Chapter 4
General Pell's Equation

This chapter gives the general theory and useful algorithms to find positive integer solutions (x, y) to general Pell's equation (4.1.1), where D is a nonsquare positive integer, and N a nonzero integer. There are five good methods for solving the general Pell's equation:

1. The Lagrange–Matthews–Mollin (LMM) method;
2. Brute-force search (which is good only if $|N|$ is small and the minimal positive solution to Pell's resolvent is small);
3. Use of quadratic rings;
4. The cyclic method;
5. Lagrange's system of reductions.

Of these five, we will present only the first three, with two versions for the third one. These two last algorithms are comparable in terms of effectiveness. For the cyclic method see [67] and for the Lagrange's system of reductions see [52] or [142].

4.1 General Theory

In a memoir of 1768, Lagrange gave a recursive method for solving the equation

$$x^2 - Dy^2 = N \tag{4.1.1}$$

with $\gcd(x, y) = 1$, where $D > 1$ is not a perfect square and $N \neq 0$, thereby reducing the problem to the situation where $|N| < \sqrt{D}$, in which case the positive solutions (x, y) are found among the pairs (p_n, q_n), with p_n/q_n a convergent of the simple continued fraction for $\sqrt{D}$.

It does not seem to be widely known that Lagrange also gave another algorithm in a memoir of 1770, which may be regarded as a generalization of the well-known

T. Andreescu, D. Andrica, *Quadratic Diophantine Equations*,
Developments in Mathematics 40, DOI 10.1007/978-0-387-54109-9_4

method of solving Pell's equation and negative Pell's equation presented in Section 3.3 by using the simple continued fraction for $\sqrt{D}$ (see [196]). Quadratic Reciprocity (see [21, 185] and [179] for various applications)

In what follows we will call (4.1.1) the *general Pell's equation*. First we will present the general method of finding the solutions to this equation following the presentation in [56, 112, 125, 126, 151] and [161].

Like in Section 3.5 we will consider the Pell's resolvent

$$u^2 - Dv^2 = 1. \tag{4.1.2}$$

Let $(u_n, v_n)_{n\geq 0}$ be the general solution to the equation (4.1.2) given in Theorem 3.2.1. Assume that equation (4.1.1) is solvable and let (x, y) be one of its solutions. Then

$$(u_n + v_n\sqrt{D})(x + y\sqrt{D}) = (u_n x + v_n yD) + (u_n y + v_n x)\sqrt{D}$$

and

$$(u_n x + v_n yD)^2 - D(u_n y + v_n x)^2 = (x^2 - Dy^2)(u_n^2 - Dv_n^2) = N \cdot 1 = N.$$

It follows that $(x_n, y_n)_{n\geq 0}$, where

$$x_n = xu_n + Dyv_n \quad \text{and} \quad y_n = yu_n + xv_n \tag{4.1.3}$$

satisfies the general Pell's equation. Hence every initial solution to (4.1.1) generates its own family of infinitely many solutions.

This method of generating solutions is called the *multiplication principle*.

The main problem here is to decide whether or not two different initial solutions generate different general solutions described above.

We say that solution $(x_n, y_n)_{n\geq 0}$ given by (4.1.3) is *associated* with the solution $(u_n, v_n)_{n\geq 0}$. The set of all solutions associated with each other forms a *class of solutions* to (4.1.1).

Next we will show a way to decide whether the two given solutions (x, y) and (x', y') belong to the same class or not. In fact, by using the method given in Theorem 3.5.2 it is easy to see that the necessary and sufficient condition for these two solutions to be associated with each other is that the numbers

$$\frac{xx' - Dyy'}{N} \quad \text{and} \quad \frac{yx' - xy'}{N}$$

are both integers.

Let K be the class consisting of the solutions $(x_n, y_n)_{n\geq 0}$ defined by (4.1.3). Then $(x_n, -y_n)_{n\geq 0}$ also constitutes a class, denoted by $\overline{K}$. The classes K and $\overline{K}$ are said to be *conjugates* of each other. Conjugate classes are in general distinct, but may sometimes coincide; in the latter case we speak of *ambiguous* classes.

Among all the solutions (x, y) in a given class K we now choose a solution (x^*, y^*) in the following way: let y^* be the least nonnegative value of y which occurs in K. If K is not ambiguous, then the number x^* is also uniquely determined, for the solution $(-x^*, y^*)$ belongs to the conjugate class $\overline{K}$. If K is ambiguous, then we get a uniquely determined x^* by prescribing that $x^* \geq 0$. The solution (x^*, y^*) defined in this way is said to be the *fundamental solution of the class*.

In the fundamental solution, the number $|x^*|$ has the least value which is possible for $|x|$ when (x, y) belongs to K. The case $x^* = 0$ can occur when the class is ambiguous, and similarly for the case $y^* = 0$.

If $N = \pm 1$, there is only one class and it is ambiguous.

Suppose now that N is positive.

Theorem 4.1.1. *If (x, y) is the fundamental solution of the class K of the equation (4.1.1) and if (u_1, v_1) is the fundamental solution of the Pell's resolvent (4.1.2), then the following inequalities hold:*

$$0 \leq |x| \leq \sqrt{\frac{(u_1 + 1)N}{2}} \tag{4.1.4}$$

$$0 < y \leq \frac{v_1}{\sqrt{2(u_1 + 1)}}\sqrt{N}. \tag{4.1.5}$$

Proof. If inequalities (4.1.4) and (4.1.5) are true for a class K, they are also true for the conjugate class $\overline{K}$. Thus we may assume that y is positive.

It is clear that

$$xu_1 - Dyv_1 = xu_1 - \sqrt{(x^2 - N)(u_1^2 - 1)} > 0. \tag{4.1.6}$$

Consider the solution $(xu_1 - Dyv_1, yu_1 - xv_1)$ which belongs to the same class as (x, y). Since (x, y) is the fundamental solution of the class and since by (4.1.6) $xu_1 - Dyv_1$ is positive, we must have $xu_1 - Dyv_1 \geq x$. From this inequality it follows that

$$x^2(u_1 - 1)^2 \geq D^2y^2v_1^2 = (x^2 - N)(u_1^2 - 1)$$

or

$$\frac{u_1 - 1}{u_1 + 1} \geq 1 - \frac{N}{x^2}$$

and finally $x^2 \leq \frac{1}{2}(u_1 + 1)N$. This proves inequality (4.1.4) and it is easily seen that (4.1.4) implies (4.1.5). □

Suppose next that $N < 0$ and call (4.1.1) the *general negative Pell's equation*. With a proof similar to the one in Theorem 4.1.1 we have

Theorem 4.1.2. *If (x, y) is the fundamental solution of the class K of the general negative Pell's equation and if (u_1, v_1) is the fundamental solution of the Pell's resolvent (4.1.2), then the following inequalities hold:*

$$0 \leq |x| \leq \sqrt{\frac{(u_1 - 1)|N|}{2}} \tag{4.1.7}$$

$$0 < y \leq \frac{v_1}{\sqrt{2(u_1 - 1)}} \sqrt{|N|}. \tag{4.1.8}$$

From Theorems 4.1.1 and 4.1.2 we deduce

Theorem 4.1.3. *If D is a nonsquare positive integer and N is a nonzero integer, then the equation (4.1.1) has a finite number of classes of solutions. The fundamental solutions of all the classes can be found after a finite number of trials by means of the inequalities (4.1.4), (4.1.5) and (4.1.7), (4.1.8). If (x^*, y^*) is the fundamental solution of the class K, then all the solutions in K are given by $(x_n, y_n)_{n\geq 0}$, where*

$$x_n = x^* u_n + D y^* v_n \quad \text{and} \quad y_n = y^* u_n + x^* v_n$$

and $(u_n, v_n)_{n\geq 0}$ represents the general solution of Pell's resolvent including ± 1, if necessary.

Remark. The upper bounds for fundamental solutions that generate the classes of solutions of general Pell's equation (4.1.1) found in Theorems 4.1.1 and 4.1.2 can still be improved. In [76] it is shown that

$$0 \leq |x| \leq \sqrt{\varepsilon |N|}, \quad 0 < y \leq \sqrt{\frac{\varepsilon |N|}{D}}$$

where $\varepsilon = u_1 + v_1 \sqrt{D}$.

In the private communication (L. Panaitopol, personal communication, December 2001) the following better upper bounds are mentioned

$$0 \leq |x| \leq \sqrt{\frac{|N| u_1 + N}{2}}, \quad 0 < y \leq \sqrt{\frac{|N| u_1 - N}{2D}}.$$

In the above delimitations (u_1, v_1) denotes the fundamental solution to the Pell's equation (4.1.2).

We denote by $k(D, N)$ the number of classes of solutions of the equation (4.1.1), and by $\mathcal{K}(D, N)$ the set of the fundamental solutions of all classes.

Theorem 4.1.4. *Let p be a prime. Then each of the general Pell's equations*

$$x^2 - D y^2 = \pm p \tag{4.1.9}$$

has at most one solution (x, y) in which x and y satisfy the inequalities (4.1.4) and (4.1.5), or (4.1.7) and (4.1.8), respectively, provided that $x \geq 0$.

If the equation (4.1.9) is solvable, then it has one or two solutions satisfying the above conditions, according as the prime p divides $2D$ or not.

Proof. Suppose that (x, y) and (x_1, y_1) are two solutions of (4.1.9) satisfying the conditions in the first part of Theorem 4.1.4. Thus the numbers x, y, x_1 and y_1 are nonnegative.

Eliminating D between relations

$$x^2 - Dy^2 = \pm p, \quad x_1^2 - Dy_1^2 = \pm p \tag{4.1.10}$$

yields $x^2y_1^2 - x_1^2y^2 = \pm p(y_1^2 - y^2)$. Thus $xy_1 \equiv x_1y \pmod{p}$.

Furthermore, from (4.1.10) we obtain

$$(xx_1 \mp Dyy_1)^2 - D(xy_1 \mp x_1y)^2 = p^2.$$

In the equation

$$\left(\frac{xx_1 \mp Dyy_1}{p}\right)^2 - D\left(\frac{xy_1 \mp x_1y}{p}\right)^2 = 1 \tag{4.1.11}$$

let us choose the sign such that the congruence $xy_1 \equiv \pm x_1y \pmod{p}$ is satisfied. Then the two squares on the left-hand side are integers. If $xy_1 \mp x_1y \neq 0$, from (4.1.11) we conclude that

$$|xy_1 \mp x_1y| \geq v_1p. \tag{4.1.12}$$

On the other hand, by applying inequalities (4.1.4) and (4.1.5), or (4.1.7) and (4.1.8), respectively, we obtain $|xy_1 \mp x_1y| < v_1p$, which is contrary to (4.1.12). The remaining case is $xy_1 \mp x_1y = 0$, which is obviously possible only for $x = x_1$ and $y = y_1$. Thus the first part of Theorem 4.1.4.

Consequently, there are at most two classes of solutions. Suppose that (x, y) and $(x, -y)$ are two solutions which satisfy inequalities (4.1.4) and (4.1.5), or (4.1.7) and (4.1.8), respectively. These solutions are associated if and only if p divides the two numbers $2xy$ and $x^2 + Dy^2 = 2Dy^2 \pm p$. Since y cannot be divisible by p, the numbers $2x$ and $2D$ are divisible by p. But if $2D$ is divisible by p, then so is $2x$. Thus, the necessary and sufficient condition for (x, y) and $(x, -y)$ to belong to the same class is that $2D$ is a multiple of p. Thus proves the second part of the theorem. □

The following example illustrates how the method described in Theorem 4.1.4 can be applied.

Consider the equation $x^2 - 2y^2 = 119$. The fundamental solution of its Pell's resolvent $u^2 - 2v^2 = 1$ is $(3, 2)$. The following solutions of our equation satisfy inequalities (4.1.4) and (4.1.5): $(11, 1)$, $(-11, 1)$, $(13, 5)$, $(-13, 5)$. It is not difficult

to show that these numbers are all fundamental solutions in different classes. Thus the number of classes is four but only solutions (11,1) and (13,5) satisfy Theorem 4.1.4. The form of the integer N is very important. For instance, in the paper [174] are considered the equations $x^2 - Dy^2 = \pm c(2^{31} - 1)$.

We will now present an example which illustrates how one can use Theorem 4.1.4. We will now rely on the result in our paper [16]. In [37] the following question is posed: Does the Diophantine equation

$$8x^2 - y^2 = 7 \tag{4.1.13}$$

have infinitely many solutions in positive integers?

Recently, in the paper [114] the more general equation $ax^2 - by^2 = c$ is considered. It is shown that if ab is not a square and the above equation has a positive integer solution (x_0, y_0), then it has infinitely many positive integer solutions. This property is a direct consequence of the multiplication principle. In the paper [143] a simple criterion for solving both equations $x^2 - Dy^2 = c$ and $x^2 - Dy^2 = -c$ is presented.

In what follows, we will find all solutions to the equation (4.1.13). We can write the equation (4.1.13) in the following equivalent form: $y^2 - 8x^2 = -7$. This is a special case of (4.1.9). In our case, $p = 7$ and p does not divide $2D = 16$. Applying Theorem 4.1.4 we deduce that the equation (4.1.13) has two classes of solutions and these are generated by $(-1, 1)$ and $(1, 1)$. The Pell's resolvent $u^2 - 8v^2 = 1$ has the fundamental solution $(u_1, v_1) = (3, 1)$ and its general solution $(u_n, v_n)_{n\geq 0}$ is given by (see formulas (3.2.6)):

$$\begin{cases} u_n = \dfrac{1}{2}\left[\left(3+\sqrt{8}\right)^n + \left(3-\sqrt{8}\right)^n\right] \\ v_n = \dfrac{1}{2\sqrt{8}}\left[\left(3+\sqrt{8}\right)^n - \left(3-\sqrt{8}\right)^n\right] \end{cases} \tag{4.1.14}$$

Applying Theorem 4.1.3 it follows that all solutions to the equation (4.1.13) are given by $(x_n, y_n)_{n\geq 0}$ and $(x'_n, y'_n)_{n\geq 0}$, where

$$\begin{cases} x_n = u_n + v_n \\ y_n = u_n + 8v_n \end{cases} \quad \text{and} \quad \begin{cases} x'_n = u_n - v_n \\ y'_n = -u_n + 8v_n \end{cases}$$

and $(u_n, v_n)_{n\geq 0}$ is defined in (4.1.14). We obtain two classes of solutions:

$$(x, y) = (1, 1),\ (4, 11),\ (23, 65),\ (134, 379), \ldots$$

and

$$(x', y') = (2, 5),\ (11, 31),\ (64, 181),\ (373, 1055), \ldots$$

respectively.

Remark. We will describe now the set of rational solutions to the Pell's equation $u^2 - Dv^2 = 1$. A family of such solutions was given in Remark 4 in Section 3.2.

For fixed positive integers m and n consider the general Pell's equation $x^2 - Dy^2 = (mn)^2$. Consider the set of all its integral solutions (x, y) satisfying $n|x$ and $m|y$ and let $\mathcal{S}_{m,n}$ be the set of all pairs $\left(\frac{x_1}{m}, \frac{y_1}{n}\right)$, where $x = x_1 n$, $y = y_1 m$. The set of all rational solutions to $u^2 - Dv^2 = 1$ is then given by $\mathcal{S} = \bigcup_{m,n \geq 1} \mathcal{S}_{m,n}$.

The following interesting result was proved in the paper [72].

Theorem 4.1.5. *Let $D = a^2 + (2b)^2$, with $a, b \in \mathbb{Z}$. If D is a prime, the following hold:*

1) The equation $x^2 - Dy^2 = a$ is solvable.
2) The equation $x^2 - Dy^2 = 4b$ is solvable.

If D is not prime, then both 1) and 2) can fail. For instance $221 = 10^2 + 11^2 = 5^2 + 14^2$, but for $a = \pm 5$ or ± 11 the equation $x^2 - 221y^2 = a$ has no solution mod 13, while for $b = \pm 5$ or ± 7 the equation $x^2 - 221y^2 = 4b$ has no solution mod 17.

4.2 Solvability of General Pell's Equation

Disregarding any time considerations, Theorem 4.1.1 may be used to determine whether any general Pell equation is solvable or not. Following the reference [204], let consider the general Pell equation $x^2 - 43y^2 = 35$. According to Theorem 4.1.1, if it is solvable, then any of its fundamental solutions (x, y) must lie within the following bounds: $0 < |x| \leq \left[\sqrt{35(3482 + 1)/2}\right] = 246$ and $0 < v \leq \left[532\sqrt{35/(2(3482 + 1))}\right] = 37$, where $(3482, 532)$ is the fundamental solution to the Pell's resolvent $u^2 - 43v^2 = 1$. After checking all 9102 possible combinations of (x, y) we see that the equation $x^2 - 43y^2 = 35$ is not solvable.

With regards to computational efficiency, the question of solvability for the considered example is no match for modern computers. But, what happens when N gets large? Clearly, $\sqrt{\frac{(u_1 - 1)|N|}{2}} \to \infty$, as $N \to \pm\infty$. Thus, Theorem 4.1.1, though a nice tool, does not allow one to efficiently decide if a particular general Pell equation is solvable. In the reference [204] is mentioned the equation $x^2 - 313y^2 = 172635965$ and the fact that, using the actual computation force, we need about 69806785 years to prove the unsolvability, following the method provided by Theorem 4.1.1. Thus, in this particular example, with $N = 172635965$ relatively small, using the approach in Theorem 4.1.1 will take a considerable amount of time.

The question of solvability of the general Pell's equation can be formulated into two problems:

Pell Decision Problem (PDP). *Given a positive integer $D \geq 2$ which is not a perfect square, and an integer N, is there an efficient means to decide if the equation (4.1.1) is solvable?*

In some situations PDP can be reduced to the case when D is a prime (see for instance Theorem 3.6.2).

Pell Search Problem (PSP). *Assuming that the equation (4.1.1) is solvable, can we find all fundamental solutions in the Pell classes in a reasonable amount of time?*

Notice that a general criterion for solvability is, in effect, a solution to a PDP. In this section we address the problem of finding a general criterion for solvability of general Pell equation and give a partial solution. Most of the tests that we develop throughout this section are based on the reference [204] and do not rely on integer factorization. However, a few of the implementations based on these results will rely heavily on the efficiency of integer factorization, which is likely no more efficient than tests based on the Pell class approach.

4.2.1 PDP and the Square Polynomial Problem

In what follows we will show that the PDP is equivalent to the problem of deciding whether or not a particular second degree polynomial with integer coefficients has a square integer value. In this respect we formulate the following concrete problem:

Square Polynomial Decision Problem (SPDP). *Does there exist an algorithm that, for any odd prime p and $N \in \mathbb{Z}$ with $\gcd(N,p) = 1$ decides if there is for some a with $N \equiv a^2 \pmod{p}$ and $n \in \mathbb{Z}$ such that $pn^2 - 2an + \dfrac{a^2 - N}{p}$ is a square?*

The SPDP and the PDP for specific D and N may be formulated in terms of arithmetical functions. Let p be a prime, $N \in \mathbb{Z}$, with $\left(\dfrac{N}{p}\right) = 1$ and consider the equation $x^2 - py^2 = N$. Since $\left(\dfrac{N}{p}\right) = 1$ we have $a^2 \equiv N \pmod{p}$ for some positive integer a. Note that, the Tonelli–Shanks algorithm, assuming the Generalized Riemann Hypothesis, efficiently find an integer a such that $a^2 \equiv N \pmod{p}$ (see [159, pp. 110–115]).

Following the reference [204], define the functions

$$\phi(p,N) = \begin{cases} 1 \text{ if } pn^2 - 2an + \dfrac{a^2 - N}{p} \text{ is a square for some} \\ \quad \text{integers } n \text{ and } a \text{ with } a^2 \equiv N \pmod{p} \\ -1 \text{ otherwise} \end{cases}$$

and

$$\psi(p,N) = \begin{cases} 1 \text{ if } x^2 - py^2 = N \text{ is solvable} \\ -1 \text{ otherwise.} \end{cases}$$

Clearly, in the definition of $\phi(p,N)$ we can assume that $a \in \mathbb{Z}_p$.

Now, we have the proper terminology to prove the following result.

Theorem 4.2.1. *Let p be an odd prime and $N \in \mathbb{Z}$ with $\left(\frac{N}{p}\right) = 1$. Then, $\psi(p,N) = 1$ if and only if $\phi(p,N) = 1$.*

Proof. If $\psi(p,N) = 1$, then we have $u^2 - pm^2 = N$ for some integers u, m. Observe that $y^2 \equiv N \pmod{p}$. To prove $\phi(p,N) = 1$ we must show that there is an integer n such that $pn^2 - 2un + \frac{u^2 - N}{p}$ is a square. But, we have $\frac{u^2 - N}{p} = m^2$, hence we choose $n = 0$. Therefore $\phi(p,N) = 1$.

Suppose $\phi(p,N) = 1$. That is, there are integers n, m and $u \in \mathbb{Z}_p$ such that $u^2 \equiv N \pmod{p}$ and $pn^2 - 2un + \frac{u^2 - N}{p} = m^2$. The last relation is equivalent to $(u + pn)^2 - pm^2 = N$, so the pair $(u + pn, m)$ is a solution to the general Pell's equation $x^2 - py^2 = N$. Thus, the relation $\psi(p,N) = 1$ holds. □

The result in Theorem 4.2.1 proves that SPDP is equivalent to PDP.

4.2.2 The Legendre Test

The Legendre symbol and the Quadratic Reciprocity Law provide the first test for the solvability of general Pell's equation.

Theorem 4.2.2. *If $\left(\frac{N}{p}\right) = -1$ then $\psi(p,N) = -1$, that is $x^2 - py^2 = N$ is not solvable.*

Proof. If the equation $x^2 - py^2 = N$ were solvable, then $u^2 - pv^2 = N$ for some integers u and v. Therefore, $u^2 - N = pv^2$, hence $u^2 \equiv N \pmod{p}$, implying $\left(\frac{N}{p}\right) = 1$, contradicting our assumption. □

Corollary 4.2.3. *If $\left(\frac{N}{p}\right) = 1$ and $\left(\frac{M}{p}\right) = -1$, then the equation*

$$x^2 - py^2 = MN$$

is not solvable.

Example 1. Consider the general Pell's equation $x^2 - 17y^2 = -46$. Using the properties of the Legendre symbol, we have

$$\left(\frac{-46}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{46}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{4}{17}\right)\left(\frac{3}{17}\right)$$
$$= \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

hence, according to Theorem 4.2.2, the considered equation is not solvable.

4.2.3 Legendre Unsolvability Tests

This subsection uses the Quadratic Reciprocity Law and some properties of the Legendre symbol to obtain some tests for the unsolvability of general Pell's equation.

Theorem 4.2.4. *Let p be an odd prime and N a positive integer. If $p \equiv 3 \pmod 4$ and $\left(\frac{N}{p}\right) = 1$, then the equation $x^2 - py^2 = -N$ is not solvable.*

Proof. If the equation is solvable, then we have $r^2 - ps^2 = -N$, for some integers r, s. It follows $r^2 \equiv -N \pmod p$, hence $\left(\frac{-N}{p}\right) = 1$. Using the standard properties of the Legendre symbol we get

$$1 = \left(\frac{-N}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{N}{p}\right)$$

and

$$\left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right) \cdot 1 = \left(\frac{-1}{p}\right)\left(\frac{N}{p}\right) = \left(\frac{-N}{p}\right) = 1.$$

By the Quadratic Reciprocity Law, this only happens when $p \equiv 1 \pmod 4$, contradicting our assumption. □

Example 2. Consider the equation $x^2 - 11y^2 = -5$. Since (4,1) is a solution to $x^2 - 11y^2 = 5$, we have $\left(\frac{5}{11}\right) = 1$. Since $11 \equiv 3 \pmod 4$, by Theorem 4.2.4, we obtain that the considered equation is not solvable.

The next result is given in [204] and it yields a general test for the unsolvability of a large class of general Pell's equations.

Theorem 4.2.5. *Let p be a prime, $p \equiv 3 \pmod 4$, and $N = m^2 n$ with n square free. If $x^2 - py^2 = N$ is solvable, then $n \equiv 1 \pmod 4$.*

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

(i) $\left(\frac{n}{p}\right) = 1$.

(ii) If q is a prime divisor of n with $q \equiv 3 \pmod 4$, then $\left(\frac{q}{p}\right) = -1$.

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

Since $u^2 - pv^2 = m^2 n$, we have $u^2 - m^2 n = pv^2$. So, $X^2 \equiv N \pmod p$ is solvable. Thus, $\left(\frac{n}{p}\right) = \left(\frac{m^2 n}{p}\right) = 1$. This proves (i).

Now suppose that q is a prime divisor of n. So, $n = qn_0$ for some $n_0 \in \mathbb{Z}$. Thus, $u^2 - pv^2 = qn_0$ and so $X^2 \equiv pv^2 \pmod p$ is solvable. So, $\left(\frac{p}{q}\right) = \left(\frac{pv^2}{q}\right) = 1$. By the Quadratic Reciprocity Law, we know that, since $p \equiv q \equiv 3 \pmod 4$, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. So, $-\left(\frac{q}{p}\right) = 1$. This proves (ii).

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

Again let $n = q_1 \dots q_r q_{r+1} \dots q_l$, where $q_1 \equiv \dots \equiv q_r \equiv 3 \pmod 4$ and $q_{r+1} \equiv \dots \equiv q_l \equiv 1 \pmod 4$. Because r is odd, by (ii) we have

$$\left(\frac{q_1}{p}\right) \dots \left(\frac{q_r}{p}\right) = (-1) \dots (-1) = (-1)^r = -1.$$

Also,

$$\left(\frac{q_{r+1}}{p}\right) \dots \left(\frac{q_l}{p}\right) = 1 \dots 1 = 1^{l-r} = 1.$$

Therefore, by (i) we obtain

$$1 = \left(\frac{n}{p}\right) = \left(\frac{q_1 \dots q_r q_{r+1} \dots q_l}{p}\right)$$
$$= \left(\frac{q_1}{p}\right) \dots \left(\frac{q_r}{p}\right) \left(\frac{q_{r+1}}{p}\right) \dots \left(\frac{q_l}{p}\right) = (-1)^r \cdot 1 = -1,$$

a contradiction. □

The result in Theorem 4.2.5, when expressed using the contrapositive, yields a nice test for unsolvability. We state this as the following consequence.

Corollary 4.2.6. *Let $N = m^2 n$ with n square free. If p is a prime with $p \equiv n \equiv 3 \pmod 4$, then the equation $x^2 - py^2 = N$ is not solvable.*

The next consequence follows immediately.

Corollary 4.2.7. *If $p \equiv N \equiv 3 \pmod 4$ and $M \equiv 1 \pmod 4$, then the equation $x^2 - py^2 = MN$ is not solvable.*

Example 3. Consider the equation $x^2 - 31y^2 = 1008$. We have $1008 = 12^2 \cdot 7$ and $7 \equiv 3 \pmod 4$. Corollary 4.2.6 allows us to conclude that the equation is not solvable.

The next result requires that we know a prime factor ≥ 3 of N.

Theorem 4.2.8. *Let q be an odd prime divisor of N. If the equation $x^2 - py^2 = N$ is solvable, then $\left(\frac{p}{q}\right) = 1$.*

Proof. Assume that $u^2 - pv^2 = N$, for some integers u, v. Because $N \equiv 0 \pmod q$, it follows $u^2 \equiv pv^2 \pmod q$.

Therefore, $\left(\frac{pv^2}{q}\right) = 1$, hence $\left(\frac{p}{q}\right) = 1$. □

In the case when we can find an odd prime divisor of N, the contrapositive to Theorem 4.2.8 provides a nice test for unsolvability.

Corollary 4.2.9. *Let q be an odd prime divisor of N. If $\left(\frac{p}{q}\right) = -1$, then the equation $x^2 - py^2 = N$ is not solvable.*

Now, we are in position to discuss the solvability of the equation

$$x^2 - 313y^2 = 172635965,$$

considered at the beginning of this section. Because 5 is a prime divisor of 172635965 and $\left(\frac{313}{5}\right) = -1$, we may use Corollary 4.2.9 to conclude the unsolvability of the equation.

Corollary 4.2.10. *Let q be an odd prime divisor of N. If p or $q \equiv 1 \pmod 4$ and $\left(\frac{q}{p}\right) = -1$, then the equation $x^2 - py^2 = N$ is not solvable.*

Proof. Because p or $q \equiv 1 \pmod 4$, we have $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = -1$, and we can use the result in Corollary 4.2.9.

Corollary 4.2.11. *Let $N = m^2 n$, where n is square free. If p is a prime with $p \equiv 5 \pmod 8$, and n is even, then the equation $x^2 - py^2 = N$ is not solvable.*

Proof. Suppose that $u^2 - pv^2 = N$, for some integers u, v. It follows $\left(\frac{N}{p}\right) = 1$, hence $\left(\frac{n}{p}\right) = \left(\frac{m^2 n}{p}\right) = 1$. Since n is even, we have $n = 2n_0$, $n_0 \in \mathbb{Z}$, and $\left(\frac{2n_0}{p}\right) = 1$. Because $p \equiv 5 \pmod 8$, we have $\left(\frac{2}{p}\right) = -1$. Therefore, n has a prime factor q such that $\left(\frac{q}{p}\right) = -1$. But, n is square free, so q must be odd. Moreover, from $p \equiv 5 \pmod 8$, it follows $p \equiv 1 \pmod 4$ and the conclusion follows from Corollary 4.2.9. □

The following application is given in the reference [204].

Example 4. Consider the equation $x^2 - 181y^2 = 1908360$. We have $181 \equiv 5 \pmod 8$ and $1908360 = 18^2 \cdot 5890$ with $5890 = 2 \cdot 5 \cdot 19 \cdot 31$ even and square free. Applying Corollary 4.2.11, it follows the unsolvability of the equation.

4.2.4 Modulo n Unsolvability Tests

We will describe a simple but useful way to test the unsolvability of general Pell's equation.

Theorem 4.2.12. *If the equation $x^2 - Dy^2 = N$ is not solvable in $\mathbb{Z}_n$, for some positive integer $n \geq 2$, then it is not solvable in integers.*

Proof. Assume that $u^2 - Dv^2 = N$ for some integers u, v. The remainder upon dividing $u^2 - Dv^2$ by n will be the same as the remainder in the division of N by n. Therefore, the equation $x^2 - Dy^2 = N$ is solvable in $\mathbb{Z}_n$. Thus, by the contrapositive, the result follows. □

Note that if the equation $x^2 - Dy^2 = N$ is solvable in $\mathbb{Z}_n$ for some positive integer $n \geq 2$, then it is not necessarily the case that it is solvable in integers.

Theorem 4.2.13. *Let p be a prime with $p \equiv 3 \pmod 4$, and N an odd integer. If the equation $x^2 - py^2 = N$ is solvable, then $N \equiv 1 \pmod 4$.*

Proof. We have $a^2 \equiv 0\,1 \pmod 4$, and by direct calculation, we see that $x^2 - oy^2 \equiv x^2 - 3y^2 \equiv 0, 1$, or $2 \pmod 4$. Therefore, if $N \equiv 3 \pmod 4$, the equation is not solvable in $\mathbb{Z}_4$, and, by mod 4 test, the equation is not solvable in integers. □

Using the same argument, but in $\mathbb{Z}_8$, we can prove the following result.

Theorem 4.2.14. *Let p be a prime with $p \equiv 1, 3$, or $5 \pmod 8$, and N an integer with $N \equiv 2 \pmod 4$. Then the equation $x^2 - py^2 = N$ is not solvable.*

4.2.5 Extended Multiplication Principle

We now give some tests for the solvability of general Pell's equation, using an extension of the multiplication principle discussed in Section 4.1.

Extended Multiplication Principle. *If $u^2 - Dv^2 = M$ and $r^2 - Ds^2 = N$, then $(ur \pm Dvs)^2 - D(us \pm vr)^2 = MN$, where the signs $+$ and $-$ correspond.*

The above identity is also called the *Bhaskara identity*, according to the name of the Hindu mathematician mentioned in Section 3.1.

We can reformulate this algebraic property as follows: If the general Pell's equations $u^2 - Dv^2 = M$ and $r^2 - Ds^2 = N$ are solvable, then the equation $x^2 - Dy^2 = MN$ is also solvable.

As an application to the Extended Multiplication Principle, we present an extension of the result involving the negative Pell's equation, and contained in Theorem 3.6.2.

Theorem 4.2.15. *Let p be a prime with $p \equiv 1 \pmod 4$. The equation*

$$x^2 - py^2 = -N$$

is solvable if and only if the equation $x^2 - py^2 = N$ is solvable.

Proof. By Theorem 3.6.2, we know that the negative Pell's equation

$$u^2 - pv^2 = -1$$

is solvable. Now, the result directly follows from the Extended Multiplicative Principle. □

Remark. Notice that if we can factor N, say $N = N_1 \dots N_s$ and show, for all $i = 1, \dots, s$, that the equation $x^2 - Dy^2 = N_i$ is solvable, then using successively the Extended Multiplication Principle we obtain that the equation $x^2 - Dy^2 = N$ is solvable.

The converse of the above remark need not hold, as the next example illustrates.

Example 5. Considering the equation $x^2 - 37y^2 = 192$, we have $192 = 4^2 \cdot 12 = 8^2 \cdot 3$. The equations $x^2 - 37y^2 = 12$ and $x^2 - 37y^2 = 4^2$ are clearly solvable, hence according to the Extended Multiplication Principle, it follows the considered equation is solvable. On the other hand, if we use the second factorization of 192, we see that $x^2 - 37y^2 = 3$ is not solvable (apply Theorem 4.1.1 where $(u_1, v_1) = (73, 12)$. Thus, we may not conclude that the unsolvability of $x^2 - 37y^2 = 3$ implies the unsolvability of $x^2 - 37y^2 = 192$.

4.3 An Algorithm for Determining the Fundamental Solutions Based on Simple Continued Fractions (The LMM Method)

We will describe an almost forgotten algorithm due to Lagrange, for deciding the solvability of general Pell's equation (4.1.1), where $\gcd(x, y) = 1$ and $D > 0$ is not a perfect square. In the case of solvability, the fundamental solutions are also constructed.

The main purpose of this section is to present a version of Lagrange's algorithm which uses only the technique of simple continued fractions.

A related algorithm is given in [158] but each of the cases $D = 2$ or $D = 3$ and $N < 0$ needs separate consideration. Also, unlike our algorithm, the approach in [158] requires the calculation of the fundamental solution of Pell's resolvent.

Lagrange's algorithm has been rediscovered in [141]. The method there is more complicated than ours, as it uses the language of ideals and semi-simple continued fractions, in addition to that of simple continued fractions.

First we need a result which is an extension of Theorem 172 in [88].

Lemma 4.3.1. *If* $\omega = \dfrac{P\zeta + R}{Q\zeta + S}$, *where* $\zeta > 1$ *and* P, Q, R, S *are integers such that* $Q > 0$, $S > 0$ *and* $PS - QR = \pm 1$, *or* $S = 0$ *and* $Q = R = 1$, *then* P/Q *is a convergent to* ω. *Moreover if* $Q \neq S > 0$, *then*

$$\frac{R}{S} = \frac{p_{n-1} + kp_n}{q_{n-1} + kq_n}, \quad k \geq 0.$$

Also, $\zeta + k$ *is the* $(n+1)$*-th complete convergent to* ω. *Here* $k = 0$ *if* $Q > S$, *while* $k \geq 1$ *if* $Q < S$.

Proof. In [88] only the case $Q > S > 0$ is considered. We write

$$\frac{P}{Q} = \langle a_0; a_1, \ldots, a_n \rangle = \frac{p_n}{q_n}$$

and assume $PS - QR = (-1)^{n-1}$. Then

$$p_n S - q_n R = PS - QR = p_n q_{n-1} - p_{n-1} q_n,$$

so $p_n(S - q_{n-1}) = q_n(R - p_{n-1})$.

Hence $q_n | (S - q_{n-1})$. Then from $q_n = Q > S > 0$ and $q_n \geq q_{n-1} > 0$, we deduce $|S - q_{n-1}| < q_n$ and hence $S - q_{n-1} = 0$. Then $S = q_{n-1}$ and $R = p_{n-1}$.

Also

$$\omega = \frac{P\zeta + R}{Q\zeta + S} = \frac{p_n\zeta + p_{n-1}}{q_n\zeta + q_{n-1}} = \langle a_0; a_1, \ldots, a_n, \zeta \rangle.$$

If $S = 0$ and $Q = R = 1$, then $\omega = [P, \zeta]$ and $P/Q = P/1 = p_0/q_0$.

If $Q = S$, then $Q = S = 1$ and $P - R = \pm 1$. If $P = R + 1$, then $\omega = [R, 1, \zeta]$, so $P/Q = (R + 1)/1 = p_1/q_1$. If $P = R - 1$, then $\omega = [R - 1, 1 + \zeta]$ and $P/Q = (R - 1)/1 = p_0/q_0$.

If $Q < S$, then from $q_n | (S - q_{n-1})$ and

$$S - q_{n-1} > Q - q_{n-1} = q_n - q_{n-1} \geq 0,$$

we have $S - q_{n-1} = kq_n$, where $k \geq 1$. Then

$$\omega = \frac{P\zeta + R}{Q\zeta + S} = \frac{p_n\zeta + p_{n-1} + kp_n}{q_n\zeta + q_{n-1} + kq_n} = \frac{p_n(\zeta + k) + p_{n-1}}{q_n(\zeta + k) + q_{n-1}}$$

and $\omega = \langle a_0; a_1, \ldots, a_n, \zeta + k \rangle$. □

Theorem 4.3.2. *Suppose $x^2 - Dy^2 = N$ is solvable in integers $x > 0$, $y > 0$, with $\gcd(x, y) = 1$ and let $Q_0 = |N|$. Then $\gcd(Q_0, y) = 1$. Define P_0 by $x \equiv -P_0 y \pmod{Q_0}$, where $D \equiv P_0^2 \pmod{Q_0}$ and $-Q_0/2 < P_0 \leq Q_0/2$.*

Let $\omega = (P_0 + \sqrt{D})/Q_0$ and let $x = Q_0X - P_0y$. Then

(i) X/y is a convergent A_{n-1}/B_{n-1} of ω if $x > 0$;
(ii) $Q_n = (-1)^n N/|N|$.

Proof. With $Q_0 = |N|$, $x = Q_0X - P_0y$ and $x^2 - Dy^2 = N$, we have

$$P_0x + Dy \equiv -P_0^2y + Dy \equiv (-P_0^2 + D)y \equiv 0 \pmod{Q_0}.$$

Hence the matrix

$$\begin{bmatrix} P & R \\ Q & S \end{bmatrix} = \begin{bmatrix} X & \frac{P_0x + Dy}{Q_0} \\ y & x \end{bmatrix}$$

has integer entries and determinant $\Delta = \pm 1$. For

$$\begin{aligned} \Delta &= Xx - \frac{y(P_0x + Dy)}{Q_0} \\ &= \frac{(x + P_0y)x}{Q_0} - \frac{y(P_0x + Dy)}{Q_0} \\ &= \frac{x^2 - Dy^2}{Q_0} = \pm 1. \end{aligned}$$

Also, if $\zeta = \sqrt{D}$ and $\omega = (P_0 + \sqrt{D})/Q_0$, it is easy to verify that $\omega = \dfrac{P\zeta + R}{Q\zeta + S}$. Then the lemma implies that X/y is a convergent to ω.

Finally, $x = Q_0X - P_0y = Q_0A_{n-1} - P_0B_{n-1} = G_{n-1}$ and

$$N = x^2 - Dy^2 = G_{n-1}^2 - DB_{n-1}^2 = (-1)^n Q_0 Q_n.$$

Hence $Q_n = (-1)^n N/|N|$. □

Remark. The solutions u of $u^2 \equiv D \pmod{Q_0}$ come in pairs $\pm u_1, \ldots, \pm u_r$, where $0 < u_i \leq Q_0/2$, together with possibly $u_{r+1} = 0$ and $u_{r+2} = Q_0/2$. Hence we can state the following:

Corollary 4.3.3. *Suppose $x^2 - Dy^2 = N$ is solvable, with $x > 0$ and $y > 0$, $\gcd(x, y) = 1$ and $Q_0 = |N|$. Let $x \equiv -P_0 y \pmod{Q_0}$, where $P_0 \equiv \pm u_i \pmod{Q_0}$ and $x = Q_0X - P_0y$. Then X/y is a convergent A_{n-1}/B_{n-1} of $\omega_i = (u_i + \sqrt{D})/Q_0$ or $\omega_i' = (-u_i + \sqrt{D})/Q_0$ and $Q_n = (-1)^n N/|N|$.*

4.3.1 An Algorithm for Solving the General Pell's Equation (4.1.1)

In view of the Corollary 4.3.3 we know that the primitive solutions to $x^2 - Dy^2 = N$ with $y > 0$ will be found by considering the continued fraction expansions of both ω_i and ω_i' for $1 \leq i \leq r + 2$.

One can show that each equivalence class contains solutions (x, y) with $x > 0$ and $y > 0$, so the necessary condition $Q_n = (-1)^n N/|N|$ occurs in both ω_i and ω_i'. Hence we need only consider ω_i.

Suppose that $\omega_i = (u_i + \sqrt{D})/Q_0 = [a_0, \ldots, a_t, \overline{a_{t+1}, \ldots, a_{t+l}}]$.

If $x^2 - Dy^2 = N$ is solvable, there are infinitely many solutions and hence $Q_n = \pm 1$ holds for ω_i for some n in the range $t + 1 \leq n \leq t + l$. Any such n must have $Q_n = 1$, as $(P_n + \sqrt{D})/Q_n$ is reduced for n in this range and so $Q_n > 0$. Moreover, if l is even, then the condition $(-1)^n = N/|N|$ is preserved.

In addition, there can be at most one such n. For if $P_n = \sqrt{D}$ is reduced, then $P_n = [\sqrt{D}]$ and hence two such occurrences of $Q_n = 1$ within a period would give a smaller period.

We also remark that l is odd if and only if the fundamental solution of Pell's equation has norm equal to -1. Consequently, a solution of $x^2 - Dy^2 = N$ gives rise to a solution of $x^2 - Dy^2 = -N$; indeed we see that if $t + 1 \leq n \leq t + l$ and $k \geq 1$, then $G_{n+kl-1} + B_{n+kl-1}\sqrt{D} = \eta_0^k(G_{n-1} + B_{n-1}\sqrt{D})$, where η_0 is the fundamental solution of $x^2 - Dy^2 = \pm 1$. Hence $G_{n+l-1}^2 - DB_{n+l-1}^2 = -(G_{n-1}^2 - DB_{n-1}^2)$ if $N(\eta_0) = -1$.

Putting these observations together, we have the following:

Theorem 4.3.4. *For $1 \leq i \leq r + 2$, let*

$$\omega_i = (u_i + \sqrt{D})/Q_0 = \langle a_0, \ldots, a_t, \overline{a_{t+1}, \ldots, a_{t+l}} \rangle.$$

(a) Then a necessary condition for $x^2 - Dy^2 = N$, $\gcd(x, y) = 1$, *to be solvable is that for some* i *in* $i = 1, \ldots, r+2$, *we have* $Q_n = 1$ *for some* n *in* $t+1 \le n \le t+l$, *where if* l *is even, then* $(-1)^n N/|N| = 1$.

(b) Conversely, suppose for ω_i, *we have* $Q_n = 1$ *for some* n *with* $t + 1 \le n \le t + l$. *Then*

(i) If l *is even and* $(-1)^n N/|N| = 1$, *then* $x^2 - Dy^2 = N$ *is solvable and it has solution* $G_{n-1} + B_{n-1}\sqrt{D}$.

(ii) If l *is odd, then* $G_{n-1} + B_{n-1}\sqrt{D}$ *is a solution of* $x^2 - Dy^2 = (-1)^n|N|$, *while* $G_{n+l-1} + B_{n+l-1}\sqrt{D}$ *is a solution of* $x^2 - Dy^2 = (-1)^{n+1}|N|$.

(iii) At least one of the $G_{n-1} + B_{n-1}\sqrt{D}$ *with least* B_{n-1} *satisfying* $Q_n = (-1)^n N/|N|$, *which arise from continued fraction expansions of* ω_i *and* ω_i', *is a fundamental solution.*

Remarks. 1) Unlike the case of Pell's equation, $Q_n = \pm 1$ can also occur for $n < t + 1$ and can contribute to a fundamental solution. If $N(\eta) = 1$, one sees that to find the fundamental solutions for both $x^2 - Dy^2 = \pm N$, it suffices to examine only the cases $Q_n = \pm 1$, $n \le t + l$. However if $N(\eta) = -1$, one may have to examine the range $t + l + 1 \le n \le t + 2l$ as well.

2) It can happen that l is even and that $x^2 - Dy^2 = N$ is solvable and has solution $x \equiv \pm u_i y \pmod{Q_0}$, while $x^2 - Dy^2 = -N$ is solvable and has solution $x \equiv \pm u_j y \pmod{Q_0}$, with $i \ne j$. (Of course, if $|N| = p$ is prime, this cannot happen, as the congruence $u^2 \equiv D \pmod{p}$ has two solutions if p does not divide D and one solution if p divides D.)

An example of this is $D = 221$, $N = 217$ (see Example 2 later). Then $u_1 = 2$, $u_2 = 33$. Also, $l = 6$ and $(2+\sqrt{221})/217$ produces the solution $-2+\sqrt{221}$ of $x^2 - 221y^2 = -217$, whereas $(33 - \sqrt{221})/217$ produces the solution $-179 + 12\sqrt{221}$ of $x^2 - 221y^2 = 217$.

Example 1 (Lagrange). $x^2 - 13y^2 = \pm 101$.

We find the solutions of $P_0^2 \equiv 13 \pmod{101}$ are ± 35.

(a) We have $\dfrac{35 + \sqrt{13}}{101} = [0, 2, 1, \overline{1, 1, 1, 1, 6}]$.

i	0	1	2	3	4	5	6	7	8
P_i	35	−35	11	−2	3	1	2	1	3
Q_i	101	−12	9	1	4	3	3	4	1
A_i	0	1	1	2	3	5	8	13	86
B_i	1	2	3	5	8	13	21	34	225

We observe that $Q_3 = Q_8 = 1$. The period length is odd, so both the equations $x^2 - 13y^2 = \pm 101$ are solvable. With $G_n = Q_0 A_n - P_0 B_n$, we have

$$G_2 = 101 \cdot 1 - 34 \cdot 3 = -4, \quad x + y\sqrt{13} = -4 + 3\sqrt{13}, \quad x^2 - 13y^2 = -101;$$

$$G_7 = 101 \cdot 13 - 35 \cdot 34 = 123, \quad x + y\sqrt{13} = 123 + 34\sqrt{13}, \quad x^2 - 13y^2 = 101.$$

(b) We have $\dfrac{-35+\sqrt{13}}{101} = [-1, 1, 2, 4, \overline{1, 1, 1, 1, 6}]$.

i	0	1	2	3	4	5	6	7	8
P_i	-35	-66	23	1	3	1	2	1	3
Q_i	101	-43	12	1	4	3	3	4	1
A_i	-1	0	-1	-4	-5	-9	-14	-23	-152
B_i	1	1	3	13	16	29	45	74	489

We observe that $Q_3 = Q_8 = 1$. Hence

$$G_2{=}101 \cdot (-1){-}(-35) \cdot 3{=}4,\ x{+}y\sqrt{13}{=}A + 3\sqrt{13},\ x^2 - 13y^2 = -101;$$

$$G_7{=}101 \cdot (-23){-}(-35) \cdot 74{=}267,\ x{+}y\sqrt{13}{=}267{+}74\sqrt{13},\ x^2{-}13y^2{=}101.$$

Hence $-4 + 3\sqrt{13}$ and $123 + 34\sqrt{13}$ are fundamental solutions for the equations $x^2 - 13y^2 = -101$ and $x^2 - 13y^2 = 101$ respectively.

We have $\eta = 649 + 180\sqrt{13}$, so the complete solution of $x^2 - 13y^2 = -101$ is given by $x + y\sqrt{13} = \pm\eta^n(\pm 4 + 3\sqrt{13})$, $n \in \mathbb{Z}$, while the complete solution of $x^2 - 13y^2 = 101$ is given by $x + y\sqrt{13} = \pm\eta^n(\pm 123 + 34\sqrt{13})$, $n \in \mathbb{Z}$.

Example 2. $x^2 - 221y^2 = \pm 217$.

We find the solutions of $P_0^2 \equiv 221 \pmod{217}$ are ± 2 and ± 33.

(a) We have $\dfrac{2+\sqrt{221}}{217} = [0, 12, \overline{1, 6, 2, 6, 1, 28}]$.

i	0	1	2	3	4	5	6	7
P_i	2	-2	14	11	13	13	11	14
Q_i	217	1	25	4	13	4	25	1
A_i	0	1	1	7	15	97	112	3233
B_i	1	12	13	90	193	1248	1441	41596

We observe that $Q_1 = Q_7 = 1$. The period length is even and $(-1)^7 = -1$. Hence the equation $x^2 - 221y^2 = -217$ is solvable.

$$G_0 = 217 \cdot 0 - 2 \cdot 1 = -2, \quad x + y\sqrt{221} = -2 + \sqrt{221}, \quad x^2 - 221y^2 = -217.$$

i	0	1	2	3	4	5	6	7	8
P_i	33	-33	13	5	7	8	7	3	4
Q_i	101	-10	9	6	5	3	10	7	9

We see that the condition $Q_n = 1$ does not holds for $3 \le n \le 8$.

4.4 Solving the General Pell's Equation

4.4.1 *The PQa Algorithm for Solving Pell's and Negative Pell's Equations*

This algorithm is at the heart of all the algorithms to solve Pell's equations presented here. The input to the algorithms is three integers, D, P_0, Q_0, where $D > 0$ is not a square, $Q_0 > 0$, and $P_0^2 \equiv D \pmod{Q_0}$. Recursively compute, for $i \geq 0$

$$a_i = \text{int}(P_i + \sqrt{D})/Q_i,$$
$$P_{i+1} = a_i Q_i - P_i,$$

and

$$Q_{i+1} = (D - P_{i+1}^2)/Q_i.$$

Also compute G_i and B_i as follows. Begin with $G_{-2} = -P_0$, $G_{-1} = Q_0$, $B_{-2} = 1$, and $B_{-1} = 0$. Then for $i \geq 0$, set $G_i = a_i G_{i-1} + G_{i-2}$, and set $B_i = a_i B_{i-1} + B_{i-2}$. Sometimes one also computes A_i as $A_{-2} = 0, A_{-1} = 1$, and $A_i = a_i A_{i-1} + A_{i-2}$ for $i \geq 0$. Then $G_i = Q_0 A_i - P_0 B_i$.

Note that $G_i^2 - DB_i^2 = (-1)^{i+1} Q_{i+1} Q_0$. This relation will be important to us because all of the methods of solution we discuss will involve setting $Q_0 = |N|$, and finding those i so that $(-1)^{i+1} Q_{i+1} = N/|N|$. Then (G_i, B_i) will be a solution to the equation being considered. From a computational viewpoint, also note that, in some sense, G_i and B_i will typically be large, while Q_0 and Q_{i+1} will be small. So this equation sometimes allows accurate computation of the left-hand side when numbers on the left-hand side exceed the machine accuracy available. Exactly how far to carry these computations is discussed with each use below.

The sequence a_i is the simple continued fraction expansion of $(P_0 + \sqrt{D})/Q_0$, and the A_i/B_i are the convergents to this continued fraction. Each of the sequences P_i, Q_i, and a_i is periodic from some point, although not necessarily the same point for all three. Starting from the right point, the periodic part of the sequence P_i is palindromic. For each of the sequences Q_i and a_i, the periodic part, less the last term, is palindromic.

To solve the equation $x^2 - Dy^2 = \pm 1$, apply the PQa algorithm with $P_0 = 0$ and $Q_0 = 1$. There will be a smallest i with $a_i = 2a_0$, which will also be the smallest $i > 0$ so that $Q_i = 1$. There are two cases to consider: this i is odd, or this i is even.

If this i is odd, then the equation $x^2 - Dy^2 = -1$ has solutions. The minimal positive solution is given by $x = G_{i-1}$, $y = B_{i-1}$. For any positive integer k, if k is odd then $x = G_{ki-1}$, $y = B_{ki-1}$ is a solution to the equation $x^2 - Dy^2 = -1$, and all solutions to this equation with x and y positive are generated this way. If k is an even positive integer, then $x = G_{ki-1}$, $y = B_{ki-1}$ is a solution to the equation

$x^2 - Dy^2 = 1$, and all solutions to this equation with x and y positive are generated this way. The minimal positive solution to $x^2 - Dy^2 = 1$ is $x = G_{2i-1}$, $y = B_{2i-1}$.

If the smallest i so that $a_i = 2a_0$ is even, then the equation $x^2 - Dy^2 = -1$ does not have any solutions. For any positive integer k, $x = G_{ki-1}$, $y = B_{ki-1}$ is a solution to the equation $x^2 - Dy^2 = 1$, and all solutions to this equation with x and y positive are generated this way. In particular, the minimal positive solution to $x^2 - Dy^2 = 1$ is $x = G_{i-1}$, $y = B_{i-1}$.

The sequences P_j and a_j are periodic with period i after the zero-th term, i.e., the first period is P_1 to P_i for the sequences P_j, and a_1 to a_i for the sequence a_j. The sequence Q_j is periodic starting at the zero-th term, i.e., the first period is Q_0 to Q_{i-1}.

In Sections 3.2–3.5 and 3.6, respectively, we give several methods to generate all solutions to either Pell's and negative Pell's equations once the minimal positive solution is found.

4.4.2 Solving the Special Equations $x^2 - Dy^2 = \pm 4$

In some ways, solutions to the equation $x^2 - Dy^2 = \pm 4$ are more fundamental than solutions to the equation $x^2 - Dy^2 = \pm 1$. The most interesting case is when $D \equiv 1 \pmod 4$, so we cover that first.

When $D \equiv 1 \pmod 4$, apply the PQa algorithm with $P_0 = 1$ and $Q_0 = 2$. There will be a smallest $i > 0$ so that $a_i = 2a_0 - 1$. This will also be the smallest $i > 0$ so that $Q_i = 2$. The minimal positive solution to $x^2 - Dy^2 = \pm 4$ is then $x = G_{i-1}$, $y = B_{i-1}$. If i is odd, it will be a solution to the -4 equation, while if i is even it will be a solution to the $+4$ equation and the -4 equation will not have solutions. Periodicity of the sequences P_i, Q_i, and a_i is similar to that for the ± 1 equation.

If $D \equiv 0 \pmod 4$, then for any solution to $x^2 - Dy^2 = \pm 4$, x must be even. Set $X = x/2$, set $Y = y$, and solve $X^2 - (D/4)Y^2 = \pm 1$. If (X, Y) is the minimal positive solution to this equation, then $x = 2X$, $y = Y$ is the minimal positive solution to $x^2 - Dy^2 = \pm 4$. Alternatively, one can apply the PQa algorithm with $P_0 = 0$ and $Q_0 = 2$. If i is the smallest index so that $a_i = 2a_0$, then the minimal positive solution is (G_{i-1}, B_{i-1}).

If $D \equiv 2$ or $3 \pmod 4$, then by considerations modulo 4 one can that both x and y must be even. Set $X = x/2$, set $Y = y/2$, and solve $X^2 - DY^2 = \pm 1$. If (X, Y) is the minimal positive solution to this equation, then $x = 2X$, $y = 2Y$ is the minimal positive solution to $x^2 - Dy^2 = \pm 4$. Alternatively, use the PQa algorithm with $P_0 = 0$ and $Q_0 = 1$, but set $G_{-2} = 0$, $G_{-1} = 2$, $B_{-2} = 2$, and $B_{-1} = 0$. If i is the smallest index so that $a_i = 2a_0$, then the minimal positive solutions is (G_{i-1}, B_{i-1}).

As with the ± 1 equation, all solutions can be generated from the minimal positive solution. Consider first the equation $x^2 - Dy^2 = 4$. If (x_1, y_1) is the minimal positive solution to this equation, then for the n-th solution we have

$$\begin{aligned} x_n + y_n\sqrt{D} &= \frac{1}{2^{n-1}}(x_1 + y_1\sqrt{D})^n \\ x_n - y_n\sqrt{D} &= \frac{1}{2^{n-1}}(x_1 - y_1\sqrt{D})^n. \end{aligned} \tag{4.4.1}$$

Therefore

$$\begin{aligned} x_n &= \left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^n + \left(\frac{x_1 - y_1\sqrt{D}}{2}\right)^n \\ y_n &= \frac{1}{\sqrt{D}}\left[\left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^n - \left(\frac{x_1 - y_1\sqrt{D}}{2}\right)^n\right]. \end{aligned} \tag{4.4.2}$$

We also have the recursion

$$\begin{aligned} x_{n+1} &= \frac{1}{2}(x_1x_n + Dy_1y_n) \\ y_{n+1} &= \frac{1}{2}(y_1x_n + x_1y_n) \end{aligned} \tag{4.4.3}$$

The relations (4.4.3) could be written in the following useful matrix form

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{pmatrix}\begin{pmatrix} x_n \\ y_n \end{pmatrix} \tag{4.4.4}$$

from where

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \frac{1}{2^n}\begin{pmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{pmatrix}^n\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \tag{4.4.5}$$

where $(x_0, y_0) = (2, 0)$ is the trivial solution.

We can express all integer solutions to the positive equation by the following formula

$$\frac{1}{2}(u_n + v_n\sqrt{D}) = \varepsilon_n\left(\frac{u_1 + v_1\sqrt{D}}{2}\right)^n, \quad n \in \mathbb{Z}, \tag{4.4.6}$$

where ε_n is 1 or -1. Indeed, for $n > 0$ and $\varepsilon_n = 1$ we get all negative solutions. For $n > 0$ and $\varepsilon_n = -1$ we obtain all solutions (u_n, v_n) with u_n and v_n negative. For $n < 0$ and $\varepsilon_n = 1$ we have (u_n, v_n) with $u_n > 0$ and $v_n < 0$, while $n < 0$ and $\varepsilon_n = -1$ gives $u_n < 0$ and $v_n > 0$. The trivial solutions $(2, 0)$ and $(-2, 0)$ are obtained for $n = 0$.

Formula (4.4.6) captures all symmetries of equation $(u, v) \to (-u, -v)$, $(u, v) \to (u, -v)$, $(u, v) \to (-u, v)$. Therefore, in 2D the points (u_n, v_n) represents the orbits of the action of the Klein four-group $\mathbb{Z}_2 \times \mathbb{Z}_2$, i.e., points obtained by the 180 degree rotation, the vertical reflection, and by the horizontal reflection.

Now suppose the equation $x^2 - Dy^2 = -4$ has solutions, let (x_1, y_1) be the minimal positive solution, and define x_n, y_n by the equation $x_n + y_n\sqrt{D} = [(x_1 + y_1\sqrt{D})^n]/(2^{n-1})$. Then if n is odd, (x_n, y_n) is a solution to the equation $x^2 - Dy^2 = -4$, and if n is even then (x_n, y_n) is a solution to the equation $x^2 - Dy^2 = 4$. All positive solutions to these two equations are so generated. The pair (x_n, y_n) in (4.4.2) also alternately generates solutions to the $+4$ and -4 equation.

The set of solutions can be summarized as follows.

Theorem 4.4.1. *Let (x_1, y_1) be the minimal positive solution to $x^2 - Dy^2 = \pm 4$. Then for any solution to $x^2 - Dy^2 = \pm 4$, there is a choice of signs $+$ and $-$, and an integer n such that*

$$\frac{1}{2}(x + y\sqrt{D}) = \pm \left(\frac{x_1 + y_1\sqrt{D}}{2} \right)^n. \tag{4.4.7}$$

In some ways, the equation $x^2 - Dy^2 = \pm 4$ is more fundamental than the equation $x^2 - Dy^2 = \pm 1$. The numbers 1 and 4 are the only N's so that, for any D, if you know the minimal positive solution to the equation $x^2 - Dy^2 = \pm N$, you can generate all solutions, and you can do this without solving any other Pell's equation. Also, if you know the minimal positive solution to $x^2 - Dy^2 = \pm 4$, you can generate all the solutions to $x^2 - Dy^2 = \pm 1$. But the converse does not hold. The best that can be said as a converse is that for D not 5 or 12, the solutions to the equation $x^2 - Dy^2 = \pm 4$ can be derived from the intermediate steps when the PQa algorithm is used to solve the equation $x^2 - Dy^2 = \pm 1$.

When $D \equiv 1 \pmod 4$, considerations modulo 4 show that for any solution to $x^2 - Dy^2 = \pm 4$, x and y are both odd or both even. If the minimal positive solution has both x and y even, then all solutions have both x and y even. In this case, every solution to $x^2 - Dy^2 = \pm 1$ is just one-half of a solution to $x^2 - Dy^2 = \pm 4$. If the minimal positive solution to $x^2 - Dy^2 = \pm 4$ has both x and y odd, then $D \equiv 5 \pmod 8$, every third solution has x and y even, and all other solutions have x and y odd. In this case, every solution to $x^2 - Dy^2 = \pm 1$ is just one-half of one of the solutions to $x^2 - Dy^2 = \pm 4$ that has both x and y even. When $D \equiv 1 \pmod 4$, the equation $x^2 - Dy^2 = -4$ has solutions if and only if the equation $x^2 - Dy^2 = -1$ has solutions.

When $D \equiv 0 \pmod 4$, considerations modulo 4 show that for any solution to $x^2 - Dy^2 = \pm 4$, x is even. If the minimal positive solution has y even, then all solutions have y even (and x is always even). In this case, every solution to $x^2 - Dy^2 = \pm 1$ is just one-half of a solution to $x^2 - Dy^2 = \pm 4$. If the minimal positive solution to $x^2 - Dy^2 = \pm 4$ has y odd, then every other solution has y even, and every other solution has y odd. In this case, every solution to $x^2 - Dy^2 = \pm 1$ is

just one-half of one of the solutions to $x^2 - Dy^2 = \pm 4$ that has x and y both even. When $D \equiv 0 \pmod 4$, it is possible for these to be solutions to $x^2 - Dy^2 = -4$, but not solutions to $x^2 - Dy^2 = 1$. This happens for $D = 8, 20, 40, 52$ and many more values. Of course, $x^2 - Dy^2 = -1$ never has solutions when $D \equiv 0 \pmod 4$.

When $D \equiv 2 \pmod 4$ or $D \equiv 3 \pmod 4$, all solutions to $x^2 - Dy^2 = \pm 4$ have both x and y even. Every solution to $x^2 - Dy^2 = \pm 1$ is just one-half of a solution to $x^2 - Dy^2 = \pm 4$. The equation $x^2 - Dy^2 = -4$ has solutions if and only if the equation $x^2 - Dy^2 = -1$ has solutions.

The cases $D \equiv 1 \pmod 4$ for D squarefree, and $D = 4r$ for $r \equiv 2$ or $3 \pmod 4$, r squarefree, are treated in [53]. The material we have presented above is not addressed directly in either [159] or [142]. For example, the proof that the method for solving the equation works in the case $d \equiv 1 \pmod 4$ is not trivially derived from the material in one or both of these sources.

Remark. Concerning the equation $x^2 - Dy^2 = -4$ the following conjecture is still open: *Let p be a prime* $\equiv 1 \pmod 4$ *and let* (x_1, y_1) *be the fundamental solution to the equation* $x^2 - py^2 = -4$. *Then* $y_1 \not\equiv 0 \pmod p$.

This has been verified for all primes $p < 2000$ with $p \equiv 5 \pmod 8$ and for all primes $p < 100000$ with $p \equiv 1 \pmod 8$. Also, it has been shown that $y_1 \not\equiv 0 \pmod p$ if and only if $B_{\frac{p-1}{4}} \not\equiv 0 \pmod p$, where the Bernoulli numbers B_n are defined by the series

$$\frac{t}{e^t - 1} = 1 - \frac{t}{2} + \sum_{n=1}^{\infty} \frac{(-1)^{n-1} B_n}{(2n)!} t^{2n}.$$

4.4.3 Structure of Solutions to the General Pell's Equation

As we have seen in Section 4.1, if (r, s) is a solution to $x^2 - Dy^2 = N$, and (t, u) is any solution to its Pell's resolvent, then for $x = rt + Dsu$, $y = ru + st$, (x, y) is a solution to the equation $x^2 - Dy^2 = N$. This follows from the multiplication principle:

$$(r^2 - Ds^2)(t^2 - Du^2) = (rt + Dsu)^2 - D(ru + st)^2.$$

This fact can be used to separate solutions to $x^2 - Dy^2 = N$ into equivalence classes. Two solutions (x, y) and (r, s) are equivalent if there is a solution (t, u) to $t^2 - Du^2 = 1$ so that $x = rt + Dsu$ and $y = ru + st$.

It may help to view the set of solutions geometrically. If $N > 0$, then, as an equation in real numbers, $x^2 - Dy^2 = N$ is a hyperbola with the x-axis as its axis, and the y-axis as an axis of symmetry. The asymptotes are the lines $x \pm y\sqrt{D} = 0$. Let (t, u) be the minimal positive solution to $x^2 - Dy^2 = 1$. Draw the graph of $x^2 - Dy^2 = N$ over the reals. Mark the point $(\sqrt{N}, 0)$, which is on this graph.

Now mark the point $(t\sqrt{N}, u\sqrt{N})$, which is also on the graph. Continue marking points so that if (x, y) is the most recent point marked, then the next point marked is $(xt + Dyu, xu + yt)$. All of the points marked so far, apart from the first, have $x > 0$ and $y > 0$. Now, for each point (x, y) that has been marked, mark all of the points $(\pm x, \pm y)$ not yet marked.

The marked points divide the graph into intervals. Make the interval $((\sqrt{N}, 0), (t\sqrt{N}, u\sqrt{N})]$ a half-open interval, and then make the other intervals on this branch half-open by assigning endpoints to one interval. Make the intervals on the other half-open by mapping (x, y) in the right branch to $(-x, -y)$ on the left branch. If there are integer solutions to $x^2 - Dy^2 = N$, then

1) No two solutions within the same (half-open) interval are equivalent,
2) Every interval has exactly one solution in each class, and
3) The order of solutions by class is the same in every interval.

Instead of starting with the point $(\sqrt{N}, 0)$, we could have started with any point (r, s) on the graph, and marked off the points corresponding to $\pm(r + s\sqrt{D})(t + u\sqrt{D})^n$. The above three comments still apply.

The situation is similar in the case $N < 0$, except that the graph has the y-axis as its axis, and the x-axis is an axis of symmetry. If the negative Pell's equation $x^2 - Dy^2 = -1$ is solvable, then any of its solutions can be used to generate a correspondence between solutions to $x^2 - Dy^2 = N$ and $x^2 - Dy^2 = -N$.

Within a class there is a unique solution with x and y nonnegative, but smaller than any nonnegative solution. This is the minimal nonnegative solution for the class. There is also either one or two solutions so that y is nonnegative, and is less than or equal to any other nonnegative y in any solution (x, y) within the class. If there is one such solution, it is called the fundamental solution. If there are two such solutions, then they will be equivalent and their x-values will be negatives of each other. In this case, the solution with the positive x-value is called the fundamental solution for the class.

When tabulating solutions, it is usually convenient to make a list consisting of one solution from each class. Often, this list will consist of the minimal nonnegative solutions, or the fundamental solutions. Given any solution in a class, it is easy to find the fundamental solution or the minimal nonnegative solution for that class.

The results are summarized in the following

Theorem 4.4.2. *Given any solution in a class, all solutions in that class are derived from solutions to the equation $x^2 - Dy^2 = 1$. If (r, s) is any particular solution to $x^2 - Dy^2 = N$, (x, y) is any other solution to the same equation in the same class as (r, s) and if (t_1, u_1) is the fundamental solution to the Pell's resolvent, then for some choice of signs $+$ and $-$, and for some integer n*

$$x + y\sqrt{D} = \pm(r + s\sqrt{D})(t_1 + u_1\sqrt{D})^n. \tag{4.4.8}$$

We can write formulas similar to those presented for cases $N = \pm 1$ and $N = \pm 4$ in Section 4.4.2.

4.4.4 Solving the Equation $x^2 - Dy^2 = N$ for $N < \sqrt{D}$

When $1 < N^2 < D$, apply the PQa algorithm with $P_0 = 0$, $Q_0 = 1$. Continue the computations until you reach the first $i > 0$ with $G_i^2 - DB_i^2 = 1$ (i.e., $Q_{i+1} = 1$ and $i + 1$ is even). For $1 \le j \le i$, if $G_j^2 - DB_j^2 = N/f^2$ for some $f > 0$, add fG_j, fB_j to the list of solutions. When done, the list of solutions will have the minimal positive member of each class.

The list of all solutions can be generated using the methods of the previous section. Alternatively, all positive solutions can be generated by extending the PQa algorithm indefinitely.

4.4.5 Solving the Equation $x^2 - Dy^2 = N$ by Brute-Force Search

Let (t, u) be the minimal positive solution to $x^2 - Dy^2 = N$. If $N > 0$, set $y_1 = 0$, and $y_2 = \sqrt{\dfrac{(t-1)N}{2D}}$. If $N < 0$, set $y_1 = \sqrt{\dfrac{|N|}{2}}$, and $y_2 = \sqrt{\dfrac{(t+1)|N|}{2D}}$. For $y_1 \le y \le y_2$, if $N + Dy^2$ is a square, set $x = \sqrt{N + Dy^2}$. If (x, y) is not equivalent to $(-x, y)$, add both to the list of solutions, otherwise just add (x, y) to the list. When finished, this list gives the fundamental solutions.

This method works well if y_2 is not too large, which means that $\sqrt{\dfrac{(t \pm 1)|N|}{2D}}$ is not too large. Hence it suffices to search between the bounds y_1 and y_2.

To generate all solutions be performing this algorithm, refer to the structure of solutions of general Pell's equation given in Section 4.4.3.

4.4.6 Numerical Examples

In order to see how the algorithms that we have presented work, we will examine a few numerical examples. Computations were done by using MATHEMATICA.

Example 1. Consider the equations

$$x^2 - 109y^2 = \pm 1.$$

Apply the PQa algorithm with $P_0 = 0$ and $Q_0 = 1$. The following table gives the index, i, and then the several calculated quantities for $i = -2$ to 30.

i	P_i	Q_i	a_i	G_i	B_i	$G^2 - 109B^2$
-2				0	1	-109
-1				1	0	1
0	0	1	10	10	1	-9
1	10	9	2	21	2	5
2	8	5	3	73	7	-12
3	7	12	1	94	9	7
4	5	7	2	261	25	-4
5	9	4	4	1138	109	15
6	7	15	1	1399	134	-3
7	8	3	6	9532	913	3
8	10	3	6	58591	5612	-15
9	8	15	1	68123	6525	4
10	7	4	4	331083	31712	-7
11	9	7	2	730289	69949	12
12	5	12	1	1061372	101661	-5
13	7	5	3	3914405	374932	9
14	8	9	2	8890182	851525	-1
15	10	1	20	181718045	17405432	9
16	10	9	2	372326272	35662389	-5
17	8	5	3	1298696861	124392599	12
18	7	12	1	1671023133	160054988	-7
19	5	7	2	4640743127	444502575	4
20	9	4	4	20233995641	1938065288	-15
21	7	15	1	24874738768	2382567863	3
22	8	3	6	169482428249	16233472466	-3
23	10	3	6	1041769308262	99783402659	15
24	8	15	1	1211251736511	116016875125	-4
25	7	4	4	5886776254306	563850903159	7
26	9	7	2	12984804245123	1243718681443	-12
27	5	12	1	18871580499429	18075659584602	5
28	7	5	3	69599545743410	6666427435249	-9
29	8	9	2	158070671986249	15140424455100	1
30	10	1	20	3231012985468390	309474916537249	-9

We have $a_0 = 10$, and the first i so that $a_i = 2a_0$ is $i = 15$, at which point $a_{15} = 20$. Hence the period of a_i is 15, which is odd, and so the equation $x^2 - 109y^2 = -1$ has solutions. The minimal positive solution to $x^2 - 109y^2 = -1$ is $x = 8890182$, $y = 851525$. The minimal positive solution to $x^2 - 109y^2 = 1$ is $x = 158070671986249$, $y = 15140424455100$.

Example 2. Let us examine now the equations

$$x^2 - 109y^2 = \pm 4.$$

As $D \equiv 1 \pmod 4$, apply the PQa algorithm with $P_0 = 1$ and $Q_0 = 2$. The following table gives the index, i, and the standard quantities for $i = -2$ to 14.

i	P_i	Q_i	a_i	G_i	B_i	$G^2 - 109B^2$
-2				-1	1	-108
-1				2	0	4
0	1	2	5	9	1	-28
1	9	14	1	11	1	12
2	5	6	2	31	3	-20
3	7	10	1	42	4	20
4	3	10	1	73	7	-12
5	7	6	2	188	18	28
6	5	14	1	261	25	-4
7	9	2	9	2537	243	28
8	9	14	1	2798	268	-12
9	5	6	2	8133	779	20
10	7	10	1	10931	1047	-20
11	3	10	1	19064	1826	12
12	7	6	2	49059	4699	-28
13	5	14	1	68123	6535	4
14	9	2	9	662166	63424	-28

We have $a_0 = 5$, and the first i so that $a_i = 2a_0 - 1$ is $i = 7$, at which point $a_7 = 9$. Hence the period of a_i is 7, which is odd, and so the equation $x^2 - 109y^2 = -4$ has solutions. The minimal positive solution to $x^2 - 109y^2 = -4$ is $x = 261$, $y = 25$. The minimal positive solution to $x^2 - 109y^2 = 4$ is $x = 68123$, $y = 6525$.

Note that the third solution to $x^2 - 109y^2 = \pm 4$ can be computed from

$$\frac{1}{4}(261 + 25\sqrt{109})^3 = 17780364 + 1703050\sqrt{109}.$$

Upon dividing by 2, we get the minimal positive solution $x = 8890182$, $y = 851525$ to negative Pell's equation $x^2 - 109y^2 = -1$.

Example 3. Consider the equation

$$x^2 - 129y^2 = -5.$$

From Theorem 4.1.4 it follows that if this equation is solvable, then it has exactly two classes of solutions.

Here $N < \sqrt{D}$. Apply the PQa algorithm with $P_0 = 0$, $Q_0 = 1$.

i	P_i	Q_i	a_i	G_i	B_i	$G^2 - 129B^2$
-2				0	1	-129
-1				1	0	1
0	0	1	11	11	1	-8
1	11	8	2	23	2	13
2	5	13	1	34	3	-5
3	8	5	3	125	11	16
4	7	16	1	159	14	-3
5	9	3	6	1079	95	16
6	9	16	1	1238	109	-5
7	7	5	3	4793	422	13
8	8	13	1	6031	531	-8
9	5	8	2	16855	1484	1
10	11	1	22	376841	33179	-8

The only $f > 0$ so that f^2 divides -5 is $f = 1$. Reviewing the above for $G_j^2 - 129B_j^2 = -5$, we find solutions (x, y) equal to (34,3) and (1238,109). Thus, there are two classes of solutions, and these are the minimal positive solutions for these classes.

Example 4. Let us use the brute-force search method to find the fundamental solutions of

$$x^2 - 61y^2 = 15.$$

The minimal positive solution to Pell's resolvent $x^2 - 61y^2 = 1$ is $x = 1766319049$, $y = 226153980$. As $N = 15$ is positive, the lower search limit for y is 0, and the upper limit is

$$\sqrt{\frac{15(1766319049 - 1)}{2 \cdot 61}} \approx 14736,702.$$

So we search on y from 0 to 14736. Only $y = 11$ and $y = 917$ yield solutions, so the four fundamental solutions are $x = \pm 86$, $y = 11$, and $x = \pm 7162$, $y = 917$.

Example 5. For the same equation above, we will apply now the LMM algorithm given in Section 4.3.

The only $f > 0$ so that f^2 divides 15 is $f = 1$. Set $m = 15$. The z's with $-15/2 < z \leq 15/2$ and $z^2 \equiv 61 \pmod{15}$ are $z = \pm 1$, $z = \pm 4$.

Upon performing the PQa algorithm with $P_0 = 1$, $Q_0 = 15$, and $d = 61$, the first $Q_i = \pm 1$ occurs at $Q_9 = 1$. The corresponding solution has $x = G_8 = 2593$ and $y = B_8 = 332$. For this (x, y), $x^2 - 61y^2 = -15$. The equation $x^2 - 61y^2 = -1$ is solvable and the minimal positive solution is $x = 29718$, $y = 3805$. Applying this to the solution $(2593, 332)$ gives the solution $x = 154117634$, $y = 19732741$ to the equation $x^2 - 61y^2 = 15$. This is equivalent to the fundamental solution $(-86, 11)$.

Performing the PQa algorithm with $P_0 = -1$, $Q_0 = 15$, and $d = 61$, gives the first $Q_i = \pm 1$ at $Q_4 = 1$, yielding the fundamental solution $(86, 11)$ to the equation $x^2 - 61y^2 = 15$.

Performing the PQa algorithm with $P_0 = 4$, $Q_0 = 15$, and $d = 61$, gives the first $Q_i = \pm 1$ ate $Q_{10} = 1$, yielding the fundamental solution $(7162, 917)$ to the equation $x^2 - 61y^2 = 15$.

Performing the PQa algorithm with $P_0 = -4$, $Q_0 = 15$, and $d = 61$, gives the first $Q_i = \pm 1$ at $Q_3 = 1$, yielding the solution $(31, 4)$ to the equation $x^2 - 61y^2 = -15$. Applying the minimal positive solution to $x^2 - 61y^2 = -1$ gives the solution $x = 1849678$, $y = 236827$ to the equation $x^2 - 61y^2 = 15$. This is equivalent to the fundamental solution $(-7162, 917)$.

4.5 Solvability and Unsolvability of the Equation $ax^2 - by^2 = c$

Using the results in our papers [13, 14] and [17] we will present two general methods for solving the equation

$$ax^2 - by^2 = c. \tag{4.5.1}$$

We will also give sufficient conditions such that equation (4.5.1) is unsolvable in positive integers. In the special case $c = 1$, the equation (4.5.1) was studied in Section 3.5.

The equation (4.5.1) is also considered in the recent paper [114], where a, b, c are positive integers with $\gcd(a, b) = 1$. The author showed that if (4.5.1) is solvable, then it has infinitely many positive integer solutions. But his result is in fact a variant of the multiplication principle.

The following result given in [172] completely solves the problem of determining all solutions to equation (4.5.1).

Theorem 4.5.1. *Let a, b be positive integers such that $\gcd(a, b) = 1$ and a is squarefree, and let c be a nonzero integer. Denote $D = ab$, $N = ac$. Then (u, v) is a solution to the general Pell's equation*

$$u^2 - Dv^2 = N \tag{4.5.2}$$

if and only if $\left(\frac{u}{a}, v\right)$ is solution to (4.5.1).

Proof. Let (x, y) be a solution to (4.5.1). It follows that $(ax)^2 - aby^2 = ac$, so (ax, y) is a solution to the associated general Pell's equation (4.5.2).

Conversely, if (u, v) is a solution to (4.5.2), from the relation $u^2 - abv^2 = ac$ we obtain $a|u^2$. Taking into account that a is squarefree it follows that $a|u$. Therefore $u = a_1 a$ and $(a_1 a)^2 - abv^2 = ac$ yield $aa_1^2 - bv^2 = c$, i.e., $\left(\frac{u}{a}, v\right)$ is a solution to (4.5.1). □

Remarks. 1) From the above result it is clear that (4.5.1) is solvable if and only if the associated general Pell's equation (4.5.2) is solvable.

2) The assumption that a is squarefree is not a restriction. Indeed, if $a = a_1 m^2$ and a_1 is squarefree, then the equation (4.5.1) becomes $a_1 X^2 - by^2 = c$, where $X = mx$, i.e., an equation of the same type.

3) In order to solve (4.5.1) we determine all solutions (u, v) to the general Pell's equation (4.5.2). The desired solutions are given by $\left(\frac{u}{a}, v\right)$.

The equation (4.5.1) is strongly connected to the general Pell's equation (4.5.2) and to the Diophantine equation

$$as^2 - bt^2 = 1. \tag{4.5.3}$$

The solvability of these three equations is studied in the following theorem [17]:

Theorem 4.5.2. *Suppose that* $\gcd(a, b) = 1$ *and* ab *is not a perfect square. Then:*

1) If the equations (4.5.2) and (4.5.3) are solvable, then (4.5.1) is also solvable and all of its solutions (x, y) *are given by*

$$x = s_0u + bt_0v, \quad y = t_0u + as_0v \tag{4.5.4}$$

where (u, v) *is any solution to (4.5.2) and* (s_0, t_0) *is the minimal solution to (4.5.3).*

2) If the equations (4.5.1) and (4.5.3) are solvable, then (4.5.2) is also solvable.

3) If the equations (4.5.1) and (4.5.2) are solvable and there exist solutions (x, y), (u, v) *such that*

$$\frac{ux - bvy}{c} \quad \textit{and} \quad \frac{-avx + uy}{c}$$

are both integers, then (4.5.3) is solvable.

Proof. 1) We have

$$ax^2 - by^2 = a(s_0u + bt_0v)^2 - b(t_0u + as_0v)^2 =$$
$$= (as_0^2 - bt_0^2)(u^2 - abv^2) = 1 \cdot c = c,$$

and it follows that (x, y), given in (4.5.4), is a solution to the equation (4.5.1).

Conversely, let (x, y) be a solution to (4.5.1), and let (s_0, t_0) be the minimal solution to the equation (4.5.3). Then (u, v), where $u = as_0x - bt_0y$ and $v = -t_0x + s_0y$ is a solution to the general Pell's equation (4.5.2). Solving the above system of linear equations with unknowns x and y yields $x = s_0u + bt_0v$ and $y = t_0u + as_0v$, i.e., (x, y) has the form (4.5.4).

2) If (x, y) and (s, t) are solutions to (4.5.1) and (4.5.3), respectively, then (u, v), with $u = asx - bty$ and $v = -tx + sy$ is a solution to (4.5.2). Moreover, each solution to (4.5.2) is of the above form. Indeed, if (u, v) is an arbitrary solution to (4.5.2), then (x, y), where $x = su + btv$ and $y = tu + asv$, is a solution to (4.5.1). Thus, solving the above system of linear equations in u, v, it follows that $u = asx - bty$ and $v = -tx + sy$.

3) Let (x, y) and (u, v) be solutions to (4.5.1) and (4.5.2), respectively, for which

$$s = \frac{ux - bvy}{c} \in \mathbb{Z} \quad \text{and} \quad t = \frac{-avx + uy}{c} \in \mathbb{Z}.$$

Then (s, t) is a solution to (4.5.3). □

Remarks. 1) The equation $8x^2 - y^2 = 7$ is solvable and all of its solutions were determined in Section 4.1. For this equation, the associated equations (4.5.2) and (4.5.3) are $u^2 - 8v^2 = 7$ and $8s^2 - t^2 = 1$, respectively. It is interesting to see that both these equations are unsolvable.

2) In case of solvability of equations (4.5.2) and (4.5.3), the formulas (4.5.4) point out an alternative way to express the solutions to equation (4.5.1).

Theorem 4.5.3. *Let a, c be relatively prime positive integers, not both perfect squares, and let b and d be integers. The equation*

$$ax^2 - cy^2 = ad - bc \tag{4.5.5}$$

is solvable if and only if the numbers $an + b$ and $cn + d$ are perfect squares for some positive integer n. In this case, the number of such n's is infinite.

Proof. If (x_0, y_0) is a solution to the equation (4.5.5), then by Theorem 4.5.2, $(x_m, y_m)_{m\geq 0}$, where

$$x_m = x_0u_m + cy_0v_m, \quad y_m = ax_0v_m + y_0u_m \tag{4.5.6}$$

are solutions to this equation. Here $(u_m, v_m)_{m\geq 0}$ denotes the general solution to Pell's equation $u^2 - acv^2 = 1$.

Then $ax_m^2 - cy_m^2 = ad - bc$, $m = 0, 1, 2, \ldots$, hence

$$a(x_m^2 - d) = c(y_m^2 - b), \quad m = 0, 1, 2, \ldots \tag{4.5.7}$$

Since a and c are relatively prime, from (4.5.7) it follows that $a|y_m^2 - b$ and $c|x_m^2 - d$, $m = 0, 1, 2, \ldots$. Let

$$n_m = \frac{y_m^2 - b}{a} = \frac{x_m^2 - d}{c}, \quad m = 0, 1, 2, \ldots \tag{4.5.8}$$

Clearly, n_m is a positive integer for each m and

$$an_m + b = y_m^2, \quad cn_m + d = x_m^2, \quad m = 0, 1, 2, \ldots$$

i.e., the numbers $an + b$ and $cn + d$ are simultaneously perfect squares for infinitely many positive integers n.

If the equation (4.5.5) is not solvable in positive integers, then $an + b$ and $cn + d$ cannot be both perfect squares. Indeed, if we assume that there is a positive integer n_0 such that $an_0 + b = y_0^2$ and $cn_0 + d = x_0^2$ for some positive integers x_0, y_0, then by eliminating n_0 it follows that $ax_0^2 - by_0^2 = ad - bc$, in contradiction with the unsolvability of equation (4.5.5). □

Theorem 4.5.4. *Let a and b be positive integers such that for all positive integers n, $an + b$ is not a perfect square. Then the equations*

$$ax^2 - (am + v_0)y^2 = c, \quad m = 0, 1, 2, \ldots \tag{4.5.9}$$

and

$$(am + w_0)x^2 - ay^2 = c, \quad m = 0, 1, 2, \ldots \tag{4.5.10}$$

are not solvable in positive integers. Here c is a nonzero integer and (u_0, v_0) and (w_0, s_0) are the minimal solutions to the equations $au - bv = c$ and $bw - as = c$, respectively.

Proof. The general solutions to the linear Diophantine equations $au - bv = c$ and $bw - as = c$ are $(u_m, v_m)_{m\geq 0}$ and $(w_m, s_m)_{m\geq 0}$, respectively, where

$$u_m = u_0 + bm, \quad v_m = v_0 + am \quad \text{and} \quad w_m = w_0 + am, \quad s_m = s_0 + bm$$

(see [198]). Assume now that equation (4.5.9) is solvable and let (x, y) be a solution. Then $ax^2 - (am + v_0)y^2 = c$. But by considerations above, $c = au_m - bv_m$. It follows that

$$ax^2 - (am + v_0)y^2 = au_m - bv_m,$$

hence the equation (4.5.3), where $d = u_m$ and $c = u_m$ is solvable. From Theorem 4.5.3 we obtain that $an + b$ is a perfect square for some n, in contradiction with the hypothesis. □

Example 1. The numbers $10n+3$ are not perfect squares, $n = 0, 1, 2, \ldots$. Choosing $c = 1$, we find the minimal solutions to the equations $10u - 3v = 1$ and $3w - 10s = 1$. They are $(1, 3)$ and $(7, 2)$, respectively. From Theorem 4.5.4 it follows that the equations

$$10x^2 - (10m + 3)y^2 = 1 \quad \text{and} \quad (10m + 7)x^2 - 10y^2 = 1, \quad m = 0, 1, 2, \ldots$$

are not solvable.

Remark. In many situations it is not easy to find the minimal solutions (u_0, v_0) and (w_0, s_0) to the equations $au - bv = c$ and $bw - as = c$, respectively. In this cases we may replace (u_0, v_0) and (w_0, s_0) by any solution to the above equations and the results in Theorem 4.5.4 remain true.

Example 2. The numbers $5n + 2$ are not perfect squares for any positive integer n. The equations $5u - 2v = c$ and $2w - 5s = c$ have $(c, 2c)$ and $(3c, c)$ among their solutions, respectively. It follows that $u_m = c + 2m$, $v_m = 2c + 5m$, and $w_m = 3c + 5m$, $s_m = c + 2m$, $m = 0, 1, 2, \ldots$.

From Theorem 4.5.3 we obtain that the equations

$$5x^2 - (5m + 2c)y^2 = c \quad \text{and} \quad (5m + 3c)x^2 - 5y^2 = c, \quad m = 0, 1, 2, \ldots$$

are not solvable.

Example 3. In a similar manner, starting with the nonsquare numbers $3n + 2$, $n = 0, 1, 2, \ldots$, we deduce that equations

$$3x^2 - (3m + c)y^2 = c \quad \text{and} \quad (3m + 2c)x^2 - 3y^2 = c, \quad m = 0, 1, 2, \ldots$$

are not solvable in positive integers.

There are many situations in which the unsolvability of an equation of the type (4.5.1) can be proven by using modular arithmetics arguments.

Example 4 ([193]). The equation

$$(4m + 3)x^2 - (4n + 1)y^2 = 1$$

where m and n are positive integers, is not solvable.

Indeed, $x^2, y^2 \equiv 0$ or $1 \pmod 4$ and so $(4m + 3)x^2 \equiv 0$ or $3 \pmod 4$ and $(4n + 1)y^2 \equiv 0$ or $1 \pmod 4$. By combining the residues, we obtain

$$(4m + 3)x^2 - (4n + 1)y^2 \not\equiv 1 \pmod 4.$$

Example 5 ([192]). In a similar manner, we can prove that equations

$$(4k + 2)x^2 - (4l + 3)y^2 = 1 \quad \text{and} \quad 7mx^2 - (7n + 1)y^2 = 1,$$

where k, l and m, n are positive integers, are also not solvable.

A criterion for solvability (unsolvability) for a class of general Pell's equations is given in [100] (see also subsection 4.2.4).

Theorem 4.5.5. *For N a squarefree integer, the equation*

$$x^2 - 2y^2 = N \tag{4.5.11}$$

is solvable if and only if it is solvable modulo N.

Proof. By multiplicativity, it suffices to show that $x^2 - 2y^2 = N$ has a solution for $N = -1$, $N = 2$, and $N = p$ for p an odd prime such that 2 is congruent to a square modulo p. For $N = -1$, use $1^2 - 2 \cdot 1^2 = -1$; for $N = 2$, use $2^2 - 2 \cdot 1^2 = 2$.

Now suppose p is an odd prime such that 2 is congruent to a square modulo p. Find x, y such that $x^2 - 2y^2$ is divisible by p but not by p^2 (if it is divisible by p^2, fix that by replacing x with $x + p$). Now form the ideal $(x + y\sqrt{D}, p)$. Its norm divides p^2 and $x^2 - 2y^2$, so it must be p. □

Incidentally, one can replace 2 by any integer D such that $\mathbb{Q}(\sqrt{D})$ has unique factorization, provided that $x^2 - Dy^2 = -1$ has a solution. It turns out (but is by no means obvious!) that unique factorization implies that D is prime, and it is believed (but not proved) that $\mathbb{Q}(\sqrt{D})$ has unique factorization for about 75 % of the primes D. Moreover, existence of a solution of $x^2 - Dy^2 = -1$ then implies $D \equiv 1 \pmod 4$, but nor every prime congruent to 1 modulo 4 will work (try $D = 5$).

4.6 Solving the General Pell Equation by Using Quadratic Rings

The main purpose of this section is to present an algorithm for finding all positive integer solutions to the general Pell's equation

$$x^2 - Dy^2 = k \tag{4.6.1}$$

where d is a nonsquare positive integer and k is a nonzero integer. We will follow the method described in [76] (see also [171]).

Let (x, y) be an integral solution of (4.6.1), i.e., $x^2 - Dy^2 = k$. We are going to use the results in Section 2.2.2. We have $N(\mu) = k$, where $\mu = x + \sqrt{D}y \in R$. If ε_0 is the fundamental unit of the ring R found in Theorem 3.4.1, then we will denote

$$\varepsilon = \begin{cases} \varepsilon_0, \text{ if } N(\varepsilon_0) = 1 \\ \varepsilon_0^2, \text{ if } N(\varepsilon_0) = -1. \end{cases}$$

Then the vectors $(1, 1)$ and $l(\varepsilon)$ form a base in the linear space $\mathbb{R}^2$. Indeed, if $\alpha(1, 1)+\beta l(\varepsilon) = 0$, with $\alpha, \beta \in \mathbb{R}$, then $\alpha+\beta \ln |\varepsilon| = 0$ and $\alpha+\beta \ln |\overline{\varepsilon}| = 0$. Since $\ln |\overline{\varepsilon}| = -\ln |\varepsilon| \neq 0$, from the previous two relations it follows that $\alpha = \beta = 0$.

If $\mu = x + y\sqrt{D} \in R$ and $N(\mu) = k$, then $k \neq 0$ implies $\mu \neq 0$, i.e., the vector $l(\mu)$ is well defined in $\mathbb{R}^2$. By using the fact that $(1, 1)$ and $l(\varepsilon)$ form a base in $\mathbb{R}^2$, we deduce the existence of $\alpha, \gamma \in \mathbb{R}$ such that $l(\mu) = \alpha(1, 1) + \gamma l(\varepsilon)$. This means that

$$\ln \mu = \alpha + \gamma \ln |\varepsilon| \quad \text{and} \quad \ln \overline{\mu} = \alpha + \gamma \ln |\overline{\varepsilon}|.$$

In particular, it follows that

$$\ln |k| = \ln |N(\mu)| = \ln |\mu| + \ln |\overline{\mu}| = 2\alpha + \gamma \ln |N(\varepsilon)| = 2\alpha,$$

i.e.,

$$\alpha = \frac{\ln |k|}{2} \quad \text{and} \quad l(\mu) = \frac{\ln |k|}{2}(1, 1) + \gamma l(\varepsilon).$$

Let a be the closest integer to γ, and let $\mu_0 = \varepsilon^{-\alpha}\mu$. Then $\mu \sim \mu_0$ and $N(\mu_0) = N(\mu) = k$. In addition,

$$l(\mu_0) = \frac{\ln |k|}{2}(1, 1) + \gamma_1 l(\varepsilon),$$

where $|\gamma_1| \leq \frac{1}{2}$ and $\gamma_1 = \gamma - a$. Therefore

$$\ln|\mu_0| = \frac{\ln|k|}{2} + \gamma_1 \ln\varepsilon \quad \text{and} \quad \ln|\overline{\mu}_0| = \frac{\ln|k|}{2} + \gamma_1 \ln|\overline{\varepsilon}| = \frac{\ln|k|}{2} - \gamma_1 \ln\varepsilon$$

(we have used here that $\varepsilon > 1$). It follows that

$$\left|\ln|\mu_0| - \frac{\ln|k|}{2}\right| \leq \frac{1}{2}\ln\varepsilon \quad \text{and} \quad \left|\ln|\overline{\mu}_0| - \frac{\ln|k|}{2}\right| \leq \frac{1}{2}\ln\varepsilon.$$

The above inequalities can be written as

$$\ln\sqrt{\frac{|k|}{\varepsilon}} \leq \ln|\mu_0| \leq \ln\sqrt{\varepsilon|k|} \quad \text{and} \quad \ln\sqrt{\frac{|k|}{\varepsilon}} \leq \ln|\overline{\mu}_0| \leq \ln\sqrt{\varepsilon|k|}.$$

We obtain

$$\sqrt{\frac{|k|}{\varepsilon}} \leq |\mu_0| \leq \sqrt{\varepsilon|k|} \quad \text{and} \quad \sqrt{\frac{|k|}{\varepsilon}} \leq |\overline{\mu}_0| \leq \sqrt{\varepsilon|k|}. \tag{4.6.2}$$

The numbers $|\mu_0|$ and $|\overline{\mu}_0|$ can be written as $s + t\sqrt{D}$, where s and t are positive integers. Since $t\sqrt{D} \leq \max\{|\mu_0|, |\overline{\mu}_0|\} \leq \sqrt{\varepsilon|k|}$, we have

$$t \leq \sqrt{\frac{\varepsilon|k|}{D}} \quad \text{and} \quad s \leq \sqrt{\varepsilon|k|}. \tag{4.6.3}$$

We will now describe the actual algorithm.

Step 1. Search for elements $\mu_1, \mu_2, \ldots, \mu_r$ in R of the form $s + t\sqrt{D}$ such that s, t are positive integers satisfying inequalities (4.6.3) and $N(\mu_i) = k$, $i = 1, 2, \ldots, r$.

From the inequalities (4.6.3) it follows that there are finitely many such μ's in R. This fact also follows from Theorem 2.2.3.

Step 2. From Theorem 3.4.1 it follows that all elements $\mu \in R$ with $N(\mu) = k$ are of the form $\mu = \pm\mu_i\varepsilon^l$ or $\mu = \pm\overline{\mu}_i\varepsilon^l$, for some $i \in \{1, 2, \ldots, r\}$ and some integer l.

Finally, let us mention that we can determine the fundamental unit $\varepsilon_0 \in R$ in a finite number of steps. For this part we refer to Section 3.3, where we employed continued fractions.

4.7 Another Algorithm for Solving General Pell's Equation

In what follows we will present a different algorithm for solving the general Pell's equation (4.6.1). Our approach is based on the one given in [171] and [95].

It suffices to consider solutions (x, y) to (4.6.1) such that the positive integers x and y are relatively prime.

If $|k| < \sqrt{D}$, then we apply Theorem 3.3.1. When $k \neq (-1)^{n-1}q_{n+1}$ for all n, the equation (4.6.1) is not solvable. When $k = (-1)^{n-1}q_{n+1}$ for some n, the pair (h_n, k_n) is a solution to the general Pell's equation (4.6.1) and all other of its integral solutions are given by

$$x + y\sqrt{D} = (\pm h_n \pm k_n\sqrt{D})\varepsilon^l, \quad l \in \mathbb{Z},$$

where is the fundamental solution of the Pell's resolvent.

If $|k| > \sqrt{D}$, then we write $k = \delta k_0$, where $\delta = \pm 1$ and k_0 is a positive integer. Since x and y are relatively prime, there exist integers x_1 and y_1 such that $xy_1 - yx_1 = \delta$.

It follows that

$$(xx_1 - Dyy_1)^2 - D = (xx_1 - Dyy_1)^2 - D(xy_1 - yx_1)^2 =$$
$$= (x^2 - Dy^2)(x_1^2 - Dy_1^2) = k(x_1^2 - Dy_1^2) = \delta k_0(x_1^2 - Dy_1^2).$$

Hence

$$(xx_1 - Dyy_1)^2 - D = \delta k_0(x_1^2 - Dy_1^2). \tag{4.7.1}$$

If (x_0, y_0) is a solution to the equation $xy_1 - yx_1 = \delta$, then the general solution to this equation is given by

$$x_1 = x_0 + tx \quad \text{and} \quad y_1 = y_0 + ty, \quad t \in \mathbb{Z}.$$

We have

$$xx_1 - Dyy_1 = xx_0 - Dyy_0 + t(x^2 - Dy^2) = xx_0 - Dyy_0 + t\delta k_0.$$

We will choose t such that

$$|xx_1 - Dyy_1| \leq \frac{k_0}{2}. \tag{4.7.2}$$

Denoting by l the positive integer $|xx_1 - Dyy_1|$, from (4.7.1) we obtain

$$x_1^2 - Dy_1^2 = \frac{l^2 - D}{\delta k_0} = \eta h, \tag{4.7.3}$$

where $\eta = \pm 1$ and h is a positive integer.

Using the inequalities $\sqrt{D} < k_0$ and $l < \frac{k_0}{2}$, from (4.7.3) it follows that

$$h \leq \frac{\max\{D, l^2\}}{k_0} < \frac{\max\left\{k_0^2, \frac{k_0^2}{4}\right\}}{k_0} = \frac{k_0^2}{k_0} = k_0.$$

If $h < k_0$, then we apply again Theorem 3.3.1 and obtain x_1 and y_1 such that $x_1^2 - Dy_1^2 = \eta h$. From the equalities $xy_1 - yx_1 = \delta$ and $xx_1 - Dyy_1 = \pm l$ we deduce the following formulas:

$$x = \frac{-\delta D y_1 \pm l x_1}{\eta h} \quad \text{and} \quad y = \frac{-\delta x_1 \pm l y_1}{\eta h}. \tag{4.7.4}$$

Hence the integers x and y can be obtained from the equality

$$\eta h(x + y\sqrt{D}) = (x_1 + y_1\sqrt{D})(\pm l - \delta\sqrt{D}).$$

Taking norms in the above equality yields

$$h^2(x^2 - Dy^2) = (x_1^2 - Dy_1^2)(l^2 - D) = \eta h \cdot \eta h \cdot \delta k_0 = h^2 \delta k_0,$$

and so $x^2 - Dy^2 = \delta k_0 = k$.

Therefore, if x and y given in (4.7.4) are integers, then (x, y) is a solution to the general Pell's equation (4.6.1).

If $h > \sqrt{D}$, then we apply again the described procedure.

The considerations above can be summarized in the following algorithm.

Step 1. Find all solutions to the congruence

$$l^2 \equiv D \pmod{k_0},$$

where l is a positive integer and $0 \leq l \leq \dfrac{k_0}{2}$. Denote by $l_1, l_2, \ldots, l_r$ those satisfying the inequalities $0 \leq l \leq \dfrac{k_0}{2}$. Set

$$\frac{l_i^2 - D}{\delta k_0} = \eta_i h_i, \quad i = 1, 2, \ldots, r,$$

where $\eta_i = \pm 1$ and h_i is a positive integer.

Step 2. If $k_0 < \sqrt{D}$, apply Theorem 3.3.1.

Step 3. If $k_0 > \sqrt{D}$, consider the equations

$$x_1^2 - Dy_1^2 = \eta_i h_i, \quad i = 1, 2, \ldots, r.$$

From the previous observations we have $0 < h_i < k_0$, $i =, 1, 2 \ldots, r$.

Step 4. Fix $i \in \{1, 2, \ldots, r\}$.

I. If $h_i < \sqrt{D}$, apply Theorem 3.3.1 to get the solutions to the equation $x_i^2 - Dy_i^2 = \eta_i h_i$. Then the solutions (x, y) are among those given by

$$x = \frac{-\delta D y_i \pm l_i x_i}{\eta_i h_i} \quad \text{and} \quad y = \frac{-\delta x_i \pm l_i y_i}{\eta_i h_i}. \tag{4.7.5}$$

II. If $h_i > \sqrt{D}$, repeat Step 3, replacing δ by η_i and k_0 by h_i. Since $0 < h_i < k_0$, after finitely many operations we will find all solutions to the given equation.

Remark. The two algorithms presented in Sections 4.5 and 4.6 are comparable. None is superior to the other and, moreover, they complete one another. The algorithm in Section 4.5 is preferable for large k's or large D's. The second is more efficient for small k's, for example when k satisfies the inequalities $-\sqrt{D} < k < \sqrt{D}$ (see also Subsection 4.3.4).

4.8 The Diophantine Equation $ax^2 + bxy + cy^2 = N$

The standard approach to solving the equation

$$ax^2 + bxy + cy^2 = N \tag{4.8.1}$$

in relatively prime integers x, y, is via reduction of quadratic forms, as in [127]. There is a parallel approach in [71] which uses continued fractions.

However, in a memoir of 1770, Lagrange, gave a more direct method for solving (4.8.1) when $\gcd(a, b, c) = \gcd(a, N) = 1$ and $D = b^2 - 4ac > 0$ is not a perfect square. This seems to have been largely overlooked. (Admittedly, the necessity part of his proof is long and not easy to follow.)

In [175], equation (4.8.1) is solved when $N = \pm\mu$, where

$$\mu = \min_{(x,y)\neq(0,0)} |ax^2 + bxy + cy^2|.$$

The approach is similar to Lagrange's reduction to the case $N = \pm 1$.

In the doctoral dissertation [157] the equation (4.8.1) is also discussed, using a standard convergent sufficiency condition of Lagrange, which resulted in the restriction $D \geq 16$, thus making rigorous the necessity part of Lagrange's discussion. Only the case $b = 0$ is discussed in detail, along the lines of [57].

The approach using the convergent criterion of Lemma 4.3.1, which results in no restriction on D, while allowing us to deal with the non-convergent case, without having to appeal to the case $\mu = 1$ in [175], whose proof is somewhat complicated.

The continued fractions approach also had the advantage that it produces the solution (x, y) with least positive y from each class, if $\gcd(a, N) = 1$.

The assumption $\gcd(a, N) = 1$ involves no loss of generality. For as pointed out by Gauss in his Disquisitiones (see [95]), there exist relatively prime integers α, γ such that $a\alpha^2 + b\alpha\gamma + c\gamma^2 = A$, where $\gcd(A, N) = 1$. Then, if $\alpha\delta - \beta\gamma = 1$, the unimodular transformation $x = \alpha X + \beta Y$, $y = \gamma X + \delta Y$ converts $ax^2 + bxy + cy^2$ to $AX^2 + BXY + CY^2$. Also, the two forms represent the same integers.

Let us illustrate how we can solve (4.8.1) via the reduction of the quadratic form in the left-hand side. By multiplying both sides of (4.8.1) by $4a$ and completing the square we obtain

$$(2ax + by)^2 - Dy^2 = 4aN, \tag{4.8.2}$$

where $D = b^2 - 4ac$. Assume that $D > 0$ and D is not a perfect square. Then (4.8.2) is a general Pell's equation. Let (u_n, v_n) be the general solution to its Pell's resolvent $u^2 - Dv^2 = 1$ and let (α, β) be the fundamental solution of the class K to the equation $X^2 - DY^2 = 4aN$ (see Section 4.1). Following [39], we have:

Theorem 4.8.1. *All integer solutions $(x_n, y_n)_{n\geq 1}$ to (4.8.1) are given by*

$$\begin{cases} x_n = \dfrac{(\alpha - b\beta)u_n - (b\alpha - D\beta)v_n}{2a} \\ y_n = \beta u_n + \alpha v_n, \end{cases} \tag{4.8.3}$$

where $(u_n, v_n)_{n\geq 1}$ is the solution to the Pell's resolvent, and (α, β) is the fundamental solution of the class K.

Proof. Let $X = 2ax + by$, $Y = y$, and $N_1 = 4aN$. By Theorem 4.1.3, we obtain the general solution to $X^2 - DY^2 = N_1$

$$X_n = \alpha u_n + D\beta v_n \quad \text{and} \quad Y_n = \beta u_n + \alpha v_n.$$

Solving the linear system

$$\begin{cases} 2ax_n + by_n = \alpha u_n + D\beta v_n \\ y_n = \beta u_n + \alpha v_n \end{cases}$$

we get the formulas (4.8.3).

Now let us show that x_n is an integer. To prove this, it is enough to show $2a \mid \alpha - b\beta$ and $2a \mid \alpha b - \beta D$. Indeed, we have $\alpha - b\beta = 2ax$ and

$$\alpha b - \beta D = \alpha b - \beta(b^2 - 4ac) = (\alpha - b\beta)b + 4ac\beta = 2axb + 4ac\beta = 2a(x\beta + 2c\beta),$$

and the properties follow. □

Example. The equation in Example 5, page 54, in the book [22] is reduced to

$$x^2 - 5xy + y^2 = -3. \tag{4.8.4}$$

In the reference [22] the equation (4.8.4) is solved by Fermat's method of infinite descent. Let us illustrate the method in Theorem 4.8.1 for finding the solutions to (4.8.4). The equation (4.8.4) is equivalent to

$$(2x - 5y)^2 - 21y^2 = -12.$$

Let $X = 2x-5y$ and $Y = y$. We obtain the general Pell's equation $X^2-21Y^2 = -12$. The Pell's resolvent $u^2-21v^2 = 1$ has the fundamental solution $(u_1, v_1) = (55, 12)$, hence its general solution $(u_n, v_n)_{n\geq 1}$ is given by $u_n + v_n\sqrt{21} = (55 + 12\sqrt{21})^n$. Using the upper bounds in the Remark after Theorem 4.1.3, we have

$$0 \leq |X| \leq \sqrt{\frac{|N|u_1 + N}{2}} = \sqrt{\frac{12 \cdot 55 - 12}{2}} = \sqrt{6 \cdot 54} = 18,$$

$$0 < Y \leq \sqrt{\frac{|N|u_1 - N}{2D}} = \sqrt{\frac{12 \cdot 55 + 12}{2 \cdot 21}} = \sqrt{16} = 4.$$

Therefore, we obtain the possibilities $|X| = 0, 1, \ldots, 18$ and $Y = 1, 2, 3, 4$. Then we get four solutions $(3, 1)$, $(-3, 1)$, $(18, 4)$, $(-18, 4)$ to the equation $X^2 - 21Y^2 = -12$. It is easy to check that these solutions are not associated with each other and they generates four classes of solutions to the above general Pell's equation. From Theorem 4.8.1 we get all integer solutions to equation (4.8.4):

$$\begin{aligned}&(4u_n + 18v_n, u_n + 3v_n), \qquad (u_n + 3v_n, u_n - 3v_n),\\ &(19u_n + 87v_n, 4u_n + 18v_n), \ (u_n - 3v_n, 4u_n - 18v_n), \ n \geq 1.\end{aligned}$$

These four classes of solutions give a partition of the solution obtained in the above-mentioned reference [22].

4.9 Thue's Theorem and the Equations $x^2 - Dy^2 = \pm N$

In this section, following the papers [86, 87, 128] and [225] we show how to obtain explicit representations of certain integers in the form $x^2 - Dy^2$ for small $D > 1$, using a constructive version of Thue's theorem based on Euclid's algorithm. Amongst other things, if $u^2 \equiv D \pmod N$, $D \not\equiv 1 \pmod N$ is solvable and $\gcd(D, N) = 1$, N odd, we show how to find the following representations:

$N = 8k \pm 1$	$N = x^2 - 2y^2$ $-N = x^2 - 2y^2$
$N = 12k + 1$	$N = x^2 - 3y^2$
$N = 12k - 1$	$-N = x^2 - 3y^2$
$N = 5k + 1$	$N = x^2 - 5y^2$
$N = 5k - 1$	$-N = x^2 - 5y^2$
$N = 24k + 1$ or $24k - 5$	$N = x^2 - 6y^2$
$N = 24k - 1$ or $24k + 5$	$-N = x^2 - 6y^2$
$N = 28k + 1,\ 28k + 9$ or $28k + 25$	$N = x^2 - 7y^2$
$N = 28k - 1,\ 28k - 9$ or $28k - 25$	$-N = x^2 - 7y^2$

4.9.1 Euclid's Algorithm and Thue's Theorem

Let a and b be natural numbers, $a > b$, where b does not divide a. Let $r_0 = a$, $r_1 = b$, and for $1 \le k \le n$, $r_{k-1} = r_k q_k + r_{k+1}$, where $0 < r_{k+1} < r_k$ and $r_n = 0$. Define sequences $s_0, s_1, \ldots, s_{n+1}$ and $t_0, t_1, \ldots, t_{n+1}$ by

$$s_0 = 1,\ s_1 = 0,\ t_0 = 0,\ t_1 = 1,\ t_{k+1} = -q_k t_k + t_{k-1},\ s_{k+1} = -q_k s_k + s_{k-1},$$

for $1 \le k \le n$. Then the following are easily proved by induction:

(i) $s_k = (-1)^k |s_k|,\ t_k = (-1)^{k+1} |t_k|$;
(ii) $0 = |s_1| < |s_2| < \ldots |s_{n+1}|$;
(iii) $1 = |t_1| < |t_2| < \cdots < |t_{n+1}|$;
(iv) $a = |t_k| r_{k-1} + |t_{k-1}| r_k$ for $1 \le k \le n+1$;
(v) $r_k = s_k a + t_k b$ for $1 \le k \le n+1$.

Theorem 4.9.1 (Thue). *Let a and b be integers, $a > b > 1$ with $\gcd(a,b) = 1$. Then the congruence $bx \equiv y \pmod{a}$ has a solution in nonzero integers x and y satisfying $|x| < \sqrt{a}$, $|y| \le a$.*

Proof. As $r_n = \gcd(a,b) = 1$, $a > \sqrt{a} > 1$, and the remainders $r_0, \ldots, r_n$ in Euclid's algorithm decrease strictly to 1, there is a unique index k such that $r_{k-1} > \sqrt{a} \ge r_k$. Then the equation $a = |t_k| r_{k-1} + |t_{k-1}| r_k$ gives $a \ge |t_k| r_{k-1} > |t_k| \sqrt{a}$. Hence $|t_k| < \sqrt{a}$.

Finally, $r_k = s_k a + t_k b$, so $b t_k \equiv r_k \pmod{a}$ and we can take $x = t_k$, $y = r_k$. □

4.9.2 The Equation $x^2 - Dy^2 = N$ with Small D

Let $N \ge 1$ be an odd integer, $D > 1$ and not a perfect square. Then a necessary condition for solvability of the equation $x^2 - Dy^2 = \pm N$ with $\gcd(x,y) = 1$ is that the congruence $u^2 \equiv D \pmod{N}$ is solvable. From now on we assume this, together with $\gcd(D,N) = 1$ and $1 < u < N$. Then the Jacobi symbol $\left(\frac{D}{N}\right) = 1$. We note that if N is prime, then $\left(\frac{D}{N}\right) = 1$ also implies that $u^2 \equiv D \pmod{N}$ is solvable.

If we take $a = N$ and $b = u$ in Euclid's algorithm, the integers $r_k^2 - D t_k^2$ decrease strictly for $k = 0, \ldots, n$, from a^2 to $1 - D t_n^2$ and are always multiples of N. For

$$r_k^2 - D t_k^2 \equiv t_k^2 u^2 - D t_k^2 \equiv t_k^2 (u^2 - D) \equiv 0 \pmod{N}.$$

If k is chosen so that $r_{k-1} > \sqrt{N} > r_k$, as in the proof of Thue's theorem, then as

$$N = r_{k-1} |t_k| + r_k |t_{k-1}| > r_{k-1} |t_k|, \tag{4.9.1}$$

we have $|t_k| < \sqrt{N}$ and

$$-DN < r_k^2 - Dt_k^2 < N. \tag{4.9.2}$$

Hence $r_k^2 - Dt_k^2 = -lN$, $-1 < l < D$. In fact, $1 \le l < D$, so

$$-DN < r_k^2 - Dt_k^2 \le -N. \tag{4.9.3}$$

Also $r_k^2 + lN = Dt_k^2$ and hence $Dt_k^2 > lN$,

$$|t_k| > \sqrt{\frac{lN}{D}}. \tag{4.9.4}$$

From equation (4.9.1), $N > r_{k-1}|t_k|$ and inequality (4.9.4) implies

$$r_{k-1} < \sqrt{\frac{DN}{l}}. \tag{4.9.5}$$

4.9.3 The Equations $x^2 - 2y^2 = \pm N$

The assumption $\left(\frac{2}{N}\right) = 1$ is equivalent to $N \equiv \pm 1 \pmod 8$. Also $1 \le l < 2$, so $l = 1$ and (4.9.3) gives $r_k^2 - 2t_k^2 = -N$. Hence from equation (4.9.5) with $D = 2$, $r_{k-1} < \sqrt{2N}$ and

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

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

Example. Let $N = 10000000033$, a prime of the form $8n + 1$. Then $u = 87196273$ gives $k = 10$, $r_{10} = 29015$, $t_{10} = -73627$, $r_9 = 118239$, $t_9 = 44612$ and $r_{10}^2 - 2t_{10}^2 = -N$, $r_9^2 - 2t_9^2 = N$.

Remark. We can express r_{k-1} and t_{k-1} in terms of r_k and t_k. The method is useful later for delineating cases when $D = 5, 6, 7$:

Using the identities

$$(r_k r_{k-1} - Dt_k t_{k-1})^2 - D(t_k r_{k-1} - t_{k-1} r_k)^2 = (r_k^2 - Dt_k^2)(r_{k-1}^2 - Dt_{k-1}^2) \tag{4.9.6}$$

and

$$(-1)^k N = r_k t_{k-1} - r_{k-1} t_k, \tag{4.9.7}$$

we deduce that

$$r_k r_{k-1} - D t_k t_{k-1} = \varepsilon N, \tag{4.9.8}$$

where $\varepsilon = \pm 1$.

From equation (4.9.8) we see that $\varepsilon = 1$, as $t_k t_{k-1} < 0$. Hence

$$r_k r_{k-1} + D T_k T_{k-1} = N, \tag{4.9.9}$$

where $T_k = |t_k|$. Then solving equations (4.9.7) and (4.9.9) with $D = 2$ for r_{k-1} and T_{k-1} yields

$$r_{k-1} = -r_k + 2T_k, \quad T_{k-1} = T_k - r_k.$$

The integers N, $|N| \leq 200$, such that the equation $x^2 - 2y^2 = N$ is solvable are: ± 1, ± 2, ± 4, ± 7, ± 8, ± 9, ± 14, ± 16, ± 17, ± 18, ± 23, ± 25, ± 28, ± 31, ± 32, ± 34, ± 36, ± 41, ± 46, ± 47, ± 49, ± 50, ± 56, ± 62, ± 63, ± 64, ± 68, ± 71, ± 72, ± 73, ± 79, ± 81, ± 82, ± 89, ± 92, ± 94, ± 97, ± 98, ± 100, ± 103, ± 112, ± 113, ± 119, ± 121, ± 124, ± 126, ± 127, ± 128, ± 136, ± 137, ± 142, ± 144, ± 146, ± 151, ± 153, ± 158, ± 161, ± 162, ± 164, ± 167, ± 169, ± 175, ± 178, ± 184, ± 188, ± 191, ± 193, ± 194, ± 196, ± 199, ± 200.

The following table presents the numbers $k(2, N)$ of classes of solutions and the sets $\mathcal{K}(2, N)$ of fundamental solutions of classes of $x^2 - 2y^2 = N$, when the equations are solvable and N is positive or negative, $|N| \leq 18$ [161].

$x^2 - 2y^2 = N$	$k(2, N)$	$\mathcal{K}(2, N)$
$x^2 - 2y^2 = 2$	1	$(2, 1)$
$x^2 - 2y^2 = -2$	1	$(4, 3)$
$x^2 - 2y^2 = 4$	1	$(6, 4)$
$x^2 - 2y^2 = -4$	1	$(2, 2)$
$x^2 - 2y^2 = 7$	2	$(3, 1),\ (5, 3)$
$x^2 - 2y^2 = -7$	2	$(1, 2),\ (5, 4)$
$x^2 - 2y^2 = 8$	1	$(4, 2)$
$x^2 - 2y^2 = -8$	1	$(8, 6)$
$x^2 - 2y^2 = 9$	1	$(9, 6)$
$x^2 - 2y^2 = -9$	1	$(3, 3)$
$x^2 - 2y^2 = 14$	2	$(4, 1),\ (8, 5)$
$x^2 - 2y^2 = -14$	2	$(2, 3),\ (6, 5)$
$x^2 - 2y^2 = 16$	1	$(12, 8)$
$x^2 - 2y^2 = -16$	1	$(4, 4)$
$x^2 - 2y^2 = 17$	2	$(5, 2),\ (7, 4)$
$x^2 - 2y^2 = -17$	2	$(1, 3),\ (9, 7)$
$x^2 - 2y^2 = 18$	1	$(6, 3)$
$x^2 - 2y^2 = -18$	1	$(12, 9)$

Here are four examples of general Pell's equations $x^2 - 2y^2 = N$, with N big: $k(2, 833) = 6$ and $\mathcal{K}(2, 833) = \{(29,2), (31,8), (35,14), (49,28), (61,38), (79,52)\}$; $k(2, 1666) = 5$ and $\mathcal{K}(2, 1666) = \{(42,7), (46,15), (54,25), (62,33), (98,63)\}$; $k(2, 2737) = 7$ and $\mathcal{K}(2, 2737) = \{(53,6), (55,12), (57,16), (75,38), (107,66), (117,74), (135,88)\}$; $k(2, 3689) = 8$ and $\mathcal{K}(2, 3689) = \{(61,4), (67,20), (71,26), (83,40), (89,46), (109,64), (121,74), (167,110)\}$.

4.9.4 The Equations $x^2 - 3y^2 = \pm N$

The assumption $\left(\frac{3}{N}\right) = 1$ is equivalent to $N \equiv \pm 1 \pmod{12}$. From equation (4.9.3), we have $-3N < r_k^2 - 3t_k^2 \leq -N$. Hence $r_k^2 - 3t_k^2 = -2N$ or $-N$.

Case 1. Assume $N \equiv 1 \pmod{12}$. Then $r_k^2 - 3t_k^2 = -N$ would imply the contradiction $r_k^2 \equiv -1 \pmod{3}$.

Hence $r_k^2 - 3t_k^2 = -2N$ and inequality (4.9.5) implies $r_{k-1} < \sqrt{\frac{3N}{2}}$. Hence

$$-2N = r_k^2 - 3t_k^2 < r_{k-1}^2 - 3t_{k-1}^2 < r_{k-1}^2 < \frac{3N}{2}.$$

Consequently, $r_{k-1}^2 - 3t_{k-1}^2 = N$.
We find $2r_{k-1} = -r_k + 3T_k$ and $2T_{k-1} = -r_k + T_k$.

Case 2. Assume $N \equiv -1 \pmod{12}$. Then $r_k^2 - 3t_k^2 = -2N$ would imply the contradiction $r_k^2 \equiv 0 \pmod{3}$. Hence $r_k^2 - 3t_k^2 = -N$ and inequality (4.9.5) implies $r_{k-1} < \sqrt{3N}$. Hence

$$-N = r_k^2 - 3t_k^2 < r_{k-1}^2 - 3t_{k-1}^2 < r_{k-1}^2 < 3N.$$

Consequently, $r_{k-1}^2 - 3t_{k-1}^2 = N$ or $2N$. However, $r_{k-1}^2 - 3t_{k-1}^2 = N$ implies the contradiction $r_{k-1}^2 \equiv -1 \pmod{3}$. Hence $r_{k-1}^2 - 3t_{k-1}^2 = 2N$.
We find $r_{k-1} = -r_k + 3T_k$ and $T_{k-1} = -r_k + T_k$.

The integers N, $|N| \leq 200$, such that the equation $x^2 - 3y^2 = N$ is solvable are: 1, 4, 6, 9, 13, 16, 22, 24, 25, 33, 36, 37, 46, 49, 52, 54, 61, 64, 69, 73, 78, 81, 88, 94, 96, 97, 100, 109, 117, 118, 121, 132, 141, 142, 144, 148, 150, 157, 166, 169, 177, 181, 184, 193, 196, 198, −2, −3, −8, −11, −12, −18, −23, −26, −27, −32, −39, −44, −47, −48, −50, −59, −66, −71, −72, −74, −75, −83, −92, −98, −99, −104, −107, −108, −111, −122, −128, −131, −138, −143, −146, −147, −156, −162, −167, −176, −179, −183, −188, −191, −192, −194, −200.

The following table contains the numbers $k(3, N)$ of classes of solutions and the sets $\mathcal{K}(3, N)$ of fundamental solutions of classes of $x^2 - 3y^2 = N$, when the equations are solvable and N is positive or negative, $|N| \leq 27$ [161].

$x^2-3y^2=N$	$k(3,N)$	$\mathcal{K}(3,N)$
$x^2-3y^2=4$	1	$(4,2)$
$x^2-3y^2=6$	1	$(3,1)$
$x^2-3y^2=9$	1	$(6,3)$
$x^2-3y^2=13$	2	$(4,1),\ (5,2)$
$x^2-3y^2=16$	1	$(8,4)$
$x^2-3y^2=22$	2	$(5,1),\ (7,3)$
$x^2-3y^2=24$	1	$(6,2)$
$x^2-3y^2=25$	1	$(10,5)$
$x^2-3y^2=-3$	1	$(3,2)$
$x^2-3y^2=-8$	1	$(2,2)$
$x^2-3y^2=-11$	2	$(1,2),\ (4,3)$
$x^2-3y^2=-12$	1	$(6,4)$
$x^2-3y^2=-18$	1	$(3,3)$
$x^2-3y^2=-23$	2	$(2,3),\ (5,4)$
$x^2-3y^2=-26$	2	$(1,3),\ (7,5)$
$x^2-3y^2=-27$	1	$(9,6)$

Here are five example of equations $x^2-3y^2=N$, with N big: $k(3,121)=3$ and $\mathcal{K}=\{(13,4),\ (14,5),\ (22,11)\}$; $k(3,253)=4$ and $\mathcal{K}(3,253)=\{(16,1),\ (19,6),\ (20,7),\ (29,14)\}$; $k(3,1573)=5$ and $\mathcal{K}(3,1573)=\{(40,3),\ (41,6),\ (44,11),\ (55,22),\ (64,29)\}$; $k(3,3289)=8$ and $\mathcal{K}(3,3289)=\{(58,5),\ (59,8),\ (61,12),\ (67,20),\ (74,27),\ (86,37),\ (94,43),\ (101,48)\}$' $k(3,3718)=6$ and $\mathcal{K}(3,3718)=\{(61,1),\ (65,13),\ (71,21),\ (79,29),\ (91,39),\ (119,59)\}$.

4.9.5 *The Equations $x^2-5y^2=\pm N$*

The assumption $\left(\frac{5}{N}\right)=1$ is equivalent to $N\equiv\pm1\pmod 5$. Then from equation (4.9.3), we have $-5N<r_k^2-5t_k^2\le -N$. Hence $r_k^2-5t_k^2=-4N,\ -3N,\ -2N$ or $-N$. We cannot have $r_k^2-5t_k^2=-3N$, as then $\left(\frac{5}{3}\right)=1$. Neither can we have $r_k^2-5t_k^2=-2N$, as N is odd.

Case 1. Assume $N\equiv 1\pmod 5$. Then $r_k^2-5t_k^2=-N$ would imply the contradiction $r_k^2\equiv -1\pmod 5$. Hence $r_k^2-5t_k^2=-4N$. Then r_k and t_k are both odd. Also, inequality (4.9.5) implies $r_{k-1}<\sqrt{\frac{5N}{4}}$. Hence $-N\le r_{k-1}^2-5t_{k-1}^2\le N$.

Then as in the remark above, we can show that

(i) if $r_{k-1}^2-5t_{k-1}^2=-N$, then

$$4r_{k-1} = -3r_k + 4T_k, \quad 4T_{k-1} = -r_k + 3T_k,$$

hence $r_k \equiv -T_k \pmod 4$.

(ii) if $r_{k-1}^2 - 5t_{k-1}^2 = N$, then

$$4r_{k-1} = -r_k + 5T_k, \quad 4T_{k-1} = -r_k + T_k,$$

hence $r_k \equiv T_k \pmod 4$.

Case 2. Assume $N \equiv -1 \pmod 5$. Then $r_k^2 - 5t_k^2 = -4N$ would imply the contradiction $r_k^2 \equiv 4 \pmod 5$. Hence $r_k^2 - 5t_k^2 = -N$. Then not both r_k and t_k are odd. Also, inequality (4.9.5) implies $r_{k-1} < \sqrt{5N}$ and we deduce that $-N < r_{k-1}^2 - 5t_{k-1}^2 \le 4N$. Consequently, $r_{k-1}^2 - 5t_{k-1}^2 = N$ or $4N$.

Then, as in the remark above, we can show

(i) if $r_{k-1}^2 - 5t_{k-1}^2 = N$, then

$$r_{k-1} = -2r_k + 5T_k, \quad T_{k-1} = -r_k + 2T_k,$$

hence $r_{k-1} \equiv -2r_k \pmod 5$.

(ii) If $r_{k-1}^2 - 5t_{k-1}^2 = 4N$, then

$$r_{k-1} = -r_k + 5T_k, \quad T_{k-1} = -r_k + T_k,$$

hence $r_{k-1} \equiv -r_k \pmod 5$.

Here is a complete classification of the possible cases:

1. $N = 5k + 1$. Then $r_k^2 - 5t_k^2 = -4N$, while r_k and t_k are odd.
   (i) $r_k \equiv -T_k \pmod 4$. Then $r_{k-1}^2 - 5t_{k-1}^2 = -N$.
   (ii) $r_k \equiv T_k \pmod 4$. Then $r_{k-1}^2 - 5t_{k-1}^2 = N$.
2. $N = 5k - 1$. Then $r_k^2 - 5t_k^2 = -N$, while r_k and t_k are not both odd.
   (i) $r_{k-1} \equiv -2r_k \pmod 5$. Then $r_{k-1}^2 - 5t_{k-1}^2 = N$.
   (ii) $r_{k-1} \equiv -r_k \pmod 5$. Then $r_{k-1}^2 - 5t_{k-1}^2 = 4N$.

The integers N, $|N| \le 200$, such that the equation $x^2 - 5y^2 = N$ is solvable are: ± 1, ± 4, ± 5, ± 9, ± 11, ± 16, ± 19, ± 20, ± 25, ± 29, ± 31, ± 36, ± 41, ± 44, ± 45, ± 49, ± 55, ± 59, ± 61, ± 64, ± 71, ± 76, ± 79, ± 80, ± 81, ± 89, ± 95, ± 99, ± 100, ± 101, ± 109, ± 116, ± 121, ± 124, ± 125, ± 131, ± 139, ± 144, ± 145, ± 149, ± 151, ± 155, ± 164, ± 169, ± 171, ± 176, ± 179, ± 180, ± 181, ± 191, ± 196, ± 199.

The following table gives the numbers $k(5, N)$ and the sets $\mathcal{K}(5, N)$ of the equations $x^2 - 5y^2 = N$, when they are solvable and N is positive or negative, $|N| \le 29$ [161].

$x^2 - 5y^2 = N$	$k(5,N)$	$\mathcal{K}(5,N)$
$x^2 - 5y^2 = 4$	3	$(3,1),\ (7,3),\ (18,8)$
$x^2 - 5y^2 = 5$	1	$(5,2)$
$x^2 - 5y^2 = 9$	1	$(27,12)$
$x^2 - 5y^2 = 11$	2	$(4,1),\ (16,7)$
$x^2 - 5y^2 = 16$	3	$(6,2),\ (14,6),\ (36,16)$
$x^2 - 5y^2 = 19$	2	$(8,3),\ (12,5)$
$x^2 - 5y^2 = 20$	3	$(5,1),\ (10,4),\ (25,11)$
$x^2 - 5y^2 = 25$	1	$(45,20)$
$x^2 - 5y^2 = -4$	3	$(1,1),\ (4,2),\ (11,5)$
$x^2 - 5y^2 = -5$	1	$(20,9)$
$x^2 - 5y^2 = -9$	1	$(6,3)$
$x^2 - 5y^2 = -11$	2	$(3,2),\ (13,6)$
$x^2 - 5y^2 = -16$	3	$(2,2),\ (8,4),\ (22,10)$
$x^2 - 5y^2 = -19$	2	$(1,2),\ (31,14)$
$x^2 - 5y^2 = -20$	3	$(5,3),\ (15,7),\ (40,18)$
$x^2 - 5y^2 = -25$	1	$(10,5)$
$x^2 - 5y^2 = -29$	2	$(4,3),\ (24,11)$

Here are three example of equations $x^2 - 5y^2 = N$, with N big: $k(5,1276) = 11$ and $\mathcal{K}(5,1276) = \{(36,2), (39,7), (41,9), (49,15), (59,21), (76,30), (84,34), (111,47), (141,61), (211,93), (284,126)\}$; $k(5,1936) = 8$ and $\mathcal{K}(5,1936) = \{(46,6), (54,14), (84,32), (116,48), (154,66), (206,90), (294,130), (396,176)\}$; $k(5,9196) = 18$ and $\mathcal{K}(5,9196) = \{(96,2), (99,11), (104,18), (111,25), (121,33), (139,45), (149,51), (176,66), (201,79), (229,93), (264,110), (321,137), (351,151), (429,187), (499,219), (576,254), (671,297), (824,366)\}$.

4.9.6 The Equations $x^2 - 6y^2 = \pm N$

The assumption $\left(\frac{6}{N}\right) = 1$ is equivalent to $N \equiv \pm 1 \pmod{24}$ or $N \equiv \pm 5 \pmod{24}$. Then from equation (4.9.3), we have $-6N < r_k^2 - 6t_k^2 \leq -N$. Hence $r_k^2 - 6t_k^2 = -5N,\ -4N,\ -3N,\ -2N$ or $-N$. Only $-4N$ is ruled out immediately and the other possibilities can occur.

As with the case $D = 5$, there is a complete classification of the possible cases:

1. $N = 24k - 1$ or $24k + 5$.

   (i) $r_k \equiv 0 \pmod{3}$. Then $r_k^2 - 6t_k^2 = -3N$, $r_{k-1}^2 - 6t_{k-1}^2 = -N$.
   (ii) $r_k \not\equiv 0 \pmod{3}$. Then $r_k^2 - 6t_k^2 = -N$.

(a) $r_{k-1} \equiv 0 \pmod 2$. Then $r_{k-1}^2 - 6t_{k-1}^2 = 2N$.
(b) $r_{k-1} \equiv 1 \pmod 2$. Then $r_{k-1}^2 - 6t_{k-1}^2 = 5N$.

2. $N = 24k + 1$ or $24k - 5$:

(i) $r_k \equiv 0 \pmod 2$. Then $r_k^2 - 6t_k^2 = -2N$, $r_{k-1}^2 - 6t_{k-1}^2 = N$.
(ii) $r_k \equiv 1 \pmod 2$. Then $r_k^2 - 6t_k^2 = -5N$.

(a) $r_k \equiv T_k \pmod 5$. Then $r_{k-1}^2 - 6t_{k-1}^2 = N$.
(b) $r_k \equiv -T_k \pmod 5$. Then $r_{k-1}^2 - 6t_{k-1}^2 = -2N$, $r_{k-2}^2 - 6t_{k-2}^2 = N$.

The integers N, $|N| \leq 200$, such that $x^2 - 6y^2 = N$ is solvable are: 1, 3, 4, 9, 10, 12, 16, 19, 25, 27, 30, 36, 40, 43, 46, 48, 49, 57, 58, 64, 67, 73, 75, 76, 81, 90, 94, 97, 100, 106, 108, 115, 120, 121, 129, 138, 139, 142, 144, 145, 147, 160, 163, 169, 171, 172, 174, 184, 190, 192, 193, 196, -2, -5, -6, -8, -15, -18, -20, -23, -24, -29, -32, -38, -45, -47, -50, -53, -54, -60, -69, -71, -72, -80, -86, -87, -92, -95, -96, -98, -101, -114, -116, -125, -128, -134, -135, -141, -146, -149, -150, -152, -159, -162, -167, -173, -180, -188, -191, -194, -197, -200.

The following table gives the numbers $k(6, N)$ and the sets $\mathcal{K}(6, N)$ of equations $x^2 - 6y^2 = N$, when they are solvable and N is positive or negative, $|N| \leq 25$ [161].

$x^2 - 6y^2 = N$	$k(6,N)$	$\mathcal{K}(6,N)$
$x^2 - 6y^2 = 3$	1	$(3,1)$
$x^2 - 6y^2 = 4$	1	$(10,4)$
$x^2 - 6y^2 = 9$	1	$(15,6)$
$x^2 - 6y^2 = 10$	2	$(4,1),\ (8,3)$
$x^2 - 6y^2 = 12$	1	$(6,2)$
$x^2 - 6y^2 = 16$	1	$(20,8)$
$x^2 - 6y^2 = 19$	2	$(5,1),\ (13,5)$
$x^2 - 6y^2 = 25$	3	$(7,2),\ (11,4),\ (25,10)$
$x^2 - 6y^2 = -2$	1	$(2,1)$
$x^2 - 6y^2 = -5$	2	$(1,1),\ (7,3)$
$x^2 - 6y^2 = -6$	1	$(12,5)$
$x^2 - 6y^2 = -8$	1	$(4,2)$
$x^2 - 6y^2 = -15$	2	$(3,2),\ (9,4)$
$x^2 - 6y^2 = -18$	1	$(6,3)$
$x^2 - 6y^2 = -20$	2	$(2,2),\ (14,6)$
$x^2 - 6y^2 = -23$	2	$(1,2),\ (19,8)$

Here are three examples of equations $x^2 - 6y^2 = N$, with N big: $k(6, 625) = 5$ and $\mathcal{K}(6, 625) = \{(29,6), (35,10), (55,20), (73,28), (125,50)\}$; $k(6, 2185) = 8$ and $\mathcal{K}(6, 2185) = \{(47,2), (49,6), (61,16), (79,26), (83,28), (113,42), (173,68), (211,84)\}$; $k(6, 9025) = 9$ and $\mathcal{K}(6, 9025) = \{(97,8), (101,14), (133,38), (155,50), (175,60), (209,76), (337,132), (389,154), (475,190)\}$.

4.9.7 The Equations $x^2 - 7y^2 = \pm N$

The assumption $\left(\frac{7}{N}\right) = 1$ is equivalent to $N \equiv 1, 3, 9, 19, 25, 27 \pmod{28}$.

As with the case $D = 6$, there is a complete classification of the possible cases:

1. $N = 28k + 1,\ 28k + 9$, or $28k + 25$.
   (i) $r_k \equiv T_k \pmod 2$. Then $r_k^2 - 7t_k^2 = -6N$.
      (a) $r_k \equiv -T_k \pmod 6$. Then $r_{k-1}^2 - 7t_{k-1}^2 = -3N$.
         (1) $r_{k-1} \equiv -T_{k-1} \pmod 3$. Then $r_{k-2}^2 - 7t_{k-2}^2 = N$.
         (2) $r_{k-1} \equiv T_{k-1} \pmod 3$. Then $r_{k-2}^2 - 7t_{k-2}^2 = 2N$.
      (b) $r_k \equiv T_k \pmod 6$. Then $r_{k-1}^2 - 7t_{k-1}^2 = N$.
   (ii) $r_k \not\equiv T_k \pmod 2$. Then $r_k^2 - 7t_k^2 = -3N$.
      (a) $r_k \equiv -T_k \pmod 3$. Then $r_{k-1}^2 - 7t_{k-1}^2 = N$.
      (b) $r_k \equiv T_k \pmod 3$. Then $r_{k-1}^2 - 7t_{k-1}^2 = 2N$.
2. $N = 28k + 3,\ 28k + 19$, or $28k + 27$.
   (i) $r_k \equiv T_k \pmod 2$. Then $r_k^2 - 7t_k^2 = -2N$.
      (a) $r_{k-1} \equiv -T_{k-1} \pmod 3$. Then $r_{k-1}^2 - 7t_{k-1}^2 = -N$.
      (b) $r_{k-1} \equiv T_{k-1} \pmod 3$. Then $r_{k-1}^2 - 7t_{k-1}^2 = 3N$.
   (ii) $r_k \not\equiv T_k \pmod 2$. Then $r_k^2 - 7t_k^2 = -N$.
      (a) $r_{k-1} \equiv -T_{k-1} \pmod 3$. Then $r_{k-1}^2 - 7t_{k-1}^2 = 3N$.
      (b) $r_{k-1} \equiv T_{k-1} \pmod 3$. Then $r_{k-1}^2 - 7t_{k-1}^2 = 6N$.

In cases 1(a)(2) and 2(i), the equations $r_{k-2}^2 - 7t_{k-2}^2 = 2N$ and $r_k^2 - 7t_k^2 = -2N$ give rise to equations $x^2 - 7y^2 = N,\ -N$, respectively, if we write $x + y\sqrt{7} = (r_{k-2} + t_{k-2}\sqrt{7})(3 + \sqrt{7})$ and $(r_k + t_k\sqrt{7})/(3 + \sqrt{7})$, respectively. For if $x + y\sqrt{7} = (r + t\sqrt{7})/(3 + \sqrt{7})$, where r and t are odd, then $x = \dfrac{3r - 7t}{2}$ and $y = \dfrac{3t - r}{2}$ are integers and $x^2 - 7y^2 = (r^2 - 7t^2)/2$.

We note that 1(a)(2) cannot occur unless $N \equiv 0 \pmod 3$. Then we have

$$r_{k-1} + \frac{-r_k + 7T_k}{6}, \quad T_{k-1} = \frac{-r_k + 5T_k}{6} \tag{4.9.10}$$

$$r_{k-2} = \frac{-r_{k-1} + 7T_{k-1}}{3}, \quad T_{k-2} = \frac{-r_{k-1} + T_{k-1}}{3}. \tag{4.9.11}$$

Then (4.9.6) implies $r_{k-1} + T_{k-1} = -r_k + 2T_k \equiv -r_k - T_k \equiv 0 \pmod 3$. Also (4.9.7) implies $r_{k-1} \equiv T_{k-1} \pmod 3$. Hence 3 divides r_{k-1} and T_{k-1} and the equation $r_{k-1}^2 - 7T_{k-1}^2 = -3N$ then implies that 3 divides N.

Example. $N = 57$. The congruence $u^2 \equiv 7 \pmod{57}$ has solutions $u \equiv \pm 8, \pm 11 \pmod{57}$. Then $u = 0$ gives $k = 2$, $r_1 = 8$, $t_1 = 1$, $r_2 = 1$, $r_2 = 1$, $t_2 = -7$, $r_k^2 - 7t_k^2 = -6N$ and $r_{k-1}^2 - 7t_{k-1}^2 = N$, while $u = 11$ gives $k = 2$, $r_1 = 11$, $t_1 = 1$, $r_2 = 2$, $t_2 = -5$ and $r_k^2 - 7t_k^2 = -3N$ and $r_{k-1}^2 - 7t_{k-1}^2 = 2N$.

The integers N, $|N| \leq 200$, such that $x^2 - 7y^2 = N$ is solvable are: 1, 2, 4, 8, 9, 16, 18, 21, 25, 29, 32, 36, 37, 42, 49, 50, 53, 57, 58, 64, 72, 74, 81, 84, 93, 98, 100, 106, 109, 113, 114, 116, 121, 128, 133, 137, 141, 144, 148, 149, 162, 168, 169, 177, 186, 189, 193, 196, 197, 200, -3, -6, -7, -12, -14, -19, -24, -27, -28, -31, -38, -47, -48, -54, -56, -59, -62, -63, -75, -76, -83, -87, -94, -96, -103, -108, -111, -112, -118, -124, -126, -131, -139, -147, -150, -152, -159, -166, -167, -171, -174, -175, -188, -192, -199.

The following table contains the numbers $k(7, N)$ and the sets $\mathcal{K}(7, N)$ of the equations $x^2 - 7y^2 = N$, when they are solvable and N is positive or negative, $|N| \leq 29$ [161].

$x^2 - 7y^2 = N$	$k(7,N)$	$\mathcal{K}(7,N)$
$x^2 - 7y^2 = 2$	1	$(3,1)$
$x^2 - 7y^2 = 4$	1	$(16,6)$
$x^2 - 7y^2 = 8$	1	$(6,2)$
$x^2 - 7y^2 = 9$	3	$(4,1),\ (11,4),\ (24,9)$
$x^2 - 7y^2 = 16$	1	$(32,12)$
$x^2 - 7y^2 = 18$	3	$(5,1),\ (9,3),\ (19,7)$
$x^2 - 7y^2 = 21$	2	$(7,2),\ (14,5)$
$x^2 - 7y^2 = 25$	1	$(40,15)$
$x^2 - 7y^2 = 29$	2	$(6,1),\ (27,10)$
$x^2 - 7y^2 = -3$	2	$(2,1),\ (5,2)$
$x^2 - 7y^2 = -6$	2	$(1,1),\ (13,5)$
$x^2 - 7y^2 = -7$	1	$(21,8)$
$x^2 - 7y^2 = -12$	2	$(4,2),\ (10,4)$
$x^2 - 7y^2 = -14$	1	$(7,3)$
$x^2 - 7y^2 = -19$	2	$(3,2),\ (18,7)$
$x^2 - 7y^2 = -24$	2	$(2,2),\ (26,10)$
$x^2 - 7y^2 = -27$	4	$(1,2),\ (6,3),\ (15,6),\ (34,13)$

Here are three examples of equations $x^2 - 7y^2 = N$, with N big: $k(7, 2349) = 10$ and $\mathcal{K}(7, 2349) = \{(51,6), (54,9), (61,14), (82,25), (93,30), (114,39), (131,46), (194,71), (243,90), (282,105)\}$; $k(7, 3249) = 9$ and $\mathcal{K}(7, 3249) = \{(64,11), (71,16), (76,19), (111,36), (132,45), (209,76), (232,85), (281,104), (456,171)\}$; $k(7, 4617) = 12$ and $\mathcal{K}(7, 4617) = \{(68,1), (72,9), (75,12), (93,24), (117,36), (128,41), (163,56), (180,63), (240,87), (348,129), (387,144), (523,196)\}$.