5-4-2012

On Representations of integers by the quadratic form x2 − Dy2

Christopher Thomas

On Representations of Integers by the Quadratic Form $x^2 - Dy^2$

by

Christopher K. Thomas

A thesis submitted in partial fulfillment of the
requirements for the degree of Master of Science
in the School of Mathematical Sciences
Rochester Institute of Technology

May 4, 2012

Dr. Anurag Agarwal, Thesis Advisor

Prof. David Barth-Hart, Committee Member

Dr. Matthew Coppenbarger, Committee Member

On Representations of Integers by the Quadratic Form $x^2 - Dy^2$

by

Christopher K. Thomas

Submitted to the
School of Mathematical Sciences
in partial fulfillment of the requirements
for the Master of Science Degree
at the Rochester Institute of Technology

Abstract

The representation of integers in binary quadratic forms has been a penchant for mathematicians throughout history including the well known Pierre de Fermat and Charles Hermite. The area has grown from simple representations as the sum of squares to representations of the form $x^2 - Dy^2$ where $D > 1$ and square-free. Based on congruence relations we will provide a classification criterion for the integers that can be represented in the form $x^2 - Dy^2$ for various values of D (specifically $D = 10$ and 11). We will also discuss methods for constructing such representations using the theory of continued fractions, quadratic reciprocity and solutions to Pell's equations.

Acknowledgements

I would like to thank a number of people for their aid and support in the creation of this thesis. I extend my most sincere thanks to my advisor Dr. Anurag Agarwal who taught me not only the intricacies of mathematics but also the inherit beauty in the subject. After having Dr. Agarwal for numerous courses, he taught me the value of problem solving and the elation possible after finding a solution to most difficult problems. I would also like to thank Dr. Matthew Coppenbarger for helping me on my first steps towards mathematical research and Professor David Barth-Hart for showing me the rich field of Number Theory. I generously thank all three for their suggestions in the creation of this thesis.

Secondly I would like to thank the cornerstone of my life, my dear friends and family who have made it possible for me to attend RIT and complete this thesis.

Finally, I would like to thank the entire faculty and staff in the School of Mathematical Sciences for their unwavering assistance while I completed this sojourn through my course work at RIT.

This is dedicated to my mother and late father; my very first instructors.

Contents

Notation

$\mathbb{N} = \{1, 2, 3, \ldots\}$
$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$
$\mathbb{Q}$ = rational numbers
$\mathbb{R}$ = real numbers
$\mathbb{C}$ = complex numbers

Chapter 1

Continued Fractions and Pell's Equation

1.1 Integer Representations, A Historical Perspective

Is it possible to represent a positive integer as the sum of the squares of two integers? After a little thought we can conclude yes since $5 = 1^2 + 2^2$. Are there more integers that satisfy this requirement? The answer is yes and, in fact, there are an infinite number of integers that can be represented as the sum of two squares. It is natural to consider primes that have this property and if p is an odd prime and $p \equiv 1 \pmod 4$ then p can be represented as the sum of two squares. Fermet later extended this to composite integers n of the form

$$n = 2^{\alpha} \prod_{p \equiv 1(4)} p^{\beta} \prod_{q \equiv 3(4)} q^{\gamma}$$

where γ must be even, and p and q are primes [5]. The problem of determining which integers have a representation is solved but finding that representation can still be a burden.

In 1848, Hermite published [3] in which he proposed an algorithmic method to find the integers for the representation using quadratic residues and continued fractions. Later in 1972, Hermite's algorithm was improved upon by Brillhart in [2] which is still the most efficient algorithm for finding the representation. The method created by Hermite and

extended upon by Brillhart was extended to other representations of the form $u^2 + 5v^2$ by Wilker in [7]. The algorithm Wilker uses is different from the one created by Hermite as it applies the well known Euclidean algorithm to find the required representation. As it often occurs, this method was then extended by Matthews in [4] to find representations of integers in the form $x^2 - Dy^2$ where $D = 2, 3, 5$, and 7. We shall extend this algorithm to find representations when $D = 10$ and $D = 11$, but first we introduce one of the first diophantine equations to have been posed.

1.2 Introduction to Pell's Equation

There are many equations that mathematicians throughout history have attempted to solve; some of those equations gave rise to new number systems, the complex field is a prime example. However some of the oldest equations were only solved using integers and in that light we have the field of **diophantine equations**. Diophantine equations are those where only integer solutions are accepted. Therefore equations that are trivial in relation to the complex or real field become quite interesting when working in the ring of integers. A famous problem submitted by Archimedes, nicknamed the "Cattle Problem", determines the number of cattle required from eight different varieties that satisfy a system of linear equations including certain requirements that two quantities are perfect squares [6]. After much simplification of the equations and requirements the problem reduces to finding integer solutions to

$$x^2 - 4729494y^2 = 1.$$

Even today, without the proper tools, it is quite an equation to solve! It falls under the category of equations known as Pell's equations.

Pell's equations are diophantine equations of the form

$$x^2 - Dy^2 = 1 \tag{1.1}$$

where $D \in \mathbb{N}$ and D is square-free. If $D < 0$ then the equation has a finite number of solutions [5]. We restrict D to be square free for the following reason. Assume D is not square-free, which implies $D = d^2k$ for some $d, k \in \mathbb{Z}$. Then we have $x^2 - k(dy)^2 = 1$ which is simply a new equation with a square-free D, namely k. If k is not square-free,

then we simply perform the same procedure until we reduce the equation to an integer which is square-free.

This equation has a rich history throughout mathematics and even well known mathematicians such as Fermat had their hand in the proverbial pot. Lagrange was the first to prove that Pell's Equation has infinitely many solutions if D is a fixed integer and not a perfect square [5]. The equation is named after mathematician John Pell even though he supplied little to the solution of such an equation. Leonard Euler mistakenly named the equation for him after some confusion between Pell and William Brouncker who was one of the first mathematicians to publish a solution technique [5],[6].

After finding solutions to (1.1), mathematicians expanded the equations to what are known as generalized Pell's equations and are given as

$$x^2 - Dy^2 = N \tag{1.2}$$

where $D \in \mathbb{N}$, D is square free, and N is non-zero.

The most efficient means for solving Pell's equations is using continued fractions. The theory of continued fractions is another historically deep area of mathematics that, to appreciate its full beauty, is beyond the scope of this paper. Certain results are needed for the solution of (1.1) and hence will be included.

1.3 Continued Fractions

A continued fraction expansion of a real number ξ is given as

$$\xi = a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \cfrac{b_3}{\cdots}}}}$$

where $a_i, b_i \in \mathbb{C}$. If $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$ for $i > 0$, and $b_j = 1$ for all j then this is considered to be a **simple continued fraction**. A commonly used notation for a simple continued

fraction, and the one we will use, is

$$\xi = \langle a_0; a_1, a_2, a_3, \cdots \rangle.$$

Each of these a_i are called **partial quotients** since they are determined by repeated use of the division algorithm. This then implies that $a_i > 0$ for all $i \geq 1$. We now have the following result for rational numbers as provided by [5].

Theorem 1. *A simple continued fraction is finite if and only if it represents a rational number.*

Proof. Let $\xi = \langle a_0; a_1, a_2, \cdots, a_n \rangle$ be a simple continued fraction. We proceed by induction. If $n = 0$ then $\xi = a_0$ and since the continued fraction is simple $\xi \in \mathbb{Q}$. Assume the result holds for some $k \in \mathbb{N}$. Now consider $\xi = \langle a_0; a_1, a_2, \cdots, a_k, a_{k+1} \rangle$. Then note that

$$\langle a_0; a_1, a_2, \cdots, a_{k+1} \rangle = a_0 + \frac{1}{\langle a_1, a_2, \cdots, a_{k+1} \rangle}$$

and since the continued fraction is simple $a_0 \in \mathbb{Q}$ so we need to establish the remaining portion is rational. By the inductive hypothesis we know $\langle a_0; a_1, a_2, \cdots, a_k \rangle$ is rational and hence $\langle a_1, a_2, \cdots, a_{k+1} \rangle$ is rational since it is a simple continued fraction which contains k terms. Therefore the entire continued fraction is rational. Thus by mathematical induction the result holds for all $k \in \mathbb{N}$. Now let ξ be a rational number which implies $\xi = \frac{x_0}{x_1}$ where $x_0, x_1 \in \mathbb{Z}$, $x_1 \neq 0$, and $\gcd(x_0, x_1) = 1$. Now applying the division algorithm to ξ using x_0 and x_1 we will obtain a series of equations of the form

$$x_i = x_{i+1} a_i + x_{i+2} \quad \text{where } 0 \leq x_{i+2} < x_{i+1}$$

where eventually $x_{i+2} = 0$ for some $i \in \mathbb{N}$. If we take each a_i as our partial quotients and form a continued fraction then, since the division algorithm is guaranteed to end, it will be finite. The result is established. ■

We now give the following recurrence relations as given by [5]

$$p_i = a_i p_{i-1} + p_{i-2} \quad \text{for } i \geq 0 \tag{1.3}$$

$$q_i = a_i q_{i-1} + q_{i-2} \quad \text{for } i \geq 0 \tag{1.4}$$

where $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, and $q_{-1} = 0$. We have the following result provided by [5].

Theorem 2. *For any positive real number ξ,*

$$\langle a_0; a_1, \cdots, a_{n-1}, \xi \rangle = \frac{\xi p_{n-1} + p_{n-2}}{\xi q_{n-1} + q_{n-2}}.$$

Proof. We proceed using induction. If $n = 0$ then we have

$$\xi = \frac{\xi p_{-1} + p_{-2}}{\xi q_{-1} + q_{-2}}$$

which holds by (1.3) and (1.4). If we assume the result holds for some $k \in \mathbb{N}$ then consider the case when $n = k + 1$. Then we have

$$\langle a_0; a_1, a_2, \cdots, a_k, \xi \rangle = \left\langle a_0; a_1, a_2, \cdots, a_{k-1}, a_k + \frac{1}{\xi} \right\rangle$$

and applying the induction hypothesis we have

$$\begin{aligned} \left\langle a_0; a_1, a_2, \cdots, a_{k-1}, a_k + \frac{1}{\xi} \right\rangle &= \frac{(a_k + \frac{1}{\xi})p_{n-1} + p_{n-2}}{(a_k + \frac{1}{\xi})q_{n-1} + q_{n-2}} \\ &= \frac{\xi a_n p_{n-1} + \xi p_{n-2} + p_{n-1}}{\xi a_n q_{n-1} + \xi q_{n-2} + q_{n-1}} \\ &= \frac{\xi p_n + p_{n-1}}{\xi q_n + q_{n-1}} \end{aligned}$$

where the final equality holds by (1.3) and (1.4). Therefore by the principle of mathematical induction the result holds for all $n \in \mathbb{N}$. ■

Adding to this result we have the following results from [5] which will all aid in the establishment of a later result.

Theorem 3. *If we define $r_n = \langle a_0; a_1, \cdots, a_n \rangle$ for all integers $n \geq 0$, then $r_n = \frac{p_n}{q_n}$ where p_n and q_n are given by (1.3) and (1.4).*

The reader may refer to [5, p. 330] for the proof.

Theorem 4. *Let* $\gcd(p_i, q_i) = 1$. *Then the equations*

$$p_i q_{i-1} - p_{i-1} q_i = (-1)^{i-1} \qquad r_i - r_{i-1} = \frac{(-1)^{i-1}}{q_i q_{i-1}}$$

hold for $i \geq 1$ and the identities

$$p_i q_{i-2} - p_{i-2} q_i = (-1)^i a_i \qquad r_i - r_{i-2} = \frac{(-1)^i a_i}{q_i q_{i-2}}$$

hold for $i > 1$.

The reader may refer to [5, p. 330,331] for the proof.

Theorem 5. *The values r_n from Theorem 3 satisfy*

$$r_0 < r_2 < r_4 < r_6 < \cdots < r_7 < r_5 < r_3 < r_1.$$

Furthermore, $\lim_{n\to\infty} r_n$ exists, and for every $j \geq 0$, $r_{2j} < \lim_{n\to\infty} r_n < r_{2j+1}$.

The reader may refer to [5, p. 331] for the proof.

The previous theorem suggests a definition for an **infinite continued fraction**. Note the definition is the same as the finite version, except that it is infinite. This also yields what is known as the n^{th} **convergent** to an infinite continued fraction, which is defined as r_n as given by Theorem 3. Therefore we have the following result which will classify irrational numbers, similar to Niven's classification of rational numbers using continued fractions [5].

Theorem 6. *The value of any infinite simple continued fraction is irrational.*

Proof. Let $\xi = \langle a_0; a_1, a_2, \cdots \rangle$. By Theorem 5 then $r_n < \xi < r_{n+1}$ for all $n \in \mathbb{N}$. Using this inequality we then have $0 < |\xi - r_n| < |r_{n+1} - r_n|$. Now by the definition of r_n in

Theorem 3 and using the identity in Theorem 4 we have

$$0 < \left| \xi - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

Now multiplying by q_n we have

$$0 < |\xi q_n - p_n| < \frac{1}{q_{n+1}}.$$

Now let us assume $\xi = \dfrac{x}{y}$ for some $x, y \in \mathbb{Z}$ such that $y > 0$, i.e. $\xi \in \mathbb{Q}$. Then the above becomes

$$0 < \left| \frac{x}{y} q_n - p_n \right| < \frac{1}{q_{n+1}}.$$

Now multiplying through by y we have

$$0 < |x q_n - y p_n| < \frac{y}{q_{n+1}}.$$

By the definition of q_n given by (1.4) we know the integers are increasing and therefore there exists an $n \in \mathbb{N}$ such that $y < q_{n+1}$. Which implies $\dfrac{y}{q_{n+1}} < 1$ and hence

$$0 < |x q_n - y p_n| < 1$$

which is a contradiction since $|x q_n - y p_n|$ must be an integer. ■

We now have a method for determining whether a continued fraction represents a rational or irrational number. However, is it possible to have two different continued fractions that represent the same number? The answer is no and is given by the following result from [5].

Theorem 7. *Two distinct infinite simple continued fractions converge to different values.*

The reader may refer to [5, p. 333] for the proof.

We have previously shown that an infinite continued fraction represents an irrational number we will now prove the converse as given in [5]. Consider an irrational number ξ

which we can rewrite as

$$\xi = \langle a_0; a_1, a_2, \cdots, a_{n-1}, \xi_n \rangle = \frac{\xi_n p_{n-1} + p_{n-2}}{\xi_n q_{n-1} + q_{n-2}}$$

where $\xi_n = a_n + \dfrac{1}{\xi_{n+1}}$ and $a_i = \lfloor \xi_n \rfloor$. Applying Theorem 4 we have

$$\xi - r_{n-1} = \frac{\xi_n p_{n-1} + p_{n-2}}{\xi_n q_{n-1} + q_{n-2}} - \frac{p_{n-1}}{q_{n-1}}.$$

Now simplifying and applying the identities from Theorem 4 we have

$$\xi - r_{n-1} = \frac{(-1)^{n-1}}{q_{n-1}(\xi_n q_{n-1} + q_{n-2})}.$$

Note that q_n is increasing and positive for all n and ξ_n is positive. Thus

$$\lim_{n\to\infty} \frac{(-1)^{n-1}}{q_{n-1}(\xi_n q_{n-1} + q_{n-2})} = 0$$

which implies

$$\xi = \lim_{n\to\infty} r_n = \lim_{n\to\infty} \langle a_0; a_1, a_2, \cdots, a_n \rangle = \langle a_0; a_1, a_2, \cdots \rangle$$

which completes the result.

We will now give results that prove continued fractions are the best approximations to irrational numbers which will later be useful when finding approximations to numbers of the form $\sqrt{D}$.

Theorem 8. *If $\frac{x}{y}$ is a rational number with $y > 0$ such that $\left|\xi - \frac{x}{y}\right| < \left|\xi - \frac{p_n}{q_n}\right|$ for some $n \geq 1$, then $y > q_n$. In fact if $|\xi y - x| < |\xi q_n - p_n|$ for some $n \geq 0$, then $y \geq q_{n+1}$.*

The reader may refer to [5, p. 338,339] for the proof.

Theorem 9. *Let ξ denote any irrational number. If there is a rational number $\frac{x}{y}$ with*

$y \geq 1$ such that

$$\left|\xi - \frac{x}{y}\right| < \frac{1}{2b^2}$$

then $\frac{x}{y}$ equals one of the convergents of the simple continued fraction expansion of ξ.

The reader may refer to [5, p. 339] for the proof.

Theorem 10. *The n^{th} convergent of $\frac{1}{x}$ is the reciprocal of the $(n-1)^{st}$ convergent of x if x is any real number greater than 1.*

The reader may refer to [5, p. 340] for the proof.

We now provide a small example of a continued fraction for an irrational number.

Example 1. Consider $\sqrt{2}$. First we have

$$\sqrt{2} = 1 + \sqrt{2} - 1 = 1 + \frac{1}{\sqrt{2}+1}$$

and

$$\sqrt{2} + 1 = 2 + \sqrt{2} - 1 = 2 + \frac{1}{\sqrt{2}+1}$$

which will continue to repeat. Therefore

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}$$

Thus we have $\sqrt{2} = \langle 1; 2, 2, 2, \cdots \rangle$.

From this example we can define what is known as a **periodic continued fraction**; if there exists an $n \in \mathbb{N}$ such that $a_r = a_{n+r}$ for all large r [5]. This can then be used to simplify the notation a bit and in our previous example we can write $\sqrt{2} = \langle 1; \overline{2} \rangle$. The following two results are useful for determining the continued fraction for **quadratic irrational numbers**, i.e. numbers of the form $\sqrt{D}$ where D is square free.

Theorem 11. *Any periodic simple continued fraction is a quadratic irrational number, and conversely.*

The reader may refer to [5, p. 345-348] for the proof.

Theorem 12. *If the positive integer D is not a perfect square, the simple continued fraction expansion of $\sqrt{D}$ has the form*

$$\sqrt{D} = \langle a_0; \overline{a_1, a_2, \cdots, a_{r-1}, 2a_0} \rangle$$

with $a_0 = \left\lfloor \sqrt{D} \right\rfloor$. Here r denotes the length of the shortest period in the expansion of $\sqrt{D}$.

The reader may refer to [5, p. 349,350] for the proof.

1.4 Solution of Pell's Equation

We now apply the previous section's results to solving Pell's equation.

Theorem 13. *If D is a positive integer and not a perfect square, then $p_n^2 - Dq_n^2 = (-1)^{n-1}k_{n+1}$ for all integers $n \geq -1$ where $k_{i+1} = \frac{D - m_{i+1}^2}{k_i}$ with $m_{i+1} = a_i k_i - m_i$.*

The proof may be found in [5, p. 352].

Theorem 14. *Let D be a positive integer, not a perfect square, and let the convergents to the continued fraction expansion of $\sqrt{D}$ be $\frac{p_n}{q_n}$. Let the integer N satisfy $|N| < \sqrt{D}$. Then any positive solution $x = s$, $y = t$ of $x^2 - Dy^2 = N$ with $\gcd(s,t) = 1$ satisfies $s = p_n$, $t = q_n$ for some positive integer n.*

Proof. Let X and Y be positive integers such that $\gcd(X,Y) = 1$ and $X^2 - \Delta Y^2 = \eta$, where $\sqrt{\Delta}$ is irrational and $0 < \eta < \sqrt{\Delta}$. Note that in this case $\Delta, \eta \in \mathbb{R}$. Then

$$\begin{aligned} \frac{X}{Y} - \sqrt{\Delta} &= \frac{X - \sqrt{\Delta}Y}{Y}\left(\frac{X + \sqrt{\Delta}Y}{X + \sqrt{\Delta}Y}\right) \\ &= \frac{X^2 - \Delta Y^2}{Y(X + \sqrt{\Delta}Y)} \\ &= \frac{\eta}{Y(X + \sqrt{\Delta}Y)} \end{aligned}$$

Note that since $\eta < \sqrt{\Delta}$ then

$$\frac{\eta}{Y(X+\sqrt{\Delta}Y)} < \frac{\sqrt{\Delta}}{Y(X+\sqrt{\Delta}Y)}$$

and hence

$$0 < \frac{X}{Y} - \sqrt{\Delta} < \frac{\sqrt{\Delta}}{Y(X+\sqrt{\Delta}Y)}.$$

Now we have

$$\frac{\sqrt{\Delta}}{Y(X+Y\sqrt{\Delta})} = \frac{1}{Y(\frac{X}{\sqrt{\Delta}}+Y)} = \frac{1}{Y^2(\frac{X}{\sqrt{\Delta}Y}+1)}$$

which with $0 < \frac{X}{Y} - \sqrt{\Delta}$ implies $\frac{X}{\sqrt{\Delta}Y} > 1$. This implies $Y^2\left(\frac{X}{Y\sqrt{\Delta}}+1\right) > 2Y^2$ and hence

$$\frac{1}{Y^2(\frac{X}{\sqrt{\Delta}Y}+1)} < \frac{1}{2Y^2}$$

which further implies

$$\left|\frac{X}{Y} - \sqrt{\Delta}\right| < \frac{1}{2Y^2}.$$

Now applying Theorem 9 this implies $\frac{X}{Y}$ is a convergent to the continued fraction of $\sqrt{\Delta}$. If we assume $N > 0$ then let $\eta = N$, $\Delta = D$, $X = s$, and $Y = t$ we have the result. If we assume the alternate, $N < 0$, then $t^2 - \left(\frac{1}{D}\right)s^2 = -\frac{N}{D}$. Now let $\eta = -\frac{N}{D}$, $\Delta = \frac{1}{D}$, $X = t$, and $Y = s$. This implies $\frac{t}{s}$ is a convergent to $\frac{1}{\sqrt{D}}$ and using Theorem 10 this implies $\frac{s}{t}$ is a convergent to $\sqrt{D}$. ■

Now we have the result necessary to find solutions to Pell's Equation provided by [5].

Theorem 15. *All positive solutions of $x^2 - Dy^2 = \pm 1$ are to be found among $x = p_n$,*

$y = q_n$, where $\frac{p_n}{q_n}$ are the convergents of the expansion of $\sqrt{D}$. If r is the period of the expansion of $\sqrt{D}$ and if r is even then $x^2 - Dy^2 = -1$ has no solution and all positive solutions of $x^2 - Dy^2 = 1$ are given by $x = p_{nr-1}$, $y = q_{nr-1}$ for $n = 1, 2, 3, \ldots$. If r is odd, then $x = p_{nr-1}$, $y = q_{nr-1}$ give all positive solutions of $x^2 - Dy^2 = -1$ for odd n and all positive solutions of $x^2 - Dy^2 = 1$ for even, non-zero n.

Proof. This result follows by applying Theorems 12, 13, and 14. ■

This introduces the idea of what is known as the **fundamental solution**. The fundamental solution of (1.1) is the solution (x_0, y_0), where x_0 is the least positive of all solutions. We now provide a result which uses this solution to find all possible solutions to (1.1) as given by [5].

Theorem 16. *If (x_1, y_1) is the fundamental solution of $x^2 - Dy^2 = 1$, then all positive solutions are given by (x_n, y_n) for $n \geq 1$ where x_n and y_n are defined by $x_n + y_n\sqrt{D} = \left(x_1 + y_1\sqrt{D}\right)^n$.*

Refer to [5, p. 354,355] for a proof.

These results give the reader a method to find solutions for (1.1), not only some but all solutions. If we know that the pair (x_1, y_1) solves (1.1) and if $a_0^2 - Db_0^2 = N$ then the integers (a_n, b_n) are solutions to $x^2 - Dy^2 = N$ where they are defined as $a_n + b_n\sqrt{D} = \left(a_0 + b_0\sqrt{D}\right)\left(x_1 + y_1\sqrt{D}\right)^n$ [5]. Therefore given the fundamental solution to (1.1) and a single solution to (1.2) we can create an infinite family of solutions of that same equation. We provide this idea as a result given by [6] as an exercise.

Theorem 17. *If (x_0, y_0) is a solution to the equation $x^2 - Dy^2 = N$ and if (x_1, y_1) is a solution to $x^2 - Dy^2 = 1$ then $(x_0x_1 + Dy_0y_1, x_0y_1 + y_0x_1)$ is another solution to $x^2 - Dy^2 = N$.*

Proof. Consider

$$\begin{aligned} N &= (x_0^2 - Dy_0^2)(x_1^2 - Dy_1^2) \\ &= (x_0x_1)^2 + D^2(y_0y_1)^2 - D(x_0y_1)^2 - D(x_1y_0)^2 \\ &= (x_0x_1)^2 + D^2(y_0y_1)^2 + 2Dx_0x_1y_0y_1 - 2Dx_0x_1y_0y_1 - D(x_0y_1)^2 - D(x_1y_0)^2 \\ &= (x_0x_1 + Dy_0y_1)^2 - D(x_0y_1 + x_1y_0)^2 \end{aligned}$$

Hence we have the result. ■

Now let us apply all of this to a specific example.

Example 2. Consider the following equations

$$x^2 - 2y^2 = 1 \tag{1.5}$$
$$x^2 - 2y^2 = 7 \tag{1.6}$$

Then from (1.3) and (1.4) we have $p_0 = 1, q_0 = 1$ and $p_1 = 3, q_1 = 2$. By Theorem 15 we have that (p_1, q_1) is a solution to (1.5). Then by inspection we have that $x = 3$ and $y = 1$ is a solution to (1.6). Then if we compute, as Theorem 16 suggests, we have $\left(2 + 3\sqrt{2}\right)^2 = 17 + 12\sqrt{2}$. A quick check shows that the pair $x = 17, y = 12$ solves (1.5). Now applying Theorem 17 we have

$$(3(17) + 2(1)(12))^2 - 2(17(1) + 12(3))^2 = 75^2 - 2(53)^2 = 7$$

thus $(75, 53)$ is another solution to (1.6).

Chapter 2

Representation of Integers

As some of the material required for the algorithm relies on quadratric reciprocity, we provide a short introduction into the subject. We also provide theorems that are used in later proofs.

2.1 Quadratic Reciprocity

Consider the following equation, $x^2 = N$ for some $N \in \mathbb{N}$. This is a straight forward equation to solve especially if we allow x to be a real solution. If we restrict the solution to the ring of integers then we decrease the solvability of the equation to N being a perfect square. We can further increase the difficulty by considering the congruence $x^2 \equiv N \pmod{P}$ where $P \in \mathbb{N}$ and $P > 1$. Which, depending on the value of N and P, can be difficult to solve. This provides the definition of a **quadratic residue**. For all N such that the $\gcd(P, N) = 1$, N is a quadratic residue modulo P if $x^2 \equiv N \pmod{P}$ has a solution [5]. Otherwise it is known as a **quadratic nonresidue** modulo P.

To ease the notation for quadratic residues, the **Legendre symbol** was created. Let p be an odd prime, then Legendre's symbol is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo } p \\ 0, & \text{if } p \mid a \\ -1, & \text{otherwise} \end{cases}$$

We will provide a theorem from [5] which provides a method to find primes which have 2 as a quadratic residue.

Theorem 18. *If p is an odd prime and $\gcd(a, 2p) = 1$, then*

$$\left(\frac{a}{p}\right) = (-1)^t \quad \textit{where} \quad t = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor; \quad \textit{also} \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

The reader may refer to [5, p. 134] for a proof.

The next theorem is one of the most useful theorems in the field of quadratic reciprocity which was introduced by Gauss.

Theorem 19. *(Gaussian Reciprocity Law) If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\{(p-1)/2\}\{(q-1)/2\}}.$$

The reader may look to [5, p. 138] for the proof.

It is natural now to question if these theorems and the Legendre symbol hold for composite numbers? Well this is where the **Jacobi symbol** comes to our aid. The Jacobi symbol is defined as

$$\left(\frac{P}{Q}\right) = \prod_{i=1}^{s} \left(\frac{P}{q_i}\right)$$

where $\left(\frac{P}{q_i}\right)$ is the Legendre symbol and Q is positive and odd, such that $Q = \prod_{i=1}^{s} q_i$, where each q_i are odd primes. Note, that if $x^2 \equiv Q \pmod{P}$ is soluble then $\left(\frac{P}{Q}\right) = 1$; however the converse is not necessarily true. This may seem counter-intuitive but the definition was created with the Gaussian Reciprocity Law in mind which will become evident.

The next theorem is helpful in the reduction of calculations for the Jacobi symbol.

Theorem 20. *Suppose that Q is odd and positive. Then*

$$\left(\frac{P}{Q}\right)\left(\frac{P'}{Q}\right) = \left(\frac{PP'}{Q}\right)$$

The proof may be found in [5, p. 144].

The following theorem is the Jacobi equivalent to the previous Legendre theorem.

Theorem 21. *If $Q > 0$ and odd, then*

$$\left(\frac{-1}{Q}\right) = (-1)^{(Q-1)/2} \quad \textit{and} \quad \left(\frac{2}{Q}\right) = (-1)^{(Q^2-1)/8}.$$

The reader may refer to [5, p. 144] for the proof.

The final theorem we cite, is the Reciprocity Law in relation to the Jacobi symbol.

Theorem 22. *If P and Q are odd and positive, and* $\gcd(P, Q) = 1$*, then*

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\{(P-1)/2\}\{(Q-1)/2\}}.$$

The proof may be found in [5, p. 145].

2.2 Euclidean Algorithm and Thue's Theorem

Euclid's algorithm is an important theorem that is taught to many students and has varied uses. The primary use is to find the greatest common divisor between two integers. If the algorithm is reversed it can be used to find the integers guaranteed by Bézout's identity, although for this use it is normally referred to as the Extended Euclidean Algorithm. This algorithm can be represented as a series of recurrence relations which we will state following the first necessary algorithm.

Theorem 23. *(Division Algorithm) Let $a, b \in \mathbb{Z}$ where $b > 0$. Then there exists unique integers q and r such that $a = bq + r$ where $0 \leq r < b$.*

A proof of this can be found in any Discrete or Number Theory text including [5, p. 5,6].

The following are the recurrence relations needed as described above, also known as the Extended Euclidean algorithm.

Theorem 24. *(Euclidean Algorithm) Let $a, b \in \mathbb{N}$, with $a > b$ and $b \nmid a$. Define the recurrence relations*

$$r_{k+1} = r_{k-1} - r_k q_k, \tag{2.1}$$
$$t_{k+1} = t_{k-1} - t_k q_k, \tag{2.2}$$
$$s_{k+1} = s_{k-1} - s_k q_k, \tag{2.3}$$

for $1 \leq k \leq n$ with initial conditions $r_0 = a$, $r_1 = b$, $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$, and where $0 < r_{k+1} < r_k$ with $r_n = 1$. Then we have the following results:

$$s_k = (-1)^k |s_k|, \tag{2.4}$$
$$t_k = (-1)^{k+1} |t_k|, \tag{2.5}$$
$$|s_3| < |s_4| < \cdots < |s_{n+1}|, \tag{2.6}$$
$$|t_2| < |t_3| < \cdots < |t_{n+1}|, \tag{2.7}$$
$$a = |t_k| r_{k-1} + |t_{k-1}| r_k \quad \text{for } 1 \leq k \leq n+1, \text{ and} \tag{2.8}$$
$$r_k = s_k a + t_k b \quad \text{for } 1 \leq k \leq n+1. \tag{2.9}$$

All of the results given above can be easily proven using induction. We now present an extremely useful theorem proven by Axel Thue that provides a bound for solving a congruence based upon certain conditions.

Theorem 25. *(Thue) Let $a, b \in \mathbb{Z}$ such that $1 < b < a$ and $\gcd(a, b) = 1$. Then the congruence $bx \equiv y \pmod{a}$ has a solution in nonzero integers x and y satisfying $|x| \leq \sqrt{a}$ and $|y| \leq \sqrt{a}$.*

Proof. Let $s = \lfloor \sqrt{a} \rfloor$. Thus $\sqrt{a} < s + 1$ which implies $a < (s+1)^2$. Now consider the integers $bx - y$ where $x \in [0, s]$ and $y \in [0, s]$. Since there are $(s+1)^2$ unique integer pairs (x, y) there will be $(s+1)^2$ integers created by these pairs of the form $bx - y$. Now if we use the integers of the form $bx - y$ as pigeons and the remainders modulo a as our pigeonholes, by the pigeonhole principle there must exist two pairs of integers that correspond to the same remainder class modulo a. Assume the two integer pairs are (x_1, y_1) and (x_2, y_2). Thus $bx_1 - y_1 \equiv bx_2 - y_2 \pmod{a}$. Rewriting we have $b(x_1 - x_2) \equiv (y_1 - y_2) \pmod{a}$. Note

these integer pairs are unique and therefore both $x_1 - x_2 = 0$ and $y_1 - y_2 = 0$ cannot hold at once. If $x_1 = x_2$ and $y_1 \neq y_2$ then $a \,|\, y_1 - y_2$. Without loss of generality assume $y_1 > y_2$, then $y_1 = am + y_2$ for some nonzero positive integer m. Which yields the contradiction $y_1 > a$. Similarly if $y_1 = y_2$ and $x_1 \neq x_2$ then $a \mid b(x_1 - x_2)$. Without loss of generality assume $x_1 > x_2$, then $\gcd(a, b) = 1$ implies $a \mid x_1 - x_2$. Thus $x_1 = an + x_2$ for some nonzero positive integer n. Again, leading to the contradiction that $x_1 > a$. Therefore $x_1 - x_2$ and $y_1 - y_2$ are nonzero integers. Note that the smallest separation of integers is a distance of 1 and the largest separation of integers is a distance of s. Therefore we have $1 \leq |x_1 - x_2| \leq s$ and $1 \leq |y_1 - y_2| \leq s$. We choose $x = x_1 - x_2$ and $y = y_1 - y_2$ and have our result. ■

2.3 Representation of Integers in the Form $x^2 - Dy^2$

We now focus on finding representations of integers in the form

$$x^2 - Dy^2 = \kappa N \tag{2.10}$$

where κ is "small", $D > 1$ and square-free, and $N > 1$ and odd. We shall disregard the case when $N = 1$ as this problem reduces to Pell's equation which has been completely solved in the first chapter. Therefore our goal is, given a square-free integer $D > 1$, for which values of N is it possible to find a representation in the form $x^2 - Dy^2$. If there is such a representation, how can we find those values x and y to have this form satisfying the condition $\gcd(x, y) = 1$? Once we find a single representation x and y, are there more integers that create this representation? If so, how can we find these solutions? Given the representation for N, can we find representations for all multiples of N, i.e. κN? As we progress through this chapter we shall see that representations for certain integers indeed exist and we can find those representations based upon the ideas developed by Hermite, Brillhart, Wilker and Matthews.

If we view (2.10) under modulo N we see $x^2 \equiv Dy^2 \pmod{N}$ and since $\gcd(y, N) = 1$, y^{-1} exists modulo N. Thus $(xy^{-1})^2 \equiv D \pmod{N}$ which we shall assume is soluble from here on. This provides us with a value, say u, for which D is a quadratic residue modulo N, i.e. $u^2 \equiv D \pmod{N}$. Therefore we have $\left(\frac{D}{N}\right) = 1$ by definition, which will become

useful when we begin to delineate different cases.

From the above, we have $u \equiv xy^{-1} \pmod{N}$ which implies $yu \equiv x \pmod{N}$. Applying Thue's theorem, we know this congruence has a solution for non-zero x and y such that $|x| \leq \sqrt{N}$ and $|y| \leq \sqrt{N}$. Therefore we know there exist integers m and j such that $uy - x = Nm$ and $u^2 - D = Nj$. Solving the first equation for u and substituting we have

$$\begin{aligned} \left(\frac{Nm + x}{y}\right)^2 - D &= Nj \\ N^2m^2 + 2Nmx + x^2 - Dy^2 &= Njy^2 \\ x^2 - Dy^2 &= N(jy^2 - Nm^2 + 2mx) \end{aligned}$$

We can thus conclude $N \,|\, x^2 - Dy^2$. Based upon the bounds provided by Thue's theorem, we know $x^2 \leq N$ and $y^2 \leq N$ so $x^2 - Dy^2 \leq N$. We also have $-Dy^2 \geq -DN$ and therefore $x^2 - Dy^2 \geq -DN$. Hence the integers given, x and y, will provide a solution to an equation within

$$-DN \leq x^2 - Dy^2 \leq N \tag{2.11}$$

Thue's theorem guarantees the existence of such integers within the given bound; however it does not yield a method to find those integers.

Suppose we apply the Euclidean algorithm where $a = N$ and $b = u$, using the three recurrence relations as well as the properties listed in the statement of the theorem. In particular, (2.9) states $r_k = Ns_k + ut_k$ for $1 \leq k \leq n + 1$. Taking this equation modulo N will yield the congruence $r_k \equiv ut_k \pmod{N}$ which is similar to the congruence given above in terms of x and y. To guarantee a solution to this congruence consider the following: first, by definition the remainders r_k are a monotonically decreasing sequence to 0. Therefore there must exist a largest index $1 \leq \lambda \leq n$ such that $r_\lambda \leq \sqrt{N}$ and therefore $r_\lambda \leq \sqrt{N} < r_{\lambda-1}$. Then (2.8) provides us with $N = |t_\lambda|\, r_{\lambda-1} + |t_{\lambda-1}|\, r_\lambda$ for the largest index λ.

Claim 1. *$|t_\lambda| < \sqrt{N}$ for all $\lambda \geq 1$.*

Proof. Suppose $\lambda = 1$, then $t_{\lambda-1} = 0$. But $|t_\lambda| = 1 < \sqrt{N}$ since $N > 1$. If $\lambda \geq 2$, then $|t_{\lambda-1}| \geq 1$ but $r_\lambda \neq 0$ since $1 \leq \lambda \leq n$. Therefore $N > |t_\lambda|\, r_{\lambda-1}$ and thus $|t_\lambda| < \sqrt{N}$. ■

Therefore we have our solution to the congruence guaranteed by Thue's theorem, using the values for $x = r_\lambda$ and $y = t_\lambda$. We will now show these values indeed provide a representation of the form $x^2 - Dy^2$.

Lemma 1. *Let $a = N$ and $b = u$ in the Euclidean algorithm. Then $r_k^2 - Dt_k^2$ is monotonically decreasing for $0 \leq k \leq n$ from N^2 to $1 - Dt_n^2$ and are always multiples of N.*

Proof. If $k = 0$ then $r_0^2 - Dt_0^2 = N^2$. If $k = n$ then $r_n^2 - Dt_n^2 = 1 - Dt_n^2$. From the Euclidean algorithm $r_0 > r_1$, and thus $N > u$. Thus $N^2 > u^2 - D$. Therefore

$$N^2 = r_0^2 - Dt_0^2 > r_1^2 - Dt_1^2 = u^2 - D$$

Also $r_1 > r_2$ by the Euclidean algorithm and thus $u > N - uq_1$ which yields $u^2 > (N - uq_1)^2$. We now have two possibilities, if $q_1 \neq 0$ then $-D \geq Dq_1^2$. Thus $u^2 - D > (N - uq_1)^2 - Dq_1^2$ which yields $r_1^2 - Dt_1^2 > r_2^2 - Dt_2^2$. If $q_1 = 0$ then $r_2 = r_0 - r_1 q_1$ which yields $r_2 + r_1 q_1 = r_0$ which is a contradiction as $r_2 < r_0$ thus $q_1 \neq 0$. Therefore we have $N^2 = r_0^2 - Dt_0^2 > r_1^2 - Dt_1^2 > r_2^2 - Dt_2^2$. For the remaining cases, $t_k^2 < t_{k+1}^2$ by (2.7) which implies $-Dt_k^2 > -Dt_{k+1}^2$. By the Euclidean algorithm, $r_k > r_{k+1}$ which implies $r_k^2 > r_{k+1}^2$. Thus $r_k^2 - Dt_k^2 > r_{k+1}^2 - Dt_{k+1}^2$. Hence we have the first result. Now consider

$$\begin{aligned} r_k^2 - Dt_k^2 &\equiv (s_k N + t_k u)^2 - Dt_k^2 \pmod{N} \\ &\equiv (s_k N)^2 + (t_k u)^2 + 2N s_k t_k u - Dt_k^2 \pmod{N} \\ &\equiv t_k^2(u^2 - D) \equiv 0 \pmod{N} \quad \because u^2 \equiv D \pmod{N} \end{aligned}$$

■

This lemma is stating regardless of which values we choose for r_k and t_k we will always find a representation in the form $x^2 - Dy^2$ for some multiple of N. In fact, our specific choice r_λ and t_λ will also provide a representation for some multiple of N.

We now proceed in determining a bound for which multiple of N will our values r_λ and t_λ yield our desired representation.

Claim 2. $r_\lambda^2 - Dt_\lambda^2 = -\ell N$ *where* $1 \leq \ell < D$

Proof. By Claim 1 we have $t_\lambda^2 < N$. This implies $-Dt_\lambda^2 > -DN$ and hence $r_\lambda^2 - Dt_\lambda^2 > -DN$. We also have $r_\lambda \leq \sqrt{N}$ which implies $r_\lambda^2 \leq N$ so $r_\lambda^2 - Dt_\lambda^2 < N$. Therefore we have $-DN < r_\lambda^2 - Dt_\lambda^2 < N$. Thus $r_\lambda^2 - Dt_\lambda^2 = -\ell N$ where $-1 < \ell < D$. If $\ell = 0$, then $D = \left(\frac{r_\lambda}{t_\lambda}\right)^2$ which contradicts the assumption that D is square-free. Consequently $r_\lambda^2 - Dt_\lambda^2 = -\ell N$ where $1 \leq \ell < D$. ■

We now know that our representation will be within the bounds of $-DN$ to $-N$ using our index of λ. However Lemma 1 stated that every index for r_k and t_k will yield a multiple of N, including the index $\lambda - 1$. Provided we can find bounds on the value for $r_{\lambda-1}$ we can find bounds for which multiple of N the values $r_{\lambda-1}$ and $t_{\lambda-1}$ will yield a representation.

Lemma 2. $|t_\lambda| > \sqrt{\frac{\ell N}{D}}$

Proof. Rewriting (2) we have $r_\lambda^2 + \ell N = Dt_\lambda^2$ which implies $Dt_\lambda^2 > \ell N$ and hence we have $|t_\lambda| > \sqrt{\frac{\ell N}{D}}$. ■

Lemma 3. $r_{\lambda-1} < \sqrt{\frac{DN}{\ell}}$

Proof. By the use of (2.8), we have $N = |t_\lambda|\, r_{\lambda-1} + |t_{\lambda-1}|\, r_\lambda > |t_\lambda|\, r_{\lambda-1}$. Applying Lemma 2 we have $N > r_{\lambda-1}\sqrt{\frac{\ell N}{D}}$ and simplifying $r_{\lambda-1} < \sqrt{\frac{DN}{\ell}}$. ■

Applying Lemmas 1 and 3 we have the following bound on the representation using the values of $\lambda - 1$.

$$r_\lambda^2 - Dt_\lambda^2 < r_{\lambda-1}^2 - Dt_{\lambda-1}^2 < \frac{DN}{\ell} \tag{2.12}$$

We continue by providing results that will allow us to delineate between which representations we have found using our values provided using λ and $\lambda - 1$.

Lemma 4. $(r_k r_{k-1} - Dt_k t_{k-1})^2 - D(t_{k-1} r_k - t_k r_{k-1})^2 = (r_k^2 - Dt_k^2)(r_{k-1}^2 - Dt_{k-1}^2)$

Proof. Consider

$$\begin{aligned}(r_k r_{k-1} - Dt_k t_{k-1})^2 - D(t_{k-1}r_k - t_k r_{k-1})^2 \\ &= (r_k r_{k-1})^2 + (Dt_k t_{k-1})^2 - D((t_{k-1}r_k)^2 - (t_k r_{k-1})^2) \\ &= r_k^2(r_{k-1}^2 - Dt_{k-1}^2) - Dt_k^2(r_{k-1}^2 - Dt_{k-1}^2) \\ &= (r_k^2 - Dt_k^2)(r_{k-1}^2 - Dt_{k-1}^2)\end{aligned}$$

■

We also have the following identity.

Lemma 5. $r_k t_{k-1} - r_{k-1}t_k = (-1)^k N$

Proof. From (2.8) we have $N = |t_k|\, r_{k-1} + |t_{k-1}|\, r_k$ and using (2.5) we can break this into two cases. If k is even then

$$N = (-1)^{k+1} t_k r_{k-1} + (-1)^k t_{k-1} r_k = t_{k-1}r_k - t_k r_{k-1} = (-1)^k N.$$

If k is odd then $N = -t_{k-1}r_k + t_k r_{k-1}$ and hence $-N = t_{k-1}r_k - t_k r_{k-1} = (-1)^k N$. Therefore the result holds for all k. ■

Now combining Lemmas 4 and 5 we have the following result.

Lemma 6. $r_k r_{k-1} - Dt_k t_{k-1} = \pm\omega N \quad$ *where* $1 \leq \omega \leq D$

Proof. Using the results from Lemma 4, Lemma 5, and (2) we have

$$(r_k r_{k-1} - Dt_k t_{k-1})^2 - DN^2 = \ell_k \ell_{k-1} N^2 \quad \text{where } 1 \leq \ell_k \ell_{k-1} < D^2.$$

Which further implies

$$r_k r_{k-1} - Dt_k t_{k-1} = \pm N\sqrt{\ell_k \ell_{k-1} + D}.$$

Note that the left side of the equation is an integer which implies the right side of the equation must also be an integer. Thus let $\omega \in \mathbb{N}$ such that $\omega^2 = \ell_k \ell_{k-1} + D$. Then we

have $1 \leq \sqrt{1+D} \leq \omega < \sqrt{D^2+D} < \sqrt{2}D$. Finally $r_k r_{k-1} - Dt_k t_{k-1} = \pm\omega N$ where $1 \leq \omega \leq D$. ■

Using (2.5), $t_k t_{k-1} < 0$ and hence

$$r_k r_{k-1} + DT_k T_{k-1} = \omega N \quad \text{where } 1 \leq \omega \leq D \tag{2.13}$$

where $T_k = |t_k|$ and $T_{k-1} = |t_{k-1}|$. Note, the left side of the equation is positive which implies the right side must also be positive. Since $N > 1$ we remove the $\pm$ requirement.

2.3.1 Representations in the Form $x^2 - 2y^2$

For the solubility of the equation, we assume $u^2 \equiv D \pmod{N}$ is soluble which implies $\left(\frac{2}{N}\right) = 1$. Thus by Theorem 21, which is applicable since $N > 1$ and odd by our assumption, we have $\left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}$. Since we need this to be one, we have the following:

$$\begin{aligned} \frac{N^2-1}{8} \equiv 0 \pmod 2 &\Rightarrow N^2 - 1 \equiv 0 \pmod{16} \\ &\Rightarrow N^2 \equiv 1 \pmod{16} \\ &\Rightarrow N \equiv \pm 1 \pmod{16} \\ &\Rightarrow N \equiv \pm 1 \pmod 8 \end{aligned}$$

Thus for the equation to be soluble we require $N \equiv \pm 1 \pmod 8$.

Now by (2) we have $r_k^2 - 2t_k^2 = -N$. Then by Lemma 3 we have $r_{k-1} < \sqrt{2N}$ which implies $r_{k-1}^2 < 2N$ and hence

$$-N = r_k^2 - 2t_k^2 < r_{k-1}^2 - 2t_{k-1}^2 < r_{k-1}^2 < 2N$$

therefore $r_{k-1}^2 - 2t_{k-1}^2 = N$.

Example 3. Consider $N = 401$. Then $u^2 \equiv 2 \pmod{401}$ yields $u \equiv \pm 53 \pmod{401}$. Applying the Euclidean algorithm we find the remainder where $r_\lambda \leq 20$ and have $\lambda = 4$. Therefore we have $r_\lambda = 7$ and $t_\lambda = -15$ yielding the representation $7^2 - 2(-15)^2 = -401$. Also $r_{\lambda-1} = 23$ and $t_{\lambda-1} = 8$ yielding the representation $23^2 - 2(8)^2 = 401$.

We will forgo the case of $D = 3$ as given in Matthews [4] and continue on to the $D = 5$ case as it provides more insight into the different representations and how to delineate between the different values.

2.3.2 Representations in the Form $x^2 - 5y^2$

Assuming $\left(\frac{5}{N}\right) = 1$, by Theorem 22 we have $\left(\frac{5}{N}\right) = \left(\frac{N}{5}\right)(-1)^{((N-1)/2)((5-1)/2)} = \left(\frac{N}{5}\right)$. This theorem applies since we assume $\gcd(D, N) = 1$ which implies $\gcd(5, N) = 1$. Since $x \equiv \pm 1 \pmod 5$ are the only quadratic residues modulo 5 this implies that $\left(\frac{N}{5}\right) = 1$ if and only if $N \equiv \pm 1 \pmod 5$. From Claim 2 we have $r_\lambda^2 - 5t_\lambda^2 = -N, -2N, -3N, -4N$. We can rule out the cases for $-3N$ and $-2N$ as follows. Assume $r_\lambda^2 - 5t_\lambda^2 = -3N$. Taking this modulo 5 we have $r_\lambda^2 \equiv \mp 3 \pmod 5$ but 2 and 3 are not quadratic residues modulo 5 hence this equation is not soluble. Now assume $r_\lambda^2 - 5t_\lambda^2 = -2N$. Then, again taking modulo 5, we have $r_\lambda^2 \equiv \mp 2 \pmod 5$ and we have the same contradiction. Thus the only possibilities are $r_\lambda^2 - 5t_\lambda^2 = -N$ or $r_\lambda^2 - 5t_\lambda^2 = -4N$ which we will now break up into cases.

Representations of $-N$

Let us take this equation modulo 5 and we have $r_\lambda^2 \equiv \mp 1 \pmod 5$ since $N \equiv \pm 1 \pmod 5$. Which implies either $r_\lambda \equiv \pm 1 \pmod 5$ or $r_\lambda \equiv \pm 2 \pmod 5$ when $N \equiv \mp 1 \pmod 5$ respectively. If we take the equation modulo 2 then we have $r_\lambda^2 - 5t_\lambda^2 \equiv -N \pmod 2$. Since N is odd we have $r_\lambda^2 - t_\lambda^2 \equiv 1 \pmod 2$ which implies $r_\lambda \equiv t_\lambda + 1 \pmod 2$. Using Lemma 3 we have $r_{\lambda-1}^2 < 5N$ and hence

$$-N = r_\lambda^2 - 5t_\lambda^2 < r_{\lambda-1}^2 - 5t_{\lambda-1}^2 < r_{\lambda-1}^2 < 5N$$

which implies $r_{\lambda-1}^2 - 5t_{\lambda-1}^2 = N, 2N, 3N, 4N$. We can again rule out the possibilities of $2N$ and $3N$ using the same argument as for $r_\lambda^2 - 5t_\lambda^2$ above by taking the equation modulo 5. Therefore $r_{\lambda-1}^2 - 5t_{\lambda-1}^2 = N$ or $r_{\lambda-1}^2 - 5t_{\lambda-1}^2 = 4N$ which again we will divide into cases.
Case I: $r_{\lambda-1}^2 - 5t_{\lambda-1}^2 = N$
Applying the same procedure used to find Lemma 6 we use Lemma 4 and find $(r_\lambda r_{\lambda-1} - 5t_\lambda t_{\lambda-1})^2 = -N^2 + 5N^2 = 4N^2$. Thus $r_\lambda r_{\lambda-1} + 5T_\lambda T_{\lambda-1} = 2N$. Henceforth we shall disregard this computation and simply refer to the application of Lemma 6. Thus using

(2.8) we also have $T_\lambda r_{\lambda-1} + r_\lambda T_{\lambda-1} = N$. Now solving these equations for $r_{\lambda-1}$ and $T_{\lambda-1}$ we have

$$r_{\lambda-1} = -2r_\lambda + 5T_\lambda \quad \text{and} \quad T_{\lambda-1} = -r_\lambda + 2T_\lambda.$$

and from these we have $r_{\lambda-1} \equiv -2r_\lambda \pmod 5$.
Case II: $r_{\lambda-1}^2 - 5t_{\lambda-1}^2 = 4N$
Using Lemma 6 we have $r_\lambda r_{\lambda-1} + 5T_\lambda T_{\lambda-1} = N$ and (2.8) we solve for $r_{\lambda-1}$ and $T_{\lambda-1}$ and have

$$r_{\lambda-1} = -r_\lambda + 5T_\lambda \quad \text{and} \quad T_{\lambda-1} = -r_\lambda + T_\lambda.$$

Thus we conclude $r_{\lambda-1} \equiv -r_\lambda \pmod 5$.

Representations of $-4N$

We begin by taking this equation modulo 5 and we have $r_\lambda^2 \equiv \mp 4 \pmod 5$. Therefore if $N \equiv -1 \pmod 5$ we have $r_\lambda \equiv \pm 2 \pmod 5$ and if $N \equiv 1 \pmod 5$ then $r_\lambda \equiv \pm 1 \pmod 5$. If we take the equation modulo 2 then we have $r_\lambda^2 - 5t_\lambda^2 \equiv -4N \pmod 2$. Thus $r_\lambda^2 - t_\lambda^2 \equiv 0 \pmod 2$ which implies $r_\lambda \equiv t_\lambda \pmod 2$. If both r_λ and t_λ are even it provides a solution provided $r_\lambda/2$ and $t_\lambda/2$ provide a representation for $-N$. Thus we can conclude r_λ and t_λ are both odd. From Lemma 3 we have $r_{\lambda-1}^2 < \frac{5N}{4}$ and thus

$$-4N = r_\lambda^2 - 5t_\lambda^2 < r_{\lambda-1}^2 - 5t_{\lambda-1}^2 < r_{\lambda-1}^2 < \frac{5N}{4}$$

which implies $r_{\lambda-1}^2 - 5t_{\lambda-1}^2 = -3N, -2N, -N, N$. The cases for $-3N$ and $-2N$ can be ruled out immediately as before and hence we only have the following two cases.
Case I: $r_{\lambda-1}^2 - 5t_{\lambda-1}^2 = -N$
From Lemma 6 we have $r_\lambda r_{\lambda-1} + 5T_\lambda T_{\lambda-1} = 3N$ and using (2.8) we solve for $r_{\lambda-1}$ and $T_{\lambda-1}$ and have

$$4r_{\lambda-1} = -3r_\lambda + 5T_\lambda \quad \text{and} \quad 4T_{\lambda-1} = -r_\lambda + 3T_\lambda.$$

Now taking the second equation modulo 4 we obtain $r_\lambda \equiv 3T_\lambda \pmod 4$.
Case II: $r_{\lambda-1}^2 - 5t_{\lambda-1}^2 = N$
From Lemma 6 we know $r_\lambda r_{\lambda-1} + 5T_\lambda T_{\lambda-1} = N$ and with (2.8) we solve for $r_{\lambda-1}$ and $T_{\lambda-1}$ and find

$$4r_{\lambda-1} = -r_\lambda + 5T_\lambda \quad \text{and} \quad 4T_{\lambda-1} = -r_\lambda + T_\lambda.$$

Performing a modulo 4 operation on the second equation yields $r_\lambda \equiv T_\lambda \pmod 4$. Recapitulating we have the following results.

1. If $N \equiv \pm 1 \pmod 5$ and $r_\lambda \equiv t_\lambda + 1 \pmod 2$ then $r_\lambda^2 - 5t_\lambda^2 = -N$.
   (a) If $r_{\lambda-1} \equiv -2r_\lambda \pmod 5$ then $r_{\lambda-1}^2 - 5t_{\lambda-1}^2 = N$.
   (b) If $r_{\lambda-1} \equiv -r_\lambda \pmod 5$ then $r_{\lambda-1}^2 - 5t_{\lambda-1}^2 = 4N$.
2. If $N \equiv \pm 1 \pmod 5$ and $r_\lambda \equiv t_\lambda \equiv 1 \pmod 2$ then $r_\lambda^2 - 5t_\lambda^2 = -4N$.
   (a) If $r_\lambda \equiv 3T_\lambda \pmod 4$ then $r_{\lambda-1}^2 - 5t_{\lambda-1}^2 = -N$.
   (b) If $r_\lambda \equiv T_\lambda \pmod 4$ then $r_{\lambda-1}^2 - 5t_{\lambda-1}^2 = N$.

The cases for $D = 6$ and $D = 7$ can be found in [4]. The following two chapters extend this to the cases where $D = 10, 11$.

Chapter 3

Representations in the Form $x^2 - 10y^2$

We will now focus on the representations of the form $x^2 - 10y^2$ and find classifications for the possible representations.

3.1 Setting Up

First, by the assumption required for the solubility of the equation we require $\left(\frac{10}{N}\right) = 1$. Using Theorem 20 we have $\left(\frac{2}{N}\right)\left(\frac{5}{N}\right) = \left(\frac{10}{N}\right) = 1$. Therefore either both Jacobi symbols are 1 or both are -1. Previously we have shown the requirements for $\left(\frac{2}{N}\right) = 1$ and $\left(\frac{5}{N}\right) = 1$ such that $N \equiv \pm 1 \pmod 8$ and $N \equiv \pm 1 \pmod 5$ respectively. We will now focus when $\left(\frac{2}{N}\right) = -1$ and $\left(\frac{5}{N}\right) = -1$. By Theorem 21 we have $\left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}} = -1$. This implies $\frac{N^2-1}{8} \equiv 1 \pmod 2$ and thus $N^2 \equiv 9 \pmod{16}$. Thus $N \equiv \pm 3 \pmod{16}$, in fact $N \equiv \pm 3 \pmod 8$. Applying Theorem 22 we have $\left(\frac{5}{N}\right) = \left(\frac{N}{5}\right)(-1)^{2\frac{N-1}{2}} = \left(\frac{N}{5}\right) = -1$. Since N is not a quadratic residue modulo 5 whenever $N \equiv \pm 2 \pmod 5$ this is our requirement.

Applying the Chinese Remainder Theorem we can combine these results as follows:

$$\begin{aligned}
&N \equiv 1 \pmod 8 \text{ and } N \equiv 1 \pmod 5 \longrightarrow N \equiv 1 \pmod{40}\\
&N \equiv 1 \pmod 8 \text{ and } N \equiv 4 \pmod 5 \longrightarrow N \equiv 9 \pmod{40}\\
&N \equiv 7 \pmod 8 \text{ and } N \equiv 1 \pmod 5 \longrightarrow N \equiv -9 \pmod{40}\\
&N \equiv 7 \pmod 8 \text{ and } N \equiv 4 \pmod 5 \longrightarrow N \equiv -1 \pmod{40}\\
&N \equiv 3 \pmod 8 \text{ and } N \equiv 2 \pmod 5 \longrightarrow N \equiv -13 \pmod{40}\\
&N \equiv 3 \pmod 8 \text{ and } N \equiv 3 \pmod 5 \longrightarrow N \equiv 3 \pmod{40}\\
&N \equiv 5 \pmod 8 \text{ and } N \equiv 2 \pmod 5 \longrightarrow N \equiv -3 \pmod{40}\\
&N \equiv 5 \pmod 8 \text{ and } N \equiv 3 \pmod 5 \longrightarrow N \equiv 13 \pmod{40}
\end{aligned}$$

By Claim 2 we then have the following possible representations

$$-9N \leq r_\lambda^2 - 10t_\lambda^2 \leq -N.$$

We first eliminate those representations that will yield no solution for $N \equiv \pm 1, \pm 9 \pmod{40}$ and begin with the equation $r_\lambda^2 - 10t_\lambda^2 = -8N$. If $N \equiv 1 \pmod{40}$ then we have $r_\lambda^2 \equiv 2 \pmod 5$ which is impossible since 2 is not a quadratic residue modulo 5. Similarly if $N \equiv 9 \pmod{40}$ or $N \equiv -9 \pmod{40}$ we have the contradictions $r_\lambda^2 \equiv 3 \pmod 5$ or $r_\lambda^2 \equiv 2 \pmod 5$ respectively. The next case is when $r_\lambda^2 - 10t_\lambda^2 = -7N$ and we have the following contradictions

$$\begin{aligned}
N \equiv 1 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 3 \pmod 5\\
N \equiv -1 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 2 \pmod 5\\
N \equiv 9 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 2 \pmod 5\\
N \equiv -9 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 3 \pmod 5
\end{aligned}$$

Consider $r_\lambda^2 - 10t_\lambda^2 = -5N$. Then $r_\lambda \equiv 0 \pmod 5$ and hence $r_\lambda = 5j$ for some $j \in \mathbb{Z}$. Using this we have $5j^2 - 2t_\lambda^2 = -N$ but this implies, assuming $N \equiv 1 \pmod{40}$, the contradiction $t_\lambda^2 \equiv 3 \pmod 5$. If we have $N \equiv -1 \pmod 5$ this implies the contradiction $t_\lambda^2 \equiv 2 \pmod 5$. Similarly if $N \equiv 9 \pmod{40}$ or $N \equiv -9 \pmod{40}$ then we have the

contradictions $t_\lambda^2 \equiv 2 \pmod 5$ or $t_\lambda^2 \equiv -3 \pmod 5$. Continuing on to the representation $r_\lambda^2 - 10t_\lambda^2 = -3N$ we have the following contradictions

$$\begin{aligned} N &\equiv 1 \pmod{40} \longrightarrow r_\lambda^2 \equiv 2 \pmod 5 \\ N &\equiv -1 \pmod{40} \longrightarrow r_\lambda^2 \equiv 3 \pmod 5 \\ N &\equiv 9 \pmod{40} \longrightarrow r_\lambda^2 \equiv 3 \pmod 5 \\ N &\equiv -9 \pmod{40} \longrightarrow r_\lambda^2 \equiv 2 \pmod 5 \end{aligned}$$

Finally we have the equation $r_\lambda^2 - 10t_\lambda^2 = -2N$ and we have the contradictions

$$\begin{aligned} N &\equiv 1 \pmod{40} \longrightarrow r_\lambda^2 \equiv 3 \pmod 5 \\ N &\equiv -1 \pmod{40} \longrightarrow r_\lambda^2 \equiv 2 \pmod 5 \\ N &\equiv 9 \pmod{40} \longrightarrow r_\lambda^2 \equiv 2 \pmod 5 \\ N &\equiv -9 \pmod{40} \longrightarrow r_\lambda^2 \equiv 3 \pmod 5 \end{aligned}$$

Therefore the only possible representations are $r_\lambda^2 - 10t_\lambda^2 = -9N, -6N, -4N, -N$ for $N \equiv \pm 1, \pm 9 \pmod{40}$.

When $N \equiv \pm 3, \pm 13 \pmod{40}$ the possible representations will vary from those with the other possible values for N. If $r_\lambda^2 - 10t_\lambda^2 = -9N$ then the following contradictions are produced

$$\begin{aligned} N &\equiv 3 \pmod{40} \longrightarrow r_\lambda^2 \equiv 3 \pmod 5 \\ N &\equiv 37 \pmod{40} \longrightarrow r_\lambda^2 \equiv 2 \pmod 5 \\ N &\equiv 27 \pmod{40} \longrightarrow r_\lambda^2 \equiv 2 \pmod 5 \\ N &\equiv 13 \pmod{40} \longrightarrow r_\lambda^2 \equiv 3 \pmod 5 \end{aligned}$$

When $r_\lambda^2 - 10t_\lambda^2 = -6N$ the following contradictions are found

$$\begin{aligned} N \equiv 3 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 2 \pmod 5 \\ N \equiv 37 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 3 \pmod 5 \\ N \equiv 27 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 3 \pmod 5 \\ N \equiv 13 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 2 \pmod 5 \end{aligned}$$

The case $r_\lambda^2 - 10t_\lambda^2 = -4N$ is also impossible as

$$\begin{aligned} N \equiv 3 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 3 \pmod 5 \\ N \equiv 37 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 2 \pmod 5 \\ N \equiv 27 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 2 \pmod 5 \\ N \equiv 13 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 3 \pmod 5 \end{aligned}$$

Finally the case $r_\lambda^2 - 10t_\lambda^2 = -N$ is impossible since

$$\begin{aligned} N \equiv 3 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 2 \pmod 5 \\ N \equiv 37 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 3 \pmod 5 \\ N \equiv 27 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 3 \pmod 5 \\ N \equiv 13 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 2 \pmod 5 \end{aligned}$$

Therefore the only possible representations are $r_\lambda^2 - 10t_\lambda^2 = -8N, -7N, -5N, -3N, -2N$ for $N \equiv \pm 3, \pm 13 \pmod{40}$.

3.2 Representations of $-9N$

We begin by classifying the representations based on the varying values for N. Therefore we have the following classifications

$$\begin{aligned} N \equiv 1 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 1 \pmod 5 \longrightarrow r_\lambda \equiv \pm 1 \pmod 5 \\ N \equiv -1 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 4 \pmod 5 \longrightarrow r_\lambda \equiv \pm 2 \pmod 5 \\ N \equiv 9 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 4 \pmod 5 \longrightarrow r_\lambda \equiv \pm 2 \pmod 5 \\ N \equiv -9 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 1 \pmod 5 \longrightarrow r_\lambda \equiv \pm 1 \pmod 5 \end{aligned}$$

Consider

$$\begin{aligned} r_\lambda^2 - 10t_\lambda^2 &\equiv 0 \pmod 9 \\ r_\lambda^2 - t_\lambda^2 &\equiv 0 \pmod 9 \end{aligned}$$

and hence $r_\lambda \equiv \pm t_\lambda \pmod 9$. We now apply Lemma 3 and have $r_{\lambda-1}^2 < \frac{10N}{9}$ and hence

$$-9N = r_\lambda^2 - 10t_\lambda^2 < r_{\lambda-1}^2 - 10t_{\lambda-1}^2 < r_{\lambda-1}^2 < \frac{10N}{9}$$

Thus the only possibilities are $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -6N, -4N, -N, N$.

We now establish a Lemma that will be useful in providing solutions for cases when $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -4N$ and $r_\lambda^2 - 10t_\lambda^2 = -4N$.

Lemma 7. *$x^2 - 10y^2 = \pm 4N$ has a possible representation if and only if $x^2 - 10y^2 = \pm N$ has a representation. Moreover, if x and y are the integers that create a representation for $\pm N$, then $2x$ and $2y$ create the representation for $\pm 4N$.*

Proof. The reverse implication is straightforward by simply using the values $2x$ and $2y$. Assume there exists a representation to $x^2 - 10y^2 = \pm 4N$, say $a, b \in \mathbb{Z}$. Then $a^2 \equiv 0 \pmod 2$ and hence $a \equiv 0 \pmod 2$. This implies $a = 2\hat{a}$ where $\hat{a} \in \mathbb{Z}$. Thus we have $4\hat{a}^2 - 10b^2 = \pm 4N$ and reducing modulo 4 we have $-2b^2 \equiv 0 \pmod 4$. This implies $b \equiv 0 \pmod 2$ and hence $b = 2\hat{b}$ for some $\hat{b} \in \mathbb{Z}$. Hence we have $4\hat{a}^2 - 10(4\hat{b}^2) = \pm 4N$ and

dividing by 4 we have $\hat{a}^2 - 10\hat{b}^2 = \pm N$. Therefore the result holds. ■

From this Lemma we can conclude that the case $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -4N$ is dependent upon the case for $-N$. However from Lemma 6 we have $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = \sqrt{19}N$ for the case $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -N$ which impossible since $\sqrt{19} \notin \mathbb{Z}$. Thus the cases for $-4N$ and $-N$ have no solutions.

Case I: $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -6N$

By Lemma 6 we have $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = 8N$ and using (2.8) we can solve for $r_{\lambda-1}$ and $T_{\lambda-1}$. Therefore we have

$$9r_{\lambda-1} = -8r_\lambda + 10T_\lambda \quad \text{and} \quad 9T_{\lambda-1} = -r_\lambda + 8T_\lambda.$$

Taking the first equation modulo 9 we have the condition $r_\lambda \equiv -T_\lambda \pmod 9$.

Case II: $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = N$

By Lemma 6 we have $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = N$ and using (2.8) we solve for $r_{\lambda-1}$ and $T_{\lambda-1}$. Thus we have

$$9r_{\lambda-1} = -r_\lambda + 10T_\lambda \quad \text{and} \quad 9T_{\lambda-1} = -r_\lambda + T_\lambda.$$

Thus taking the second equation modulo 9 we have the classification $r_\lambda \equiv T_\lambda \pmod 9$. Also note that since there is a representation then by Lemma 7 $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 4N$ also has a representation.

3.3 Representations of $-8N$

A representation for $-8N$ is reliant upon $-2N$ as is evident by the following lemma.

Lemma 8. *$x^2 - 10y^2 = \pm 8N$ has a possible representation if and only if $x^2 - 10y^2 = \pm 2N$ has a representation. Moreover, if x and y are the integers that create a representation for $\pm 2N$, then $2x$ and $2y$ create the representation for $\pm 8N$.*

Proof. The reverse implication is straightforward by simply using the values $2x$ and $2y$. Assume there exists $a, b \in \mathbb{Z}$ such that $a^2 - 11b^2 = \pm 8N$. Now taking the equation modulo 2 we have $a^2 \equiv 0 \pmod 2$ which implies $a \equiv 0 \pmod 2$. Thus there exists $\hat{a} \in \mathbb{Z}$ such

that $a = 2\hat{a}$. Thus $a^2 - 10b^2 = 4\hat{a}^2 - 10b^2 = \pm 8N$ so $-5b^2 \equiv 0 \pmod 2$ so $b \equiv 0 \pmod 2$. Therefore there exists $\hat{b} \in \mathbb{Z}$ such that $b = 2\hat{b}$. Hence $a^2 - 10b^2 = 4\hat{a}^2 - 10(4\hat{b}^2) = -8N$ so $\hat{a}^2 - 10\hat{b}^2 = \pm 2N$. ■

3.4 Representations of $-7N$

A potential representation for $-7N$ is impossible when $N \equiv \pm 3, \pm 13 \pmod{40}$.

Lemma 9. *The representation $x^2 - 10y^2 = -7N$ is impossible.*

Proof. Let $N \equiv \pm 3, \pm 13 \pmod{40}$ and assume $a, b \in \mathbb{Z}$ such that $a^2 - 10b^2 = -7N$. Then $a^2 - 10b^2 \equiv a^2 - 3b^2 \equiv 0 \pmod 7$. Therefore $a^2 \equiv 3b^2 \pmod 7$ and the only possibilities are $a^2 \equiv 1, 2, 4 \pmod 7$. If $a^2 \equiv 2 \pmod 7$ then $3b^2 \equiv 2 \pmod 7$ so $b^2 \equiv 10 \pmod 7$ which is a contradiction. Also if $3b^2 \equiv 4 \pmod 7$ then $b^2 \equiv 6 \pmod 7$ which is impossible. Finally if $3b^2 \equiv 1 \pmod 7$ then $b^2 \equiv 5 \pmod 7$ which is also a contradiction. Therefore such a and b cannot exist. ■

3.5 Representations of $-6N$

We now have the following classification for solutions to this equation as follows:

$$\begin{aligned}
N \equiv 1 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 4 \pmod 5 \longrightarrow r_\lambda \equiv \pm 2 \pmod 5 \\
N \equiv -1 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 1 \pmod 5 \longrightarrow r_\lambda \equiv \pm 1 \pmod 5 \\
N \equiv 9 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 1 \pmod 5 \longrightarrow r_\lambda \equiv \pm 1 \pmod 5 \\
N \equiv -9 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 4 \pmod 5 \longrightarrow r_\lambda \equiv \pm 2 \pmod 5
\end{aligned}$$

If we mod this equation by 6 we have

$$\begin{aligned}
r_\lambda^2 - 10t_\lambda^2 &\equiv 0 \pmod 6 \\
r_\lambda^2 - 4t_\lambda^2 &\equiv 0 \pmod 6 \\
r_\lambda &\equiv \pm 2t_\lambda \pmod 6
\end{aligned}$$

Now applying Lemma 3 we have $r_{\lambda-1}^2 < \frac{5N}{3}$ and hence

$$-6N = r_\lambda^2 - 10t_\lambda^2 < r_{\lambda-1}^2 - 10t_{\lambda-1}^2 < r_{\lambda-1}^2 < \frac{5N}{3}.$$

Therefore the only possible representations are $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -4N, -N, N$ eliminating the others based on the congruences for N. Note the case for $-4N$ is dependent upon the case for $-N$ based upon Lemma 7.

Case I: $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -N$

Now using Lemma 6 we have $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = 4N$ and using (2.8) we solve for $r_{\lambda-1}$ and $T_{\lambda-1}$ and find

$$6r_{\lambda-1} = -4r_\lambda + 10T_\lambda \quad \text{and} \quad 6T_{\lambda-1} = -r_\lambda + 4T_\lambda.$$

Therefore reducing the second equation modulo 3 we have $r_\lambda \equiv T_\lambda \pmod 3$. Therefore taking these solutions and applying Lemma 7 we will have the solutions to $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -4N$.

Case II: $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = N$

From Lemma 6 we have $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = 2N$ and using (2.8) we again solve for $r_{\lambda-1}$ and $T_{\lambda-1}$. We then find the following equations

$$6r_{\lambda-1} = -2r_\lambda + 10T_\lambda \quad \text{and} \quad 6T_{\lambda-1} = -r_\lambda + 2T_\lambda.$$

Which yields the following classification $r_\lambda \equiv -T_\lambda \pmod 3$. In addition we can find solutions to $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 4N$ by applying Lemma 7.

3.6 Representations of $-5N$

This representation is only possible if $N \equiv \pm 3, \pm 13 \pmod{40}$. Applying Lemma 3 we have

$$-5N = r_\lambda^2 - 10t_\lambda^2 < r_{\lambda-1}^2 - 10t_{\lambda-1}^2 < 2N$$

Therefore the only possible representations will be $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -4N, -3N, -2N, -N, N$. We can eliminate the possibilities of $-4N$ and $-N$ based on the same contradictions found above. We can also eliminate the cases for $-2N$ and N using Lemma 6 as $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = \sqrt{20}N$ and $\sqrt{5}N$ respectively.
Case I: $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -3N$

Using Lemma 6, $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = 5N$. Hence $r_{\lambda-1} = 2T_\lambda - r_\lambda$ and $5T_{\lambda-1} = -r_\lambda + 5T_\lambda$ using (2.8) and solving for $r_{\lambda-1}$ and $T_{\lambda-1}$. Finally taking the first equation modulo 2 we have $r_{\lambda-1} \equiv r_\lambda \pmod 2$ and the second equation modulo 5 yields $r_\lambda \equiv 0 \pmod 5$.

3.7 Representations of $-4N$

We refer the reader to the case of $r_\lambda^2 - 10t_\lambda^2 = -N$ based on Lemma 7.

3.8 Representations of $-3N$

The representation for $-3N$ is only possible when $N \equiv \pm 3, \pm 13 \pmod{40}$. If $r_\lambda^2 - 10t_\lambda^2 = -3N$ then $r_\lambda^2 - t_\lambda^2 \equiv 0 \pmod 3$. Therefore $r_\lambda \equiv \pm t_\lambda \pmod 3$. Using Lemma 3 we construct the bound for the $\lambda - 1$ case as

$$-3N = r_\lambda^2 - 10t_\lambda^2 < r_{\lambda-1}^2 - 10t_{\lambda-1}^2 < \frac{10N}{3}$$

We can eliminate the case of $-N$ as it will yield a similar contradiction as above based upon quadratic reciprocity. We can also eliminate the case for N using Lemma 6 as $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = \sqrt{6}N$. Thus the only possibilities are $-N, 2N, 3N$.
Case I: $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -2N$

In this case we have, $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = 4N$ by Lemma 6. Solving (2.8) and the aforementioned equation for $r_{\lambda-1}$ and $T_{\lambda-1}$ yield

$$-3r_{\lambda-1} = 4r_\lambda - 10T_\lambda \quad \text{and} \quad -3T_{\lambda-1} = r_\lambda - 4T_\lambda.$$

The first equation is equivalent to $7r_{\lambda-1} \equiv 4r_\lambda \pmod{10}$ and the second yields $T_\lambda \equiv r_\lambda$

(mod 3).
Case I: $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 2N$

This case yields $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = 2N$ and using (2.8) we solve for $r_{\lambda-1}$ and $T_{\lambda-1}$. Therefore

$$-3r_{\lambda-1} = 2r_\lambda - 10T_\lambda \quad \text{and} \quad -3T_{\lambda-1} = r_\lambda - 2T_\lambda.$$

Which gives us the classifications of $7r_{\lambda-1} \equiv 2r_\lambda \pmod{10}$ and $T_\lambda \equiv 2r_\lambda \pmod 3$.
Case I: $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 3N$

By Lemma 6 we have $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = N$ and using (2.8) we have

$$-3r_{\lambda-1} = r_\lambda - 10T_\lambda \quad \text{and} \quad -3T_{\lambda-1} = r_\lambda - T_\lambda.$$

These two equations yield the classifications $7r_{\lambda-1} \equiv r_\lambda \pmod{10}$ and $r_\lambda \equiv T_\lambda \pmod 3$ respectively.

3.9 Representations of $-2N$

This representation will only be possible provided $N \equiv \pm 3, \pm 13 \pmod{40}$ and therefore $r_\lambda^2 \equiv 0 \pmod 2$ so $r_\lambda \equiv 0 \pmod 2$. Applying Lemma 3 we have

$$-2N = r_\lambda^2 - 10t_\lambda^2 < r_{\lambda-1}^2 - 10t_{\lambda-1}^2 < 5N$$

We can eliminate the case for $-N$ as we did for the λ values. The values for $N, 2N, 4N$ are impossible using Lemma 6 as $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = \sqrt{8}N, \sqrt{6}N, \sqrt{2}N$ respectively.
Case I: $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 3N$

Then $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = 2N$ by Lemma 6 which, along with (2.8), yield

$$-r_{\lambda-1} \equiv r_\lambda - 5T_\lambda \quad \text{and} \quad -2T_{\lambda-1} = r_\lambda - 2T_\lambda.$$

These two equations yield the classifications $-r_{\lambda-1} \equiv r_\lambda \pmod 5$ and $r_\lambda \equiv 0 \pmod 2$.

3.10 Representations of $-N$

We again classify the solution based upon the value of N and thus

$$\begin{aligned}
N \equiv 1 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 4 \pmod 5 \longrightarrow r_\lambda \equiv \pm 2 \pmod 5 \\
N \equiv -1 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 1 \pmod 5 \longrightarrow r_\lambda \equiv \pm 1 \pmod 5 \\
N \equiv 9 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 1 \pmod 5 \longrightarrow r_\lambda \equiv \pm 1 \pmod 5 \\
N \equiv -9 \pmod{40} &\longrightarrow r_\lambda^2 \equiv 4 \pmod 5 \longrightarrow r_\lambda \equiv \pm 2 \pmod 5
\end{aligned}$$

Claim 3. *If* $r_\lambda^2 - 10t_\lambda^2 = -N$ *then* $r_\lambda \equiv \pm t_\lambda \pmod 4$.

Proof. Assume the opposite, that is; assume $r_\lambda \equiv 2t_\lambda \pmod 4$. Therefore $r_\lambda = 4k + 2t_\lambda$ for some $k \in \mathbb{Z}$. Thus

$$\begin{aligned}
r_\lambda^2 - 10t_\lambda^2 &= 16k^2 + 4t_\lambda^2 + 16kt_\lambda - 10t_\lambda^2 \\
&= 16k^2 + 16kt_\lambda - 6t_\lambda^2
\end{aligned}$$

Therefore $r_\lambda^2 - 10t_\lambda^2 \equiv 0 \pmod 2$ which is a contradiction since N is odd. ■

Now applying Lemma 3 we have $r_{\lambda-1}^2 < 10N$ and hence

$$-N = r_\lambda^2 - 10t_\lambda^2 < r_{\lambda-1}^2 - 10t_{\lambda-1}^2 < r_{\lambda-1}^2 < 10N$$

Therefore the only representations will be $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = N, 4N, 6N, 9N$ based on the values of N.

Case I: $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 9N$

Applying Lemma 6 we have $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = N$ and using (2.8) we can solve for $r_{\lambda-1}$ and $T_{\lambda-1}$. Then we have the following two equations

$$r_{\lambda-1} = -r_\lambda + 10T_\lambda \quad \text{and} \quad T_{\lambda-1} = -r_\lambda + T_\lambda.$$

Now taking the first equation modulo 5 we have $-r_\lambda \equiv r_{\lambda-1} \pmod 5$.

Case II: $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 6N$

Now using Lemma 6 we have $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = 2N$ and using (2.8) we solve for $r_{\lambda-1}$ and $T_{\lambda-1}$. This leaves us with the following two equations

$$r_{\lambda-1} = -2r_\lambda + 10T_\lambda \quad \text{and} \quad T_{\lambda-1} = -r_\lambda + 2T_\lambda.$$

Now taking the first equation modulo 2 we have $r_{\lambda-1} \equiv 0 \pmod 2$.

Case III: $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 4N$

We refer the reader to the next equation using Lemma 7.

Case IV: $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = N$

Again using Lemma 6 we have $r_\lambda r_{\lambda-1} + 10T_\lambda T_{\lambda-1} = 3N$ and using (2.8) we solve for $r_{\lambda-1}$ and $T_{\lambda-1}$. Then we have

$$r_{\lambda-1} = -3r_\lambda + 10T_\lambda \quad \text{and} \quad T_{\lambda-1} = -r_\lambda + 3T_\lambda.$$

We now take the first equation modulo 5 and have $-3r_\lambda \equiv r_{\lambda-1} \pmod 5$. Using Lemma 7 we now have a representation for $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 4N$ as well.

3.11 Summary

We will now summarize all classifications found in the previous sections above. If $N \equiv \pm 1, \pm 9 \pmod{40}$ then

1. representations of the form $r_\lambda^2 - 10t_\lambda^2 = -9N$ are classified as $r_\lambda \equiv \pm t_\lambda \pmod 9$.
   (a) $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -6N$ if $r_\lambda \equiv -T_\lambda \pmod 9$.
   (b) $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = N$ if $r_\lambda \equiv T_\lambda \pmod 9$.
   (c) If $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = N$ then $(2r_{\lambda-1})^2 - 10(2t_{\lambda-1})^2 = 4N$.
2. representations of the form $r_\lambda^2 - 10t_\lambda^2 = -6N$ are classified as $r_\lambda \equiv \pm 2t_\lambda \pmod 6$.
   (a) $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -N$ if $r_\lambda \equiv T_\lambda \pmod 3$.
   (b) If $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -N$ then $(2r_{\lambda-1})^2 - 10(2t_{\lambda-1})^2 = -4N$.
   (c) $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = N$ if $r_\lambda \equiv -T_\lambda \pmod 3$.

(d) If $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = N$ then $(2r_{\lambda-1})^2 - 10(2t_{\lambda-1})^2 = 4N$.

3. representations of the form $r_\lambda^2 - 10t_\lambda^2 = -N$ are classified as $r_\lambda \equiv \pm t_\lambda \pmod 4$.

   (a) $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 9N$ if $-r_\lambda \equiv r_{\lambda-1} \pmod 5$.

   (b) $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 6N$ if $r_{\lambda-1} \equiv 0 \pmod 2$.

   (c) $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = N$ if $-3r_\lambda \equiv r_{\lambda-1} \pmod 5$.

   (d) If $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = N$ then $(2r_{\lambda-1})^2 - 10(2t_{\lambda-1})^2 = 4N$.

4. if $r_\lambda^2 - 10t_\lambda^2 = -N$ then $(2r_\lambda)^2 - 10(2t_\lambda)^2 = -4N$.

If $N \equiv \pm 3, \pm 13 \pmod{40}$ then

1. representations of the form $r_\lambda^2 - 10t_\lambda^2 = -5N$ are classified as $r_\lambda \equiv 0 \pmod 5$.

   (a) $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -3N$ if $r_{\lambda-1} \equiv r_\lambda \pmod 2$.

2. representations of the form $r_\lambda^2 - 10t_\lambda^2 = -3N$ are classified as $r_\lambda \equiv \pm t_\lambda \pmod 3$.

   (a) $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = -2N$ if $-3r_{\lambda-1} \equiv 4r_\lambda \pmod{10}$.

   (b) $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 2N$ if $-3r_{\lambda-1} \equiv 2r_\lambda \pmod{10}$.

   (c) $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 3N$ if $-3r_{\lambda-1} \equiv r_\lambda \pmod{10}$.

3. representations of the form $r_\lambda^2 - 10t_\lambda^2 = -2N$ are classified as $r_\lambda \equiv 0 \pmod 2$.

   (a) $r_{\lambda-1}^2 - 10t_{\lambda-1}^2 = 3N$ if $-r_{\lambda-1} \equiv r_\lambda \pmod 5$.

4. if $r_\lambda^2 - 10t_\lambda^2 = -2N$ then $(2r_\lambda)^2 - 10(2t_\lambda)^2 = -8N$.

Example 4. Consider $N = 6172961$ where $N \equiv 1 \pmod{40}$. Then we find solutions to the equation $x^2 - 10y^2 = -6172961$ with $u = 100186$ as $(r_8, t_8) = (493, 801)$. Also $(r_7, t_7) = (7517, -308)$ solves $x^2 - 10y^2 = 9N$. If $u = 2988656$ then we have $(r_9, t_9) = (1483, -915)$ solves $x^2 - 10y^2 = -N$ and $(r_8, t_8) = (6184, 347)$ solves $x^2 - 10y^2 = -6N$. All calculations were completed with use of the Matlab functions in the Appendices.

Chapter 4

Representations in the Form $x^2 - 11y^2$

We will now focus on the representations of the form $x^2 - 11y^2$ and find classifications for the possible representations.

4.1 Setting Up

First we must satisfy the requirement that we can find a value u such that $u^2 \equiv 11 \pmod{N}$ and hence we need $\left(\frac{11}{N}\right) = 1$. Therefore Theorem 22 yields
$\left(\frac{11}{N}\right) = \left(\frac{N}{11}\right)(-1)^{(N-1)/2}$. Thus

$$(-1)^{(N-1)/2} = \begin{cases} 1, & \text{if } N \equiv 1 \pmod{4} \\ -1, & \text{if } N \equiv 3 \pmod{4} \end{cases}$$

as well

$$\left(\frac{N}{11}\right) = \begin{cases} 1, & \text{if } N \equiv 1, 3, 4, 5, 9 \pmod{11} \\ -1, & \text{if } N \equiv -1, -3, -4, -5, -9 \pmod{11} \end{cases}$$

Therefore we have the following two cases:
Case I: If $N \equiv 1 \pmod{4}$ and $N \equiv 1, 3, 4, 5, 9 \pmod{11}$.

Using the Chinese Remainder Theorem we can combine these congruences and find

$$N \equiv 1, 5, 9, 25, 37 \pmod{44}.$$

Case II: If $N \equiv 3 \pmod 4$ and $N \equiv -1, -3, -4, -5, -9 \pmod{11}$.

Applying the Chinese Remainder Theorem we have

$$N \equiv -1, -5, -9, -25, -37 \pmod{44}.$$

Thus combining these cases to satisfy the assumptions for our representation we have

$$N \equiv \pm 1, \pm 5, \pm 9, \pm 25, \pm 37 \pmod{44}. \tag{4.1}$$

Using Claim 2 we have

$$-10N \leq r_\lambda^2 - 11t_\lambda^2 \leq -N$$

and considering each representation separately along with each value given by the congruences in (4.1). We will show the calculation of the first case and simply state the remaining cases as the calculations are similar. We first consider $r_\lambda^2 - 11t_\lambda^2 = -10N$ then we have the following cases:

1. If $N \equiv 1 \pmod{44}$ then $r_\lambda^2 \equiv 1 \pmod{11}$ and hence $r_\lambda \equiv \pm 1 \pmod{11}$.
2. If $N \equiv -1 \pmod{44}$ then $r_\lambda^2 \equiv 10 \pmod{11}$ which forms a contradiction.
3. If $N \equiv 5 \pmod{44}$ then $r_\lambda^2 \equiv 5 \pmod{11}$ and hence $r_\lambda \equiv \pm 4 \pmod{11}$.
4. If $N \equiv -5 \pmod{44}$ then $r_\lambda^2 \equiv 6 \pmod{11}$ which forms a contradiction.
5. If $N \equiv 9 \pmod{44}$ then $r_\lambda^2 \equiv 9 \pmod{11}$ and hence $r_\lambda \equiv \pm 3 \pmod{11}$.
6. If $N \equiv -9 \pmod{44}$ then $r_\lambda^2 \equiv 2 \pmod{11}$ which forms a contradiction.
7. If $N \equiv 25 \pmod{44}$ then $r_\lambda^2 \equiv 3 \pmod{11}$ and hence $r_\lambda \equiv \pm 5 \pmod{11}$.
8. If $N \equiv -25 \pmod{44}$ then $r_\lambda^2 \equiv 8 \pmod{11}$ which forms a contradiction.

9. If $N \equiv 37 \pmod{44}$ then $r_\lambda^2 \equiv 4 \pmod{11}$ and hence $r_\lambda \equiv \pm 2 \pmod{11}$.

10. If $N \equiv -37 \pmod{44}$ then $r_\lambda^2 \equiv 7 \pmod{11}$ which forms a contradiction.

Therefore $r_\lambda^2 - 11t_\lambda^2 = -10N$ is only soluble when $N \equiv 1, 5, 9, 25, 37 \pmod{44}$. Summarizing the remaining results we have:

1. If $r_\lambda^2 - 11t_\lambda^2 = -9N$, and $N \equiv -1, -5, -9, -25, -37 \pmod{44}$ we have $r_\lambda \equiv \pm 3, \pm 1, \pm 2, \pm 4, \pm 5 \pmod{11}$ respectively.

2. If $r_\lambda^2 - 11t_\lambda^2 = -8N$, and $N \equiv 1, 5, 9, 25, 37 \pmod{44}$ we have $r_\lambda \equiv \pm 5, \pm 2, \pm 4, \pm 3, \pm 1 \pmod{11}$ respectively.

3. If $r_\lambda^2 - 11t_\lambda^2 = -7N$, and $N \equiv 1, 5, 9, 25, 37 \pmod{44}$ we have $r_\lambda \equiv \pm 2, \pm 3, \pm 5, \pm 1, \pm 4 \pmod{11}$ respectively.

4. If $r_\lambda^2 - 11t_\lambda^2 = -6N$, and $N \equiv 1, 5, 9, 25, 37 \pmod{44}$ we have $r_\lambda \equiv \pm 4, \pm 5, \pm 1, \pm 2, \pm 3 \pmod{11}$ respectively.

5. If $r_\lambda^2 - 11t_\lambda^2 = -5N$, and $N \equiv -1, -5, -9, -25, -37 \pmod{44}$ we have $r_\lambda \equiv \pm 4, \pm 5, \pm 1, \pm 2, \pm 3 \pmod{11}$ respectively.

6. If $r_\lambda^2 - 11t_\lambda^2 = -4N$, and $N \equiv -1, -5, -9, -25, -37 \pmod{44}$ we have $r_\lambda \equiv \pm 2, \pm 3, \pm 5, \pm 1, \pm 4 \pmod{11}$ respectively.

7. If $r_\lambda^2 - 11t_\lambda^2 = -3N$, and $N \equiv -1, -5, -9, -25, -37 \pmod{44}$ we have $r_\lambda \equiv \pm 5, \pm 2, \pm 4, \pm 3, \pm 1 \pmod{11}$ respectively.

8. If $r_\lambda^2 - 11t_\lambda^2 = -2N$, and $N \equiv 1, 5, 9, 25, 37 \pmod{44}$ we have $r_\lambda \equiv \pm 3, \pm 1, \pm 2, \pm 4, \pm 5 \pmod{11}$ respectively.

9. If $r_\lambda^2 - 11t_\lambda^2 = -N$, and $N \equiv -1, -5, -9, -25, -37 \pmod{44}$ we have $r_\lambda \equiv \pm 1, \pm 4, \pm 3, \pm 5, \pm 2 \pmod{11}$ respectively.

4.2 Representations of $-10N$

By the first section in this chapter we have if $N \equiv 1, 5, 9, 25, 37 \pmod{44}$ then $r_\lambda \equiv \pm 1, \pm 4, \pm 3, \pm 5, \pm 2 \pmod{11}$ respectively. We also have

$$\begin{aligned} r_\lambda^2 - 11t_\lambda^2 &\equiv 0 \pmod{10} \\ r_\lambda^2 - t_\lambda^2 &\equiv 0 \pmod{10} \\ r_\lambda &\equiv \pm t_\lambda \pmod{10} \end{aligned}$$

Using Lemma 3 we have $r_{\lambda-1}^2 < \frac{11N}{10}$. Therefore

$$-10N = r_\lambda^2 - 11t_\lambda^2 < r_{\lambda-1}^2 - 11t_{\lambda-1}^2 < r_{\lambda-1}^2 < \frac{11N}{10}$$

and thus the only possible cases are when

$$r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = -9N, -8N, -7N, -6N, -5N, -4N, -3N, -2N, -N, N.$$

We can eliminate the cases for $-9N, -8N, -5N, -4N, -3N, -N$ immediately based upon the congruences given. Thus we reduce the possible cases to $-7N, -6N, -2N, N$. For the case $-6N$ applying Lemma 6 we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = \sqrt{71}N$ which is impossible. Similarly for the case $-2N$ we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = \sqrt{31}N$ which makes this impossible.

Case I: $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = -7N$

Using Lemma 6 we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = 9N$ and using (2.8) we solve for $r_{\lambda-1}$ and $T_{\lambda-1}$ as

$$10r_{\lambda-1} = -9r_\lambda + 11T_\lambda \quad \text{and} \quad 10T_{\lambda-1} = -r_\lambda + 9T_\lambda.$$

Taking the second equation modulo 10 we have $r_\lambda \equiv 9T_\lambda \pmod{10}$.

Case II: $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = N$

Again using Lemma 6 we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = N$ and by (2.8) we have

$$10r_{\lambda-1} = -r_\lambda + 11T_\lambda \quad \text{and} \quad 10T_{\lambda-1} = -r_\lambda + T_\lambda.$$

Thus taking the second equation modulo 10 we have $r_\lambda \equiv T_\lambda \pmod{10}$.

4.3 Representations of $-9N$

We provide a lemma that will yield solutions to this equation.

Lemma 10. *$x^2 - 11y^2 = \pm 9N$ has a possible representation if and only if $x^2 - 11y^2 = \pm N$ has a representation. Moreover, if x and y are the integers that create a representation for $-N$, then $3x$ and $3y$ create the representation for $\pm 9N$.*

Proof. The reverse implication is straightforward by simply using the values $3x$ and $3y$. Assume there exists a representation in the form $x^2 - 10y^2 = \pm 9N$, say $a, b \in \mathbb{Z}$. Therefore $a^2 - 11b^2 \equiv 0 \pmod{3}$. Note that $a^2 \equiv 1 \pmod{3}$ unless $a \equiv 0 \pmod{3}$ and the same holds for b. Therefore if a and b are not multiples of 3 then

$$a^2 - 11b^2 \equiv 1 - 11 \equiv 2 \pmod{3}$$

which is a contradiction. If either a or b is a multiple of 3, but not both then we have

$$x^2 - 11y^2 \equiv 1 \pmod{3}$$

which again forms a contradiction. Therefore $a = 3\hat{a}$ and $b = 3\hat{b}$ for some $\hat{a}, \hat{b} \in \mathbb{Z}$. Thus

$$\begin{aligned} a^2 - 11b^2 &= \pm 9N \\ 9\hat{a}^2 - 11(9\hat{b}^2) &= \pm 9N \\ \hat{a}^2 - 11\hat{b}^2 &= \pm N \end{aligned}$$

Therefore the result holds. ■

Thus the only representation is found from the representation to the case $x^2 - 11y^2 = -N$.

4.4 Representations of $-8N$

We now establish another lemma to find solutions to this case.

Lemma 11. *$x^2-11y^2 = \pm 8N$ has a possible representation if and only if $x^2-11y^2 = \pm 2N$ has a representation. Moreover, if x and y are the integers that create a representation for $\pm 2N$, then $2x$ and $2y$ create the representation for $\pm 8N$.*

Proof. The reverse implication is straightforward by simply using the values $2x$ and $2y$. Assume there exists $a, b \in \mathbb{Z}$ such that $a^2 - 11b^2 = \pm 8N$. Now taking the equation modulo 2 we have $a^2 - 11b^2 \equiv 0 \pmod 2$ which implies $a \equiv b \pmod 2$. Now we assume a and b are both odd. Then we have $a \equiv \pm 1 \pmod 4$ and the same for b. Thus $a^2 \equiv b^2 \equiv 1 \pmod 4$ and hence $a^2 - 11b^2 \equiv 2 \pmod 4$ which is a contradiction. Therefore $a = 2\hat{a}$ and $b = 2\hat{b}$. So we have $(2\hat{a})^2 - 11(2\hat{b})^2 = \pm 8N$ which implies $\hat{a}^2 - 11\hat{b}^2 = -2N$. ■

4.5 Representations of $-7N$

Using the first section we have this equation is soluble when $N \equiv 1, 5, 9, 25, 37 \pmod{44}$ then $r_\lambda \equiv \pm 2, \pm 3, \pm 5, \pm 1, \pm 4 \pmod{11}$ respectively. Viewing this in modulo 7 we have,

$$\begin{aligned} r_\lambda^2 - 11t_\lambda^2 &\equiv 0 \pmod 7 \\ r_\lambda^2 - 4t_\lambda^2 &\equiv 0 \pmod 7 \\ r_\lambda &\equiv \pm 2t_\lambda \pmod 7 \end{aligned}$$

Using Lemma 3 we have

$$-7N = r_\lambda^2 - 11t_\lambda^2 < r_{\lambda-1}^2 - 11t_{\lambda-1}^2 < \frac{11N}{7}$$

Thus the possible equations for the $k-1$ values are

$$r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = -6N, -5N, -4N, -3N, -2N, -N, N$$

however we can rule out the $-5N, -4N, -3N, -N$ cases immediately based on the values of N. The case for $-6N$ we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = \sqrt{29}N$ which is impossible.
Case I: $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = -2N$

Now Lemma 6 yields $r_\lambda r_{\lambda-1} - 11t_\lambda t_{\lambda-1} = 5N$ and using (2.8) we can solve for $r_{\lambda-1}$

and $T_{\lambda-1}$. Thus we have

$$7r_{\lambda-1} = -5r_\lambda + 11T_\lambda \quad \text{and} \quad 7T_{\lambda-1} = -r_\lambda + 5T_\lambda.$$

Now taking the first equation modulo 7 we have $r_\lambda \equiv 5T_\lambda \pmod 7$.
Case II: $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = N$

Using Lemma 6 we have $r_\lambda r_{\lambda-1} - 11t_\lambda t_{\lambda-1} = 2N$ and solving as before we have

$$7r_{\lambda-1} = -2r_\lambda + 11T_\lambda \quad \text{and} \quad 7T_{\lambda-1} = -r_\lambda + 2T_\lambda.$$

Therefore taking the second equation modulo 7 we have $r_\lambda \equiv 2T_\lambda \pmod 7$.

4.6 Representations of $-6N$

First note this equation is only soluble when $N \equiv 1, 5, 9, 25, 37 \pmod{44}$. Also for all values of N, $N \equiv 1 \pmod 4$ which implies $-6N \equiv 2 \pmod 4$.

Lemma 12. *There are no representations in the form $x^2 - 11y^2 = -6N$.*

Proof. Assume this equation has a solution say a and b. Then from the equation we have $a^2 \equiv 2 - b^2 \pmod 4$. This implies $2 - b^2 \equiv 0 \pmod 4$ or $2 - b^2 \equiv 1 \pmod 4$. Assuming the former we have $b^2 \equiv 2 \pmod 4$ which forms a contradiction. Therefore the latter holds and we have $b \equiv \pm 1 \pmod 4$ which further implies $a \equiv \pm 1 \pmod 4$. Therefore $a = 4i \pm 1$ and $b = 4j \pm 1$ for some $i, j \in \mathbb{Z}$. Thus we have

$$\begin{aligned} (4i \pm 1)^2 - 11(4j \pm 1)^2 &= -6N \\ 16i^2 + 1 \pm 8i - 11(16j^2 + 1 \pm 8j) &= -6N \\ 1 - 11 &\equiv -6N \pmod 8 \\ 3 &\equiv N \pmod 4 \end{aligned}$$

Which forms a contradiction as $N \equiv 1 \pmod 4$ for all soluble values of N. ■

4.7 Representations of $-5N$

Using the first section in this chapter we have $N \equiv -1, -5, -9, -25, -37 \pmod{44}$ and hence $r_\lambda \equiv \pm 4, \pm 5, \pm 1, \pm 2, \pm 3 \pmod{11}$ respectively. Consider

$$\begin{aligned} r_\lambda^2 - 11t_\lambda^2 &\equiv 0 \pmod 5 \\ r_\lambda^2 - t_\lambda^2 &\equiv 0 \pmod 5 \end{aligned}$$

which implies $r_\lambda \equiv \pm t_\lambda \pmod 5$. Note: The values r_λ and t_λ that provide representations for $-10N$ will also satisfy this condition; however, they will also satisfy the condition $r_\lambda \equiv \pm t_\lambda \pmod 2$. Using Lemma 3 we have

$$-5N = r_\lambda^2 - 11t_\lambda^2 < r_{\lambda-1}^2 - 11t_{\lambda-1}^2 < r_{\lambda-1}^2 < \frac{11N}{5}$$

Based on the values for N we can eliminate the case for $-2N$ immediately. Thus the only soluble equations are $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = -4N, -3N, -N, N, 2N$. The case $-4N$ we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = \sqrt{31}N$ and hence this case is impossible. Similarly for $-3N$ we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = \sqrt{26}N$ and hence impossible. Also for the N case we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = \sqrt{6}N$ and hence no solution.

Case I: $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = -N$

From Lemma 6 we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = 4N$ and using (2.8) we can solve for $r_{\lambda-1}$ and $T_{\lambda-1}$ as

$$5r_{\lambda-1} = -4r_\lambda + 11T_\lambda \quad \text{and} \quad 5T_{\lambda-1} = -r_\lambda + 4T_\lambda.$$

Now taking the second equation modulo 5 we have $4r_\lambda \equiv T_\lambda \pmod 5$.

Case II: $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = 2N$

Again we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = N$ and thus we have

$$5r_{\lambda-1} = -r_K + 11T_\lambda \quad \text{and} \quad 5T_{\lambda-1} = -r_\lambda + T_\lambda.$$

Now taking the second equation modulo 5 we have $r_\lambda \equiv T_\lambda \pmod 5$.

4.8 Representations of $-4N$

We provide a lemma as before to find solutions to this equation.

Lemma 13. *$x^2 - 11y^2 = \pm 4N$ has a possible representation if and only if $x^2 - 11y^2 = \pm N$ has a representation. Moreover, if x and y are the integers that create a representation for $\pm N$, then $2x$ and $2y$ create the representation for $\pm 4N$.*

The proof is similar to the one given for $-8N$ given above.

4.9 Representations of $-3N$

Note this equation is only soluble when $N \equiv -1, -5, -9, -25, -37 \pmod{44}$ and thus $N \equiv -1 \pmod 4$ for all values of N. This implies $-3N \equiv 3 \pmod 4$ for all values of N.

Lemma 14. *The representation $x^2 - 11y^2 = -3N$ is impossible.*

Proof. Assume the above representation is possible with values a and b. Then from the above notes we have $a^2 \equiv 3 - b^2 \pmod 4$ and therefore $3 - b^2 \equiv 0 \pmod 4$ or $3 - b^2 \equiv 1 \pmod 4$. If we assume the former we have $b^2 \equiv 3 \pmod 4$ which forms a contradiction. If we assume the latter we have $b^2 \equiv 2 \pmod 4$ which also forms a contradiction. Hence there is no representation. ■

4.10 Representations of $-2N$

Again we have this equation is only soluble when $N \equiv 1, 5, 9, 25, 37 \pmod{44}$ and hence $r_\lambda \equiv \pm 3, \pm 1, \pm 2, \pm 4, \pm 5 \pmod{11}$. If we view this equation modulo 2 we have

$$\begin{aligned} r_\lambda^2 - 11t_\lambda^2 &\equiv 0 \pmod 2 \\ r_\lambda^2 - t_\lambda^2 &\equiv 0 \pmod 2 \\ r_\lambda &\equiv \pm t_\lambda \pmod 2 \end{aligned}$$

Note: The values r_λ and t_λ that provide a representation for $-10N$ will also satisfy this condition; however they will also satisfy $r_\lambda \equiv \pm t_\lambda \pmod 5$. Now applying Lemma 3 we

have

$$-2N < r_{\lambda-1}^2 - 11t_{\lambda-1}^2 < \frac{11N}{2}$$

Therefore the only possibilities we have are

$$r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = N, 2N, 3N, 4N, 5N$$

Similarly from the above cases we have Lemma 6 provides contradictions for the cases $2N, 3N$, and $4N$.

Case I: $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = N$

As with the previous equations we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = 3N$ and hence

$$2r_{\lambda-1} = -3r_\lambda + 11T_\lambda \quad \text{and} \quad 2T_{\lambda-1} = -r_\lambda + 3T_\lambda.$$

Now taking the second equation modulo 11 we have $3r_{\lambda-1} \equiv r_\lambda \pmod{11}$.

Case II: $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = 5N$

Now we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = N$ and using (2.8) we have

$$2r_{\lambda-1} = -r_\lambda + 11T_\lambda \quad \text{and} \quad 2T_{\lambda-1} = -r_\lambda + T_\lambda.$$

Taking the first equation modulo 11 we have $9r_{\lambda-1} \equiv r_\lambda \pmod{11}$.

4.11 Representations of $-N$

We have $N \equiv -1, -5, -9, -25, -37 \pmod{44}$ and hence $r_\lambda \equiv \pm 1, \pm 4, \pm 3, \pm 5, \pm 2 \pmod{11}$. First note $N \equiv \pm k \pmod{44}$ where $k = 1, 5, 9, 25$, or 37 yields $N \equiv 1 \pmod{2}$. Therefore

$$\begin{aligned} r_\lambda^2 - 11t_\lambda^2 &\equiv 1 \pmod 2 \\ r_\lambda^2 - t_\lambda^2 &\equiv 1 \pmod 2 \\ (r_\lambda - t_\lambda)^2 &\equiv 1 \pmod 2 \\ r_\lambda &\equiv 1 + t_\lambda \pmod 2 \end{aligned}$$

Applying Lemma 3 we have $-N < r_{\lambda-1}^2 - 11t_{\lambda-1}^2 < 11N$ and hence the only possible equations are

$$r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = N, 2N, 3N, 4N, 5N, 6N, 7N, 8N, 9N, 10N.$$

However Lemma 6 provides contradictions for the cases $N, 3N, 4N, 5N, 6N, 8N$, and $9N$.
Case I: $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = 2N$

From (6) we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = 3N$ and hence

$$r_{\lambda-1} = -3r_\lambda + 11T_\lambda \quad \text{and} \quad T_{\lambda-1} = -r_\lambda + 3T_\lambda.$$

Now taking the first equation modulo 11 we have $8r_\lambda \equiv r_{\lambda-1} \pmod{11}$.
Case II: $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = 7N$ We have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = 2N$ and therefore

$$r_{\lambda-1} = -2r_\lambda + 11T_\lambda \quad \text{and} \quad T_{\lambda-1} = -r_\lambda + 2T_\lambda.$$

Taking the first equation modulo 11 we have $9r_\lambda \equiv r_{\lambda-1} \pmod{11}$.
Case III: $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = 10N$

By (6) we have $r_\lambda r_{\lambda-1} + 11T_\lambda T_{\lambda-1} = N$ and hence we have

$$r_{\lambda-1} = -r_\lambda + 11T_\lambda \quad \text{and} \quad T_{\lambda-1} = -r_\lambda + T_\lambda.$$

Taking the first equation modulo 11 we finally have $-r_\lambda \equiv r_{\lambda-1} \pmod{11}$.

4.12 Summary

We will now summarize all classifications found in the previous sections above.

1. Representations of the form $r_\lambda^2 - 11t_\lambda^2 = -10N$ when $N \equiv 1, 5, 9, 25, 37 \pmod{44}$ will be given when $r_\lambda \equiv \pm t_\lambda \pmod{10}$.
   (a) $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = -7N$ if $r_\lambda \equiv 9T_\lambda \pmod{10}$.
   (b) $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = N$ if $r_\lambda \equiv T_\lambda \pmod{10}$.

2. Representations of the form $r_\lambda^2 - 11t_\lambda^2 = -9N$ are found from representations of $r_\lambda^2 - 11t_\lambda^2 = -N$.

3. Representations of the form $r_\lambda^2 - 11t_\lambda^2 = -8N$ are found from representations of $r_\lambda^2 - 11t_\lambda^2 = -2N$.

4. Representations of the form $r_\lambda^2 - 11t_\lambda^2 = -7N$ when $N \equiv 1, 5, 9, 25, 37 \pmod{44}$ will be given when $r_\lambda \equiv \pm 2t_\lambda \pmod{7}$.

   (a) $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = -2N$ if $r_\lambda \equiv 5T_\lambda \pmod{7}$.

   (b) $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = N$ if $r_\lambda \equiv 2T_\lambda \pmod{7}$.

5. Representations of the form $r_\lambda^2 - 11t_\lambda^2 = -6N$ are impossible.

6. Representations of the form $r_\lambda^2 - 11t_\lambda^2 = -5N$ when $N \equiv -1, -5, -9, -25, -37 \pmod{44}$ will be given when $r_\lambda \equiv \pm t_\lambda \pmod{5}$.

   (a) $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = -N$ if $4r_\lambda \equiv T_\lambda \pmod{5}$.

   (b) $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = 2N$ if $r_\lambda \equiv T_\lambda \pmod{5}$.

7. Representations of the form $r_\lambda^2 - 11t_\lambda^2 = -4N$ are found from representations of $r_\lambda^2 - 11t_\lambda^2 = -N$.

8. Representations of the form $r_\lambda^2 - 11t_\lambda^2 = -3N$ are impossible.

9. Representations of the form $r_\lambda^2 - 11t_\lambda^2 = -2N$ when $N \equiv 1, 5, 9, 25, 37 \pmod{44}$ are given when $r_\lambda \equiv t_\lambda \pmod{2}$.

   (a) $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = N$ if $3r_{\lambda-1} \equiv r_\lambda \pmod{11}$.

   (b) $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = 5N$ if $9r_{\lambda-1} \equiv r_\lambda \pmod{11}$.

10. Representations of the form $r_\lambda^2 - 11t_\lambda^2 = -N$ when $N \equiv -1, -5, -9, -25, -37 \pmod{44}$ are given when $r_\lambda \equiv t_\lambda + 1 \pmod{2}$.

    (a) $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = 2N$ if $8r_\lambda = r_{\lambda-1} \pmod{11}$.

    (b) $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = 7N$ if $9r_\lambda \equiv r_{\lambda-1} \pmod{11}$.

(c) $r_{\lambda-1}^2 - 11t_{\lambda-1}^2 = 10N$ if $-r_\lambda \equiv r_{\lambda-1} \pmod{11}$.

Example 5. Consider $N = 6790187$ where $N \equiv -25 \pmod{44}$. Then we have $u = 2944782$ with $(r_{12}, t_{12}) = (1538, 1817)$ which solves $x^2 - 11^2 = -5N$. Also $(r_{11}, t_{11}) = (2767, -1146)$ which solves $x^2 - 11y^2 = -N$. All calculations were completed using the Matlab functions in the Appendices.

Chapter 5

Future Research

We have found representations of integers of the form x^2-10y^2 and x^2-11y^2 expanding on the representations provided by Matthews in [4]. Unfortunately at this juncture we do not have a method to find all possible solutions to the Diophantine equation $x^2 - 10y^2 = \kappa N$ and similarly for $D = 11$. This is a future avenue of research which we are currently working on based upon Lemma 1 which states the values given by the Euclidean algorithm, r_k and t_k, always yield multiples of N in the form $r_k^2 - Dt_k^2$. At this stage, we find our problem is our saving grace in our representation problem. Thue's theorem and our bounds for r_λ and t_λ disregard solutions to the Diophantine equation because the values are above $\sqrt{N}$. We are in the process of finding a method to obtain these solutions through a more defined process rather than just checking all values for r_k and t_k.

Secondly, the representations given by the Euclidean algorithm need not be primitive as there is no necessity r_λ and t_λ be coprime; however we conjecture $\gcd(r_\lambda, t_\lambda)$ divides κ where $r_\lambda^2 - Dt_\lambda^2 = \kappa N$. If this conjecture holds the primality of N is inconsequential as the important aspect is the multiple of N. If this conjecture holds any representation we find for N will be primitive and hence yielding a solution to the equivalent diophantine equation.

Furthermore, we could extend this process to representations for larger values of D, say 13, 14, 15, etcetera. By extending this to these varying values of D we may find some inherit qualities between these different representations and generalize our result to any D. This would not be as significant as providing a solution to the Diophantine equation

$x^2 - Dy^2 = N$, but it would certainly be a step in the right direction.

Finally, we may extend this work to other representations where D has a certain form itself. For example, is it possible to apply our process to find representations in the form $x^2 - k(k+1)y^2$? Additionally, what if we extend this process to not only quadratic Diophantine equations but also quartic Diophantine equations similar to those explored by Agarwal in [1]. Assuming our process would find solutions to all of these various equations it must imply there is something inherently common to these equations. If we can find this common ground between these equations we may be able to find this commonality among other Diophantine equations which may allows us to extend our process to those equations as well.

Appendix A

Quadratic Residue Function

```
function u = quadRes(D,N)
%QUADRES Finds a quadratic residue congruent to D modulo N.
%

%Initialize variables
u = [0];
writeCount = 1;

%Loop through potential residues and check if congruent
for j=1:N-1
    if mod(j.^2,N) == mod(D,N)
        u(writeCount) = j;
        writeCount = writeCount + 1;
    end
end

return
```

Appendix B

Algorithmic Function

```
function [sol,rk,tk,k] = Pell(N,D,u)
%PELL Creates solutions using algorithm
%   where x^2-Dy^2=N
% Returns:  sol - vector containing the solutions for the various rk,tk
%           rk  - the values of rk obtained from Euclidean Algorithm
%           tk  - the values of tk obtained from Euclidean Algorithm
%           k   - the index obtained from performing the Euclidean
%           Algorithm
%
%Initalize variables
A = [N 1 0; u 0 1];     %The original matrix
r = [N u]';             %The vector containing the remainders
s = [1 0]';             %The vector containing the s values
t = [0 1]';             %The vector containing the t values
q = [0]';               %The quotients
k = 0;                  %The index in the Euclidean Algorithm
done = 0;               %Boolean variable for looping
i=1;

while ~done
```

```
%Determine which row to perform operation
if i > 2
    if mod(i,2) == 1
        row = 1;
    else
        row = 2;
    end
else
    row = i;
end

%Find Quotient
if row == 1
    q(i) = floor(A(row,1)/A(row+1,1));
else
    q(i) = floor(A(row,1)/A(row-1,1));
end

%Perform Row Reduction
if row == 1
    B(row,:) = -q(i)*A(row+1,:)+A(row,:);
    B(row+1,:) = A(row+1,:);
else
    B(row,:) = -q(i)*A(row-1,:)+A(row,:);
    B(row-1,:) = A(row-1,:);
end

%Update relations
cur_i = i;
r(i+2) = B(row,1);
s(i+2) = B(row,2);
```

```
    t(i+2) = B(row,3);
    cur_i = i+2;

    %Check if r_k < sqrt(N)
    done = (r(cur_i)) < sqrt(N); %&& (r(cur_i-1)) > sqrt(N) ;

    %Update required items
    i=i+1;
    A = B;
end

k = cur_i;
r;
s;
t;

%Pell Values
p1 = r(k)^2 - D*t(k)^2;
s1 = p1;
p2 = r(k-1)^2-D*t(k-1)^2;
s2 = p2;
if k > 2
    p3 = r(k-2)^2-D*t(k-2)^2;
    s3 = p3;
    if k > 3
        p4 = r(k-3)^2-D*t(k-3)^2;
        s4 = p4;
        if k > 4
            p5 = r(k-4)^2-D*t(k-4)^2;
            s5 = p5;
            if k > 5
                p6 = r(k-5)^2-D*t(k-5)^2;
```

```
                s6 = p6;
                sol = [s1 s2 s3 s4 s5 s6];
            else
                sol = [s1 s2 s3 s4 s5];
            end
        else
            sol = [s1 s2 s3 s4];
        end
    else
        sol = [s1 s2 s3];
    end
else
    sol = [s1 s2];
end

temp_r = fliplr(r');
temp_t = fliplr(t');
if size(temp_r,2)>6
    rk = temp_r(1,1:6);
else
    rk = temp_r;
end
if size(temp_t,2)>6
    tk = temp_t(1,1:6);
else
    tk = temp_t;
end

%Create vector for Equation (8)
for i=2:size(r)
    e_N(i-1) = r(i)*r(i-1)-D*t(i)*t(i-1);
end
```

```
for i=1:size(e_N')
    e(i) = e_N(i)/N;
end

return
```

Bibliography

[1] A. Agarwal, *Some Quartic Diophantine Equations*, Ph.D. thesis, SUNY Buffalo, 2005.

[2] John Brillhart, *Note on representing a prime as a sum of two squares*, Mathematics of Computation **26** (1972), no. 120, 1011–1013.

[3] Charles Hermite, *Note au sujet de l'article précédent*, Journal de mathématiques pures et appliquées 1^{re} série **13** (1848), 15.

[4] Keith Matthews, *Thue's Theorem and the Diophantine Equation* $x^2 - Dy^2 = \pm N$, Mathematics of Computation **71** (2001), no. 239, 1281–1286.

[5] I. Niven, H.S. Zuckerman, and H.L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, New York, 1991.

[6] Joseph H. Silverman, *A Friendly Introduction to Number Theory*, Prentice Hall, 2005.

[7] Peter Wilker, *An efficient algorithmic solution of the diophantine equation* $u^2 + 5v^2 = m$, Mathematics of Computation **35** (1980), no. 152, 1347–1352.