Solving Pell Equations

Matthew Wright

May 2, 2006

Department of Mathematical Sciences
Messiah College
Grantham, PA

Dr. Lamarr Widmer, advisor

This paper is submitted in partial fulfillment of the
requirements for departmental honors in mathematics.

Abstract

This paper is an investigation of Pell Equations–equations of the form $x^2 - dy^2 = k$ where d is a nonsquare, positive integer, k is an integer, and we are looking for integer solutions in x and y. We will provide motivation, both algebraic and geometric, for this definition of Pell Equations. Next, we will examine the $k = 1$ case, proving not only that it is solvable, but also that infinitely many solutions can be obtained easily from the fundamental solution. We will classify some Pell Equations as solvable or unsolvable when $k \neq 1$, examining in detail the $k = 4$ case. After explaining several patterns that appear when $k = 4$ and $d \equiv 5 \pmod 8$, we will prove the existence of a fundamental solution for these cases. Finally, we will briefly examine how a computer may be used to find solutions, especially the fundamental solution, for Pell Equations.

Contents

1 Introduction

In number theory, Pell Equations fall in the category of Diophantine equations. Named after the Greek mathematician Diophantus, *Diophantine equations* are equations for which integer solutions are desired. Specifically, *Pell Equations* have the form $x^2 - dy^2 = k$, where d and k are fixed and we are looking for integers x and y that satisfy the equation. Some mathematicians specify that $k = 1$, but we will allow k to be any nonzero integer. We further qualify the integer d to be positive and nonsquare. This qualification is helpful because it leaves open the possibility of infinitely many solutions in positive integers x and y.

1.1 Why must d be positive?

If d were negative, such as $d = -p$, then the equation of interest becomes $x^2 + py^2 = k$, which has the form of an ellipse. This ellipse has x-intercepts at $\pm\sqrt{k}$ and y-intercepts at $\pm\sqrt{\frac{k}{p}}$. By plotting the ellipse on the Cartesian plane (see Figure 1), we can easily see that the integers on the y-axis between 0 and $\pm\sqrt{\frac{k}{p}}$ are the only possible positive integers that might correspond to points on the ellipse with integer coordinates. Therefore, there can be no more than $\lfloor\sqrt{\frac{k}{p}}\rfloor$ solutions in positive integers to the equation $x^2 + py^2 = k$.

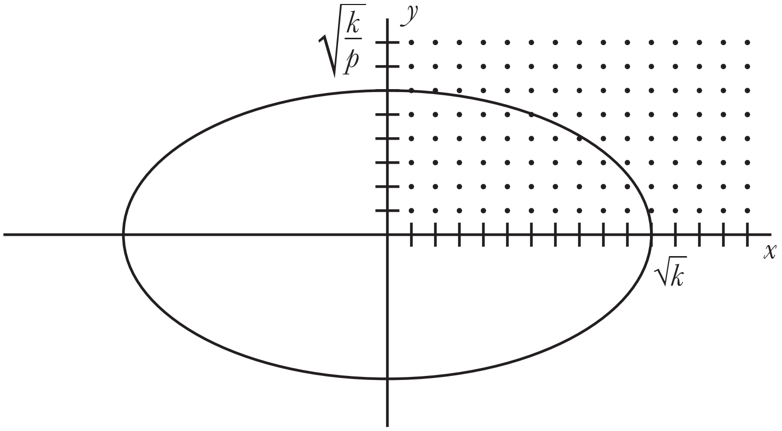

Figure 1: Equations of the form $x^2 + py^2 = 1$ have finitely many positive integer solutions (x, y).

1.2 Why must d be nonsquare?

If d is a square, such as $d = q^2$, where q is a positive integer, then the equation becomes $x^2 - q^2y^2 = k$, which factors into

$$(x + qy)(x - qy) = k \tag{1}$$

Since x, y, and q are all positive integers, the left-hand side of (1) must be two integers whose product is k. For each pair of positive integers m and n, $m > n$, such that $mn = k$, there might exist integers x and y that satisfy

$$\begin{cases} x + qy = m \\ x - qy = n \end{cases}$$

Therefore, the number of positive integer solutions that satisfy (1) is bounded by half the number of positive integers which divide k. It could also happen that the equation has no solutions, as in the case $x^2 - y^2 = 10$.

We can also see that an equation of the form $x^2 - q^2y^2 = k$ has finitely many integer solutions by the following graphical argument. First, sketch the graph of the hyperbola $x^2 - q^2y^2 = k$ on the Cartesian plane. Except for a small region near the origin (the region in Figure 2, for example), the hyperbola is very close to its asymptotes. The asymptotes are of the form $x + qy = 0$ and $x - qy = 0$, so they are lines through the origin with slopes of $\pm 1/q$. The hyperbola might pass through points with integer coefficients near the origin, but it soon gets too close to its asymptotes to pass through any such points.

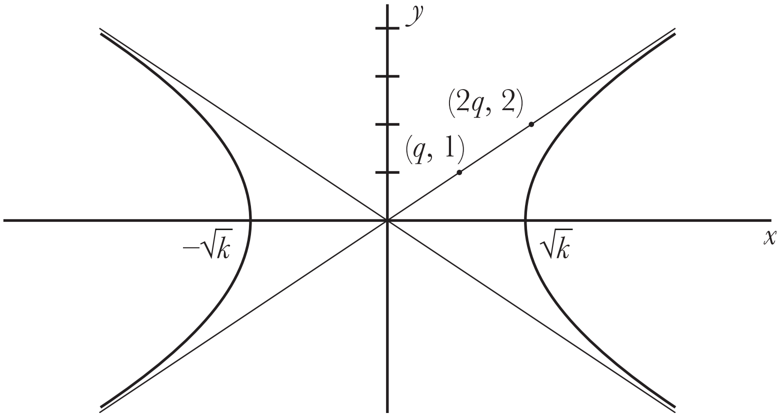

Figure 2: The graph of a hyperbola, $x^2 - q^2y^2 = k$ and its asymptotes, $x + qy = 0$ and $x - qy = 0$.

Figure 3 shows a portion of the asymptote $x - qy = 0$ on a grid of points with integer coordinates. Circled points are those closest to the asymptote, but not on the asymptote. The magnification in Figure 3 helps determine the distance from any such point to the asymptote. Call this distance a. By the Pythagorean Theorem, we have

$$\begin{aligned}(aq)^2 &= a^2 + 1\\ a^2q^2 - a^2 &= 1\\ a^2(q^2-1) &= 1\\ a^2 &= \frac{1}{q^2-1}\\ a &= \sqrt{\frac{1}{q^2-1}}\end{aligned}$$

Therefore, there are no points with integer coefficients whose distance d from an asymptote is $0 < d < \sqrt{\frac{1}{q^2-1}}$

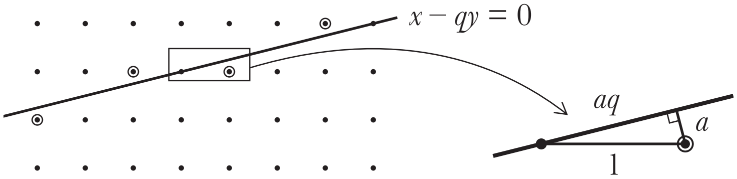

Figure 3: The asymptote $x - qy = 0$ on a grid of points with integer coordinates.

Let $f(x)$ be the branch of the hyperbola in the first quadrant:

$$f(x) = \sqrt{\frac{x^2-k}{q^2}}, \quad x \geq \sqrt{k}.$$

We know that $\lim_{x\to\infty} f(x) = \frac{x}{q}$ and $f(x) \neq \frac{x}{q}$ for any x. So for each $\epsilon > 0$ there exists $x_0 > 0$ such that

$$x > x_0 \quad \text{implies} \quad 0 < \left| f(x) - \frac{x}{q} \right| < \epsilon$$

Let $\epsilon = \sqrt{\frac{1}{q^2-1}}$. Then there exists $x_0 > 0$ such that for all $x > x_0$, the graph of $f(x)$ is closer than $\sqrt{\frac{1}{q^2-1}}$ from its asymptote, but never touches its asymptote. Therefore, $f(x)$ does not pass through any integer coordinates for $x > x_0$.

We see that $f(x)$ may only pass through integer coordinates when $\sqrt{k} < x < x_0$, so $f(x)$ cannot pass through infinitely many points with integer coordinates. Therefore, $x^2 - q^2y^2 = k$ has finitely many integer solutions.

1.3 Pell Equation

Having motivated the choice of d positive and nonsquare, we arrive at the following definition:

Definition 1. *A* ***Pell Equation*** *is an equation of the form $x^2 - dy^2 = k$, where d is a positive nonsquare integer and k is a nonzero integer, for which we attempt to find integer solutions x and y.*

Pell Equations have been of interest to mathematicians for centuries. Archimedes' famous cattle problem leads to a Pell Equation. The Indian mathematican Brahmagupta in the sixth century had methods to find solutions to $x^2 - dy^2 = 1$, and he could generate infinitely many solutions from an initial solution. In Europe, Pierre de Fermat studied the equation and inspired some of his contemporaries to do the same. John Pell was an English mathematician who appears to have had a reputation as an algebraist in the middle of the 17th century, but he did hardly any work with the equation that bears his name [2]. Leonhard Euler credited the equation to Pell in a letter to Goldbach in 1730, and the name stuck [1].

2 The Equation $x^2 - dy^2 = 1$ is Solvable

Pell Equations where $k = 1$ are of special interest to mathematicians because they have infinitely many solutions. In fact, some authors define Pell Equations to be of the form $x^2 - dy^2 = 1$, not considering equations where $k \neq 1$ as our broader definition permits. In this section, we will prove that the equation $x^2 - dy^2 = 1$ has a solution in positive integers x and y. We will begin with the following lemma:

Lemma 1. *For a given integer N, there are positive integers u and v for which*

$$\left|u - v\sqrt{d}\right| < \frac{1}{N} \leq \frac{1}{v} \tag{2}$$

and

$$\left|u^2 - v^2\right| \leq 2\sqrt{d} + 1 \tag{3}$$

To make the proof easier, we introduce some notation. For any number α, we will denote by $\langle\alpha\rangle$ the *fractional part* of α. That is, $\langle\alpha\rangle = \alpha - \lfloor\alpha\rfloor$, where $\lfloor\alpha\rfloor$ is the greatest integer that does not exceed α.

Proof. Consider the $N + 1$ numbers, all of which are between 0 and 1:

$$\langle\sqrt{d}\rangle, \langle 2\sqrt{d}\rangle, \ldots, \langle N\sqrt{d}\rangle, \langle(N+1)\sqrt{d}\rangle \tag{4}$$

Also consider the N intervals $\{t : \frac{i}{N} < t < \frac{i+1}{N}\}$, where $0 \leq i \leq N-1$. Each of these intervals has width $1/N$. Note that together, this set of intervals spans the numbers from 0 to 1, except for the the numbers i/N, which are the endpoints of the intervals. These boundaries, i/N, never equal any of the numbers in (4) since all of the numbers are irrational.

By the pigeonhole principle, if we place the $N + 1$ numbers in the N intervals, at least one interval must contain at least two of the numbers. Call two of these numbers $\langle q\sqrt{d}\rangle$ and $\langle s\sqrt{d}\rangle$, with $q > s$. Call the interval that contains these numbers $\left(\frac{i}{N}, \frac{i+1}{N}\right)$. Therefore, we have

$$\frac{i}{N} < \langle q\sqrt{d}\rangle < \frac{i+1}{N} \qquad \text{and} \qquad \frac{i}{N} < \langle s\sqrt{d}\rangle < \frac{i+1}{N}$$

Define p and r to be the integer parts of $q\sqrt{d}$ and $s\sqrt{d}$, respectively. Therefore, $p - \lfloor q\sqrt{d} \rfloor = q\sqrt{d} - \langle q\sqrt{d}\rangle$ and $r = \lfloor s\sqrt{d} \rfloor = s\sqrt{d} - \langle s\sqrt{d}\rangle$.

Since $q > s$ and $\sqrt{d} > 1$, $\lfloor q\sqrt{d} \rfloor > \lfloor s\sqrt{d} \rfloor$ and $p > r$.

Since q and s are each between 1 and $N+1$, their difference cannot exceed N. Therefore, $q - s \leq N$.

Since $\langle q\sqrt{d}\rangle$ and $\langle s\sqrt{d}\rangle$ both fall in the same interval of width $1/N$, their difference is less than $1/N$. Therefore,

$$\begin{aligned}
\left|\langle q\sqrt{d}\rangle - \langle s\sqrt{d}\rangle\right| &< \frac{1}{N} \\
\left|\left(q\sqrt{d} - p\right) - \left(s\sqrt{d} - r\right)\right| &< \frac{1}{N} \\
\left|(q-s)\sqrt{d} - (p-r)\right| &< \frac{1}{N} \\
\left|(p-r) - (q-s)\sqrt{d}\right| &< \frac{1}{N}
\end{aligned}$$

Let $u = p - r$ and $v = q - s$. Then $q - s = v \leq N$, so $\frac{1}{v} \geq \frac{1}{N}$. Therefore, we have found two integers u and v that satsify $\left|u - v\sqrt{d}\right| < \frac{1}{N} \leq \frac{1}{v}$, or more importantly

$$\left|u - v\sqrt{d}\right| \leq \frac{1}{v} \tag{5}$$

which proves the first part of Lemma 1.

To prove the second part of Lemma 1, we begin with the following identity:

$$u + v\sqrt{d} = (u - v\sqrt{d}) + 2v\sqrt{d} \tag{6}$$

Multiplying equations (5) and (6), we have

$$\begin{aligned}
(u + v\sqrt{d})\left|u - v\sqrt{d}\right| &\leq \frac{1}{v}[(u - v\sqrt{d}) + 2v\sqrt{d}] \\
\left|u^2 - dv^2\right| &\leq \frac{u - v\sqrt{d}}{v} + 2\sqrt{d} \qquad (7)
\end{aligned}$$

Beginning with inequality (5), we arrive at the following:

$$\begin{aligned}
\left|u - v\sqrt{d}\right| &\leq \frac{1}{v} \\
\frac{u - v\sqrt{d}}{v} \leq u - v\sqrt{d} \leq \left|u - v\sqrt{d}\right| &\leq \frac{1}{v} \leq 1
\end{aligned}$$

so

$$\frac{u - v\sqrt{d}}{v} \leq 1 \tag{8}$$

Combining inequalities (7) and (8), we have

$$\left|u^2 - dv^2\right| \leq \frac{u - v\sqrt{d}}{v} + 2\sqrt{d} \leq 1 + 2\sqrt{d}$$

Therefore, we conclude that

$$\left|u^2 - dv^2\right| \leq 2\sqrt{d} + 1$$

and this proves the second part of Lemma 1. □

In proving Lemma 1, we began by choosing the first $N+1$ consecutive multiples of $\sqrt{d}$ and examining their fractional parts:

$$\langle\sqrt{d}\rangle, \langle 2\sqrt{d}\rangle, \ldots, \langle N\sqrt{d}\rangle, \langle (N+1)\sqrt{d}\rangle \tag{9}$$

Now, there are infinitely many non-overlapping sets of $N+1$ consecutive multiples of $\sqrt{d}$ that we could have chosen, and each set works equally well in proving the lemma. For example, we could have chosen either of the following:

$$\langle (N+2)\sqrt{d}\rangle, \langle (N+3)\sqrt{d}\rangle, \ldots, \langle (2N+2)\sqrt{d}\rangle$$
$$\langle (2N+3)\sqrt{d}\rangle, \langle (2N+4)\sqrt{d}\rangle, \ldots, \langle (3N+3)\sqrt{d}\rangle$$

In any such set, we can find two numbers whose fractional parts lie in the same interval. Therefore, each set produces the numbers u and v that satisfy the equations of Lemma 1. Since we can choose non-overlapping sets, u and v will be unique to each set. Therefore, we can find infinitely many pairs (u, v) that satisfy

$$\left|u - v\sqrt{d}\right| < \frac{1}{N} \leq \frac{1}{v} \qquad \text{and} \qquad \left|u^2 - v^2\right| \leq 2\sqrt{d} + 1 \tag{10}$$

Note that $|u^2 - dv^2|$ is an integer. Therefore, there are infinitely many solutions to $u^2 - dv^2 = j$, where j is an integer bounded by $|j| \leq 2\sqrt{d} + 1$. Since we have finitely many possibilities for j and infinitely many solutions (u, v), there must be at least one j with infinitely many solutions (u, v). Let k be this particular value of j. Therefore, there are infinitely many solutions (u, v) to $u^2 - dv^2 = k$.

The second lemma we will use in our proof is the following:

Lemma 2. *If (x_1, y_1) and (x_2, y_2) are integer solutions of $x^2 - dy^2 = k$ such that*

$$x_1 \equiv x_2 \pmod{k} \qquad \textit{and} \qquad y_1 \equiv y_2 \pmod{k}$$

Then the equation $x^2 - dy^2 = 1$ has a solution in positive integers.

Proof. We have the following two equations:

$$x_1^2 - dy_1^2 = k \qquad \text{and} \qquad x_2^2 - dy_1^2 = k \tag{11}$$

Multiplying the equations together, we have

$$\begin{aligned}
(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) &= k^2 \\
x_1^2x_2^2 - dx_1^2y_2^2 - dx_2^2y_1^2 + d^2y_1^2y_2^2 &= k^2 \\
\left(x_1^2x_2^2 - 2dx_1x_2y_1y_2 + d^2y_1^2y_2^2\right) - d\left(x_1^2y_2^2 - 2dx_1x_2y_1y_2 + x_2^2y_1^2\right) &= k^2 \\
\left(x_1x_2 - dy_1y_2\right)^2 - d\left(x_1y_2 - x_2y_1\right)^2 &= k^2 \\
\left(\frac{x_1x_2 - dy_1y_2}{k}\right)^2 - d\left(\frac{x_1y_2 - x_2y_1}{k}\right)^2 &= 1 \qquad (12)
\end{aligned}$$

Equation (12) has the desired form, so the lemma is proved if we can show that the quantities in parentheses are integers.

Since $x_1 \equiv x_2 \pmod{k}$ and $y_1 \equiv y_2 \pmod{k}$, then

$$x_1x_2 - dy_1y_2 \equiv x_1x_1 - dy_1y_1 = x_1^2 - dy_1^2$$

But $x_1^2 - y_1^2 = k$ and $k \equiv 0 \pmod{k}$, so $x_1^2 - dy_1^2 \equiv 0 \pmod{k}$. Therefore,

$$x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_1^2 \equiv 0 \pmod{k} \qquad (13)$$

Also, we see that $x_1y_2 \equiv x_2y_1 \pmod{k}$, which implies that

$$x_1y_2 - x_2y_1 \equiv 0 \pmod{k} \qquad (14)$$

Combining the results of equations (13) and (14), we see that the quantities in parentheses in equation (12) are integers, so

$$\left(\frac{x_1x_2 - dy_1y_2}{k}, \frac{x_1y_2 - x_2y_1}{k}\right)$$

is an integer solution of $x^2 - dy^2 = 1$ and we have proved Lemma 2. □

We are now ready to prove the main theorem of this section:

Theorem 1. *The equation $x^2 - dy^2 = 1$ has a solution in positive integers x and y for all positive, nonsquare integers d.*

Proof. We have found a value of k for which there exist infinitely many solutions (u, v) of $u^2 - dv^2 = k$. There are only k^2 unique ordered pairs modulo k. Since we have more than $k^2 + 1$ solutions (each of which is an ordered pair), at least two of them must be equivalent modulo k. Call these two pairs (x_i, y_i) and (x_j, y_j), with $x_i \equiv x_j$ and $y_i \equiv y_j \pmod{k}$. By Lemma 2, the equation $x^2 - dy^2 = 1$ has a solution in positive integers. □

3 The Fundamental Solution

In the previous section we proved that there exists a positive integer solution (x, y) to the equation $x^2 - dy^2 = 1$ when d is positive and nonsquare, In this section we will see that there is a solution, known as the *fundamental solution*, from which all other positive integer solutions may be obtained. Specifically, we will prove that the fundamental solution is smallest positive integer solution to $x^2 - dy^2 = 1$. We will also see how all other positive integer solutions can be obtained from the fundamental solution.

3.1 Sequence of Solutions

From any solution of $x^2 - dy^2 = 1$, we can obtain infinitely many solutions. Suppose (x_1, y_1) is a solution of $x^2 - dy^2 = 1$. We can obtain another solution by the following process:

$$\begin{aligned}
x_1^2 - dy_1^2 &= 1 \\
(x_1 + y_1\sqrt{d})(x_1 - y_1\sqrt{d}) &= 1 \\
(x_1 + y_1\sqrt{d})^2(x_1 - y_1\sqrt{d})^2 &= 1 \\
\left(x_1^2 + 2x_1y_1\sqrt{d} + dy_1^2\right)\left(x_1^2 - 2x_1y_1\sqrt{d} + dy_1^2\right) &= 1 \\
\left((x_1^2 + dy_1^2) + (2x_1y_1)\sqrt{d}\right)\left((x_1^2 + dy_1^2) - (2x_1y_1)\sqrt{d}\right) &= 1 \\
\left(x_1^2 + dy_1^2\right)^2 - d\left(2x_1y_1\right)^2 &= 1
\end{aligned}$$

We have again obtained the form of a Pell Equation, and we can see that $(x_1^2 + dy_1^2, 2x_1y_1)$ is a solution. Applying the process again, we can obtain yet another solution, and so on, obtaining as many solutions as we desire.

Alternately, suppose we consider integer powers of $(x_1 + y_1\sqrt{d})$:

$$\begin{aligned}
\left(x_1 + y_1\sqrt{d}\right)^n &= x_1^n + C_1\sqrt{d}x_1^{n-1}y_1 + C_2dx_1^{n-2}y_1^2 + C_3d^{3/2}x_1^{n-3}y_1^3 + \cdots + d^{n/2}y_1^n \\
&= \left(x_1^n + C_2dx_1^{n-2}y_1^2 + \cdots\right) + \sqrt{d}\left(C_1x_1^{n-1}y_1 + C_3x_1^{n-3}y_1^3 + \cdots\right) \\
&= x_n + y_n\sqrt{d}
\end{aligned}$$

where C_i are the binomial coefficients: $C_i = \binom{n}{i} = \frac{n!}{(n-i)!i!}$. Since each integer power can be written in a form similar to the original, we define x_n and y_n as follows:

$$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n \tag{15}$$

We will now prove the following theorem:

Theorem 2. *If $x_1 > 1$, $y_1 \geq 1$, and $\left(x_n + y_n\sqrt{d}\right) = \left(x_1 + y_1\sqrt{d}\right)^n$, then $x_{n+1} > x_n$ and $y_{n+1} > y_n$ for positive n.*

Proof by Induction. Initial Case: We find that $x_2 = x_1^2 + dy_1^2$ and $y_2 = 2x_1y_1$. Since $x_1 > 1$, $y_1 \geq 1$, and d is a positive integer, it is clear that $x_2 > x_1$ and $y_2 > y_1$.

Induction: Assume we have a solution (x_n, y_n) with x_n and y_n positive integers greater than 1. We have:

$$\begin{aligned}
x_{n+1} + y_{n+1}\sqrt{d} &= \left(x_1 + y_1\sqrt{d}\right)^{n+1} \\
&= \left(x_1 + y_1\sqrt{d}\right)\left(x_1 + y_1\sqrt{d}\right)^{n} \\
&= \left(x_1 + y_1\sqrt{d}\right)\left(x_n + y_n\sqrt{d}\right) \\
&= (x_1x_n + dy_1y_n) + (x_1y_n + x_ny_1)\sqrt{d}
\end{aligned}$$

Therefore, $x_{n+1} = x_1x_n + dy_1y_n$ and $y_{n+1} = x_1y_n + x_ny_1$. Note that $x_1x_n > x_n$ and $dy_1y_n > 0$. Thus, $x_{n+1} = x_1x_n + dy_1y_n > x_n$. Also, $x_1y_n > y_n$ and $x_ny_1 > 0$, so $y_{n+1} = x_1y_n + x_ny_1 > y_n$. Therefore, we have $x_{n+1} > x_n$ and $y_{n+1} > y_n$. □

We have established that the sequences $\{x_n\}$ and $\{y_n\}$ are strictly increasing when defined according to equation (15). This suggests that if we want the integer powers of $(x_1 + y_1\sqrt{d})$ to generate *all* positive integer solutions of $x^2 - dy^2 = 1$, then x_1 and y_1 should be as small as possible. First, however, we must answer the question: Does the solution with the smallest value of x also contain the smallest value of y?

3.2 Ordering the Solutions

To answer the question posed above, we must examine the ordering of the solutions. It turns out that the solution with the smallest value of x does contain the smallest value of y. Specifically, we will prove the following theorem:

Theorem 3. *If p, q, r, and s are positive integers for which $p > r$ and*

$$p^2 - dq^2 = r^2 - ds^2 = k \tag{16}$$

then $q > s$ and $p + q\sqrt{d} > r + s\sqrt{d}$.

Proof. Since $p > r$ and $r \geq 1$, it follows that $p^2 > r^2$. We can rewrite equation (16) as $p^2 - r^2 = d(q^2 - s^2)$. Since $p^2 - r^2 > 0$ and $d > 0$, it follows that $q^2 - s^2 > 0$, and $q^2 > s^2$. Therefore, $q > s$.

Next, we have $p > r$ and $q > s$. Since $\sqrt{d}$ is positive, $q\sqrt{d} > s\sqrt{d}$. It follows that $p + q\sqrt{d} > r + s\sqrt{d}$. □

Therefore, we now define x_1 and y_1 so that both are positive integers and x_1 is the smallest positive integer x satisfying the equation $x^2 - d^2 = 1$. We know from Theorem 3 that y_1 is the smallest positive integer y satisfying the equation, so (x_1, y_1) is the smallest positive integer solution to $x^2 - dy^2 = 1$.

3.3 Smallest is Fundamental

In this section, we will show that any arbitrary positive integer solution of $x^2 - dy^2 = 1$ can be obtained from the smallest positive integer solution. Specifically, suppose that $u > 0$, $v > 0$, and $u^2 - dv^2 = 1$. We will show that there exists a positive integer m such that $u + v\sqrt{d} = (x_1 + y_1\sqrt{d})^m$.

Since x_1 is the smallest positive integer satisfying $x^2 - dy^2 = 1$, it must be true that $u \geq x_1$. If $u > x_1$, then by Theorem 3, $u + v\sqrt{d} > x_1 + y_1\sqrt{d}$. If $u = x_1$, then clearly $v = y_1$, and $u + v\sqrt{d} = x_1 + y_1\sqrt{d}$. Therefore, we have

$$u + v\sqrt{d} \geq x_1 + y_1\sqrt{d} \tag{17}$$

Next, we will define the positive integer m by the condition

$$\left(x_1 + y_1\sqrt{d}\right)^m \leq \left(u + v\sqrt{d}\right) < \left(x_1 + y_1\sqrt{d}\right)^{m+1} \tag{18}$$

That is, the m^{th} solution generated from (x_1, y_1) is the largest solution not exceeding $(u.v)$. Another way of stating equation (18) is

$$x_m + y_m\sqrt{d} \leq u + v\sqrt{d} < x_{m+1} + y_{m+1}\sqrt{d}$$

We will now assemble an important inequality in three parts. First, consider $(x_1 + y_1\sqrt{d})^{-m}$:

$$(x_1 + y_1\sqrt{d})^{-m} = \frac{1}{(x_1 + y_1\sqrt{d})^m} \cdot \frac{(x_1 - y_1\sqrt{d})^m}{(x_1 - y_1\sqrt{d})^m} = \frac{(x_1 - y_1\sqrt{d})^m}{(x_1^2 - dy_1^2)^m} \tag{19}$$

Since $x_1^2 - dy_1^2 = 1$, the denominator in (19) is 1, and we have

$$(x_1 + y_1\sqrt{d})^{-m} = (x_1 - y_1\sqrt{d})^m$$

Therefore,

$$(u + v\sqrt{d})(x_1 + y_1\sqrt{d})^{-m} = (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^m \tag{20}$$

Second, the following begins with the left inequality of (18):

$$\begin{aligned} (x_1 + y_1\sqrt{d})^m &\leq (u + v\sqrt{d}) \\ (x_1 + y_1\sqrt{d})^m(x_1 + y_1\sqrt{d})^{-m} &\leq (u + v\sqrt{d})(x_1 + y_1\sqrt{d})^{-m} \\ 1 &\leq (u + v\sqrt{d})(x_1 + y_1\sqrt{d})^{-m} \end{aligned} \tag{21}$$

Third, the following begins with the right inequality of (18):

$$\begin{aligned} (u + v\sqrt{d}) &< (x_1 + y_1\sqrt{d})^{m+1} \\ (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^m &< (x_1 + y_1\sqrt{d})^{m+1}(x_1 - y_1\sqrt{d})^m \\ (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^m &< (x_1 + y_1\sqrt{d})^{m+1}(x_1 + y_1\sqrt{d})^{-m} \\ (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^m &< (x_1 + y_1\sqrt{d}) \end{aligned} \tag{22}$$

Combining equation (20) with inequalities (21) and (22), we have the following inequality:

$$1 \leq (u + v\sqrt{d})(x_1 + y_1\sqrt{d})^{-m} = (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^m < (x_1 + y_1\sqrt{d}) \tag{23}$$

Inequality (23) is key to the rest of the proof. Specifically, we will show that the leftmost inequality is in fact an equality. That is, we will show that $1 = (u + v\sqrt{d})(x_1 + y_1\sqrt{d})^{-m}$.

3.4 Define a and b

Suppose that a and b are integers determined by

$$a + b\sqrt{d} = (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^m \tag{24}$$

We will make three observations. First, we will show that $a^2 - db^2 = 1$.

$$\begin{aligned} a + b\sqrt{d} &= (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^m \\ a + b\sqrt{d} &= (u + v\sqrt{d})(x_m - y_m\sqrt{d}) \\ a + b\sqrt{d} &= (ux_m - dvy_m) + \sqrt{d}(vx_m - uy_m) \end{aligned} \tag{25}$$

By equation (25), we can see that $a^2 - db^2 = 1$ as follows:

$$\begin{aligned} a^2 - db^2 &= (ux_m - dvy_m)^2 - d(vx_m - uy_m)^2 \\ &= \Big[(ux_m - dvy_m) + \sqrt{d}(vx_m - uy_m)\Big]\Big[(ux_m - dvy_m) - \sqrt{d}(vx_m - uy_m)\Big] \\ &= (u + v\sqrt{d})(x_m - y_m\sqrt{d})(x_m + y_m\sqrt{d})(u - v\sqrt{d}) \\ &= (u^2 - dv^2)(x_m^2 - dy_m^2) \\ &= 1 \end{aligned}$$

Second, we will show that $a - b\sqrt{d} = (a + b\sqrt{d})^{-1} > 0$. To begin,

$$\begin{aligned} a^2 - db^2 &= 1 \\ (a + b\sqrt{d})(a - b\sqrt{d}) &= 1 \\ (a - b\sqrt{d}) &= (a + b\sqrt{d})^{-1} \end{aligned} \tag{26}$$

From inequality (23), we know that $1 \leq (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^m$. Combining this with the definition of $a + b\sqrt{d}$ from (24), we see that $1 \leq a + b\sqrt{d}$ which implies that $a + b\sqrt{d}$ is positive. The multiplicative inverse of $a + b\sqrt{d}$ must also be positive, so from equation (26), we see

$$(a - b\sqrt{d}) = (a + b\sqrt{d})^{-1} > 0. \tag{27}$$

Third, we will show that $a - b\sqrt{d} \leq 1 \leq a + b\sqrt{d}$. We know from equation (26) that $(a + b\sqrt{d})(a - b\sqrt{d}) = 1$, and we just stated that $1 \leq (a + b\sqrt{d})$. The multiplicative inverse of $a + b\sqrt{d}$, which is $a - b\sqrt{d}$, must be less than one. Threrefore,

$$a - b\sqrt{d} \leq 1 \leq a + b\sqrt{d}. \tag{28}$$

This completes our three observations about a and b.

In order for the inequality (28) to hold, b must be greater than or equal to zero. Here's why:

$$\begin{aligned} a - b\sqrt{d} &\leq a + b\sqrt{d} \\ -b\sqrt{d} &\leq b\sqrt{d} \\ 0 &\leq 2b\sqrt{d} \\ 0 &\leq b \end{aligned}$$

From inequality (27), we have $a - b\sqrt{d} > 0$ which implies $a > b\sqrt{d}$. Since $b \geq 0$, it follows that $b\sqrt{d} \geq 0$, and $a > 0$. Therefore, we have the following conditions on a and b:

$$a > 0 \qquad \text{and} \qquad b \geq 0. \tag{29}$$

3.5 Obtain a Contradiction

By equation (24) and inequality (22), we have:

$$\begin{aligned} &a + b\sqrt{d} = (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^m < (x_1 + y_1\sqrt{d}) \\ &a + b\sqrt{d} < x_1 + y_1\sqrt{d} \end{aligned} \tag{30}$$

Since $a + b\sqrt{d} \not> x_1 + y_1\sqrt{d}$, then by the contrapositive of Theorem 3, a and b are not both positive integers. (Note that everything else in the hypothesis of 3 must be true: we defined x_1 and y_1 to be positive integers, and we know that $a^2 + b^2\sqrt{d} = x_1^2 + y_1^2\sqrt{d} = 1$. Additionally, if a is positive, $a > x_1$ since x_1 is the smallest x-value that satisfies $x^2 - dy^2 = 1$ and $a \neq x_1$ since $a = x_1$ would imply $a + b\sqrt{d} = x_1 + y_1\sqrt{d}$, which is false.) We know that $a > 0$ and $b \geq 0$ from equation (29). The only way to satisfy these conditions and make a and b not both positive is to let $b = 0$. In this case, $a = 1$ since $a^2 - db^2 = 1$. Therefore, by the defintion of a and b in equation (24), we have

$$\begin{aligned} a + b\sqrt{d} &= (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^m \\ 1 &= (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^m \\ 1 &= (u + v\sqrt{d})(x_1 + y_1\sqrt{d})^{-m}. \end{aligned} \tag{31}$$

By equation (31), $(u + v\sqrt{d}) = (x_1 + y_1\sqrt{d})^m$. We have now proved the following theorem:

Theorem 4. *If $(x, y) = (u, v)$ is a positive integer solution of $x^2 - dy^2 = 1$, then there exists a positive integer m such that $u + v\sqrt{d} = (x_1 + y_1\sqrt{d})^m$, where (x_1, y_1) is the fundamental solution of $x^2 - dy^2 = 1$.*

Proof. The proof is contained in section 3.3. □

4 What About $k \neq 1$?

We have proved the existence of a fundamental solution for equations of the form $x^2 - dy^2 = 1$, but what happens for other values of k? Sometimes solutions exist for particular values of d and k, and other times no solution can be found. With a definition and a theorem we can quickly identify many Pell Equations that have no solution at all.

4.1 Identifying Unsolvable Pell Equations

Definition 2. *An integer a is a **quadratic residue modulo** m if there exists an integer n, $0 < n < m$, such that $n^2 \equiv a \pmod{m}$. If no such integer n exists, then a is a **quadratic nonresidue modulo** m.*

Theorem 5. *If k is a quadratic nonresidue modulo d, then the Pell Equation $x^2 - dy^2 = k$ has no integer solution.*

Proof. First, rewrite the Pell Equation as:

$$y^2 = \frac{x^2 - k}{d}. \tag{32}$$

The right-hand side of equation (32) must be an integer if it is to be a perfect square. This implies that $x^2 - k$ must be divisible by d, or $x^2 - k \equiv 0 \pmod{d}$. In other words, x can only be a solution if $x^2 \equiv k \pmod{d}$. But this can only happen if k is a quadratic residue modulo d. If k is a quadratic nonresidue modulo d, then no integer x exists such that $x^2 \equiv k \pmod{d}$, and there cannot possibly be an integer y that satisfies equation (32). Therefore, the Pell Equation $x^2 - dy^2 = k$ has no integer solution if k is a quadratic nonresidue modulo d. □

Theorem 5 can identify Pell Equations for which no integer solution exists. The inverse of Theorem 5 is not true. For example, $7 \equiv 1$ is a quadratic residue modulo 3, but the equation $x^2 - 3y^2 = 7$ does not have an integer solution.[1]

Additionally, the proof of Theorem 5 can help us search for solutions to a Pell Equation. Suppose we wish to look for a solution to $x^2 - dy^2 = k$ by choosing an x-value and checking to see if the corresponding y-value is an integer. Which x-values should we test? Provided that k is a quadratic residue modulo d, the proof above suggests that we should only choose x-values whose square is congruent to k modulo d. Our task is especially easy if d is a prime, say $d = p$. Since $\mathbb{Z}_p$, the set of integers modulo p, is a field, there are exactly two integers in $\mathbb{Z}_p$ whose squares are congruent to k modulo d. Specifically, if one of these two integers is m, the other is $p - m$. Therefore, the set of x-values that make the right-hand side of equation (32) an integer are:

$$\{m, p - m, p + m, 2p - m, 2p + m, 3p - m, \ldots\}$$

[1] The fact that $x^2 - 3y^2 = 7$ has no solution can be verified by considering the integers modulo 4. The only quadratic residues modulo 4 are 0 and 1, so x^2 and y^2 must each be congruent to either 0 or 1 modulo 4. In this case, $x^2 - 3y^2$ will never be congruent to 3 modulo 4. Therefore, $x^2 - 3y^2 \neq 7$.

Our task would then be to test each of these values until we (hopefully) find one that makes $(x^2 - k)/d$ a perfect square.

4.2 If k is a Square

While the previous section identified many Pell Equations without solutions, we can also identify many Pell Equations with $k \neq 1$ that have solutions. Consider the following theorem:

Theorem 6. *If k is a perfect square, then the Pell Equation $x^2 - dy^2 = k$ is solvable in integers for all positive, nonsquare integers d.*

Proof. Since k is a perfect square, let $k = m^2$. Theorem 1 says that the equation $x^2 - dy^2 = 1$ is solvable in integers for all positive, nonsquare integers d. Let (u, v) be a solution, and we have:

$$u^2 - dv^2 = 1 \tag{33}$$

Multiply both sides of equation (33) by m^2 to obtain:

$$\begin{aligned} m^2(u^2 - dv^2) &= 1 \cdot m^2 \\ m^2u^2 - dm^2v^2 &= m^2 \\ (mu)^2 - d(mv)^2 &= k \end{aligned}$$

Therefore, (mu, mv) is a solution to $x^2 - dy^2 = k$ where $x = m^2$. We see that beginning with any solution of $x^2 - dy^2 = 1$ we can produce a solution of $x^2 - dy^2 = k$ simply by multiplying our given solution by m. □

In fact, Pell Equations with k square have infinitely many solutions. Pell Equations where $k = 1$ have infinitely many solutions, each of which corresponds to a solution in the case where k is a square.

5 Investigation of $x^2 - dy^2 = 4$

Having proved that equations of the form $x^2 - dy^2 = 4$ have integer solutions, we will now investigate patterns that occur in such solutions. Since $4 = 2^2$, we know by Theorem 6 that if (u, v) is a solution of $x^2 - dy^2 = 1$, then $(2u, 2v)$ is a solution of $x^2 - dy^2 = 4$. This method of finding solutions obtains only even solutions. Might odd solutions ever exist to Pell Equations with $k = 4$? The following theorem limits the values of d for which odd solutions might appear:

Theorem 7. *If $x^2 - dy^2 = 4$ can be solved for odd integers x and y, then $d \equiv 5 \pmod 8$.*

Proof. Let x and y be odd integers such that $x^2 - dy^2 = 4$. Note that the square of any odd integer is congruent to 1 (mod 8), so $x^2 \equiv y^2 \equiv 1 \pmod 8$.

$$\begin{aligned} x^2 - dy^2 &= 4 \\ 1 - d &\equiv 4 \pmod 8 \\ -d &\equiv 3 \pmod 8 \\ d &\equiv 5 \pmod 8 \end{aligned}$$

Therefore, $d \equiv 5 \pmod 8$. □

Theorem 7 says that if odd solutions exist, then $d \equiv 5 \pmod 8$, but it does not provide any examples of odd solutions. We will investigate equations $x^2 - dy^2 = 4$ with $d \equiv 5 \pmod 8$ to see if odd solutions actually exist.

5.1 Cases when $d \equiv 5 \pmod 8$

It is not difficult to find odd integers x and y that satisfy an equation of the form $x^2 - dy^2 = 4$ with $d \equiv 5 \pmod 8$. Considering the case $d = 5$, we find that the first solution is $x = 3$, $y = 1$. The eleven smallest positive integer solutions appear in Table 1.

x	y
3	1
7	3
18	8
47	21
123	55
322	144
843	377
2207	987
5778	2584
15127	6765

Table 1: Solutions to $x^2 - 5y^2 = 4$

Observe in Table 1 that every third solution is even, while the other solutions are odd. Furthermore, the even solutions are those guaranteed by Theorem 6; that is, they are twice the integer solutions of $x^2 - 5y^2 = 1$. For example, $(18, 8)$ is a solution of $x^2 - 5y^2 = 4$, and $(9, 4)$ is a solution of $x^2 - 5y^2 = 1$. Does this pattern of odd and even solutions continue, and does it exist in the solutions for other Pell Equations with $d \equiv 5 \pmod 8$ and $k = 4$? Examining the solutions to equations with $d = 13$ and $d = 21$ (see Tables 2 and 3), we again see the pattern of two odd solutions followed by one even solution. Again, each even solution corresponds to a solution of the equation with $k = 1$. Why might this be?

x	y
11	3
119	33
1298	360
14159	3927
154451	42837
1684802	467280
18378371	5097243
200477279	55602393
2186871698	606529080

Table 2: Solutions to $x^2 - 13y^2 = 4$

x	y
5	1
23	5
110	24
527	115
2525	551
12098	2640
57965	12649
277727	60605
1330670	290376
6375623	1391275

Table 3: Solutions to $x^2 - 21y^2 = 4$

5.2 Odd-Even Solution Patterns

In this section, we will use the convention that (x_1, y_1) is the smallest positive integer solution to $x^2 - dy^2 = 4$. Suppose that (x_n, y_n) satisfies $x_n^2 - dy_n^2 = 4^n$. Then,

$$\begin{aligned}
(x_1^2 - dy_1^2)(x_n^2 - dy_n^2) &= 4 \cdot 4^n \\
(x_1 + y_1\sqrt{d})(x_n + y_n\sqrt{d})(x_1 - y_1\sqrt{d})(x_n - y_n\sqrt{d}) &= 4^{n+1} \\
\Big((x_1x_n + dy_1y_n) + (x_1y_n + x_ny_1)\sqrt{d}\Big)\Big((x_1x_n + dy_1y_n) - (x_1y_n + x_ny_1)\sqrt{d}\Big) &= 4^{n+1} \\
(x_1x_n + dy_1y_n)^2 - d(x_1y_n + x_ny_1)^2 &= 4^{n+1}
\end{aligned}$$

Therefore, we see that solutions (x_n, y_n) of $x_n^2 - dy_n^2 = 4^n$ can be found recursively by

$$x_{n+1} = x_1x_n + dy_1y_n \qquad \text{and} \qquad y_{n+1} = x_1y_n + x_ny_1. \tag{34}$$

Note that since (x_n, y_n) satisfy $x_n^2 - dy_n^2 = 4^n$, solutions to $x^2 - dy^2 = 4$ are given by $\left(\frac{x_n}{2^{n-1}}, \frac{y_n}{2^{n-1}}\right)$.

The following theorem, then, explains the pattern of odd and even solutions that we have seen in some Pell Equations with $d \equiv 5 \pmod 8$ and $k = 4$:

Theorem 8. *Suppose that $d \equiv 5 \pmod 8$ and the smallest positive integer solution of $x^2 - dy^2 = 4$ is (x_1, y_1), with x_1 and y_1 both odd. With x_n and y_n as defined in equation (34), the first solution to be divisible by 2^n occurs at $n = 3$ and provides a solution of $x^2 - dy^2 = 1$.*

Proof. First, we have $x_1^2 - dy_1^2 = 4$ with x_1 and y_1 both odd. By equation (34) and the fact that the square of any odd integer is congruent to 1 (mod 8), x_2 and y_2 are congruent to:

$$\begin{aligned} x_2 &\equiv x_1^2 + 5y_1^2 \equiv 6 \\ y_2 &\equiv 2x_1y_1 \equiv 2 \text{ or } 6 \end{aligned}$$

In either case, x_2 and y_2 contain exactly one factor of two, so we can divide by two and obtain $\left(\frac{x_2}{2}\right)^2 - d\left(\frac{y_2}{2}\right)^2 = 4$, and we have the second odd solution to $x^2 - dy^2 = 4$.

Next, x_3 and y_3 are congruent to:

$$\begin{aligned} x_3 &\equiv x_1x_2 + 5y_1y_2 \equiv x_1(x_1^2 + 5y_1^2) + 5y_1(2x_1y_1) \equiv x_1^3 + 5x_1y_1^2 + 10x_1y_1^2 \\ &\equiv x_1 + 5x_1 + 2x_1 \equiv 8x_1 \equiv 0 \\ \text{and} \\ y_3 &\equiv y_1x_2 + x_1y_2 \equiv y_1(x_1^2 + 5y_1^2) + x_1(2x_1y_1) \equiv x_1^2y_1 + 5y_1^3 + 2x_1^2y_1 \\ &\equiv y_1 + 5y_1 + 2y_1 \equiv 8y_1 \equiv 0 \end{aligned}$$

We see that x_3 and y_3 both contain a factor of 2^3. Thus, we can divide them by 4 to obtain a solution to $x^2 - dy^2 = 4$, or by 8 to obtain a solution to $x^2 - dy^2 = 1$. □

Furthermore, we can observe that x_3 and y_3 do not both contain factors of 16. If they did, then $x_3/8$ and $y_3/8$ would both be even, and we would not have a solution of $x^2 - dy^2 = 1$. Since $\left(\frac{x_3}{8}\right)^2 - d\left(\frac{y_3}{8}\right)^2 = 1$, one of x_3 and y_3 has a factor of 8 and not 16.

The next theorem shows that if the initial solution of $x^2 - dy^2 = 4$ is odd, then every third solution corresponds to a solution of $x^2 - dy^2 = 1$.

Theorem 9. *If x_n and y_n are solutions of $x_n^2 - dy_n^2 = 4^n$, with $d \equiv 5 \pmod 8$, and x_1 and y_1 (the smallest such solution) are both odd, and x_k and y_k satisfy*

$$\left(\frac{x_k}{2^k}\right)^2 - d\left(\frac{y_k}{2^k}\right)^2 = 1,$$

then x_{k+3} and y_{k+3} are the next solution to provide a solution to $x^2 - dy^2 = 1$.

Proof. As in the previous proof, we use the recursion defined in equation (34) to obtain successive solutions to $x_n^2 - dy_n^2 = 4^n$. We obtain the following congruences:

$$\begin{aligned} x_{k+1} &\equiv x_1x_k + 5y_1y_k \\ y_{k+1} &\equiv x_1y_k + y_1x_k \\ \\ x_{k+2} &\equiv 6x_k + 2x_1y_1y_k \\ y_{k+2} &\equiv 2x_1x_ky_1 + 6y_k \\ \\ x_{k+3} &\equiv 8x_1x_k + 8y_1y_k \equiv 0 \\ y_{k+3} &\equiv 8x_ky_1 + 8x_1y_k \equiv 0 \end{aligned}$$

Since $\left(\frac{x_k}{2^k}\right)^2 - d\left(\frac{y_k}{2^k}\right)^2 = 1$, we know that x_k and y_k each contain k multiples of 2, and they do not both contain $k+1$ multiples of 2. With the first iteration, x_{k+1} and y_{k+1} both contain exactly k multiples of 2, providing the odd solution $\left(\frac{x_{k+1}}{2^k}, \frac{y_{k+1}}{2^k}\right)$ to $x^2 - dy^2 = 4$. At the second iteration, we gain a factor of 2, so x_{k+2} and y_{k+2} both contain exactly $k+1$ factors of 2, providing a solution to $x^2 - dy^2 = 4$. At the third iteration, the coefficients of 8 indicate that both x_{k+3} and y_{k+3} have three more factors of 2 than x_k and y_k. We see that $\frac{x_{k+3}}{2^{k+3}}$ and $\frac{y_{k+3}}{2^{k+3}}$ are both integers, and they satisfy $x^2 - dy^2 = 1$. Therefore, every third solution of $x^2 - dy^2 = 4$ is even, and can be divided by two to obtain a solution of $x^2 - dy^2 = 1$. □

Corollary 1. *If x_1 and y_1 are both odd, then x_{3i} and y_{3i} always provide a solution to $x^2 - dy^2 = 1$ for any positive integer i.*

Proof. Theorem 8 says that if x_1 and y_1 are both odd, then the first even solution of $x^2 - dy^2 = 4$ is (x_3, y_3). Theorem 9 says that if (x_k, y_k) is an even solution of $x^2 - dy^2 = 4$, then the next even solution is (x_{k+3}, y_{k+3}). Therefore, all of the even solutions occur with subscripts that are multiples of 3. In other words, (x_{3i}, y_{3i}) is always an even solution, so it can be divided by 2 to obtain $\left(\frac{x_{3i}}{2}, \frac{y_{3i}}{2}\right))$, which is a solution of $x^2 - dy^2 = 1$. □

5.3 More Patterns in Solutions

If we examine solutions to Pell Equations $x^2 - dy^2 = 4$ for many values of d, $d \equiv 5 \pmod 8$, we encounter many patterns. Table 4 lists the smallest positive integer solution for the first 30 Pell Equations of this form ($5 \leq d \leq 237$). First, we observe that for some values of d, the smallest solution is even. These cases are indicated in bold in Table 4. In these cases, Theorems 8 and 9 do not apply, since they require that x_1 and y_1 be odd. The author does not know why the smallest positive integer solution of $x^2 - dy^2 = 4$ is even for some values of $d \equiv 5 \pmod 8$, but such values of d appear to be scattered haphazardly through Table 4. Additionally, in these cases, the only solutions to $x^2 - dy^2 = 4$ are those that are twice the solutions to $x^2 - dy^2 = 1$.

Notice that each odd integer greater than 1 appears as an x-value in the solution for some d in the table. Also notice that these odd integers also appear as y-values in the solution for

d	x	y	d	x	y	d	x	y
5	3	1	85	83	9	165	13	1
13	11	3	93	29	3	173	171	13
21	5	1	**101**	**402**	**40**	181	1703027	126585
29	27	5	109	68123	6525	**189**	**110**	**8**
37	**146**	**24**	117	11	1	**197**	**786**	**56**
45	7	1	125	123	11	205	43	3
53	51	7	133	173	15	213	73	5
61	1523	195	**141**	**190**	**16**	221	15	1
69	25	3	149	3723	305	229	227	15
77	9	1	157	45371	3621	237	77	5

Table 4: Solutions to $x^2 - dy^2 = 4$ for $d \equiv 5 \pmod 8$

d following the row in which they appeared as an x-value. We can explain these occurrances by the following two theorems:

Theorem 10. *Let m be odd and $d = m^2 - 4$. Then $d \equiv 5 \pmod 8$ and $(x, y) = (m, 1)$ is the solution to $x^2 - dy^2 = 4$.*

Proof. Since m is odd, $m^2 \equiv 1 \pmod 8$. Then $d = m^2 - 4 \equiv -3 \equiv 5 \pmod 8$. Let $(x, y) = (m, 1)$, and it follows that:

$$x^2 - dy^2 = m^2 - (m^2 - 4)(1)^2 = m^2 - m^2 + 4 = 4$$

Therefore, $(x, y) = (m, 1)$ is the solution of $x^2 - dy^2 = 4$ with $d = m^2 - 4$. □

The previous proof explains why the list of solutions of $x^2 - dy^2 = 4$, $d \equiv 5 \pmod 8$, contains solutions $(m, 1)$ for every odd integer m (see Table 4). The next theorem explains the solutions $(m^2 + 2, m)$.

Theorem 11. *Let m be odd and $d = m^2 + 4$. Then $d \equiv 5 \pmod 8$ and $(x, y) = (m^2 + 2, m)$ is the solution to $x^2 - dy^2 = 4$.*

Proof. Since m is odd, $m^2 \equiv 1 \pmod 8$. Then $d = m^2 + 4 \equiv 5 \pmod 8$. Let $(x, y) = (m^2 + 2, m)$, and it follows that:

$$x^2 - dy^2 = (m^2 + 2)^2 - (m^2 + 4)m^2 = m^4 + 4m^2 + 4 - m^4 - 4m^2 = 4$$

Therefore, $(x, y) = (m^2 + 2, m)$ is the solution of $x^2 - dy^2 = 4$ with $d = m^2 + 4$. □

6 The Fundamental Solution Revisited

We will now prove the most exciting result of our work with $x^2 - dy^2 = 4$. There exists a fundamental solution to $x^2 - dy^2 = 4$, $d \equiv 5 \pmod 8$ from which all other solutions can be obtained. This proof is similar to the proof from section 3 of the existence of a fundamental solution for equations of the form $x^2 - dy^2 = 1$.

6.1 Preliminary Work

From any solution to $x^2 - dy^2 = 4$, we can obtain another solution as follows. Let (x_1, y_1) be a solution. Then,

$$\begin{aligned} x_1^2 - dy_1^2 &= 4 \\ (x_1 + y_1\sqrt{d})(x_1 - y_1\sqrt{d}) &= 4 \\ (x_1 + y_1\sqrt{d})^2(x_1 - y_1\sqrt{d})^2 &= 4^2 \\ \left(x_1^2 + 2x_1y_1\sqrt{d} + dy_1^2\right)\left(x_1^2 - 2x_1y_1\sqrt{d} + dy_1^2\right) &= 4^2 \\ \left((x_1^2 + dy_1^2) + (2x_1y_1)\sqrt{d}\right)\left((x_1^2 + dy_1^2) - (2x_1y_1)\sqrt{d}\right) &= 4^2 \\ \left(x_1^2 + dy_1^2\right)^2 - d\left(2x_1y_1\right)^2 &= 4^2 \\ \left(\frac{x_1^2 + dy_1^2}{2}\right)^2 - d\left(\frac{2x_1y_1}{2}\right)^2 &= 4 \end{aligned}$$

Therefore, for any solution (x_1, y_1) of $x^2 - dy^2 = 4$, define x_n and y_n such that

$$x_n + y_n\sqrt{d} = \frac{(x_1 + y_1\sqrt{d})^n}{2^{n-1}}. \tag{35}$$

It follows that $(x_n - y_n\sqrt{d}) = \frac{(x_1 - y_1\sqrt{d})^n}{2^{n-1}}$ and $x_n^2 - dy_n^2 = 4$. Moreover, $x_{n+1} > x_n$ and $y_{n+1} > y_n$). As in section 3, this suggests that if x_1 and y_1 are to generate all the other solutions, then they should be as small as possible. Therefore, we will define (x_1, y_1) to be a positive integer solution to $x^2 - dy^2 = 4$, $d \equiv 5 \pmod 8$, with x_1 as small as possible.

Recall from Theorem 3 that if (p, q) and (r, s) are both positive integer solutions to $x^2 - dy^2 = 4$ and $p > r$, then $q > s$ and $p + q\sqrt{d} > r + s\sqrt{d}$. This helps us order the solutions of $x^2 - dy^2 = 4$, since the solution with the m^{th}-smallest x-value also contains the m^{th}-smallest y-value.

6.2 An Arbitrary Solution (u, v)

Suppose that (u, v) is an arbitrary positive integer solution of $x^2 - dy^2 = 4$. Since x_1 is the smallest positive integer x satisfying $x^2 - dy^2 = 4$, then $u \geq x_1$. If $u > x_1$, then $u + v\sqrt{d} > x_1 + y_1\sqrt{d}$ by the above paragraph. If $u = x_1$, then clearly $v = y_1$ and $u + v\sqrt{d} = x_1 + y_1\sqrt{d}$. Therefore, we have $u + v\sqrt{d} \geq x_1 + y_1\sqrt{d}$.

As in Section 3, we define the positive integer m so that the m^{th} solution generated from (x_1, y_1) is the largest not exceeding (u, v). That is,

$$\begin{gathered} x_m + y_m\sqrt{d} \leq u + v\sqrt{d} < x_{m+1} + y_{m+1}\sqrt{d} \\ \frac{(x_1 + y_1\sqrt{d})^m}{2^{m-1}} \leq u + v\sqrt{d} < \frac{(x_1 + y_1\sqrt{d})^{m+1}}{2^m} \end{gathered} \tag{36}$$

Working with inequality (36):

$$\begin{aligned}
\frac{(x_1 + y_1\sqrt{d})^m}{2^{m-1}} &\leq u + v\sqrt{d} < \frac{(x_1 + y_1\sqrt{d})^{m+1}}{2^m} \\
\frac{(x_1 - y_1\sqrt{d})^m}{2^m}\frac{(x_1 + y_1\sqrt{d})^m}{2^{m-1}} &\leq (u + v\sqrt{d})\frac{(x_1 - y_1\sqrt{d})^m}{2^m} < \frac{(x_1 + y_1\sqrt{d})^{m+1}}{2^m}\frac{(x_1 - y_1\sqrt{d})^m}{2^m} \\
\frac{4^m}{2^{2m-1}} &\leq (u + v\sqrt{d})\frac{(x_1 - y_1\sqrt{d})^m}{2^m} < (x_1 + y_1\sqrt{d})\frac{4^m}{4^m} \\
2 &\leq (u + v\sqrt{d})\frac{(x_1 - y_1\sqrt{d})^m}{2^m} < x_1 + y_1\sqrt{d} \qquad (37)
\end{aligned}$$

Our task is now to show that the left-hand inequality of (37) is, in fact, an equality.

6.3 Define a and b

Suppose that a and b are the positive integers determined by

$$a + b\sqrt{d} = (u + v\sqrt{d})\frac{(x_1 - y_1\sqrt{d})^m}{2^m}. \qquad (38)$$

In Section 3.3, it was obvious that a and b must be integers, but this time it is not obvious, since we are dividing by 2^m. We can prove that a and b must be integers as follows:

$$\begin{aligned}
a + b\sqrt{d} &= (u + v\sqrt{d})\frac{1}{2} \cdot \frac{(x_1 - y_1\sqrt{d})^m}{2^{m-1}} \\
a + b\sqrt{d} &= \frac{1}{2}(u + v\sqrt{d})(x_m - y_m\sqrt{d}) \\
a + b\sqrt{d} &= \frac{ux_m - dvy_m}{2} + \frac{vx_m - uy_m}{2}\sqrt{d}
\end{aligned}$$

Since (u, v) and (x_m, y_m) both satisfy $x^2 - dy^2 = 4$ and $d \equiv 5 \pmod 8$, u and v have the same parity, and x_m and y_m have the same parity. If either (u, v) or (x_m, y_m) are even, then $(ux_m - dvy_m, vx_m - uy_m)$ is even. Otherwise, both (u, v) and (x_m, y_m) are both odd, but $(ux_m - dvy_m, vx_m - uy_m)$ is still even. Therefore, $a = \frac{ux_m - dvy_m}{2}$ and $b = \frac{vx_m - uy_m}{2}$ are both integers.

Consider $a^2 - db^2$:

$$\begin{aligned}
a^2 - db^2 &= \left(\frac{ux_m - dvy_m}{2}\right)^2 - d\left(\frac{vx_m - uy_m}{2}\right)^2 \\
&= \frac{1}{4}\left((ux_m - dvy_m) + \sqrt{d}(vx_m - uy_m)\right)\left((ux_m - dvy_m) - \sqrt{d}(vx_m - uy_m)\right) \\
&= \frac{1}{4}\left((u + v\sqrt{d})(x_m - y_m\sqrt{d})\right)\left((x_m + y_m\sqrt{d})(u - v\sqrt{d})\right) \\
&= \frac{1}{4}(u^2 - dv^2)(x_m^2 - dy_m^2) \\
&= \frac{1}{4} \cdot 4 \cdot 4 \\
&= 4
\end{aligned}$$

Therefore, $x^2 - db^2 = 4$.

Since $a^2 - db^2 = 4$, we have $(a - b\sqrt{d})(a + b\sqrt{d}) = 4$, so $a + b\sqrt{d}$ and $a - b\sqrt{d}$ have the same sign. However, $2 \leq a + b\sqrt{d}$ by inequality (37). Therefore, $a + b\sqrt{d}$ and $a - b\sqrt{d}$ are both positive, and since their product is 4, we have:

$$0 < a - b\sqrt{d} \leq 2 \qquad \text{and} \qquad 2 \leq a + b\sqrt{d}. \tag{39}$$

We will now show that a must be positive and b must be nonnegative. From the inequalities in (39), we have:

$$\begin{aligned}
a - b\sqrt{d} &\leq a + b\sqrt{d} \\
-b\sqrt{d} &\leq b\sqrt{d} \\
0 &\leq 2b\sqrt{d} \\
0 &\leq b
\end{aligned}$$

Therefore, b is nonnegative. Since $0 < a - b\sqrt{d}$, we have $b\sqrt{d} < a$, and it follows that $0 \leq b\sqrt{d} < a$. This implies that $0 < a$, so a is positive.

6.4 Obtain a Contradiction

We will now obtain a contradiction to complete our proof. Combining the definition of a and b from equation (38) with inequality (36), we have $a + b\sqrt{d} < x_1 + y_1\sqrt{d}$. This does not satisfy the conclusion of Theorem 3, so something in the hypothesis of the theorem must be false. That is, it cannot be true that a, b, x_1, and y_1 are positive integers for which $a^2 - db^2 = 4$, $x_1^2 - dy_1^2 = 4$, and $a > x_1$. However, it *is* true that $a^2 - db^2 = 4$ and $x_1^2 - dy_1^2 = 4$, and a, x_1, and y_1 are positive integers. We know that since a is a positive integer, then $a > x_1$ by the minimality of x_1. The only possibility is that b is not positive. Therefore, $b = 0$.

Since we previously showed that $a^2 - db^2 = 4$, we now see that $a = 2$. Thus, we have:

$$\begin{aligned}2 &= a + b\sqrt{d}\\ 2 &= (u + v\sqrt{d})\frac{(x_1 - y_1\sqrt{d})^m}{2^m}\\ 4 &= (u + v\sqrt{d})\frac{(x_1 - y_1\sqrt{d})^m}{2^{m-1}}.\end{aligned}$$

However, it is also true that

$$4 = x_m^2 - dy_m^2 = \frac{(x_1 - y_1\sqrt{d})^m}{2^{m-1}} \cdot \frac{(x_1 - y_1\sqrt{d})^m}{2^{m-1}}.$$

Therefore, it follows that

$$u + v\sqrt{d} = \frac{(x_1 + y_1\sqrt{d})^m}{2^{m-1}}$$

and we can finally conclude that $u + v\sqrt{d} = x_m + y_m\sqrt{d}$ by the definition of $x_n + y_n\sqrt{d}$ in equation (35). In summary, we have proved the following theorem:

Theorem 12. *If $(x, y) = (u, v)$ is a positive integer solution of $x^2 - dy^2 = 4$, with $d \equiv 5 \pmod 8$, then there exists a positive integer m such that*

$$u + v\sqrt{d} = \frac{(x_1 + y_1\sqrt{d})^m}{2^{m-1}}$$

where (x_1, y_1) is the fundamental solution of $x^2 - dy^2 = 4$.

Proof. The proof is contained in Section 6. □

Interestingly, the proof of Theorem 12 holds for any odd d, though we know from Theorem 7 that if $x^2 - dy^2 = 4$ can be solved for odd integers x and y, then $x \equiv 5 \pmod 8$.

7 Programming

In order to quickly find solutions to lots of Pell Equations, I wrote a computer program. After the user enters values of d and k, my program checks many integers x in an attempt to find one that makes y an integer. My program is somewhat more efficient than an exhaustive search that tests all positive integers x; as discussed in Section 4.1, my program only tests values of x whose square is congruent to k modulo d. Using such an exhaustive search, my program can quickly solve Pell Equations that have solutions with x less than a few billion. It is true that more sophisticated methods exist to find solutions to Pell Equations. One clever method is credited to the eleventh-century Indian mathematician Bhaskara and is the subject of a paper I wrote for Senior Math Seminar titled *Bhaskara's Method for Solving Pell Equations* [4]. The generally accepted method for solving Pell Equations today involves continued fractions, but I have not studied it.

My program, PellSolver, has two modes: it can solve a single equation or many equations at once. If the user chooses to solve a single equation, the program asks for values of d and k, as well as a maximum value of x to test. The program identifies the Pell Equation as unsolvable if k is a quadratic nonresidue modulo d. Otherwise, the program tests all values of x whose square is congruent to k modulo d, stopping when it finds an integer solution (x, y) or when x reaches the user-specified maximum. If the search is successful, the program outputs the smallest positive integer solution to the Pell Equation, as well as the amount of time it took to find the solution.

Solving many equations with a single command is useful if we wish to investigate patterns in solutions while varying d, k, or both. For example, the solutions found to Pell Equations where $d \equiv 5 \pmod 8$ and $k = 4$ in Table 4 of Section 5.3 were found using PellSolver. If the user chooses to solve many equations, the program asks for minimum and maximum values of d. If these values are different, the program asks for a step by which to increment d to obtain the next equation. For example, to solve $x^2 - dy^2 = 4$ for values of d between 5 and 45 with $d \equiv 5 \pmod 8$, the user would choose d-minimum as 5, d-maximum as 45, and d-step as 8. The program allows the user to adjust k similarly, by specifying a minumum, maximum, and a step. Lastly, the program asks for a maximum value of x as an upper limit to test. For each specified value of k, the program then attempts to solve $x^2 - dy^2 = k$ for each specified value of d. (That is, incrementing d and k is accomplished with nested loops, with k being incremented in the outer loop and d in the inner loop.)

Sample output from PellSolver follows, with user input in **bold**:

```
PellSolver Menu:
1. Solve a single equation
2. Solve many equations
3. Quit
1
We will attempt to find solutions to equations of the form x^2- dy^2 = k
Enter a value for d:
46
Enter a value for k:
1
Enter a max value for x:
10000000
Solution: x = 24335, y = 3588   found in 0 ms


PellSolver Menu:
1. Solve a single equation
2. Solve many equations
3. Quit
1
```

```
We will attempt to find solutions to equations of the form x^2- dy^2 = k
Enter a value for d:
4
ERROR: d=4 is a perfect square


PellSolver Menu:
1. Solve a single equation
2. Solve many equations
3. Quit
2

Enter a min value for d:
50
Enter a max value for d:
55
Enter a step for d:
1
Enter a min value for k:
1
Enter a max value for k:
1
Enter a max value for x:
100000000
x^2 - 50y^2 = 1 -- Solution: x = 99, y = 14
x^2 - 51y^2 = 1 -- Solution: x = 50, y = 7
x^2 - 52y^2 = 1 -- Solution: x = 649, y = 90
x^2 - 53y^2 = 1 -- Solution: x = 66249, y = 9100
x^2 - 54y^2 = 1 -- Solution: x = 485, y = 66
x^2 - 55y^2 = 1 -- Solution: x = 89, y = 12
The search took 70 milliseconds.
```

The Java source code for my program is included in Appendix A.

8 Table of Solutions

Table 5 contains the fundamental solutions of the Pell Equations $x^2 - dy^2 = 1$ for nonsquare $d < 100$.

d	x	y	d	x	y	d	x	y
2	3	2	37	73	12	69	7775	936
3	2	1	38	37	6	70	251	30
5	9	4	39	25	4	71	3480	413
6	5	2	40	19	3	72	17	2
7	8	3	41	2049	320	73	2281249	267000
8	3	1	42	13	2	74	3699	430
10	19	6	43	3482	531	75	26	3
11	10	3	44	199	30	76	57799	6630
12	7	2	45	161	24	77	351	40
13	649	180	46	24335	3588	78	53	6
14	15	4	47	48	7	79	80	9
15	4	1	48	7	1	80	9	1
17	33	8	50	99	14	82	163	18
18	17	4	51	50	7	83	82	9
19	170	39	52	649	90	84	55	6
20	9	2	53	66249	9100	85	285769	30996
21	55	12	54	485	66	86	10405	1122
22	197	42	55	89	12	87	28	3
23	24	5	56	15	2	88	197	21
24	5	1	57	151	20	89	500001	53000
26	51	10	58	19603	2574	90	19	2
27	26	5	59	530	69	91	1574	165
28	127	24	60	31	4	92	1151	120
29	9801	1820	61	1766319049	226153980	93	12151	1260
30	11	2	62	63	8	94	2143295	221064
31	1520	273	63	8	1	95	39	4
32	17	3	65	129	16	96	49	5
33	23	4	66	65	8	97	62809633	6377352
34	35	6	67	48842	5967	98	99	10
35	6	1	68	33	4	99	10	1

Table 5: Fundamental solutions to $x^2 - dy^2 = 1$ for nonsquare $d < 100$

References

[1] Barbeau, Edward J. *Pell's Equation*. Springer, 2000.

[2] "Pell, John." *Dictionary of Scientific Biography*. Vol 10, pg 495. New York: Charles Scribner's Sons.

[3] Vanden Eynden, Charles. *Elementary Number Theory*, second edition. McGraw Hill, 2001.

[4] Wright, Matthew. "Bhaskara's Method for Solving Pell Equations." 2006.

A Listing of PellSolver

```
/* class: PellSolver
 * author: Matthew Wright
 * date: 3 April 2006
 * version: 6
 */

import java.io.*;
import java.math.*;
import java.util.*;

class PellSolver
{
 public static void main(String[] args) throws IOException
 {
  boolean repeat = true;
  while(repeat)
  {
   System.out.println("PellSolver Menu:\n1. Solve a single equation\n"+
    "2. Solve many equations\n3. Quit");
   BufferedReader in = new BufferedReader(new InputStreamReader(System.in));
   int choice = (new Integer(in.readLine())).intValue();
   switch(choice)
   {
    case 1:  solveOne();
        break;
    case 2: solveMany();
        break;
    default:  repeat = false;
   }
  }//end while
 }//end main()

 //method to solve a single Pell Equation
 public static void solveOne() throws IOException
 {
  //variables
  long max;
  boolean debug = false;

  //Objects
  BufferedReader in = new BufferedReader(new InputStreamReader(System.in));
  int d, k;

  //get input
  System.out.println("We will attempt to find solutions to equations of the form"+
    "x^2- dy^2 = k");
  System.out.println("Enter a value for d: ");
  d = Integer.parseInt(in.readLine());

```

```
    //d cannot be a square
    if(Math.floor(Math.sqrt(d)) - Math.sqrt(d) == 0)
    {
      System.out.println("ERROR: d="+d+" is a perfect square\n\n");
      return;
    }

    System.out.println("Enter a value for k: ");
    k = Integer.parseInt(in.readLine());
    System.out.println("Enter a max value for x: ");
    max = Long.parseLong(in.readLine());

    //create a Pell object
    Pell eq = new Pell(d, k, true);

    //start timer
    long beginTime = System.currentTimeMillis();

    //look for a solution
    Pair solution = null;
    try
    {
       solution = eq.smartSearch(0, max);
    }
    catch(QuadraticNonresidueException e)
    {
      System.out.println("NO SOLUTION because "+k+" is a quadratic nonresidue mod "+d+"\n\n");
    }

    //stop timer
    long timeElapsed = System.currentTimeMillis() - beginTime;

    //do we have a solution?
    if(solution == null)
    {
      System.out.println("Max value reached; no solution found in "+timeElapsed+" ms\n\n");
    }
    else
    {
      System.out.println("Solution: x = "+solution.x+", y = "+solution.y+"   found in "+
        timeElapsed+" ms\n\n");
    }

  }//end solveOne()

  //method to solve many Pell Equations
  public static void solveMany() throws IOException
  {
    //variables
    int d1,   //starting value for d
        d2,    //ending value for d
        dd=1,  //d step (default is 1)
        k1,    //starting value for k
        k2,    //ending value for k
        dk=1,  //k step (default is 1)
        max;  //max value for x

    //use a BufferedReader for input
    BufferedReader in = new BufferedReader(new InputStreamReader(System.in));

    //input d
    System.out.println("\nEnter a min value for d: ");
    d1 = Integer.parseInt(in.readLine());
    System.out.println("Enter a max value for d: ");
    d2 = Integer.parseInt(in.readLine());
    if(d1 != d2)
    {
      System.out.println("Enter a step for d: ");
      dd = Integer.parseInt(in.readLine());
    }

    //input k
    System.out.println("Enter a min value for k: ");
    k1 = Integer.parseInt(in.readLine());
    System.out.println("Enter a max value for k: ");
    k2 = Integer.parseInt(in.readLine());
    if(k1 != k2)
    {
      System.out.println("Enter a step for k: ");
      dk = Integer.parseInt(in.readLine());
    }

    //input max
    System.out.println("Enter a max value for x: ");
    max = Integer.parseInt(in.readLine());

    //start timer
    long beginTime = System.currentTimeMillis();

    //loop k
    for(;k1 <= k2; k1+=dk)
    {
      //loop d
      for(int di = d1; di <= d2; di+=dd)
      {
        //make sure d is nonsquare
        if(Math.floor(Math.sqrt(di)) - Math.sqrt(di) == 0)
        {
          continue;
        }

        //create a Pell object
    Pell eq = new Pell(di, k1, true);

    //look for a solution
    Pair solution = null;
    try
    {
     solution = eq.smartSearch(0, max);
     //did we find a solution?
     if(solution == null)
     {
      System.out.println(eq+" !! Max value reached; no solution found.");
     }
     else
     {
      System.out.println(eq+" -- Solution: x = "+solution.x+", y = "+solution.y);
     }
    }
    catch(QuadraticNonresidueException e)
    {
     System.out.println(eq+" !! NO SOLUTION because "+k1+
      " is a quadratic nonresidue mod "+di);
    }
   }//end loop d
  }//end loop k

  //stop timer
  long timeElapsed = System.currentTimeMillis() - beginTime;
  System.out.println("The search took "+timeElapsed+" milliseconds.\n\n");
 }//end solveMany()
}//end class PellSolver6

class Pell
{
 //data members
 int d, k;
 boolean output;

 //constructor
 public Pell(int d, int k, boolean o)
 {
  this.d = d;
  this.k = k;
  this.output = o;
 }

 //method to exhaustively search to find the smallest positive integer solution greater
 //  than start
 //tests all values of x between start and start + max
 //returns null if no solution is found
 public Pair exhaustiveSearch(int start, long max)
 {
  boolean found = false;
  for(long x = start; x <= start+max; x++)
  {
   //show output, if necessary
   if(output && (x-start)%1000000 == 0)
   {
    System.out.println("-testing x="+x);
   }

   //test this value of x
   Pair xy = testX(x);
   if(xy == null)  //no solution
   {
    continue;
   }
   else //solution found!
   {
    return xy;
   }

  }//end for

  //no solution found
  return null;

 }//end exhaustiveSearch()

 //method to see if x is a solution to the Pell equation
 //returns the solution as a Pair (x, y) if it is a solution
 //returns null otherwise
 public Pair testX(long x)
 {
  //**first, (x^2 - k)/d must be a positive integer, that is, (x^2 - k) must be positive
  //  and congruent to 0 mod d
  if((x*x - k)%d != 0 || (x*x - k) <= 0)
  {
   return null;
  }

  //**second, (x^2 - k)/d must be a square
  long maybeSquare = (x*x - k)/d;

  //I think we might encounter with round-off error, so I prefer to work with integers
  //---->Could we lose precision while converting a long to a double?
  long rootTest = (long) Math.floor(Math.sqrt((double) maybeSquare));
  if(rootTest*rootTest == maybeSquare)
  {
   //we have a solution!
   return new Pair(x, rootTest);
  }
  rootTest++;
  if(rootTest*rootTest == maybeSquare)
  {
   //we have a solution!
   return new Pair(x, rootTest);
  }

  //not a solution
  return null;

 }//end testX()

 //method to intelligently search to find the smallest positive integer solution
 //returns null if no solution is found
 public Pair smartSearch(int start, long max) throws QuadraticNonresidueException
 {
  //if d is prime, then check to see if k is a quadratic residue mod d
  if(dPrime())
  {
   //check to see if k is a quadratic residue mod d
   int a = kPrimeQuadRes();

   //if k is a quadratic residue mod d, then test values of x congruent to +/- a (mod d)
   if(a != -1)
   {
    //for each base congruent to 0 (mod d) between start and start + max,
    //test each x equal to (base - a) or (base + a)
    //(this loop may test more values than strictly necessary at the endpoints)
    for(long base = start - (start%d); base < start + max; base += d)
    {
      //test base - a
      Pair xy;
      if(base - a > start)
      {
        xy = testX(base - a);
        if(xy != null)
        {
          //we have a solution!
          return xy;
        }
      }

      //test base + a
      if(base + a > 0)
      {
        xy = testX(base + a);
        if(xy != null)
        {
          //we have a solution!
          return xy;
        }
      }

    }//end for

    //we did not find a solution
    return null;

   }
   else  //if k is a quadratic nonresidue mod d, then there is no solution
   {
    throw(new QuadraticNonresidueException());
   }
  }
  else  //d is not prime
  {
   //find quadratic residues
   int[] a = kQuadRes();

   //if there are quadratic residues, then test values of x congruent to them (mod d)
   if(a.length > 0)
   {
    //for each base congruent to 0 (mod d) between start and start + max,
    //test each x equal to base + (a quadratic residue)
    //(this loop may test more values than strictly necessary at the endpoints)
    for(long base = start - (start%d); base < start + max; base += d)
    {
      for(int i=0; i<a.length; i++)
      {
        if(base + a[i] > 0)
        {
          Pair xy = testX(base + a[i]);
          if(xy != null)
          {
            //we have a solution!
            return xy;
          }
        }
      }
    }//end for

    //we did not find a solution
    return null;
   }
   else  //then there are no quadratic residues, so there is no solution
   {
    throw(new QuadraticNonresidueException());
   }
  }
 }//end smartSearch()


 //method to determine whether d is prime
```

```
public boolean dPrime()
{
  int sqrt = (int) Math.floor(Math.sqrt((double) this.d));
  for(int i=2; i<=sqrt; i++)
  {
    if(d%i == 0)  //then i divides n
    {
      return false;
    }

  }

  return true;
}//end dPrime()

//method to determine whether k is a quadratic residue mod d
//pre:  d must be prime, to guarantee that there are exactly two solutions to a^2
//      congruent to k (mod d)
//      specifically, a and -a (mod d)
//post: returns the smallest nonnegative integer whose square is congruent to k mod d
//      returns -1 if k is a quadratic nonresidue mod d
public int kPrimeQuadRes()
{
  int kMod = k%d;
  //kMod should not be negative
  if(kMod<0)
    kMod+=d;

  for(int i=0; i<d; i++)
  {
    if((i*i)%d == kMod)
    {
      return i;
    }
  }
  return -1;

}//end kQuadRes()

//method to find all integers (mod d) whose squares are congruent to k (mod d)
//this method will work even if k is composite
//post: returns an array of int
//      if no such integers exist, returns an array of length 0
public int[] kQuadRes()
{
  Vector v = new Vector();

  int kMod = k%d;
  //kMod should not be negative
  if(kMod<0)
    kMod+=d;
    for(int i=0; i<d; i++)
    {
      if((i*i)%d == kMod)
      {
        v.add(new Integer(i));
      }
    }

    //create array
    int[] a = new int[v.size()];
    for(int i=0; i<v.size(); i++)
    {
      a[i] = ((Integer) v.get(i)).intValue();
    }

    return a;
  }//end kQuadRes

  //method to output this Pell as a string
  public String toString()
  {
    return "x^2 - "+d+"y^2 = "+k;
  }
}//end class Pell

class Pair
{
  //data members
  public long x, y;

  //constructor
  public Pair(long x, long y)
  {
    this.x = x;
    this.y = y;
  }
}//end class Pair

//class QuadraticNonresidueException
//thrown if k turns out to be a quadratic nonresidue mod d, in which case the Pell equation
//  cannot have solutions
class QuadraticNonresidueException extends Exception
{
  public QuadraticNonresidueException()
  {
    super();
  }
}//end class QuadraticNonresidueException
```