficeint means for finding all solutions taken on by convergents in the continued fraction expansion of $\sqrt{P}$. This algorithm is described in the next subsection.

3.3 Applications to a General Criterion for Solvability of Pell-Like Equations

Using Theorems 3.13 and 3.14, we now have a means for finding all solutions taken on by convergents in the continued fraction expansion of $\sqrt{P}$.

Let CS be the set of all solutions taken on by convergents of $\sqrt{P}$. Recall that by Theorem 1.5, we may compute the numerator, p_k, and denominator, q_k, of any convergent according to the following recursive formulas:

(i) $p_0 = a_0$, $p_1 = a_1a_0 + 1$, and $p_k = a_kp_{k-1} + p_{k-2}$

(ii) $q_0 = 1$, $q_1 = a_1$, and $q_k = a_kq_{k-1} + q_{k-2}$.

We now describe an algorithm for finding all solutions taken on by convergents. We will refer to it as the *Convergent Solutions algorithm*:

1. Compute $s_i = p_i^2 - P \cdot q_i^2$ for each $0 \leq i \leq r-1$.

2. If $P \equiv 1 \bmod 4$, then $CS = \{\pm s_i : 0 \leq i \leq r-1\}$.

3. If $P \equiv 3 \bmod 4$, then $CS = \{s_i : 0 \leq i \leq r-1\}$.

That the Convergent Solutions Algorithm correctly outputs all solutions taken on by convergents can easily be proved using Theorems 3.13 and 3.14. Indeed, if $P \equiv 3 \mod 4$, then by Theorem 3.14.b, $CS = \{s_i : 0 \leq i \leq r-1\}$. If $P \equiv 1 \mod 4$ and for some $k \in \mathbb{N}$, $C_k \to N$, then by Theorem 3.14.a, $C_i \to N$ for $0 \leq i \leq 2r-1$. If $0 \leq i \leq r-1$, then we are done. If $r \leq i \leq 2r-1$ then we may apply Theorem 3.13.a to obtain that $C_{i-r} \to -N$. This proves the correctness of the Convergent Solutions algorithm.

The efficiency of the Convergent Solutions algorithm revolves around the time that it takes to compute C_0, C_1, C_2,...,C_{r-1}, which is, roughly, the same as the length of the period, r in the continued fraction expansion of $\sqrt{P}$. Recall from 1.2.3 that, for some constant A, that $A{\cdot}\log(P) < r < 0.72\sqrt{P}{\cdot}\log(P)$ and it is anticipated that $A \cdot \sqrt{P} < r < 0.72\sqrt{P}{\cdot}\log(P)$. Under these considerations, the Convergent Solutions algorithm may take a considerable amount of time to produce all convergent solutions.

The Convergent Solutions Algorithm can be used to determine the unsolvability of some Pell-Like equations. Recall that, by Theorem 1.23, If $|k| < \sqrt{P}$, then all solutions to $X^2 - PY^2 = k$ are among the convergents in the continued fraction expansion of $\sqrt{P}$. Thus, $k \in \{x \in \mathbb{Z} : |x| < \sqrt{P}\} - CS \Rightarrow X^2 - PY^2 = k$ is not solvable.

For example consider $P = 41$. Using the Convergent Solutions Algorithm we arrive at $CS = \{5, -5, -1, 1\}$. Since $[\sqrt{41}] = 6$, we have $\{x \in \mathbb{Z} : |x| < \sqrt{P}\} - CS = \{\pm 2, \pm 3, \pm 4, \pm 6\}$. That is, $X^2 - PY^2 = k$ is not solvable when $k \in \{\pm 2, \pm 3, \pm 4, \pm 6\}$.

We now turn to the decision problem for convergent solutions of Pell-Like equations. When the period, r of the continued fraction expansion of $\sqrt{P}$ is 1 or 2, we can give general formulas for all solutions taken on by convergents.

Theorem 3.15 *Let P be an odd prime and $r = 1$ be the length of the period in the continued fraction expansion of $\sqrt{P}$.*

Then, $C_n \to 1$ when n is odd and $C_n \to -1$ when n is even.

Proof: Since $r = 1$, we have, by Theorem 1.20, $p_{k-1}^2 - Pq_{k-1}^2 = (-1)^k$ for each convergent C_k in the continued fraction expansion of $\sqrt{P}$. Since $r = 1$, the continued fraction for $\sqrt{P}$ has no middle term. So, $P \equiv 1 \bmod 4$. Thus, all convergent solutions are given within the first two iterations of the period. So, when n is even $p_n^2 - Pq_n^2 = p_0^2 - Pq_0^2 = (-1)^1 = -1$. When n is odd we have, $p_n^2 - Pq_n^2 = p_1^2 - Pq_1^2 = (-1)^2 = 1$. □

In the proof of Theorem 3.16, we will use a fact that is worth recording on its own. That is, *for any prime P, $C_0 \to [\sqrt{P}]^2 - P$*. Indeed, for $p_0 = a_0 = [\sqrt{P}]$ and $q_0 = 1$. Thus, $p_0^2 - Pq_0^2 = [\sqrt{P}]^2 - P$.

Theorem 3.16 *Let P be an odd prime and $r = 2$ be the length of the period in the continued fraction expansion of $\sqrt{P}$.*

Then, $C_n \to 1$ when n is odd and $C_n \to [\sqrt{P}]^2 - P$ when n is even.

Proof: Since $r = 2$, we have, by Theorem 1.20, $p_{2k-1}^2 - Pq_{2k-1}^2 = (-1)^{2k} = 1$ for each convergent C_k in the continued fraction expansion of $\sqrt{P}$. Thus, when n is odd, $C_n \to 1$.

Since $r = 2$, there is no middle term in the continued fraction expansion of $\sqrt{P}$. Thus, by the Middle Term Theorem, $P \equiv 3 \bmod 4$. So, by Theorem 3.14, for any $m \in \mathbb{N}$, $C_m \to N \Rightarrow C_0 \to N$ or $C_1 \to N$. So, $N = 1$, when m is odd and $N = [\sqrt{P}]^2 - P$ when m is even. $\square$

It can be shown that for odd primes P, Q with $P = n^2 + 1$, $Q = m^2 + 2$, $\sqrt{P} = [n, \overline{2n}]$ and $\sqrt{Q} = [n, \overline{n, 2n}]$. Thus, by Theorems 3.15 and 3.16, we have $CS_{\sqrt{P}} = \{1, -1\}$ and $CS_{\sqrt{Q}} = \{1, [\sqrt{P}]^2 - P\}$.

Why stop here? Indeed, we could prove analogous theorems for $r \geq 3$. The problem is that, using the methods of Theorems 3.15 and 3.16, we gain no more effeciency than that of the convergent solutions algorithm. For example, if $r = 3$ then the most general form at our disposal is to state that $C_1 \to (a_0a_1+1)^2 - Pa_1^2$. Since a_1 is specific to $\sqrt{P}$, we gain no more effeciency than purely computing $(a_0a_1+1)^2 - Pa_1^2$.

Using Theorems 3.15, 3.16, we can answer the decision problem for many Pell-Like equations. As an example, consider $P = 5477$. We have $\sqrt{5477} = [74, \overline{148}]$. Thus, by Theorem 3.15 $CS_{\sqrt{5477}} = \{-1, 1\}$. Since $[\sqrt{5477}] = 74$, we have $k \in [-74, 74] - \{-1, 1\} \subseteq \mathbb{Z} \Rightarrow X^2 - PY^2 = k$ is not solvable.

In [3] Feit proved the following.

Theorem 3.17 *Let P be prime such that $P = a^2 + (2b)^2$, with a, $b \in \mathbb{Z}$. Then,*

(a) $X^2 - PY^2 = a$ is always solvable.

(b) $X^2 - PY^2 = 4b$ is always solvable.

This powerful result allows us to easily prove the last theorem of this section.

Theorem 3.18 *Let P be prime such that $P = a^2 + (2b)^2$, with a, $b \in \mathbb{Z}$. Then, $C_i \to a$ for some $0 \leq i \leq 2r-1$, where r is the length of the period in the continued fraction expansion of $\sqrt{P}$.*

Proof: By Theorem 3.16 we know that $X^2 - PY^2 = a$ is solvable. Since $a^2 < a^2 + (2b)^2 = P$, we have $a < \sqrt{P}$. Thus, by Lagrange's Theorem, the only solutions to $X^2 - PY^2 = a$ come from the convergents in the continued fraction expansion of $\sqrt{P}$. So, $C_m \to a$ for some $m \in \mathbb{N}$. Since P may be written as a sum of squares, we know, by Fermat's Great Theorem, that $P \equiv 1 \bmod 4$. So, by Theorem 3.13, $C_i \to a$ for some $0 \leq i \leq 2r-1$. $\square$

Using Theorems 3.3 and 3.10 we can prove a slightly weaker version of Theorem 3.17.a. That is, *either $X^2 - PY^2 = a$ is solvable or $X^2 - PY^2 = 2b$ is solvable, where P is a prime such that $P = a^2 + (2b)^2$, with a, $b \in \mathbb{Z}$.* Indeed, for by Theorem 3.10 either $\frac{a+\sqrt{P}}{2b}$ or $\frac{2b+\sqrt{P}}{a}$ is a complete quotient in the continued fraction expansion for $\sqrt{P}$. Thus, by Theorem 3.3 we have that either $X^2 - PY^2 = a$ or $X^2 - PY^2 = 2b$ is solvable.

3.4 Summary

The Middle Term Theorem has far reaching applications. As a characterization of congruency modulo 4 the Middle Term Theorem, along with Theorem 3.3, has allowed us to easily discuss the solvability and unsolvability of many Pell-Like equations.

In 1.2.3 and 3.3 we remarked that computing the length of the period, r, in the continued fraction expansion of $\sqrt{P}$ for a prime P may not be able to be done efficiently. It is the author's opinion that all algorithms that compute convergent solutions will rely on computing the length of r. Thus, the author conjectures that, for many Pell-Like equations, the convergent solutions search problem will be answered in the negative, provided that the suggested bound $A \cdot \sqrt{P} < r$, where A is a constant, is confirmed.

These considerations illustrate the importance of Theorems 3.15, 3.16, and 3.17 and continued research in this direction. Using the methods of Theorems 3.15 and 3.16, we can, for sufficiently small r, compute all elements of $CS_{\sqrt{P}}$, where P is prime. This solves both the convergent solutions decision and search problems for many Pell-Like equations.

Moreover, the author believes that the results of Theorem 3.17 are only the beginning. Results of this type are immediate solutions to specific convergent solutions decision problems. Further research in this direction will surely need to incorporate Brahmagumpta's Identity, Lagrange's Theorem, and the methods of this chapter. As a tool for gathering data to this end, Theorem 3.14 is indispensable.

Chapter 4

APPLICATIONS TO CRYPTOGRAPHY

4.1 Introduction

We use the common practice that the sender of a secret message is given the name Bob and the receiver is Alice. There are many mathematical methods for ensuring that no third party, say Eve (for eavesdropper), can view the message when it is passed from Bob to Alice. The goal of this introduction is to discuss the general form of one type of these methods known as public key cryptography.

Let m' denote a *word* from the alphabet $A = \{a, A, b, B, ..., z, Z, 0, 1, 2, ..., 9, \epsilon\}$, where ϵ denotes the empty character (or space). There are many standard ways that allow one to convert m' into a unique natural number, say m, and convert m back to its original message m'. We assume that we have chosen one of these methods and that we will use it for every conversion.

Let M denote the set of all natural numbers that represent any word from A. So, $m \in M$. We refer to M as the *message space* and any element of M as a *plaintext message*.

Let $C = \mathbb{N}$. We refer to C as the *ciphertext space* and any element of C as a

ciphertext. Any bijection from M to C or from C to M is called a *key*. Let K denote the set of all keys.

Using the above terminology we may view encryption as a key from M to C and decryption as a key from C to M. Thus, for $e \in K$ and $d = e^{-1}$, the encryption of the message m is $e(m)$ and the decryption is $d(e(m)) = e^{-1}(e(m)) = m$.

In public key cryptosystems, the receiving party, Alice, creates a public and private key, say e, d, respectively, with the property that $d = e^{-1}$. Alice makes e accessible to anyone. To encrypt m, Bob obtains e and computes $e(m) = c$. Bob then sends c to Alice. Once Alice has received c, she computes $d(c) = m$.

In a secure public key cryptosystem, it is computationally infeasible to compute $d(m)$ given e [7].

4.2 LGroups

We will now define a group based on solutions to Pell-like equations that has many applications to Cryptography.

Let P, q be odd primes and $G = \{(x, y) \in \mathbb{Z}_q^2 : x^2 - Py^2 = k\}$, where $(k/P) = (k/q) = 1$. We can define a binary operation on G as follows. Since $(k/q) = 1$ we know there is $a \in \mathbb{Z}$ such that $a^2 \equiv k \bmod q$. Thus, for $(x, y), (z, w) \in G$, we may define $(x, y) \cdot (z, w) = (\frac{xz+Pyw}{a}, \frac{xw+yz}{a})$.

Theorem 4.1 *Let G be defined as above and $a \in \mathbb{Z}$ such that $a^2 \equiv k \bmod q$. Then, $(G, \cdot)$ is an Abelian group.*

Proof: We first show that G is closed under the operation $\cdot$. To make things simpler we work in integers mod q which is a field and the equation at hand is an element of $\mathbb{Z}_q[x, y]$. Let (x,y),(z,w) be in G. Consider $(x, y) \cdot (z, w) = (\frac{xz+pyw}{a}, \frac{xw+yz}{a})$. We claim that $(\frac{xz+pyw}{a})^2 - p \cdot (\frac{xw+yz}{a})^2 = k$. Note first that $(xz + pyw)^2 = x^2z^2 + 2pxyzw+p^2y^2w^2$ and $(xw+yz)^2 = x^2w^2+2xyzw+y^2z^2$. So, $(\frac{xz+pyw}{a})^2-p\cdot(\frac{xw+yz}{a})^2 = \frac{x^2z^2+2pxyzw+p^2y^2w^2-px^2w^2-2pxyzw-py^2z^2}{a^2} = \frac{x^2z^2+p^2y^2w^2-px^2w^2-py^2z^2}{a^2} = \frac{z^2(x^2-py^2)-pw^2(x^2-py^2)}{a^2} = \frac{(x^2-py^2)(z^2-pw^2)}{a^2} = \frac{kk}{a^2} = \frac{k^2}{a^2} = \frac{k^2}{k} = k$.

We now show that $(a, 0)$ is the identity for $(G, \cdot)$. Let $(x, y) \in G$. Then, $(x, y) \cdot (a, 0) = (\frac{xa}{a}$ mod q,$\frac{ya}{a}$ mod q) = (x mod q, y mod q) = (x, y).

We now show that G contains inverses. Let $(x, y) \in G$ and $(z, w) = (x, q - x)$. Then $(x, y) * (x, q - y) = (\frac{x^2-py^2+pqy}{a}$ mod q, $\frac{xq+xy-xy}{a}$ mod q) = ($\frac{x^2-py^2}{a}$ mod q, $\frac{xq}{a}$ mod q) = ($\frac{a^2}{a}$ mod q, 0 mod q) = $(a, 0)$. Thus, $(x, y)^{-1} = (x, q - x)$.

In [4] it was proven that the operation $\cdot$ is associative.

G is abelian, since $(x, y) * (z, w) = (\frac{xz+pyw}{a}$ mod q,$\frac{xw+yz}{a}$ mod q) = ($\frac{zx+pwy}{a}$ mod q,$\frac{zy+wx}{a}$ mod q) = $(z, w) * (x, y)$. □

D. Hinkel proved, in [4], that for arbitrary $r, D \in \mathbb{Z}_q$, the group $L_{\mathbb{Z}_q} = \{(x, y) \in \mathbb{Z}_q^2 : x^2 - Dy^2 = r^2\}$ is cyclic and has order $q-(D/q)$. This result yields the following corollaries.

Corollary 4.2 $|G| = q - (P/q)$.

Corollary 4.3 *LGroups are cyclic.*

In the next three sections we discuss some cryptographic applications of LGroups. Please see Appendix A.2 for MAPLE procedures that apply the operation $\cdot$, find inverses and compute the order of LGroups.

4.3 Feige-Fiat-Shamir Authentication

When transferring information over the Internet or airwaves it is imperative that entities are able to authenticate their identity to one another. In practice, authentication between machines happens far more often than between humans. For example, when one uses their cell phone it must authenticate its identity with the call center for billing purposes. One method for authentication is the Feige-Fiat-Shamir authentication schema.

Feige-Fiat-Shamir authentication is an example of what is known as a *Zero-Knowledge Proof*. The essential idea behind a zero-knowledge proof of identity is that neither parties involved in the authentication process need to disclose any information that could be used by a malicious party.

We now describe the Feige-Fiat-Shamir authentication schema. Alice proves her identity to Bob in t executions of the following algorithm. We describe the kth iteration of the t step process.

1. Alice chooses $g_1, g_2, ..., g_n \in G$ and computes $v_i = (g_i^2)^{-1}$, for each $1 \leq i \leq n$. Her private key is the n-tuple $(g_1, g_2, ..., g_n)$. Her public key is $(v_1, v_2, ..., v_n, G)$.

2. Alice chooses $r \in G$ and computes $X = r^2$ and sends X (publicly) to Bob.

3. Bob sends $(e_1, e_2, ..., e_n)$ where $e_j \in \{0, 1\}$ to Alice.

4. Alice then computes $Y = r \cdot \prod_{i=1}^{n}(g_i^{e_i})$ and sends Y to Bob.

5. Bob then computes $Z = Y^2 \cdot \prod_{i=1}^{n}(v_i^{e_i})$.

If $X = Z$, then Bob accepts Alice's proof of identity for the kth execution. They repeat this process t times.

The best possible attack on Feige-Fiat-Shamir Authentication schema has a $\frac{1}{2^{kt}}$ probability of successfully forging someones identity [7].

For MAPLE implementations of the Feige-Fiat-Shamir authentication schema please see appendix A.3.

4.4 The Diffie-Hellman Key Exchange

Symmetric Key Cryptography relies on the assumption that both communicating parties share a private key. Thus, the problem of establishing a shared private key is central to the issue of security in a symmetric key cryptographic system.

The Diffie-Hellman key exchange protocol allows two parties to securely create a shared key for symmetric key cryptographic purposes. Its security is based on the computational infeasibilty of the discrete log problem.

Remark 4.4 Let G be an LGroup and $g \in G$. Choose $x \in \mathbb{N}$ and compute $b = x \cdot g$. Make g and b public. The discrete log problem is the problem of finding x. □

We will now implement the Diffie-Hellman key exchange protocol in LGroups.

Suppose that Alice and Bob want to communicate securely using a symettric key cryptosystem. To implement the Diffie-Hellman Key exchange they do the following:

1. They agree on a *public* LGroup, G and $g \in G$.

2. Alice and Bob choose random natural numbers x and y (respectively) and compute $u = x \cdot g$, $v = y \cdot g$ (respectively).

3. Alice publicly sends u to Bob and Bob publicly sends v to Alice.

4. Alice then computes $K_a = x \cdot v$ and Bob computes $K_b = y \cdot u$.

Theorem 4.5 *The Diffie-Hellman Key exchange protocol based on LGroups works.*

Proof: $K_a = x \cdot v = \prod_{i=1}^{x} v = \prod_{i=1}^{x}(y \cdot g) = \prod_{i=1}^{x}(\prod_{j=1}^{y} g) = \prod_{j=1}^{y}(\prod_{i=1}^{x} g) = \prod_{j=1}^{y}(x \cdot g) = \prod_{j=1}^{y} u = y \cdot u = K_b$, where the fifth equality, upon switching the order of the products, follows from the associativity of $\cdot$ as proved in Theorem 4.3. $\square$

With regards to the above theorem, we let $K = K_a = K_b$ be the shared private key that Alice and Bob may now use to communicate secretly. Notice that G, g, u, and v are all public. However, K is kept secret by the computational infeasibility of solving the discrete log problem in the amount of time necessary for Alice and Bob to exchange a message.

Please see Appendix A.2 for MAPLE implementations of relevant procedures.

4.5 LGroup El Gamal

We now implement an *El Gamal* style cryptosystem using LGroups. The security of an El Gamal system relies on the computational infeasibility of the discrete log

problem.

Suppose that Alice wishes to receive a secret message from Bob. She must first create a public key so that Bob can encrypt a message for her:

1. She chooses an LGroup, say G, $g \in$, and a random $x \in \mathbb{N}$.

2. She then computes $b = g^x$.

3. Her public key is (b, g, G).

4. She also needs to create a private key to be able to decrypt the ciphertext after recieving it. Let x be Alice's private key.

Let m be the message Bob wants to send to Alice. We assume that, through a prescribed standard protocol, m has been converted, by Bob, into $M \in G$. We call this embedding m in the group, G. For a MAPLE implementation of a standard embedding procedure see Appendix A.4.

Bob uses Alice's public key to encrypt M as follows:

1. Bob chooses a random $r \in \mathbb{N}$.

2. Bob computes, in G, $y = g^r$, $s = b^r$, and then $e = s \cdot m$.

3. Bob's encrypted message is the pair (e, y).

4. Bob sends (e, y) to Alice.

To decrypt (e, y), Alice does the following:

1. She computes $d = y^x$ and then $C = d^{-1} \cdot e$.

2. She then unembeds C from G to get M.

Theorem 4.6 *The El Gamal decryption algorithm based on LGroups works.*

Proof: Recall from above that $b = g^x$. So, $b \cdot g^{-x} = 1$, where 1 denotes the identity in G. Thus, using the formulas derived above, we have $d^{-1} = (y^x)^{-1} = y^{-x} = (g^r)^{-x} = (g^{-x})^r$ and $e = s \cdot M = b^r \cdot M$. So, $C = d^{-1} \cdot e = (g^{-x})^r \cdot b^r \cdot M = (b \cdot g^{-x})^r \cdot M = (1)^r \cdot M = 1 \cdot M = M$. $\square$

For MAPLE implementations of an LGroup El Gamal Cryptosystem, see Appendix A.4.

4.6 LGroup RSA

The Rivest-Shamir-Adleman (RSA) cryptosystem can be implemented on any group G provided that the order of G can be computed and there is a method for embedding messages into G. We now describe the RSA key generation algorithm for an arbitrary group.

Suppose that Alice wishes to receive a secret message from Bob. To create a public and private RSA key Alice does the following:

1. She chooses a group, say G.

2. She computes the order of G which we will denote $|G|$.

3. Alice then chooses a random $r \in \mathbb{N}$ such that $gcd(|G|, r) = 1$ and computes $n = r^{-1} \bmod |G|$. Note that the existence of such an n is guaranteed by the the fact that $gcd(|G|, r) = 1$.

4. Alice's public key is (r, G). Alice's private key is n.

The security of the RSA cryptosystem relies on the computational infeasibility of

the integer factorization problem. Since there is no factorization problem inherant in their definition, RSA *cannot* be implemented on LGroups.

A natural fix for LGroups is to change the prime q to a composite integer R. Since the Legendre function can be generalized to the Jacobi function, we can still require $(k/P) = (k/R) = 1$ and the group operation still makes sense. However, this leads to two open problems whose resolution is necessary for RSA to be implemented on these modified LGroups.

Remark 4.7 Open Problem 1: embedding messages into a modified LGroup. Let m be the padded ASCII message and $G = \{(x, y) \in \mathbb{Z}^2 : x^2 - Py^2 = k \bmod R\}$, where $R = r \cdot s$ for primes r, s. To implement RSA, we need to find a point in G to represent m.

If we attempt to use a Koblitz style embedding procedure, this reduces to the problem of solving $\frac{x^2-k}{P} = y^2 \bmod R$. But, we need the factorization of R to do this, which is private.

If we attempt to use a Lucas Group style embedding (see 4.6.2 below), then we must be able to compute $P = m^2 - a^2$. But, we are not guaranteed that $m^2 - a^2$ is prime. The problem with this approach is that requiring P to be prime is too restrictive for a Lucas Style Embedding.

There is no known embedding procedure for RSA on modified LGroups.

Remark 4.8 Open Problem 2: computing the order of a modified LGroup. We do not yet know the order, in general, for modified LGroups. We conjecture that for the

modified LGroup $G = \{(x, y) \in \mathbb{Z}^2 : x^2 - Py^2 = k \bmod R\}$, where $R = s \cdot t$ for primes s, t, $|G| = (s-\text{Legendre}(P, s)) \cdot (t-\text{Legendre}(P, t))$.

4.7 Wiener's Attack on RSA

Since a major portion of our work above uses the theory of continued fractions, we include a discussion of an attack on the Rivest-Shamir-Adleman (RSA) cryptosystem that uses this theory. For completeness we state the RSA Algorithm for $\mathbb{Z}_R$.

Suppose that Bob wishes to send a secret message to Alice. Alice creates RSA public and private keys as follows:

1. Choose two primes p and q and compute $R = p \cdot q$.
2. Compute $\phi = (p-1)(q-1)$.
3. Choose $e \in \mathbb{Z}$ such that $1 < e < \phi$ and $gcd(e, \phi) = 1$.
4. Choose $d \in \mathbb{Z}$ such that $1 < d < \phi$ and $ed \equiv 1 \bmod \phi$.
5. Alice's private key is (e, R) and her private key is (d, R).

To encrypt a message for Alice, Bob does the following:

1. Get Alice's public key (e, R).
2. Represent the message as a number M in the interval $[1, R-1]$. M is referred to as the plaintext.
3. Compute $C = M^e \bmod R$. This is the ciphertext.
4. Send C to Alice.

To decrypt M Alice does the following:

Compute $M = C^d \bmod R$.

Remark 4.9 The RSA problem. The problem of recovering the plaintext M from the ciphertext C given the public key (e, R) is known as the RSA problem.

Remark 4.10 The integer factorization problem. For $n \in \mathbb{Z}$, the *integer factorization problem* is: find the prime factorization of n.

There is no efficient algorithm that can, in general, solve the RSA problem [7]. However, if one can find the prime factorization of R, then one can efficiently solve the RSA problem. Indeed, for knowing that $R = p \cdot q$ allows one to compute ϕ. This, in turn, allows one to compute $d = e^{-1} \bmod \phi$, since (e, R) is public. Thus, the security of the RSA cryptosystem revolves around the intractability of the integer factorization problem.

4.7.1 Wiener's Attack on Traditional RSA

In 1989 Michael Wiener developed an attack on the RSA cyptosystem which employs the theory of continued fractions. His attack allows one to find the secret RSA exponent, d, provided that d is sufficiently small.

Let $\frac{p}{q}, \frac{p'}{q'}, \delta \in \mathbb{Q}$, with $\delta > 0$, and suppose that $\frac{p'}{q'} = \frac{p}{q} \cdot (1 - \delta)$. That is, $\frac{p'}{q'}$ is a close (for δ small) underestimate of $\frac{p}{q}$.

In [11] Wiener showed that, assuming $\delta < \frac{1}{(3/2)pq}$, we may find $\frac{p}{q}$. We describe the ith step of the algorithm:

1. Compute the ith quotient, a_i', of the continued fraction expansion of $\frac{p'}{q'}$.

2. Using Theorem 1.6, construct $\frac{r}{s} = [a'_0, a'_1, a'_2, ..., a'_{i-1}, a'_i + 1]$ if i is even and $\frac{r}{s} = [a'_0, a'_1, a'_2, ..., a'_{i-1}, a'_i]$ if i is odd.

3. Check if $\frac{r}{s} = \frac{p}{q}$.

It may seem peculiar, in step 2, that we add 1 to the ith quotient. By Theorem 1.9, we have $C'_i \leq \frac{p'}{q'}$, when i is even and $C'_i \geq \frac{p'}{q'}$, when i is odd, where C'_i denotes the ith convergent in the continued fraction expansion of $\frac{p'}{q'}$. If i is odd, then, since $\frac{r}{s} = C'_i$, we have $\frac{p'}{q'} < \frac{r}{s} \leq \frac{p}{q}$. If i is even then adding 1 to the ith quotient ensures that we have $C'_i < \frac{p'}{q'} < \frac{r}{s} \leq \frac{p}{q}$.

Let (R, e) be an RSA public key and d be the corresponding RSA private key.

We have $e \cdot d \equiv 1 \bmod lcm(p-1, q-1)$. So, there is $K \in \mathbb{Z}$ such that $ed = K \cdot lcm(p-1, q-1) + 1$. We know, from elementary number theory, that for any $a, b \in \mathbb{Z}$, $gcd(a, b) \cdot lcm(a, b) = a \cdot b$. Thus, if we let $H = gcd(p-1, q-1)$, $ed = K \cdot lcm(p-1, q-1) + 1$ becomes $ed = \frac{K}{H}(p-1)(q-1) + 1$. Since it is possible that $gcd(K, H) \neq 1$, we let $k = \frac{K}{gcd(K,H)}$ and $h = \frac{H}{gcd(K,H)}$. So, $\frac{k}{h} = \frac{K}{H}$, which yields $ed = \frac{k}{h}(p-1)(q-1) + 1$ or equivalently, $edh = k(p-1)(q-1) + h$.

In [11] Wiener showed that, assuming $kdh < \frac{R}{(3/2)(p+q)}$, $\frac{e}{pq}$ is a close enough estimate of $\frac{k}{dh}$ to invoke steps one and two of the algorithm described above as the first of a series of tests that allow one to find d. Thus, we make this assumption and proceed to describe these tests, which we perform, until failure, for each successive guess of $\frac{k}{dh}$. If, during the ith stage, a test fails, then we know that our ith guess of $\frac{k}{dh}$ was incorrect and we must move on to the $(i+1)$st series of these tests. We additionally

assume, as Wiener did, that $ed > R$. Thus, $R < ed = \frac{k}{h}(p-1)(q-1)+1 \Rightarrow k > h$.

Wiener's RSA Attack: Let $\frac{e}{pq} = [a'_0, a'_1, a'_2, ..., a'_i, ..., a'_{m-1}, a'_m]$ be the continued fraction expansion of $\frac{e}{pq}$.

1. Invoke steps one and two of Wiener's Continued Fraction Algorithm to obtain $\frac{r}{s} = [a'_0, a'_1, a'_2, ..., a'_{i-1}, a'_i + 1]$ if i is even and $\frac{r}{s} = [a'_0, a'_1, a'_2, ..., a'_{i-1}, a'_i]$ if i is odd.

2. By step 1, s is our guess (for this stage) of dh. Thus, we guess that $edh = e \cdot s$.

3. Using $edh = k(p-1)(q-1)+h$, we guess $(p-1)\cdot(q-1)$ by computing $[edh/k]$. If this guess is 0, then we move on to the $(i+1)$st series of tests.

4. Using $edh = k(p-1)(q-1)+h$, we guess h by computing edh mod k.

5. Using our guess of $(p-1)\cdot(q-1)$ and the identity $\frac{pq-(p-1)(q-1)+1}{2} = \frac{p+q}{2}$, we guess $\frac{p+q}{2}$. If $\frac{p+q}{2}$ is not an integer, then we move on to the $(i+1)$st series of tests.

6. Using our guess of $\frac{p+q}{2}$ and the identity $(\frac{p+q}{2})^2 - pq = (\frac{p-q}{2})^2$, we compute a guess of $(\frac{p-q}{2})^2$. If $(\frac{p-q}{2})^2$ is not an integer, then we move on to the $(i+1)$st series of tests.

7. If $(\frac{p-q}{2})^2$ is an integer, then we know that all quantities that we have calculated in the ith stage are correct and we may conclude that $d = \frac{dh}{h}$.

4.7.2 Wiener's Attack on Lucas Group RSA

Let $x \in \mathbb{Z}^+$, $D = x^2 - 4$, and $R \in \mathbb{Z}$ with $R > 2$ and $gcd(2D, R) = 1$. Define $L(D,R) = \{(a,b) \in \mathbb{Z}_R^2 : a^2 - Db^2 = 4 \bmod R\}$. Also, define a binary operation on $L(D,R)$ as follows: $(u,v)\cdot(w,z) = (\frac{R+1}{2}(uz + Dvw), \frac{R+1}{2}(uw + vz))$.

Theorem 4.11 $(L(D,R),\cdot)$ *as defined above is an abelian group.*

We will refer to the group $L(D,R)$ as a *Lucas Group*. Lucas Groups have many applications to cryptography, including RSA. We now describe how to construct public and private Lucas Group RSA keys.

Suppose that Alice wishes to create Lucas Group RSA public and private keys. To do so Alice does the following:

1. Choose odd primes p and q.
2. Compute $R = p \cdot q$ and $\Gamma(R) = (p^2-1)(q^2-1)$.
3. Choose $n < R$ such that $gcd(n, \Gamma(R)) = 1$.
4. Compute $m = n^{-1} \bmod \Gamma(R)$.
5. Alice's public key is (R,n) and Alice's private key is m.

Let M be a message that Bob wants to send to Alice. To encrypt M Bob does the following:

1. Obtain Alice's public key (R,n).
2. Compute $D = M^2 - 4$. Then, $(M,1) \in L(D,R)$.
3. Compute $C = (M,1)^n$ in $L(D,R)$.
4. The encrypted message is C.

Wiener's attack on RSA can be adapted to Lucas Groups. Since Lucas Groups are very similar to LGroups, our motivation is that if RSA is eventually implemented on LGroups then one may easily adapt Wiener's attack on RSA to LGroup RSA.

We assume that Alice has created Lucas group RSA public and private keys, (R, n) and m, respectively, where $R = p \cdot q$ and both p and q are prime. Recall that $m \cdot n \equiv 1 \mod \Gamma(R)$. Thus, there is $k \in \mathbb{Z}$ such that $\Gamma(R) \cdot k + 1 = m \cdot n$.

Theorem 4.12 *Let R, m, n, and k be defined as above. If $q < p < 4q$ and $m < \frac{R^{1/2}}{10}$ and $k \leq min\{m, n\}$, then $\frac{k}{m}$ is a convergent in the continued fraction expansion of $\frac{n}{R^2}$.*

Proof: We first collect the following two facts:

(a) $\frac{k}{m} < 1$.

(b) $p^2 + q^2 < 5R$.

To prove (a), note that if $\frac{k}{m} > 1$, then $k > m$, contrary to assumption.

We now prove (b). Note that $q < p \Rightarrow q^2 < p \cdot q = R$ and $q < p \Rightarrow q \cdot p < p^2 \Rightarrow R < p^2$. So, $q^2 < R < p^2 < 4R$. So, $p^2 + q^2 < 4R + q^2 < 5R$.

We show $\frac{k}{m} - \frac{n}{R^2} < \frac{1}{2m^2}$. Then, by an application of Theorem 1.18, the result follows.

So, $\frac{k}{m} - \frac{n}{R^2} = \frac{kR^2 - nm}{mR^2} = \frac{kR^2 - k\Gamma(R) - 1}{mR^2} = \frac{k(R^2 - \Gamma(R)) - 1}{mR^2} = \frac{k(R^2 - (p^2-1)(q^2-1)) - 1}{mR^2} = \frac{k(R^2 - (R^2 - p^2 - q^2 + 1))}{mR^2} = \frac{k(R^2 - R^2 + p^2 + q^2 - 1) - 1}{mR^2} = \frac{k(p^2+q^2-1)-1}{mR^2} < \frac{k(p^2+q^2)}{mR^2} < \frac{5kR}{mR^2} = \frac{5k}{mR} < \frac{5}{R} < \frac{1}{2m^2}$, where the second, third, and fourth inequalities follow from (b), (a), and the assumption $m < \frac{R^{1/2}}{10}$, respectively. $\square$

Theorem 4.12 shows that, assuming $q < p < 4q$ and $m < \frac{R^{1/2}}{10}$ and $k \leq \min\{m, n\}$, a modification of Wiener's attack on RSA for Lucas Groups will not be in vain. Indeed, since if $\frac{k}{m}$ is not a convergent in the continued fraction expansion of $\frac{n}{R^2}$ then the algorithm described in paragraph three of 4.7.1 will never yield any possible

candidates for $\frac{k}{m}$.

Notice that the definition of D for Lucas groups may be generalized to $D = x^2 - t$ such that Jacobi$(t, R) = 1$, where Jacobi(,) denotes Jacobi's generalization of the Legendre function. Moreover, the group operation still works. We refer to groups formed with this slight variation as generalized Lucas Groups.

All odd primes may be expressed as a difference of squares [2]. Thus, all LGroups are generalized Lucas groups. If, in the future, RSA is implemented on LGroups, then our work in this subsection shows that Wiener's attack on RSA may be implemented on LGroups.

4.8 Summary

LGroups have far reaching applications to cryptography. As is illustrated above, they may be used for authentication, El Gamal, and symmetric key cryptosystems. However, LGroups cannot, at this time, be used for RSA. This is due to the use of primes in the definition of LGroups.

The study of LGroups allows one to gain a deeper understanding of cryptographic groups and their subtlties. When creating groups for cryptography one must be careful to consider what types of cryptography a group will be used for. As in the case of LGroups and RSA, the integer factorization problem cannot be implemented in a way that allows messages to be embedded.

A resolution of open problem 1 would be astounding. It does not seem likely,

given various attempts made by the author, that open problem 1 will ever be resolved. However, solutions to problems once thought unsolvable is the essence of mathematics and the author hopes to, one day, see a solution.

Open problem 2 seems much more attainable. Since LGroups are generalized Lucas groups and the conjecture for open problem 2 holds for Lucas Groups, open problem 2 does not seem far from a solution.

The work we have done here is only the beginning. As cryptographic technology advances and new techniques are created LGroups may find their place in this exciting field. In fact, new cryptosystems may be created using the problems introduced in this thesis. Further research in this direction is encouraged.

REFERENCES

[1] Edward J. Barbeau. *Pell's Equation.* Springer, New York, 2003.

[2] David M. Burton. *Elementary Number Theory*, McGraw-Hill, 1998.

[3] Walter Feit. *Some Diophantine Equations of the Form* $X^2 - PY^2 = Z$, Proceedings of the American Mathematical Society 129(2) (2000), $623 - 625$.

[4] D. E. Hinkel. *Investigation of Lucas sequences*, Master's Thesis, 2007.

[5] Sergey Khrushchev. *Orthogonal Polynomials and Continued Fractions*, Cambridge University Press, 2008.

[6] Donald E. Knuth. *The Art of Programming*, Addison-Wesley, 1973, 1968.

[7] A.J. Menezes, P.C. Van Oorshot, S.A. Vanstone. *The Handbook of Applied Cryptography.* CRC Press, 1996.

[8] C. D. Olds. *Continued Fractions.* Random House, Yale University, 1963.

[9] Don Redmond. *Number Theory*, Marcel Dekker, 1996.

[10] R.G. Stanton, C. Sudler , H.C. Williams. *An Upper Bound for the Period of the Simple Continued Fraction for* $\sqrt{P}$, Pacific Journal of Mathematics 67(2) (1976), $525 - 536$.

[11] Michael J. Wiener. *Cryptanalysis of Short RSA Secret Exponents*, IEEE Transactions on Information Theory 36 (1998), $553 - 558$.

Appendix A

MAPLE PROCEDURES

A.1 Data Collection Procedures

Using the Computer Algebra System MAPLE over 800 pages of data was collected in connection with this Thesis. Most, if not all, of the new results presented in this work were discovered by analyzing this data. Throughout this appendix, we will give the motivation behind each of the MAPLE procedures presented and state some of the theorems came out of the data collected by particular procedures.

The next procedure takes an integer as input and outputs the square free part. This procedure was used in other procedures that implemented Theorems 2.13 and 2.14. Its efficiency is no better than that of integer factorization.

```
GetSqrFreePart:=proc(K)
local X,i,n,SqrFreePart:
if(issqrfree(K)) then
   RETURN(K):
else
   X:=ifactors(K):
   n:=nops(X[2]):
   SqrFreePart:=1:
   for i from 1 to n do
       if(X[2][i][2] mod 2 =1) then
           SqrFreePart:=SqrFreePart*X[2][i][1]:
       fi:
   od:
   RETURN(SqrFreePart):
fi:
end:
```

This procedure is a variation of the one above. It returns the odd square free part of an input integer.

```
GetOddSqrFreePart:=proc(k)
local sqrfreePart:
sqrfreePart:=GetSqrFreePart(k):
if(sqrfreePart mod 2 =0) then
```

```
      RETURN(sqrfreePart/2):
  else
      RETURN(sqrfreePart):
fi:
end:
```

This procedure finds and returns all squares mod n. This was used to develop the Mod N Test.

```
GetSquaresModn:=proc(n)
local i, j, u, m, SquareList, notinlist, temp:
SquareList[1]:=0:
SquareList[2]:=1:
m:=2:                    # n is number of things in list
for i from 2 to n-1 do
   u:=i^2 mod n:
   notinlist:=true:
############## test to see if u is in the list ###########
   for j from 1 to m do
       if(u=SquareList[j]) then
          notinlist:=false:
       fi:
   od:
#############################################################
   if(notinlist) then
       m:=m+1:
       SquareList[m]:=u:
   fi:
od:
temp:=convert(SquareList,list):
RETURN(temp):
end:
```

This procedure was created before there was a Convergent Solutions algorithm. It does essentially the same thing, but with far less efficiency. This was used to develop Chapter Three.

```
GetConverSolnList:=proc(P,Bound)
local i,j,n,m,x,y,temp,z,C,TempList,NotInList:
C:=cfrac(sqrt(P),Bound,'quotients'):
x:=nthnumer(C,0):
y:=nthdenom(C,0):
z:=x^2-P*y^2:
TempList[1]:=z:
```

```
n:=1:
for i from 1 to Bound do
x:=nthnumer(C,i):
y:=nthdenom(C,i):
z:=x^2-P*y^2:
NotInList:=true:
############## test to see if z is in the list ###########
   for j from 1 to n do
       if(z=TempList[j]) then
          NotInList:=false:
       fi:
   od:
#############################################################
   if(NotInList) then
       n:=n+1:
       TempList[n]:=z:
   fi:
od:
temp:=convert(TempList,list):
RETURN(temp):
end:
```

This procedure finds the fundamental solution to any Pell equation. I wrote it at the very beginning of this project. I would definitely do it differently now that I have a much better handle on continued fractions. Still, it works. This is the basis for everything.

```
pellFS := proc (p, BD)
local k, u, x, y, z, C;
C := cfrac(sqrt(p), BD);
for k to BD do
x := nthnumer(C, k);
y := nthdenom(C, k);
z := x^2-p*y^2;
u := evalf(sqrt(p));
if u < x then
if z = 1 then
RETURN([x, y])
end if
end if
end do;
RETURN([-1, -1])
end proc
```

This procedure is used in the next procedure.

```
getdelta := proc (p, BD)
local x, y, d, D, u;
x := pellFSX(p, BD);
y := pellFSY(p, BD);
u := evalf(sqrt(p));
d := evalf(x+y*u);
D := evalf(1/2+(1/2)*d*x/(d-1));
if 0 < x then
RETURN(D)
end if;
if x = -1 then
RETURN(-1)
end if
end proc
```

This procedure finds the fundamental solution to any Pell-Like equation, if it exists. I wrote it at the very beginning of this project. I would definitely do it differently now that I have a much better handle on continued fractions. Still, it works. This is the basis for everything.

```
> PLFS := proc (p, k, BD)
local d, u, v, x, y, s, t, z, U;
d := getdelta(p, BD);
u := evalf(sqrt(p));
v := evalf(sqrt(k*d));
U := floor(v);
if d = -1 then
RETURN([-1, 1])
else for x to U do
y := sqrt((x^2-k)/p);
t := floor(y);
s := x^2-p*y^2;
if type(y, integer) then
if s = k then
RETURN([x, y])
end if
end if
end do;
RETURN([-1, -1])
end if;
RETURN([-1, -2])
```

```
end proc;
```

The following four procedures use Brahmagumpta's Lemma to produce as many solutions to a particular Pell-Like equation as desired. I conjecture that the algorithms employed here generate all solutions.

```
GenerateASoln:=proc(p,k,soln,Bound) # soln is a point
local PellFS,X,Y,i,temp:
PellFS:=pellFS(p,Bound):
if(PellFS[1]=-1) then
   RETURN("Bound too small"):
else
   X[1]:=soln[1]*PellFS[1]-p*soln[2]*PellFS[2]:
   Y[1]:=soln[1]*PellFS[2]-soln[2]*PellFS[1]:
   print([X[1],Y[1]]):
fi:
end:

GenerateASoln2:=proc(p,k,soln,Bound) # soln is a point
local PellFS,X,Y,i,temp:
PellFS:=pellFS(p,Bound):
if(PellFS[1]=-1) then
   RETURN("Bound too small"):
else
   X[1]:=soln[1]*PellFS[1]-p*soln[2]*PellFS[2]:
   Y[1]:=soln[1]*PellFS[2]-soln[2]*PellFS[1]:
   RETURN([X[1],Y[1]]):
fi:
end:

GenerateManySoln:=proc(p,k,soln,Bound) # soln is a point
local PellFS,X,Y,i,temp:
PellFS:=pellFS(p,Bound):
if(PellFS[1]=-1) then
   RETURN("Bound too small"):
else
   X[1]:=soln[1]*PellFS[1]+p*soln[2]*PellFS[2]:
   Y[1]:=soln[1]*PellFS[2]+soln[2]*PellFS[1]:
   print([X[1],Y[1]]):
   for i from 2 to Bound do
```

```
   X[i]:=X[i-1]*PellFS[1]+p*Y[i-1]*PellFS[2]:
   Y[i]:=X[i-1]*PellFS[2]+Y[i-1]*PellFS[1]:
   print([X[i],Y[i]]):
   od:
fi:
end:

GenerateSoln:=proc(P,k,Soln,Bound)
local X:
print(Soln):
GenerateManySoln(P,k,Soln,Bound):
X:=GenerateASoln2(P,k,Soln,Bound):
print(X):
GenerateManySoln(P,k,X,Bound):
end:
```

This procedure tests to see if for a particular k we have $|k| < 1 + 2\sqrt{P}$.

```
SolnKNotInI:=proc(p,k,BD)
local x,y,z:
for x from 1 to BD do
for y from 1 to BD do
z:=x^(2)-p*y^(2):
if(z=k)then
print([x,y]):
fi:
od:
od:
end:
```

This procedure is employed in the Mod N Test.

```
NotSolvableModn:=proc(P,K,n)
local p, i, j, z, m, k, SqrList:
p:=P mod n:
k:=K mod n:
SqrList:=GetSquaresModn(n):
m:=nops(SqrList):
for i from 1 to m do
for j from 1 to m do
   z:=(SqrList[i]-p*SqrList[j]) mod n:
   if(z=k) then
          RETURN(false):
   fi:
```

```
od:
od:
RETURN(true):
end:
```

This is the Mod N Test.

```
ModnTest:=proc(P,K,LowerBound,UpperBound)
local i:
for i from LowerBound to UpperBound do
   if(NotSolvableModn(P,K,i)) then
         printf("not solvable mod %d",i):
         RETURN():
   fi:
od:
printf("test not conclusive"):
end:
```

This procedure was used to produce my initial base of data; nothing pretty here, but it got the job done.

```
ExhaustiveSearch:=proc(P,k,BD)
local x,y,z,u,v,soln,FS,temp:
print(P mod 4):
print(issqrfree(k)):
temp:=floor(evalf(1+2*sqrt(P))):
if((-temp)<k and k<temp) then
print("K in I"):
else
print("K not in I"):
fi:
if(legendre(k,P)=1) then
   print("legendre(k,P)=1"):
fi:
if(legendre(k,P)=-1) then
   print("legendre(k,P)=-1"):
fi:
if(legendre(k,P)=0) then
   print("legendre(k,P)=0"):
fi:
soln:=0:
if(legendre(k,P)=1 or legendre(k,P)=0) then
temp:=Test5(P,k):
```

```
if(temp=1) then
   RETURN("not solvable by Theorem 5"):
fi:
temp:=Test6(P,k):
if(temp=1) then
   RETURN("not solvable by Theorem 6"):
fi:
temp:=Test7(P,k):
if(temp=1) then
   RETURN("not solvable by Theorem 7"):
fi:
temp:=Test8(P,k):
if(temp=1) then
   RETURN("not solvable by Theorem 8"):
fi:
   for x from 1 to BD do
   for y from 1 to BD do
   z:=x^2-P*y^2:
   if(z=k)then
      print([x,y]):
      soln:=1:
   fi:
   od:
   od:
   if(soln=0) then
      FS:=PLFS(P,k,BD):
      if(FS[1]>0) then
         print(FS):
      else
         if(FS[2]=1) then
             print("Bound too small"):
         fi:
         if(FS[2]=-1) then
             print("Legendre(k,p)=1 but the equation
             is Not Solvable"):
         fi:
      fi:
   fi:
else
   print("not solvable"):
fi:
end:
```

This next series of procedures implements the Theorems in 2.11.

```
Test5:=proc(P,k) # returns 1 if not solvable, -1 when test is
inconclusive or k =1
local sqrfreePart:
sqrfreePart:=GetSqrFreePart(k):
if(sqrfreePart mod 4 =3 and P mod 4 =3) then
   RETURN(1):
else
   RETURN(-1):
fi:
end:

Test6:=proc(P,k) # k must not be perfect square
returns 1 if not solvable,
 -1 when test is inconclusive
local sqrfreePart, oddsqrfreePart, numberOfPrimes
InOddSqrFreePart,i,qq:
sqrfreePart:=GetSqrFreePart(k):
if(P mod 8 =5 and type(sqrfreePart/2,integer)
and legendre(2,P)=-1) then
   RETURN(1):
fi:
oddsqrfreePart:=GetOddSqrFreePart(k):
numberOfPrimesInOddSqrFreePart:=nops(ifactors
(oddsqrfreePart)[2]):
for i from 1 to numberOfPrimesInOddSqrFreePart do
       qq:=ifactors(oddsqrfreePart)[2][i][1]:
       if(legendre(P,qq)=-1) then
       RETURN(1):
       fi:
od:
RETURN(-1):
end:
```

I used this next procedure to collect data on convergent solutions.

```
PLConverSoln:=proc(P,SolnBound)
local C,n,ConverSolnList,i,x,y,z,j:
ConverSolnList:=GetConverSolnList(P,SolnBound):
```

```
n:=nops(ConverSolnList):
C:=cfrac(sqrt(P),SolnBound,'quotients'):
print(ConverSolnList):
for i from 1 to n do
printf("---------------- x^2-%dy^2=%d----------------",
P,ConverSolnList[i]):
print():
for j from 0 to SolnBound do
x:=nthnumer(C,j):
y:=nthdenom(C,j):
z:=x^2-P*y^2:
if(z=ConverSolnList[i]) then
   print([x,y,j]):
fi:
od:
print():
print():
od:
end:
```

A.2 LGroup Procedures

The following MAPLE procedures implement operations on LGroup.

This procedure applys the LGroup operation.

```
LGroupApplyOp:=proc(g,h,G) # g, h elements in group G
local x, y:
x:=(g[1]*h[1]+G[1]*g[2]*h[2])/G[3] mod G[2]:
y:=(g[1]*h[2]+h[1]*g[2])/G[3] mod G[2]:
RETURN([x,y]):
end:
```

This procedure computes the inverse of an element of an LGroup.

```
ComputeInverse:=proc(pt,G)
local z:
z:=G[2]-pt[2]:
RETURN([pt[1],z]):
end:
```

This procedure finds $2g$.

```
LGroupDouble:=proc(pt,G)
RETURN(LGroupApplyOp(pt,pt,G)):
end:
```

This procedure computes xg, for any scalar x and any $g \in G$.

```
LGroupTimes:=proc(Point,scalar,Group)
local m, pt, x, j:
if ((Point = LGroupIdentity) or (scalar = 0)) then
   RETURN(LGroupIdentity):
else
  m :=scalar:
  pt:=Point:
  x :=LGroupIdentity:
  for j from 1 to scalar do
    if (m mod 2 = 0) then
      m := m/2:
    else
      m:= (m-1)/2:
      x:= LGroupApplyOp(x,pt,Group):
    fi:
     if (m = 0) then
      RETURN(x):
     fi:
        pt:= LGroupDouble(pt,Group):
  od:
fi:
end:
```

This procedure searches, within bounds, for an element of G. Notice the logic used: we first use the Legendre function to test if there is an integer, say x, such that $x^2 = (i^2 - k)/P$ mod Q and secondly the Tonelli Shanks algorithm is used to find such an x. LGroupSearch is also used to find r.

```
LGroupSearch:=proc(lower,upper,P,k,Q)
local i, temp, foundx, foundy:
for i from lower to upper do
temp:=(i^2-k)/P mod Q:
if(legendre(temp,Q)=1) then
   foundx:=i:
   foundy:=TonSh(temp,Q):
   RETURN([foundx,foundy]):
fi:
od:
```

```
print("need different bounds"):
end:
```

This procedure computes the order of G.

```
LGroupOrder:=proc(G)
local k:
k:=LGroupApplyOp([G[3],0],[G[3],0],G):
RETURN(G[2]-legendre(k/P)):
end:
```

This procedure finds g^{-1}.

```
ComputeInverse:=proc(pt,Q)
local z:
z:=Q-pt[2]:
RETURN([pt[1],z]):
end:

LGroupOrder:=proc(G)
RETURN(G[2]-legendre(G[1]/G[2])):
end:
```

A.3 Feige-Fiat-Shamir Authentication Procedures

The following procedures are specific to the FFS authentication scheme.

The GetPrivateKey procedure generates such a k tuple.BoundList is a one dimensional array consisting of bounds within which each component of the k-tuple is chosen. For example BoundList= $[[100, 200], [250, 400], [1000, 5000]]$.

```
GetPrivateKey:=proc(BoundList,t,P,k,Q) # t=|boundlist|
local i, X, Y:
#t:=nops(BoundList):
for i from 1 to t do
X[i]:=LGroupSearch(BoundList[i][1],BoundList[i][2],P,k,Q):
od:
Y:=convert(X,list):
RETURN(Y):
end:
```

The ComputePublicKey Procedure computes the FFS public key which is another k tuple.

```
ComputePublicKey:=proc(SList,t,P,a,Q)
local i, y, v, temp:
#t:=nops(SList):
for i from 1 to t do
temp:=ApplyOp(SList[i][1],SList[i][2],SList[i][1],
SList[i][2],P,a,Q):
#find s[i]^2
v[i]:=ComputeInverse(temp,Q): # find s[i]^2 inverse
#print(v[i]):
od:
y:=convert(v,list):
RETURN(y):
end:
```

The first step in FFS is for Alice to choose $r \in G$ and compute $x := r^2$ and send this x to Bob. The ComputeX Procedure computes such an x given some choice of r.

```
ComputeX:=proc(pt,P,a,Q)
RETURN(ApplyOp(pt[1],pt[2],pt[1],pt[2],P,a,Q)):
end:
```

The ComputeY Procedure computes such a Y given an eList.

```
ComputeY:=proc(pt,SList,eList,t,P,a,Q)
local i, y, temp:
if(eList[1]=0) then
   temp:=LGroupIdentity:
else
   temp:=SList[1]:
fi:
for i from 2 to t do
   if(eList[i]=0) then
      temp:=ApplyOp(temp[1],temp[2],LGroupIdentity[1],
      LGroupIdentity[2],P,a,Q):
   else
      temp:=ApplyOp(temp[1],temp[2],SList[i][1],
      SList[i][2],P,a,Q):
   fi:
od:
y:=ApplyOp(pt[1],pt[2],temp[1],temp[2],P,a,Q):
RETURN(y):
end:
```

The next step is for Bob to compute $Z := Y^2 * V_1^{e_1} * ... * V_k^{e_k}$. The ComputeZ Procedure computes such a Z given a Y.

```
ComputeZ:=proc(pt,VList,eList,t,P,a,Q) # pt should be y computed above
local i, y, z, temp:
if(eList[1]=0) then
   temp:=LGroupIdentity:
else
   temp:=VList[1]:
fi:
for i from 2 to t do
   if(eList[i]=0) then
      temp:=ApplyOp(temp[1],temp[2],LGroupIdentity[1],
      LGroupIdentity[2],P,a,Q):
   else
      temp:=ApplyOp(temp[1],temp[2],VList[i][1],VList[i][2],P,a,Q):
   fi:
od:
y:=ApplyOp(pt[1],pt[2],pt[1],pt[2],P,a,Q):
z:=ApplyOp(y[1],y[2],temp[1],temp[2],P,a,Q):
RETURN(z):
end:
```

The last step is authentication verification. To do this Bob checks if $Z = X$. If so, then Bob accepts Alice. The CheckFFS Procedure checks if $Z = X$ and returns true if Alice's identity is authenticated and false if her authentication is denied.

```
CheckFFS:=proc(X,Z)
if(X[1]-Z[1]=0 and X[2]-Z[2]=0) then
RETURN(true):
else
RETURN(false):
fi:
end:
```

A.4 LGroup El Gamal Procedures

The LGroup Numbered Procedure is used in the LGroup Embed Procedure.

```
LGroupNumberembed:=proc(xvalue,Gp,tolerance)
local j, lb, ub, pt:
print(Gp[2]);
```

```
if((xvalue+1)*tolerance-1 < Gp[2]) then
pt:=LGroupSearch(xvalue*tolerance, (xvalue+1)*tolerance-1,Gp):

RETURN(pt):
else
printf("The embedding interval is too large for the group\n"):
fi:
end:
```

The LGroupEmbed procedure embeds messages into LGroups.

```
LGroupEmbed:=proc(Message,Gp,tolerance)
 local AMessage, noofpackets, j, pt, N:
 AMessage:=ASCIIPad(Message,floor(Gp[2]/(tolerance+1))):
 noofpackets:=nops(AMessage):
 for j from 1 to noofpackets do
  N:=(op(0,op(1,AMessage))[j]);
  pt[j]:=LGroupNumberembed(N,Gp,tolerance):
 od:
 pt:=convert(pt,list):
 RETURN(pt):
end:
```

The LGroupUnembed procedure unembeds messages from LGroups.

```
LGroupUnembed:=proc(ptlist,tolerance)
local j, k, X, N:
k:=nops(ptlist):
for j from 1 to k do
  X[j]:=floor(ptlist[j][1]/tolerance):
od:
X:=convert(X,list):
ASCIIDepad(X);
end:
```

The LGroupPubKey procedure generates an LGroup El Gamal public key.

```
LGroupPubKey:=proc(lowerbound,upperbound,x,G)
local g,b:
g:=LGroupSearch(lowerbound,upperbound,G):
b:=LGroupTimes(g,x,G):
RETURN([b,g,G]):
end:
```

The LGroupEncryption procedure encrypts a plaintext.

```
LGroupEncryption:=proc(r,PubKey,M)
local y,s,e:
y:=LGroupTimes(PubKey[2],r,PubKey[3]):
s:=LGroupTimes(PubKey[1],r,PubKey[3]):
e:=LGroupApplyOp(s,M,PubKey[3]):
RETURN([e,y]):
end:
```

The LGroupDecryption procedure decrypts a cyphertext.

```
LGroupDecryption:=proc(e,y,x,G)
local c, d:
d:=LGroupTimes(y,x,G):
c:=LGroupApplyOp(ComputeInverse(d,G),e,G):
RETURN(c):
end:
```

Appendix B

A POLYNOMIAL TIME ALGORITHM FOR DETERMINING IF AN INTEGER IS A SQUARE

B.1 The Issquare Algorithm

Let $n \in \mathbb{Z}^+$ and consider $I_1 = [0, n]$. An analogous algorithm can be described when $n < 0$. If $n = 1$ then, clearly, n is a square. Thus, we assume $n > 1$. Define $f(x) = x^2 - n$. It is clear that f is continuous. Moreover, $f(0) = -n < 0$ and $f(n) = n^2 - n > 0$. Thus, we may apply the Intermediate Value Theorem to obtain $x_0 \in I_1$ such that $f(x_0) = 0$. Now, consider $[0, \frac{n}{2}]$ and $[\frac{n}{2}, n]$. Since f, when restricted to I_1, is one-to-one, we may conclude that $x_0 \in [0, \frac{n}{2}]$ or $x_0 \in [\frac{n}{2}, n]$ and not both. We compute $f(0)$, $f(\frac{n}{2})$, and $f(n)$. There are three possibilities: $f(0) < 0$, $f(\frac{n}{2}) < 0$, and $f(n) > 0$ or $f(0) < 0$, $f(\frac{n}{2}) > 0$, and $f(n) > 0$ or $f(\frac{n}{2}) = 0$. If the first case holds, then we choose $I_2 = [\frac{n}{2}, n]$. If the second case holds, then we choose $I_2 = [0, \frac{n}{2}]$. If the third holds then, we set $\alpha = \frac{n}{2}$ and check if $\alpha^2 = n$. If so, then we know that n is a square. Otherwise, we know that n is not a square.

Suppose that $I_m = [a, b]$ has been defined and $x_0 \in I_m$. We describe how to define I_{m+1}. Since f, when restricted to I_m, is one-to-one, we may conclude that $x_0 \in [a, \frac{a+b}{2}]$ or $x_0 \in [\frac{a+b}{2}, b]$ and not both. We compute $f(a)$, $f(\frac{a+b}{2})$, and $f(b)$. There are three possibilities: $f(a) < 0$, $f(\frac{a+b}{2}) < 0$, and $f(b) > 0$ or $f(a) < 0$, $f(\frac{a+b}{2}) > 0$, and $f(b) > 0$ or $f(\frac{a+b}{2}) = 0$. If the first case holds, then we choose $I_{m+1} = [\frac{a+b}{2}, b]$. If the second case holds, then we choose $I_{m+1} = [a, \frac{n}{2}]$. If the third holds then, we set $\alpha = \frac{a+b}{2}$ and check if $\alpha^2 = n$. If so, then we know that n is a square. Otherwise, we know that n is not a square.

We repeat this process until, for some integer k, $(\frac{1}{2})^k \cdot n < 1$. Then, $x_0 \in I_k \subset [0, n]$ and $\text{length}(I_k) < 1$. Note that we can make this final interval as small as desired.

We search I_k for an integer. Since $\text{length}(I_k) < 1$, there is at most one integer in I_k. If there is no integer in I_k, then we know that n is not a square. If we find an integer, say α, the we check if $\alpha^2 = n$. If not, then we know that n is not a square. If so, then we know that n is a square.

B.2 Time Complexity Considerations

A real valued function f is said to be *Big O* of a real valued function g, if for all sufficiently large x we have $f(x) \leq a \cdot g(x)$ for some constant a. If f is Big O of g,

we write $f = O(g)$. Some important properties of Big O notation are summarized in the following theorem. For a proof see [6].

Theorem B.1 *Let f and g be real valued functions. Then,*
(a) $O(f) + O(f) = O(f)$
(b) $O(f) \cdot O(g) = O(f \cdot g)$

An algorithm is said to run in *polynomial time* if and only if its running time is upper bounded by a polynomial in the size of the input for the algorithm. The size of the input, n, for the issquare algorithm is less than or equal to $\log_2(n)$. Thus, if we can find a polynomial, say f, such that the running time of the issquare algorithm is less than or equal to $f(\log_2(n))$, then we may conclude that the issquare algorithm runs in polynomial time.

Phrased in terms of Big O notation, if we can show that there is a polynomial f such that the issquare algorithm has a running time of $O(f(\log_2(n)))$, then we may conclude that the issquare algorithm runs in polynomial time.

Let $COMP$ denote the greatest number of computations performed in each step of the issquare algorithm and S denote the number of steps in the issquare algorithm.

It is well known that squaring an integer, subtracting integers, and making a comparison of two integers are all polynomial time operations. Indeed, for squaring an integer x is $O(\log_2(x^2))$, subtraction of $x^2 - P$ is $O(\max\{\log_2(P), \log_2(x^2)\})$, and a comparison of integers a, b is $O(\max\{\log_2(a), \log_2(b)\})$. Thus, by Theorem B.1.a $COMP$ is polynomial time in $\log_2(P)$.

The issquare algorithm has, at most, $S = \log_2(P)$ steps. Thus, the runtime of the issquare algorithm is bounded above by $S \cdot COMP$, which, by Theorem B.1.b is polynomial time. So, the issquare algorithm runs in polynomial time.