Chapter 3
Pell's Equation

3.1 History and Motivation

Euler, after a cursory reading of Wallis's *Opera Mathematica*, mistakenly attributed the first serious study of nontrivial solutions to equations of the form $x^2 - Dy^2 = 1$, where $x \neq 1$ and $y \neq 0$, to John Pell. However, there is no evidence that Pell, who taught at the University of Amsterdam, had ever considered solving such equations. They should be probably called Fermat's equations, since it was Fermat who first investigated properties of nontrivial solutions of such equations. Nevertheless, Pellian equations have a long and rich history and can be traced back to the Greeks. For many details we refer to the books [75] and [212] (see also the reference [22, pp. 118–120]). Theon of Smyrna used x/y to approximate $\sqrt{2}$, where x and y were integral solutions to $x^2 - 2y^2 = 1$. In general, if $x^2 = Dy^2 + 1$, then $x^2/y^2 = D + 1/y^2$. Hence, for y large, x/y is a good approximation of $\sqrt{D}$, a fact well known to Archimedes.

The famous Archimedes's *problema bovinum* can be reduced to a such equation and it took two thousand years to solve (see [65]).

More precisely, it is reduced to the Pell's equation $x^2 - 4729494y^2 = 1$. The least positive solution, for which y has 41 digits, was discovered by Carl Amthov in 1880. For a nice presentation of the story of this problem we refer to the book [212].

In *Arithmetica*, Diophantus asks for rational solutions to equations of the type $x^2 - Dy^2 = 1$. In the case where $D = m^2 + 1$, Diophantus offered the integral solution $x = 2m^2 + 1$ and $y = 2m$. Pell type equations are also found in Hindu mathematics. In the fourth century, the Indian mathematician Baudhayana noted that $x = 577$ and $y = 408$ is a solution of $x^2 - 2y^2 = 1$ and used the fraction $\frac{577}{408}$ to approximate $\sqrt{2}$. In the seventh century, Brahmagupta considered solutions to the Pell's equation $x^2 - 92y^2 = 1$, the smallest solution being $x = 1151$ and $y = 120$. In the twelfth century, the Hindu mathematician Bhaskara found the least

T. Andreescu, D. Andrica, *Quadratic Diophantine Equations*,
Developments in Mathematics 40, DOI 10.1007/978-0-387-54109-9_3

positive solution to the Pell's equation $x^2 - 61y^2 = 1$ to be $x = 226153980$ and $y = 1766319049$.

In 1657, Fermat stated without proof that if D is positive and not a perfect square, then Pell's equation has an infinite number of solutions. For if (x, y) is a solution to $x^2 - Dy^2 = 1$, then we have $1^2 = (x^2 - Dy^2)^2 = (x^2 + Dy)^2 - (2xy)^2D$. Thus, $(x^2 + Dy, 2xy)$ is also a solution to $x^2 - Dy^2 = 1$. Therefore, if Pell's equation has a solution, then it has infinitely many.

In 1657, Fermat challenged William Brouncker and John Wallis to find integral solutions to the equations $x^2 - 151y^2 = 1$ and $x^2 - 313y^2 = -1$. He cautioned them not to submit rational solutions for even the lowest type of arithmetician could devise such answers. Wallis replied with $(1728148040, 140634693)$ as a solution to the first equation.

In 1770 Euler was looking for positive integers m and n such that $n(n+1)/2 = m^2$. To accomplish this, he multiplied both sides of the latter equation by 8 and added 1 to obtain $(2n+1)^2 = 8m^2 + 1$. He let $x = 2n + 1$ and $y = 2m$ so that $x^2 - 2y^2 = 1$. Solutions to this Pell's equation produce square-triangular numbers since we have

$$\frac{\left(\frac{x-1}{2}\right)\left(\frac{x-1}{2}+1\right)}{2} = \left(\frac{y}{2}\right)^2.$$

That is, the $\left(\frac{x-1}{2}\right)^{th}$ triangular number equals the $\left(\frac{y}{2}\right)^{th}$ square number. For example, from the solution $x = 3$ and $y = 2$, it follows that $m = n = 1$, yielding the square-triangular number 1. A natural question arises. Does the method generate all square-triangular numbers? If one is more methodical about how one obtains the solutions, one can see that it does.

Since $1 = x^2 - 2y^2 = (x - y\sqrt{2})(x + y\sqrt{2})$, it follows that

$$\begin{aligned} 1 = 1^2 &= (x - y\sqrt{2})^2(x + y\sqrt{2})^2 \\ &= ((2y^2 + x^2) - 2xy\sqrt{2})((2y^2 + x^2) + 2xy\sqrt{2}) \\ &= (2y^2 + x^2)^2 - 2(2xy)^2. \end{aligned}$$

Thus, if (x, y) is a solution to $1 = x^2 - 2y^2$, then so is $(2y^2 + x^2, 2xy)$. For example, the solution $(3, 2)$ generates the solution

$$(2 \cdot 2^2 + 3^2, 2 \cdot 2 \cdot 3) = (17, 12).$$

The solution $(17, 12)$ generates the solution

$$(2 \cdot 12^2 + 17^2, 2 \cdot 12 \cdot 17) = (577, 408).$$

The square-triangular number generated by the solution $(2y^2+x^2, 2xy)$ to $1 = x^2 - 2y^2$ is distinct from the square-triangular number generated by the solution (x, y). Therefore, there exist an infinite number of square-triangular numbers. Lagrange, in a series of papers presented to the Berlin Academy between 1768 and 1770, showed that a similar procedure will determine all solutions to $x^2 = Dy^2 + 1$, where D is positive and nonsquare. In 1766, Lagrange proved that the equation $x^2 = Dy^2 + 1$ has an infinite number of solutions whenever D is positive and not square.

The Diophantine quadratic equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \tag{3.1.1}$$

with integral coefficients a, b, c, d, e, f reduces in its main case to a Pell-type equation. Next, we will sketch the general method of reduction. The equation (3.1.1) represents a conic in the xOy Cartesian plane, therefore solving (3.1.1) in integers means finding all lattice points situated on this conic. We will solve the equation (3.1.1) by reducing the general equation of the conic to its canonical form. Following the ideas from [13, 14, 160, 168] we introduce the discriminant of the equation (3.1.1) by $\Delta = b^2 - 4ac$. When $\Delta < 0$, the conic defined by (3.1.1) is an ellipse and in this case the given equation has only a finite number of solutions. If $\Delta = 0$, then the conic given by (3.1.1) is a parabola. If $2ae - bd = 0$, then the equation (3.1.1) becomes $(2ax + by + d)^2 = d^2 - 4af$ and it is not difficult to solve. In the case $2ae - bd \neq 0$, by performing the substitutions $X = 2ax + by + d$ and $Y = (4ae - 2bd)y + 4af - d^2$, the equation (3.1.1) reduces to $X^2 + Y = 0$ which is also easy to solve. The most interesting case is $\Delta > 0$, when the conic defined by (3.1.1) is a hyperbola. Using a sequence of substitutions, the equation (3.1.1) reduces to a general Pell-type equation

$$X^2 - DY^2 = N. \tag{3.1.2}$$

To illustrate the process described above, we will consider the equation $2x^2 - 6xy + 3y^2 = -1$ (Berkely Math. Circle 2000–2001 Monthly Contest #4, Problem 4, [22, p. 120]). We notice that $\Delta = 12 > 0$, hence the corresponding conic is a hyperbola. The equation can be written as $x^2 - 3(y-x)^2 = 1$ and by performing the substitutions $X = x$ and $Y = y - x$, we reduce it to the Pell's equation $X^2 - 3Y^2 = 1$.

Finally, let us mention that other authors reduce the equation (3.1.1) to the form $Ax^2 + Bxy + Cy^2 = k$ (see, for example [203]). Formulas yielding an infinite set of integral solutions of the Diophantine equation $x^2 + bx + c = ky^2$ are given in [80].

3.2 The General Solution by Elementary Methods

We will present an elementary approach to solving the Pell's equation due to Lagrange (see, for example, [93, 112, 125, 126, 191, 198] and [212]). We will follow the presentation of our papers [13–15].

Theorem 3.2.1. *If D is a positive integer that is not a perfect square, then the equation*

$$u^2 - Dv^2 = 1 \tag{3.2.1}$$

has infinitely many solutions in positive integers and the general solution is given by $(u_n, v_n)_{n\geq 0}$,

$$u_{n+1} = u_1u_n + Dv_1v_n, \quad v_{n+1} = v_1u_n + u_1v_n, \tag{3.2.2}$$

where (u_1, v_1) is its fundamental solution, i.e., the minimal solution different from the trivial solution $(u_0, v_0) = (1, 0)$.

Proof. First, we will prove that the equation (3.2.1) has a fundamental solution.

Let c_1 be an integer greater than 1. We will show that there exist integers $t_1, w_1 \geq 1$ such that

$$|t_1 - w_1\sqrt{D}| < \frac{1}{c_1}, \quad w_1 \leq c_1.$$

Indeed, considering $l_k = [k\sqrt{D} + 1]$, $k = 0, \ldots, c_1$, yields $0 < l_k - k\sqrt{D} \leq 1$, $k = 0, \ldots, c_1$, and since $\sqrt{D}$ is an irrational number, it follows that $l_{k'} \neq l_{k''}$ whenever $k' \neq k''$.

There exist $i, j, p \in \{0, 1, 2, \ldots, c_1\}$, $i \neq j$, $p \neq 0$, such that

$$\frac{p-1}{c_1} < l_i - i\sqrt{D} \leq \frac{p}{c_1} \quad \text{and} \quad \frac{p-1}{c_1} < l_j - j\sqrt{D} \leq \frac{p}{c_1}$$

because there are c_1 intervals of the form $\left(\frac{p-1}{c_1}, \frac{p}{c_1}\right)$, $p = 1, \ldots, c_1$ and $c_1 + 1$ numbers of the form $l_k - k\sqrt{D}$, $k = 0, \ldots, c_1$.

From the inequalities above it follows that $|(l_i - l_j) - (j - i)\sqrt{D}| < \frac{1}{c_1}$ and setting $|l_i - l_j| = t_1$ and $|j - i| = w_1$ yields $|t_1 - w_1\sqrt{D}| < \frac{1}{c_1}$ and $w_1 \leq c_1$.

Multiplying this inequality by $t_1 + w_1\sqrt{D} < 2w_1\sqrt{D} + 1$ gives

$$|t_1^2 - Dw_1^2| < 2\frac{w_1}{c_1}\sqrt{D} + \frac{1}{c_1} < 2\sqrt{D} + 1.$$

Choosing a positive integer $c_2 > c_1$ such that $|t_1 - w_1\sqrt{D}| > \frac{1}{c_2}$, we obtain positive integers t_2, w_2 with the properties

$$|t_2^2 - Dw_2^2| < 2\sqrt{D} + 1 \quad \text{and} \quad |t_1 - t_2| + |w_1 - w_2| \neq 0.$$

By continuing this procedure, we find a sequence of distinct pairs $(t_n, w_n)_{n\geq 1}$ satisfying the inequalities $|t_n^2 - Dw_n^2| < 2\sqrt{D}+1$ for all positive integers n. It follows that the interval $(-2\sqrt{D}-1, 2\sqrt{D}+1)$ contains a nonzero integer k such that there exists a subsequence of $(t_n, w_n)_{n\geq 1}$ satisfying the equation $t^2 - Dw^2 = k$. This subsequence contains at least two pairs (t_s, w_s), (t_r, w_r) for which $t_s \equiv t_r (\mathrm{mod}\ |k|)$, $w_s \equiv w_r (\mathrm{mod}\ |k|)$, and $t_s w_r - t_r w_s \neq 0$, otherwise $t_s = t_r$ and $w_s = w_r$, in contradiction with $|t_s - t_r| + |w_s - w_r| \neq 0$ see [21] and [23] for general properties of congruences).

Let $t_0 = t_s t_r - Dw_s w_r$ and let $w_0 = t_s w_r - t_r w_s$. Then

$$t_0^2 - Dw_0^2 = k^2. \tag{3.2.3}$$

On the other hand, $t_0 = t_s t_r - Dw_s w_r \equiv t_s^2 - Dw_0^2 \equiv 0 (\mathrm{mod}\ |k|)$, and it follows immediately that $w_0 \equiv 0 (\mathrm{mod}\ |k|)$. The pair (u, v), where $u = \dfrac{t_0}{|k|}$, $v = \dfrac{w_0}{|k|}$ is a nontrivial solution to Pell's equation (3.2.1).

Let (u_1, v_1) be the least such solution, i.e., with u (and implicitly v) minimal.

We show now that the pair (u_n, v_n) defined by (3.2.2) satisfies Pell's equation (3.2.1). We proceed by induction with respect to n. Clearly, (u_1, v_1) is a solution to the equation (3.2.1). If (u_n, v_n) is a solution to this equation, then

$$\begin{aligned} u_{n+1}^2 - Dv_{n+1}^2 &= (u_1 u_n + Dv_1 v_n)^2 - D(v_1 u_n + u_1 v_n)^2 \\ &= (u_1^2 - Dv_1^2)(u_n^2 - Dv_n^2) = 1, \end{aligned}$$

i.e., the pair (u_{n+1}, v_{n+1}) is also a solution to the equation (3.2.1).

It is not difficult to see that for all positive integer n,

$$u_n + v_n\sqrt{D} = (u_1 + v_1\sqrt{D})^n. \tag{3.2.4}$$

Clearly, (3.2.4) also yields the trivial solution $(u_0, v_0) = (1, 0)$.

Let $z_n = u_n + v_n\sqrt{D} = (u_1 + v_1\sqrt{D})^n$ and note that $z_0 < z_1 < \cdots < z_n < \ldots$. We will prove now that all solutions to the equation (3.2.1) are of the form (3.2.4). Indeed, if the equation (3.2.1) had a solution (u, v) such that $z = u + v\sqrt{D}$ is not of the form (3.2.4), then $z_m < z < z_{m+1}$ for some integer m. Then $1 < (u+v\sqrt{D})(u_m - v_m\sqrt{D}) < u_1 + v_1\sqrt{D}$, and therefore $1 < (uu_m - Dvv_m) + (u_m v - uv_m)\sqrt{D} < u_1 + v_1\sqrt{D}$. On the other hand, $(uu_m - Dvv_m)^2 - D(u_m v - uv_m)^2 = (u^2 - Dv^2)(u_m^2 - Dv_m^2) = 1$, i.e., $(uu_m - Dvv_m, u_m v - uv_m)$ is a solution of (3.2.1) smaller than (u_1, v_1), in contradiction with the assumption that (u_1, v_1) is the minimal nontrivial solution. □

Remarks. 1) The relations (3.2.1) could be written in the following useful matrix form

$$\begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix} = \begin{pmatrix} u_1 & Dv_1 \\ v_1 & u_1 \end{pmatrix} \begin{pmatrix} u_n \\ v_n \end{pmatrix}$$

from where

$$\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 & Dv_1 \\ v_1 & u_1 \end{pmatrix}^n \begin{pmatrix} u_0 \\ v_0 \end{pmatrix}. \tag{3.2.5}$$

If

$$\begin{pmatrix} u_1 & Dv_1 \\ v_1 & u_1 \end{pmatrix}^n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}$$

then it is well-known that each of a_n, b_n, c_n, d_n is a linear combination of λ_1^n, λ_2^n, where λ_1, λ_2 are the eigenvalues of the matrix $\begin{pmatrix} u_1 & Dv_1 \\ v_1 & u_1 \end{pmatrix}$. By using (3.2.5), after an easy computation it follows that

$$\begin{aligned} u_n &= \frac{1}{2}[(u_1 + v_1\sqrt{D})^n + (u_1 - v_1\sqrt{D})^n], \\ v_n &= \frac{1}{2\sqrt{D}}[(u_1 + v_1\sqrt{D})^n - (u_1 - v_1\sqrt{D})^n] \end{aligned} \tag{3.2.6}$$

2) The solutions of Pell's equation given in one of the forms (3.2.4) or (3.2.6) may be used in the approximation of the square roots of positive integers that are not perfect squares. Indeed, if (u_n, v_n) are the solutions of the equation (3.2.1), then

$$u_n - v_n\sqrt{D} = \frac{1}{u_n + v_n\sqrt{D}}$$

and so

$$\frac{u_n}{v_n} - \sqrt{D} = \frac{1}{v_n(u_n + v_n\sqrt{D})} < \frac{1}{\sqrt{D}v_n^2} < \frac{1}{v_n^2}.$$

It follows that

$$\lim_{n\to\infty} \frac{u_n}{v_n} = \sqrt{D} \tag{3.2.7}$$

i.e., the fractions $\frac{u_n}{v_n}$ approximate $\sqrt{D}$ with an error less than $\frac{1}{v_n^2}$.

3) Consider the plane transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$, given by

$$T(x, y) = (u_1x + Dv_1y, v_1x + u_1y),$$

where (u_1, v_1) is the fundamental solution of Pell's equation (3.2.1). Let $(T^n)_{n\geq 0}$ be the discrete dynamical system generated by transformation T, where T^n

denotes the n^{th} iteration of T. The result in Theorem 3.2.1 shows that the orbit of point (u_0, v_0) of this dynamical system consists of lattice points on the hyperbola $x^2 - Dy^2 = 1$.

4) It is not difficult to find rational solutions to equation (3.2.1). Simply divide the relation

$$(r^2 + D)^2 - D(2r)^2 = (r^2 - D)^2$$

by $(r^2 - D)^2$ to obtain

$$u = \frac{r^2 + D}{r^2 - D}, \quad v = \frac{2r}{r^2 - D}, \quad r \in \mathbb{Q}.$$

In the next sections we will see how we can describe all rational solutions to (3.2.1).

5) Dirichlet in 1837 published explicit formulae giving some solutions of Pell's equations in terms of trigonometric functions. For example, for $D = 13$ he has obtained $x_1 + y_1\sqrt{13} = \eta^2$, where

$$\eta = \frac{\sin\frac{2\pi}{13}\sin\frac{5\pi}{13}\sin\frac{6\pi}{13}}{\sin\frac{\pi}{13}\sin\frac{3\pi}{13}\sin\frac{4\pi}{13}} \in \mathbb{Q}(\sqrt{13}).$$

6) Concerning Pell's equation there is the following conjecture [150]: *Let p be a prime $\equiv 3 \pmod 4$. Consider Pell's equation $u^2 - pv^2 = 1$ and its fundamental solution (u_1, v_1). Then $v_1 \not\equiv 0 \pmod p$.*

This has been verified for all such primes $p < 18000$. It has been shown that $v_1 \not\equiv 0 \pmod p$ if and only if $E_{\frac{p-3}{4}} \not\equiv 0 \pmod p$, where the Euler numbers E_n are defined by the powers series

$$\sec t = \sum_{n=0}^{\infty} \frac{E_n}{(2n)!} t^{2n}.$$

There is a similar conjecture when $p \equiv 1 \pmod 4$.

3.3 The General Solution by Continued Fractions

The approach in this section is based on the material contained in Chapter 2, Section 2.1. More specifically, the method we are going to present is based on expanding $\sqrt{D}$ into a continued fraction as in Theorem 2.1.21, with convergents h_n/k_n, and with q_n defined by equations (2.1.13) with $\xi_0 = \sqrt{D}$, $q_0 = 1$, $m_0 = 0$. Our presentation is based on [1, 46, 159] and [164].

Theorem 3.3.1. *If D is a positive integer not a perfect square, then $h_n^2 - Dk_n^2 = (-1)^{n-1}q_{n+1}$ for all integers $n \geq -1$.*

Proof. From equations (2.1.8) and (2.1.13) we have

$$\sqrt{D} = \xi_0 = \frac{\xi_{n+1}h_n + h_{n-1}}{\xi_{n+1}k_n + k_{n-1}} = \frac{(m_{n+1} + \sqrt{D})h_n + q_{n+1}h_{n-1}}{(m_{n+1} + \sqrt{D})k_n + q_{n+1}k_{n-1}}.$$

We simplify this equation and separate it into a rational and a purely irrational part much as we did in (2.1.16). Each part must be zero so we get two equations, and we can eliminate m_{n+1} from them. The final result is

$$h_n^2 - Dk_n^2 = (h_nk_{n-1} - h_{n-1}k_n)q_{n+1} = (-1)^{n-1}q_{n+1}$$

where we used Theorem 2.1.5 in the last step. □

Corollary 3.3.2. *Taking r as the length of the period of the expansion of $\sqrt{D}$, as in Theorem 2.1.21, we have for $n \geq 0$,*

$$h_{nr-1}^2 - Dk_{nr-1}^2 = (-1)^{nr}q_{nr} = (-1)^{nr}.$$

With n even, this gives infinitely many solutions of $x^2 - Dy^2 = 1$ in integers, provided D is positive and not a perfect square.

It can be seen that Theorem 3.3.1 gives us solutions to (3.1.2) for certain values of N. In particular, Corollary 3.3.2 gives infinitely many solutions of $x^2 - Dy^2 = 1$ by the use of even values nr. Of course, if r is even, all values of nr are even. If r is odd, Corollary 3.3.2 gives infinitely many solutions to $x^2 - Dy^2 = -1$ by the use of odd integers $n \geq 1$. The next result shows that every solution to $x^2 - Dy^2 = \pm 1$ can be obtained from the continued fraction expansion of $\sqrt{D}$. But first we make this simple observation: Apart from such trivial solutions as $x = \pm 1$, $y = 0$ of $x^2 - Dy^2 = 1$, all solutions to $x^2 - Dy^2 = N$ fall into sets of four by all combinations of signs $\pm x$, $\pm y$. Hence it is sufficient to discuss the positive solutions $x > 0$, $y > 0$.

Theorem 3.3.3. *Let D be a positive integer not a perfect square, and let the convergents to the continued expansion of $\sqrt{D}$ be h_n/k_n. Let the integer N satisfy $|N| < \sqrt{D}$. Then any positive solution $x = s$, $y = t$ to $x^2 - Dy^2 = N$, with $\gcd(s, t) = 1$, satisfies $s = h_n$, $t = k_n$ for some positive integer n.*

Proof. Let E and M be positive integers such that $\gcd(E, M) = 1$ and $E^2 - \rho M^2 = \sigma$, where $\sqrt{\rho}$ is irrational and $0 < \sigma < \sqrt{\rho}$. Here ρ and σ are real numbers, not necessarily integers. Then

$$\frac{E}{M} - \sqrt{\rho} = \frac{\sigma}{M(E + M\sqrt{\rho})},$$

and hence we have

$$0 < \frac{E}{M} - \sqrt{\rho} < \frac{\sqrt{\rho}}{M(E + M\sqrt{\rho})} = \frac{1}{M^2(E/(M\sqrt{\rho}) + 1)}.$$

Also, $0 < E/M - \sqrt{\rho}$ implies $E/(M\sqrt{\rho}) > 1$, and therefore

$$\left| \frac{E}{M} - \sqrt{\rho} \right| < \frac{1}{2M^2}.$$

By Theorem 2.1.14, E/M is a convergent in the continued fraction expansion of $\sqrt{\rho}$.

If $N > 0$, we take $\sigma = N$, $\rho = D$, $E = s$, $M = t$, and the theorem holds in this case.

If $N < 0$, then $t^2 - (1/D)s^2 = -N/D$, and we take $\sigma = -N/D$, $\rho = 1/D$, $E = t$, $M = s$. We find that t/s is a convergent in the expansion of $1/\sqrt{D}$. Then Theorem 2.1.15 shows that s/t is a convergent in the expansion of $\sqrt{D}$. □

The following result is a corollary of Theorems 2.1.21, 3.3.1, and 3.3.3.

Theorem 3.3.4. *All positive solutions to $x^2 - Dy^2 = \pm 1$ are to be found among $x = h_n$, $y = k_n$, where h_n/k_n are the convergents of the expansion of $\sqrt{D}$. If r is the period of the expansion of $\sqrt{D}$, as in Theorem 2.1.21 and if r is even, then $x^2 - Dy^2 = -1$ has no solution, and all positive solutions to $x^2 - Dy^2 = 1$ are given by $x = h_{nr-1}$, $y = k_{nr-1}$ for $n = 1, 2, 3, \ldots$. On the other hand, if r is odd, then $x = h_{nr-1}$, $y = k_{nr-1}$ give all positive solutions to $x^2 - Dy^2 = -1$ for $n = 1, 3, 5, \ldots$, and all positive solutions to $x^2 - Dy^2 = 1$ for $n = 2, 4, 6, \ldots$.*

The sequences of pairs $(h_0, k_0), (h_1, k_1), \ldots$ will include all positive solutions to $x^2 - Dy^2 = 1$. Furthermore, $a_0 = [\sqrt{D}] > 0$, so the sequence $h_0, h_1, h_2, \ldots$ is strictly increasing. If we let (x_1, y_1) denote the first solution that appears, then for every other solution (x, y) we have $x > x_1$, and hence $y > y_1$ also. Having found this least positive solution by means of continued fractions, we can find all the remaining positive solutions by a simpler method, which is in fact similar to the second part of the proof of Theorem 3.2.1. □

Following the same argument as in the last part of the proof in Theorem 3.2.1, we conclude that all nonnegative solutions are given by (x_n, y_n) for $n = 0, 1, 2, \ldots$, where x_n and y_n are the integers defined by $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$.

To illustrate the above method, we will consider the numerical example given by the equation $x^2 - 29y^2 = 1$. The expansion of $\sqrt{29}$ is $\sqrt{29} = \langle 5; \overline{2, 1, 1, 2, 10} \rangle$, so we have $n = 5$, an odd number. The first five convergents are $\frac{5}{1}, \frac{11}{2}, \frac{16}{3}, \frac{27}{5}, \frac{70}{13} = \frac{h_5}{k_5}$. But $x = h_5 = 70$, $y = k_5 = 13$ give $x^2 - 29y^2 = -1$. Hence, we must move on to the next period. The next period gives the convergents $\frac{727}{135}, \frac{1524}{283}, \frac{2251}{418}, \frac{3775}{701}, \frac{9801}{1820} = \frac{h_{10}}{k_{10}}$ and so by taking $x = h_{10} = 9801$, $y = k_{10} = 1820$, we obtain the smallest solution to our equation.

3.4 The General Solution by Quadratic Rings

The following proof uses results about quadratic rings introduced in Section 2.2. If D is a positive integer that is not a perfect square, consider the commutative quadratic ring $R = \{m + n\sqrt{D};\ m, n \in \mathbb{Z}\}$ endowed with the norm $N(\mu) = \mu \cdot \overline{\mu}$, where $\mu = a + b\sqrt{D}$ and $\overline{\mu} = a - b\sqrt{D}$.

For an element μ in R, $\mu \neq 0$, we will denote by $l(\mu)$ the vector in $\mathbb{R}^2$ defined by $l(\mu) = (\ln|\mu|, \ln|\overline{\mu}|)$.

The next result is fundamental for the method we are going to describe. For the proof we will use the approach given in [171] and [95].

Theorem 3.4.1. *In the ring R there exists a unit $\varepsilon_0 \neq \pm 1$ such that for any other unit ε in R the relation $\varepsilon = \pm\varepsilon_0^k$ holds for some integer k and some choice of signs $+$ and $-$.*

Proof. Let q be a real number such that $q > 2\sqrt{D}$. For all nonzero elements α in R with $|N(\alpha)| \leq q$, we denote by Y_α the set in $\mathbb{R}^2$ given by

$$Y_\alpha = \{(x, y) \in H :\ x \geq \ln|\alpha| \text{ and } y \geq \ln|\overline{\alpha}|\},$$

where H is the plane defined by the equation $x + y = \ln q$.

We will first prove that for all nonzero α in R the set Y_α is bounded in $\mathbb{R}^2$. Indeed, if $(x, y) \in Y_\alpha$, then $x \geq \ln|\alpha|$ and $y \geq \ln|\overline{\alpha}|$. Taking into account that $x + y = \ln q$ yields $x = \ln q - y \leq \ln q - \ln|\overline{\alpha}|$ and $y = \ln q - x \leq \ln q - \ln|\alpha|$, it follows that Y_α is contained into a rectangle in H. Moreover, if $|N(\alpha)| \leq q$, then Y_α is nonempty. Indeed, the inequality $|N(\alpha)| = |\alpha \cdot \overline{\alpha}| \leq q$ implies $\ln|\alpha| + \ln|\overline{\alpha}| \leq q$, hence $Y_\alpha \neq \emptyset$.

We will show now that for any unit ε in R the following equality holds:

$$Y_{\alpha\varepsilon} = Y_\alpha + l(\varepsilon).$$

This means that $x + y = \ln q$, $x \geq \ln|\alpha|$ and $y \geq \ln|\overline{\alpha}|$. Let

$$(x_1, y_1) = (x, y) + l(\varepsilon) = (x + \ln|\varepsilon|, y + \ln|\overline{\varepsilon}|).$$

Then

$$x_1 + y_1 = x + y + \ln|\varepsilon| + \ln|\overline{\varepsilon}| = x + y + \ln|\varepsilon \cdot \overline{\varepsilon}| = \ln q,$$

because $x + y = \ln q$ and $|\varepsilon \cdot \overline{\varepsilon}| = |N(\varepsilon)| = 1$. From Proposition 2.2.2, ε is a unit of R if and only if $N(\varepsilon) = \pm 1$. Also

$$x_1 = x + \ln|\varepsilon| \geq \ln|\alpha| + \ln|\varepsilon| = \ln|\alpha\varepsilon|$$

and

$$y_1 = y + \ln|\overline{\varepsilon}| \geq \ln|\overline{\alpha}| + \ln|\overline{\varepsilon}| = \ln|\overline{\alpha} \cdot \overline{\varepsilon}| = \ln|\overline{\alpha\varepsilon}|,$$

because from Proposition 2.2.4 the conjugate is multiplicative. This shows that $(x_1, y_1) \in Y_{\alpha\varepsilon}$, hence we have the inclusion

$$Y_\alpha + l(\varepsilon) \subseteq Y_{\alpha\varepsilon}.$$

For the converse inclusion consider $(x_1, y_1) \in Y_{\alpha\varepsilon}$. This means that $x_1 + y_1 = \ln q$ and

$$x_1 \geq \ln|\alpha\varepsilon|, \quad y_1 \geq \ln|\overline{\alpha} \cdot \overline{\varepsilon}| = \ln|\overline{\alpha\varepsilon}|.$$

Letting $x = x_1 - \ln|\varepsilon|$ and $y = y_1 - \ln|\overline{\varepsilon}|$ we have

$$\begin{aligned} x + y &= \ln q, \\ x &\geq \ln|\alpha\varepsilon| - \ln|\varepsilon| = \ln|\alpha|, \\ y &\geq \ln|\overline{\alpha\varepsilon}| - \ln|\overline{\varepsilon}| = \ln|\overline{\alpha}|. \end{aligned}$$

It follows that $(x, y) \in Y_\alpha$ and that $(x_1, y_1) = (x, y) + l(\varepsilon)$, i.e., $Y_{\alpha\varepsilon} \subseteq Y_\alpha + l(\varepsilon)$. Therefore, for any nonzero element α in R with $|N(\alpha)| \leq q$ and for any unit ε in R, we have $Y_{\alpha\varepsilon} = Y_\alpha + l(\varepsilon)$.

Now we will prove that

$$H \subseteq \bigcup_{\substack{|N(\alpha)| \leq q \\ \alpha \in R, \alpha \neq 0}} Y_\alpha.$$

For this, let $(x, y) \in H$ and let $x_1, y_1 \in \mathbb{R}_+^*$ such that $x = \ln x_1$ and $y = \ln y_1$. The equality $x + y = \ln q$ implies $x_1 y_1 = q$. Denote

$$X = [-x_1, x_1] \times [-y_1, y_2].$$

If λ is the Lebesgue measure in $\mathbb{R}^2$, then

$$\lambda(X) = 4x_1 y_1 = 4q > 4 \cdot 2\sqrt{D} = 4\lambda(T),$$

where $T = \{x(1,1) + y(\sqrt{D}, -\sqrt{D}) : x, y \in [0,1)\}$ is the fundamental parallelepiped associated with the complete lattice in $\mathbb{R}^2$, $\Lambda = \{m(1,1) + n(\sqrt{D}, -\sqrt{D}) : m, n \in \mathbb{Z}\}$. The lattice Λ is complete because the vectors $(1,1)$ and $(\sqrt{D}, -\sqrt{D})$ are linearly independent over $\mathbb{R}$. It is known that $\lambda(T) = |\det A_D| = 2\sqrt{D}$, where A_D is the matrix

$$A_D = \begin{pmatrix} 1 & 1 \\ \sqrt{D} & -\sqrt{D} \end{pmatrix}.$$

Using the Minkowski's Fundamental Theorem (see [165]), it follows that there exist integers m and n such that

$$(m,n) \neq (0,0) \text{ and } m(1,1) + n(\sqrt{D}, -\sqrt{D}) \in X \cap \Lambda.$$

From the definition of the set X we obtain

$$|m + n\sqrt{D}| \leq x_1 \text{ and } |m - n\sqrt{D}| \leq y_1.$$

Setting $\alpha = m + n\sqrt{D}$ and taking into account that $(m,n) \neq (0,0)$ yields that α is a nonzero element of the ring R and that

$$|N(\alpha)| = |\alpha\overline{\alpha}| = |\alpha||\overline{\alpha}| = |m + n\sqrt{D}||m - n\sqrt{D}| \leq x_1 y_1 = q.$$

Because

$$x = \ln x_1 \geq \ln |m + n\sqrt{D}| = \ln |\alpha| \text{ and } y = \ln y_1 \geq \ln |m - n\sqrt{D}| = \ln |\overline{\alpha}|,$$

it follows that $(x,y) \in Y_\alpha$, i.e., the inclusion $H \subseteq \cup Y_\alpha$ is proved. By using Theorem 2.2.3 we deduce the existence of a finite number of elements $\alpha_1, \alpha_2, \ldots, \alpha_r \in R$ with the property that each α in R with $|N(\alpha)| \leq q$ is divisibility associated with one of the elements $\alpha_1, \alpha_2, \ldots, \alpha_r$.

The sets Y_{α_i}, $i = 1, 2, \ldots, r$ are bounded, hence the set $Y = \bigcup_{i=1}^{r} Y_{\alpha_i}$ is also bounded in $\mathbb{R}^2$. Let $(x,y) \in H$. Using the above considerations, it follows that there exists a nonzero element α in R such that $|N(\alpha)| \leq q$ and that $(x,y) \in Y_\alpha$. By the choice of elements $\alpha_1, \alpha_2, \ldots, \alpha_r$, there exists $i \in \{1, 2, \ldots, r\}$ such that $\alpha = \varepsilon\alpha_i$, where ε is unit in the ring R. Hence

$$(x,y) \in Y_\alpha = Y_{\alpha_i \varepsilon} = Y_{\alpha_i} + l(\varepsilon),$$

and so $H \subseteq Y + L$, where

$$L = \{l(\varepsilon) : \varepsilon \text{ unit in } R\}.$$

It is clear that $(0,0) \in L$, because $(0,0) = l(1)$, and that $(L,+)$ is a subgroup of the commutative group $(\mathbb{R}^2, +)$. Since the set Y is bounded, and the set H is not, it follows that L is an infinite set, in particular $L \neq \{(0,0)\}$. Assume there is a sequence $(\varepsilon_n)_{n \geq 1}$ of units in R such that $\lim_{n\to\infty} l(\varepsilon_n) = (0,0)$ and that $\varepsilon_n \neq \pm 1$ for all positive integers n. This shows that $\lim_{n\to\infty} |\varepsilon_n| = \lim_{n\to\infty} |\overline{\varepsilon}_n| = 1$, and so $\lim_{n\to\infty} \max\{|\varepsilon_n|, |\overline{\varepsilon}_n|\} = 1$. It is not difficult to see that either $|\varepsilon_n|$ or $|\overline{\varepsilon}_n|$ has the form $m + m'\sqrt{D}$ for some nonnegative integers m and m'.

For $n \geq 1$, $\max\{|\varepsilon_n|, |\overline{\varepsilon}_n|\} \geq \sqrt{D} \geq 2$, so $D \geq 2$. For $n = 0$, taking into account that $\varepsilon_n \neq \pm 1$ for all n, yields $\max\{|\varepsilon_n|, |\overline{\varepsilon}_n|\} \geq m \geq 2$. In both cases, $\max\{|\varepsilon_n|, |\overline{\varepsilon}_n|\} \geq \sqrt{2}$, so $\lim\limits_{n\to\infty} \max\{|\varepsilon_n|, |\overline{\varepsilon}_n|\} \neq 1$ and $\lim\limits_{n\to\infty} l(\varepsilon_n) \neq (0,0)$. From all of the above, it follows that there is a unit $\varepsilon_0 \neq \pm 1$ in R such that

$$\|l(\varepsilon_0)\| = \min\{\|l(\varepsilon)\| : \varepsilon \text{ is a unit in } R,\ \varepsilon \neq \pm 1\},$$

where $\|\cdot\|$ denotes the well-known Euclidean norm in $\mathbb{R}^2$. We have used above that $l(\varepsilon) = (0,0)$ if and only if $\varepsilon = \pm 1$. In particular, it follows that $\|l(\varepsilon_0)\| > 0$. Replacing, if necessary, ε_0 by $\pm\overline{\varepsilon}_0$ or by $-\varepsilon_0$, and taking into account that

$$\|l(\varepsilon_0)\| = \|l(-\varepsilon_0)\| = \|l(\overline{\varepsilon}_0)\| = \|l(-\overline{\varepsilon}_0\|,$$

one can assume that $\varepsilon_0 = m + m'\sqrt{D}$, where m, m' are nonnegative integers such that $(m, m') \neq (1, 0)$. This means that $\varepsilon_0 > 1$. Such a unit ε_0 is called the fundamental unit of the ring R. Since $\ln|\varepsilon| + \ln|\overline{\varepsilon}| = \ln 1 = 0$, for all units ε in R, the following relation holds: $L \subseteq \{(x,y) \in \mathbb{R}^2 : x + y = 0\}$. If $l(\varepsilon_0) = (\alpha, -\alpha)$, where $\alpha = \ln|\varepsilon_0| = \ln\varepsilon_0 > 0$ and $l(\varepsilon) = (\beta, -\beta)$ is another element of the set L with $\beta > 0$, let k be a positive integer such that $k\alpha \leq \beta \leq (k+1)\alpha$ (we have $\|l(\varepsilon)\| = \beta\sqrt{2} \geq \|l(\varepsilon_0)\| = \alpha\sqrt{2}$, hence $\beta \geq \alpha$ and $k \geq 1$). Let $\varepsilon_1 \in R, \varepsilon_1 = \varepsilon \cdot \varepsilon_0^{-k}$. Then

$$l(\varepsilon_1) = l(\varepsilon) - kl(\varepsilon_0) = (\beta - k\alpha, -\beta + k\alpha).$$

If $\beta - k\alpha > 0$, then $\varepsilon_1 \neq \pm 1$ and

$$\|l(\varepsilon_1)\| = \sqrt{2}(\beta - k\alpha) < \sqrt{2}((k+1)\alpha - k\alpha) = \sqrt{2} \cdot \alpha = \|l(\varepsilon_0)\|,$$

in contradiction with the choice of ε_0. Therefore $\beta = k\alpha$, $l(\varepsilon_1) = 0$, which implies the equality $\varepsilon = \pm\varepsilon_0^k$. Note that if $l(\varepsilon) = (\beta, -\beta)$ and $\beta < 0$, then the same argument above for $\overline{\varepsilon}$ shows that there exists a nonnegative integer k with the property $\overline{\varepsilon} = \pm\varepsilon_0^k$.

From all the considerations above it follows that all units in the ring R are of the form $\pm\varepsilon_0^k$ for some integer k. □

Theorem 3.4.1 facilitates finding all positive integer solutions to the Pell's equation $x^2 - Dy^2 = 1$. In this respect, consider a solution (u, v) and denote $\varepsilon = u + v\sqrt{D}$. Then $N(\varepsilon) = u^2 - Dv^2 = 1$, so ε is a unit in the ring R. Applying the result in the Theorem 3.4.1, it follows that $\varepsilon = \pm\varepsilon_0^k$, for some k and for some choice of signs $+$ and $-$. In addition, if we assume $(u, v) \neq (1, 0)$, then $\varepsilon > 1$. Taking into consideration that $\varepsilon_0 > 1$ and that $\varepsilon = \pm\varepsilon_0^k > 1$, we see that the integer k is positive and that we must to choose the sign $+$. Therefore, $\varepsilon = \varepsilon_0^k$, where k is a positive integer. Moreover, if $N(\varepsilon_0) = -1$, then one needs the necessary condition k even (indeed, $1 = N(\varepsilon) = N(\varepsilon_0)^k = (-1)^k$ in the case $N(\varepsilon_0) = -1$).

The general solution to Pell's equation $x^2 - Dy^2 = 1$ could be also written recursively as follows:

$$x_0 = 1,\ y_0 = 0$$
$$x_1 = m,\ y_1 = n \text{ if } N(\varepsilon_0) = 1,\ \varepsilon_0 = m + n\sqrt{D}$$
$$x_1 = m^2 + Dn^2,\ y_1 = 2mn \text{ if } N(\varepsilon_0) = -1$$

$$\begin{cases} x_{k+1} = mx_k + Dny_k \\ y_{k+1} = nx_k + my_k \end{cases}, \text{ if } N(\varepsilon_0) = 1$$

$$\begin{cases} x_{k+1} = (m^2 + Dn^2)x_k + 2Dmny_k \\ y_{k+1} = 2mnx_k + (m^2 + Dn^2)y_k \end{cases}, \text{ if } N(\varepsilon_0) = -1.$$

3.5 The Equation $ax^2 - by^2 = 1$

In the present section we will study the more general equation

$$ax^2 - by^2 = 1, \tag{3.5.1}$$

where a and b are positive integers. Taking into account the considerations in Section 3.1 we have $\Delta = 4ab > 0$, hence (3.5.1) can be reduced to a Pell's equation. In the paper [144] is given a continued fraction approach.

We will use the results in [13, 14] and [15].

Proposition 3.5.1. *If $ab = k^2$, where k is an integer greater than 1, then the equation (3.5.1) does not have solutions in positive integers.*

Proof. Assume that (3.5.1) has a solution (x, y), where x, y are positive integers. Then $ax^2 - by^2 = 1$, and clearly a and b are relatively prime. From the condition $ab = k^2$ it follows that $a = k_1^2$ and $b = k_2^2$ for some positive integer k_1 and k_2. The relation $k_1^2x^2 - k_2^2y^2 = 1$ can be written as $(k_1x - k_2y)(k_1x + k_2y) = 1$. It follows that $1 < k_1x + k_2y = k_1x - k_2y = 1$, a contradiction. □

We will call *Pell's resolvent* of (3.5.1) the equation

$$u^2 - abv^2 = 1. \tag{3.5.2}$$

Theorem 3.5.2. *Suppose that the equation (3.5.1) has solutions in positive integers and let (x_0, y_0) be its smallest solution. The general solution to (3.5.1) is $(x_n, y_n)_{n\geq 0}$, where*

$$x_n = x_0u_n + by_0v_n, \quad y_n = y_0u_n + ax_0v_n, \tag{3.5.3}$$

and $(u_n, v_n)_{n\geq 0}$ is the general solution to Pell's resolvent (3.5.2).

Proof. We will prove first that $(x_n, y_n)_{n\geq 0}$ is a solution to the equation (3.5.1). Indeed,

$$ax_n^2 - by_n^2 = a(x_0u_n + by_0v_n)^2 - b(y_0u_n + ax_0v_n)^2 =$$
$$= (ax_0^2 - by_0^2)(u_n^2 - abv_n^2) = 1 \cdot 1 = 1.$$

Conversely, let (x, y) be a solution to the equation (3.5.1). Then (u, v), where $u = ax_0x - by_0y$ and $v = y_0x - x_0y$, is a solution to Pell's resolvent (3.5.2). Solving the above system of linear equations with unknowns x and y yields $x = x_0u + by_0v$ and $y = y_0u + ax_0v$, i.e., (x, y) has the form (3.5.3). □

Remarks. 1) A simple algebraic computation yields the following relation between the fundamental solution (u_1, v_1) to Pell's resolvent and the smallest solution (x_0, y_0) to equation (3.5.1): $u_1 \pm v_1\sqrt{ab} = (x_0\sqrt{a} \pm y_0\sqrt{b})^2$, where the signs + and – correspond.

2) Using formulas (3.2.6), from (3.5.3) it follows that

$$x_n = \frac{1}{2}\left(x_0 + \frac{y_0}{a}\sqrt{ab}\right)\left(u_1 + v_1\sqrt{ab}\right)^n + \frac{1}{2}\left(x_0 - \frac{y_0}{a}\sqrt{ab}\right)\left(u_1 - v_1\sqrt{ab}\right)^n$$
$$y_n = \frac{1}{2}\left(y_0 + \frac{x_0}{b}\sqrt{ab}\right)\left(u_1 + v_1\sqrt{ab}\right)^n + \frac{1}{2}\left(y_0 - \frac{x_0}{b}\sqrt{ab}\right)\left(u_1 - v_1\sqrt{ab}\right)^n.$$

Taking into account Remark 1, the above formulas can be written as

$$x_n = \frac{1}{2\sqrt{a}}\left[\left(x_0\sqrt{a} + y_0\sqrt{b}\right)^{2n+1} + \left(x_0\sqrt{a} - y_0\sqrt{b}\right)^{2n+1}\right]$$
$$y_n = \frac{1}{2\sqrt{b}}\left[\left(x_0\sqrt{a} + y_0\sqrt{b}\right)^{2n+1} - \left(x_0\sqrt{a} - y_0\sqrt{b}\right)^{2n+1}\right].$$

This last form of solutions appears in [219] but the method given there is much more complicated.

3) The general solution (3.5.3) can be written in the following matrix form

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} x_0 & by_0 \\ y_0 & ax_0 \end{pmatrix}\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \begin{pmatrix} x_0 & by_0 \\ y_0 & ax_0 \end{pmatrix}\begin{pmatrix} u_1 & abv_1 \\ v_1 & u_1 \end{pmatrix}^n \begin{pmatrix} u_0 \\ v_0 \end{pmatrix}.$$

To illustrate the above method, let us consider the following equation: $6x^2 - 5y^2 = 1$. Its smallest solution is $(x_0, y_0) = (1, 1)$. The Pell's resolvent is $u^2 - 30v^2 = 1$, whose fundamental solution is $(11, 2)$. The general solution to the equation considered is $x_n = u_n + 5v_n$, $y_n = u_n + 6v_n$, $n = 0, 1, \ldots$ where $(u_n, v_n)_{n\geq 0}$ is the general solution to Pell's resolvent, i.e., $u_{n+1} = 11u_n + 60v_n$, $v_{n+1} = 2u_n + 11v_n$, $n = 0, 1, \ldots$ with $u_0 = 11$, $v_0 = 2$.

A closed form for these solutions can be found by using the above Remark 2. We obtain

$$x_n = \frac{1}{2\sqrt{6}}\left[\left(\sqrt{6}+\sqrt{5}\right)^{2n+1} + \left(\sqrt{6}-\sqrt{5}\right)^{2n+1}\right]$$
$$y_n = \frac{1}{2\sqrt{5}}\left[\left(\sqrt{6}+\sqrt{5}\right)^{2n+1} - \left(\sqrt{6}-\sqrt{5}\right)^{2n+1}\right].$$

Remarks. 1) In the paper [84] is given a nice survey concerning the history and various approaches in solving the equation (3.5.1).

2) The next result is due in [152]: If $1 < a < b$ are integers such that ab is square-free, then at most one of the two equations

$$ax^2 - by^2 = \pm 1 \tag{3.5.4}$$

is solvable.

3) In Example 3, page 140 of [22], it is shown that if $a, b \geq 1$ are integers such that ab is not a perfect square and both equations (3.5.4) are solvable, then $a = 1$ or $b = 1$.

3.6 The Negative Pell Equation and the Pell–Stevenhagen Constants

While the Pell's equation $x^2 - Dy^2 = 1$ is always solvable if the positive integer D is not a perfect square, as we have proven in the previous sections, the equation

$$x^2 - Dy^2 = -1 \tag{3.6.1}$$

is solvable only for certain values of D.

We have seen in Theorem 3.3.4 that if r is the period of the expansion of $\sqrt{D}$ in continued fractions, then, if r is even, the equation (3.6.1) has no solution. If r is odd, then $x = h_{nr-1}$ and $y = k_{nr-1}$ give all positive solutions to (3.6.1) for $n = 1, 3, 5, \ldots$.

Next, we will write the solutions to the equation (3.6.1) by using our method in Section 3.5.

The equation (3.6.1) is known as the *negative Pell's equation*. From the Theorem 3.5.2 the following theorem follows:

Theorem 3.6.1. *Suppose that the equation (3.6.1) has solutions in positive integers and let (x_0, y_0) be its smallest solution. The general solution to (3.6.1) is given by $(x_n, y_n)_{n\geq 0}$ where*

$$x_n = x_0u_n + Dy_0v_n, \quad y_n = y_0u_n + x_0v_n \tag{3.6.2}$$

and $(u_n, v_n)_{n\geq 0}$ is the general solution to Pell's equation $u^2 - Dv^2 = 1$.

Remarks. 1) Between (x_0, y_0) and (u_1, v_1) there is the following important connection:

$$u_1 \pm v_1\sqrt{D} = \left(x_0 \pm y_0\sqrt{D}\right)^2,$$

where the signs + and – correspond.

2) By using formulas (3.6.2) we obtain the solutions to the negative Pell's equation in explicit form:

$$\begin{aligned} x_n &= \frac{1}{2}\left(x_0 + y_0\sqrt{D}\right)\left(u_1 + v_1\sqrt{D}\right)^n + \frac{1}{2}\left(x_0 - y_0\sqrt{D}\right)\left(u_1 - v_1\sqrt{D}\right)^n \\ y_n &= \frac{1}{2}\left(y_0 + \frac{x_0}{D}\sqrt{D}\right)\left(u_1 + v_1\sqrt{D}\right)^n + \frac{1}{2}\left(y_0 - \frac{x_0}{D}\sqrt{D}\right)\left(u_1 - v_1\sqrt{D}\right)^n. \end{aligned} \tag{3.6.3}$$

Formulas (3.6.3) can be also written as

$$\begin{aligned} x_n &= \frac{1}{2}\left[\left(x_0 + y_0\sqrt{D}\right)^{2n+1} + \left(x_0 - y_0\sqrt{D}\right)^{2n+1}\right] \\ y_n &= \frac{1}{2\sqrt{D}}\left[\left(x_0 + y_0\sqrt{D}\right)^{2n+1} - \left(x_0 - y_0\sqrt{D}\right)^{2n+1}\right] \end{aligned} \tag{3.6.4}$$

3) The general solution (3.6.2) can be expressed in the following matrix form

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} x_0 & Dy_0 \\ y_0 & x_0 \end{pmatrix}\begin{pmatrix} u_n \\ v_n \end{pmatrix} = \begin{pmatrix} x_0 & Dy_0 \\ y_0 & x_0 \end{pmatrix}\begin{pmatrix} u_1 & Dv_1 \\ v_1 & u_1 \end{pmatrix}^n \begin{pmatrix} u_0 \\ v_0 \end{pmatrix}.$$

The following result points out an important class of solvable negative Pell's equations. The proof is adapted from [151].

Theorem 3.6.2. *Let p be a prime ≥ 3. The negative Pell's equation*

$$x^2 - py^2 = -1$$

is solvable in positive integers if and only if $p \equiv 1 \pmod 4$.

Proof. First suppose that the equation is solvable. Then there are positive integers u, v such that $u^2 - pv^2 = -1$. So, $u^2 - (-1) = pv^2$, implying $\left(\frac{-1}{p}\right) = 1$, where $\left(\frac{a}{p}\right)$ denotes the Legendre symbol. According to Theorem 4.3.1.5) in [22, pp. 178–179] we have $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, hence $p \equiv 1 \pmod 4$.

Let (u_0, v_0) be the fundamental solution to the Pell's resolvent $u^2 - pv^2 = 1$. Then $u_0^2 - 1 = pv_0^2$, and u_0 cannot be even, for in this case we should have $-1 \equiv p \pmod 4$. Hence u_0 is odd and the numbers $u_0 - 1$ and $u_0 + 1$ have the greatest common divisor 2. Therefore $u_0 \pm 1 = 2\alpha^2$ and $u_0 \mp 1 = 2p\beta^2$, where α and β are positive integers such that $v_0 = 2\alpha\beta$. By elimination of u_0 we get $\pm 1 = \alpha^2 - p\beta^2$. Since $\beta < v_0$, we cannot have the upper sign. Thus the lower sign must be taken and the theorem is proved. □

Remarks. 1) To give an example of an unsolvable negative Pell's equation we will show that the equation $x^2 - 34y^2 = -1$ has no solution. The fundamental solution of Pell's resolvent is $(35, 6)$. If the equation $x^2 - 34y^2 = -1$ were solvable and had the fundamental solution (x_0, y_0), then by Theorem 3.3.4 we would have $x_0^2 + 34y_0^2 = 35$ and $2x_0y_0 = 6$. But this system of equations has no solutions in positive integers and thus the equation $x^2 - 34y^2 = -1$ is not solvable.

2) In the paper [58] is proved that the proportion of square-free D divisible by k primes of the form $4m + 1$ for which the negative Pell equation is solvable is at least 40 %.

The following short and completely elementary criterion concerning the solvability of the negative Pell equation was obtained in the paper [146].

Theorem 3.6.3. *If $D \equiv 1, 2 \pmod 4$ is a non-square integer, then there is a solution to (3.6.1) if and only if $u_1 \equiv -1 \pmod{2D}$, where (u_1, v_1) is the fundamental solution to the Pell equation $u^2 - Dv^2 = 1$.*

Proof. If (3.6.1) is solvable with the smallest solution (x_0, y_0), then we have $u_1 = x_0^2 + Dy_0^2 = -1 + 2Dy_0^2 \equiv -1 \pmod{2D}$ (see Remark 1) after Theorem 3.6.1).

Conversely, assume that the fundamental solution (u_1, v_1) to $u^2 - Dv^2 = 1$ satisfies $u_1 \equiv -1 \pmod{2D}$. It follows that $u_1 = -1 + 2Dk$, for some positive integer k. We have $(-1 + 2Dk)^2 - Dv_1^2 = 1$, which gives $Dk^2 - k - v_1'^2 = 0$, where $v_1 = 2v_1'$. Therefore,

$$k(Dk - 1) = v_1'^2,$$

from which it follows that $k = r^2$ and $Dk - 1 = s^2$ as $\gcd(k, Dk - 1) = 1$. Thus $Dk - 1 = Dr^2 - 1 = s^2$ which gives $s^2 - Dr^2 = -1$, hence the negative Pell equation is solvable. □

Remark. In [147] is explored the central norm in the simple continued fraction expression of $\sqrt{D}$, where $D \geq 2$ is not a perfect square. The obtained results are used by the authors in the study of solvability of the negative Pell's equation.

In what follows we will present a result concerning the negative Pell's equation based on our paper [18]. We begin with a representation theorem of the Fibonacci sequence that will turn to be useful in the proof of our result.

We consider the Diophantine equation

$$x^2 + y^2 + 1 = xyz. \tag{3.6.5}$$

First we will establish the necessary condition of solvability for equation (3.6.5) and then we will determine all its solutions in terms of the well-known Fibonacci sequence $(F_m)_{m\geq 1}$.

Theorem 3.6.4. *The equation (3.6.5) is solvable if and only if $z = 3$. In this case all of its solutions (x, y) are given by*

$$(1, 1),\ (F_{2n+1}, F_{2n-1}),\ (F_{2n-1}, F_{2n+1}),\ n \geq 1.$$

Proof. Let (x, y, z) be a solution with $z \neq 3$. Then $x \neq y$, for otherwise $x^2(z-2) = 1$, which is impossible, since $z - 2 \neq 1$. We have

$$\begin{aligned} 0 = x^2 + y^2 + 1 - xyz &= (x - yz)^2 + y^2 + 1 + xyz - y^2z^2 \\ &= (yz - x)^2 + y^2 + 1 - (yz - x)yz \end{aligned}$$

hence $(yz - x, y, z)$ is also a solution, since $x(yz - x) = xyz - x^2 = y^2 + 1 > 0$ implies $yz - x > 0$. Note that if $x > y$, then $x^2 > y^2 + 1 = x(yz - x)$. Hence $x > yz - x$, which shows that the newly obtained solution is smaller than the initial solution, in the sense that $x + y > (yz - x) + y$. However, under the assumption that $x \neq y$, this procedure can be continued indefinitely, which is impossible, since in the process we construct a decreasing sequence of positive integers, a contradiction. This contradiction shows that there are no solutions if $z \neq 3$.

Clearly, (1,1) is a solution to the equation

$$x^2 + y^2 + 1 = 3xy.$$

Let (a, b), $a > b$, be another solution. Then $b^2 + (3b - a)^2 + 1 = 3b(3b - a)$, so $(b, 3b - a)$ is also a solution. From

$$(a - b)(a - 2b) = a^2 - 3ab + 2b^2 = b^2 - 1 > 0$$

it follows that $a > 2b$, hence $3b - a < b$. So the new solution has a smaller b.

It follows that we reach a solution with $b = 1$, hence with $a^2 + 2 = 3a$, in which case $a = 1$ or $a = 2$. It follows that all solutions are obtained from $(a_1, b_1) = (1, 1)$ by the recursion

$$(a_{n+1}, b_{n+1}) = (b_n, 3b_n - a_n).$$

The sequences $(a_n)_{n\geq 1}$ and $(b_n)_{n\geq 1}$ satisfy the same recursion: $x_{n+1} = 3x_n - x_{n-1}$, $x_1 = 1$, $x_2 = 2$. This recursion characterizes the Fibonacci numbers of odd index. Therefore, $(a_n, b_n) = (F_{2n+1}, F_{2n-1})$, $n \geq 1$.

The solutions are $(1, 1),\ (F_{2n+1}, F_{2n-1}),\ (F_{2n-1}, F_{2n+1})$, for $n \geq 1$. □

The following result points out a family of unsolvable negative Pell's equations [199]:

Theorem 3.6.5. *Let k be an integer greater than 2. The equation*

$$x^2 - (k^2 - 4)y^2 = -1 \tag{3.6.6}$$

is solvable if and only if $k = 3$.

Proof. We will show that the equation

$$u^2 - (k^2 - 4)v^2 = -4 \tag{3.6.7}$$

is not solvable if $k \neq 3$. Assume the contrary, and let (u, v) be a solution to (3.6.7). Then u and kv have the same parity. Consider $x = \dfrac{u + kv}{2}$. Then $u = 2x - kv$ and (3.6.7) becomes

$$x^2 + v^2 + 1 = xvk.$$

Since $k \neq 3$, this contradicts the result in Theorem 3.6.4.

Assume now that for $k \neq 3$, the negative Pell's equation (3.6.6) has a solution (x, y). Multiplying both sides by 4 yields

$$(2x)^2 - (k^2 - 4)(2y)^2 = -4,$$

contradicting the above result concerning equation (3.6.7).

When $k = 3$ equation (3.6.6) becomes

$$x^2 - 5y^2 = -1. \tag{3.6.8}$$

The smallest solution to (3.6.8) is (2,1). From formulas (3.6.3) it follows that all solutions to (3.6.8) are given by $(x_n, y_n)_{n\geq 0}$, where

$$x_n = \frac{1}{2}\left[\left(2 + \sqrt{5}\right)^{2n+1} + \left(2 - \sqrt{5}\right)^{2n+1}\right]$$

$$y_n = \frac{1}{2\sqrt{5}}\left[\left(2 + \sqrt{5}\right)^{2n+1} - \left(2 - \sqrt{5}\right)^{2n+1}\right]$$

Remark. A complicated method for proving the result in Theorem 3.6.4 was given in [169].

The problem of determining those D for which the negative Pell's equation (3.6.1) is solvable in positive integers has a long history. We mentioned at the beginning of this section that if D is a positive nonsquare the solvability or unsolvability of (3.6.1) can be determined by expanding $\sqrt{D}$ as an ordinary continued fraction

$$\sqrt{D} = \langle a_0; \overline{a_1, \ldots, a_r} \rangle.$$

Then (3.6.1) is solvable or not according to whether r is odd or even. If r is odd, then

$$\frac{x_0}{y_0} = \langle a_0, a_1, \ldots, a_{r-1} \rangle$$

is the fundamental solution of (3.6.1).

A second approach to this problem involves using generalized residue symbol criteria derived from D to determine conditions on D which guarantee that (3.6.1) is solvable or unsolvable. This approach was initiated by Legendre in 1785. He proved that if D is a prime congruent to $1 \pmod 4$, then (3.6.1) is solvable (see Theorem 3.6.2), while if a prime p congruent to $3 \pmod 4$ divides the squarefree part of D, then (3.6.1) is unsolvable. Dirichlet observed that $D = pq$ with $p \equiv q \equiv 1 \pmod 4$ and $(p/q)_4 = (q/p)_4 = -1$, then (3.6.1) is solvable. For $D = p_1 \ldots p_N$ in [210] are given quadratic residue criteria among p which when they held would guarantee that (3.6.1) is solvable. In the paper [195] applied methods of class field theory were used to show that in the case $D = pq$ with $p \equiv q \equiv 1 \pmod 4$ equation (3.6.1) is unsolvable when $(p/q)_4 \neq (q/p)_4$, while in the case $(p/q)_4 = (q/p)_4 = 1$ the equation (3.6.1) is sometimes solvable and sometimes not. In the papers [195] and [181] it is proved that these residue symbol criteria were related to the structure of the 2-Sylow subgroup of an appropriate ring class group $\mathbb{Q}[\sqrt{D}]$. In [180, 181] is introduced a "conditional Artin symbol" defined in terms of generators of certain class fields, by means of which it is given a set of necessary and sufficient conditions for (3.6.1) to be solvable. In [153] it is acknowledged that the problem of determining those D for which (3.6.1) is solvable is still open, presumably due to the nonexplicit character of conditions in [180] and [181]. Explicit residue symbol conditions for special types of D are still being found, e.g., [99] and [177].

The residue symbol approach can be extended to yield an algorithm determining the solvability of negative Pell's equation whose main bottleneck is finding a factorization of D. In the paper [108] it is proved that there is an algorithm when given a positive integer D together with (i) a complete prime factorization of D and (ii) a quadratic nonresidue n_i for each prime p_i dividing D, determines whether the equation (3.6.1) is solvable in positive integers or not, and which always terminates in $O((\ln D)^5 (\ln \ln D)(\ln \ln \ln D))$ elementary operations.

In the paper [81] it is shown that for a nonsquare positive integer D, the negative Pell equation (3.6.1) is solvable if and only if there exist a primitive Pythagorean triple (A, B, C) and positive integers a, b such that $D = a^2 + b^2$ and $aA - bB = \pm 1$. It is also possible to describe a method to generate families of such integers D stemming from the solutions to the linear equation $aA - bB = \pm 1$.

If p is a prime such that $2p = a^4 + s^2$, where $a^2 \equiv \pm s \equiv 9 \pmod{16}$, then the negative Pell's equation $x^2 - 2py^2 = -1$ has no solution [44]. If $D = 2p$, where $p = c^2 + 8D^2$ and D is odd, then the equation (3.6.1) has no solutions [69]. If $p = c^2 + qD^2$ and D is odd when $p \equiv 1 \pmod 4$ and $(p/q) = 1$, then the negative Pell's equation $t^2 - pqu^2 = -1$ has no solutions [109].

While the set of positive integers D for which the Pell's equation is solvable is well known (it is the set of all nonsquare positive integers), the set $\mathcal{D}$ of all positive integers D for which the negative Pell's equation is solvable is far from being known. Only recently has progress been made in the study of the set $\mathcal{D}$. We will mention a few results and some open problems concerning the set $\mathcal{D}$.

Without loss of generality one can, however, assume that D is square-free. Moreover, (3.6.1) can have solutions only if D has no prime divisors $\equiv 3 \pmod 4$. Consider the case in which $D = p'_1 p'_2 \dots p'_r$, $p'_1 < p'_2 < \cdots < p'_r$ and $p'_k \equiv 1 \pmod 4$. In 1834, G. L. Dirichlet had shown that (3.6.1) has solutions when $r = 1$ (see Theorem 3.6.2) and also when $r = 2$ provided $(p'_1/p'_2) = -1$. He had even considered the case when $r = 3$. In [155] it is shown that (3.6.1) has solutions for all odd r's, provided $(p'_i/p'_j) = -1$ for each $i < j \le r$.

Define the *Pell constant* (see [73, pp. 119–120])

$$P = 1 - \prod_{\substack{j \ge 1 \\ j \text{ odd}}} \left(1 - \frac{1}{2^j}\right) = 0,5805775582\dots$$

needed in what follows. The constant P is irrational [206] but only conjectured to be transcendental. Define also the function ψ by

$$\psi(p) = \frac{2 + (1 + 2^{1-\nu_p})p}{2(p+1)}$$

where ν_p is the exponent of 2 into factorization in $p - 1$.

For any set S of positive integers, let $f_S(n)$ denote the number of elements in S not exceeding n. In [43, 206, 207] several conjectures regarding the distribution of $\mathcal{D}$ were formulated. For example, it was conjectured that the counting function $f_{\mathcal{D}}$ satisfies the following relation [207]:

$$\lim_{n\to\infty} \frac{\sqrt{\ln n}}{n} f_{\mathcal{D}}(n) = \frac{3P}{2\pi} \prod_{\substack{p \text{ prime} \\ p \equiv 1 \pmod 4}} \left(1 + \frac{\psi(p)}{p^2 - 1}\right)\left(1 - \frac{1}{p^2}\right)^{1/2} = 0,28136\dots$$

Let U be the set of positive integers not divisible by 4, and let V be the set of positive integers not divisible by any prime congruent to 3 modulo 4. Clearly, $\mathcal{D}$ is a subset of $U \cap V$, and $U \cap V$ is the set of positive integers that can be written as a sum of two coprime squares. By the above conjectured and by a coprimality result given in [182], the density of $\mathcal{D}$ inside $U \cap V$ is [207]:

$$\lim_{n\to\infty} \frac{f_{\mathcal{D}}(n)}{f_{U\cap V}(n)} = P \prod_{\substack{p \text{ prime} \\ p \equiv 1 \pmod 4}} \left(1 + \frac{\psi(p)}{p^2 - 1}\right)\left(1 - \frac{1}{p^2}\right) = 0,57339\dots$$

Here is another conjecture involving the Pell constant. Let W be the set of squarefree integers, that is, integers which are divisible by no square exceeding 1. In [206] it is conjectured that

$$\lim_{n\to\infty} \frac{\sqrt{\ln n}}{n} f_{\mathcal{D}\cap W}(n) = \frac{6}{\pi^2} PK = 0,2697318462\ldots$$

where K is the Landau–Ramanujan constant. Clearly, U is a subset of W, and $V \cap W$ is the set of positive squarefree integers that can be written as a sum of two (coprime) squares. By the second conjectured limit and by a squarefree result one obtains that the density of $\mathcal{D} \cap W$ inside $V \cap W$ is [43]:

$$\lim_{n\to\infty} \frac{f_{\mathcal{D}\cap W}(n)}{f_{V\cap W}(n)} = P = 0,5805775582\ldots$$

An interesting connection to continued fractions is given in [207]: an integer $D > 1$ is in $\mathcal{D}$ if and only if $\sqrt{D}$ is irrational and has a regular continued fraction expansion with odd period length (see also Theorem 3.3.4).

If $D > 1$ is a squarefree integer with no prime factor p, $p \equiv 3 (\mathrm{mod}\ 4)$, with exactly n prime factors, and if $\mathcal{D}_n(X)$ denotes the set of those $D \leq X$, in the paper [58] the authors study the distribution of such D which lie in $\mathcal{D}$. An explicit number λ_n is given such that

$$\liminf_{X\to\infty} \frac{\#(\mathcal{D}_n(X) \cap \mathcal{D})}{\#\mathcal{D}_n(X)} \geq \lambda_n.$$

Moreover, it is conjectured that

$$\lim_{X\to\infty} \frac{\#(\tilde{\mathcal{D}}(X) \cap \mathcal{D})}{\#\tilde{\mathcal{D}}(X)} \geq \lambda_\infty$$

where $\tilde{\mathcal{D}}(X) = \bigcup_{n=1}^{\infty} \mathcal{D}_n(X)$, and $\lambda_\infty = \lim_{n\to\infty} \lambda_n = 0,419\ldots$.