Journal of Number Theory 131 (2011) 1597–1615

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Diophantine equations of Pellian type

Franz Halter-Koch

Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzenzs-Universität Graz, A-8010 Graz, Heinrichstraße 36, Austria

ARTICLE INFO

Article history:
Received 24 August 2010
Revised 17 December 2010
Accepted 17 February 2011
Available online 16 April 2011
Communicated by Michael E. Pohst

MSC:
11D09
11A55
11R11

Keywords:
Diophantine equations
Continued fractions
Quadratic orders

ABSTRACT

We investigate the solutions of diophantine equations of the form $dx^2 - d^*y^2 = \pm t$ for $t \in \{1, 2, 4\}$ and their connections with ideal theory, continued fractions and Jacobi symbols.

1. Introduction and history

The aim of this article is a thorough study of diophantine equations of the form

$$dx^2 - d^*y^2 = \pm 1, \quad \text{where } d, d^* \in \mathbb{N} \text{ and } dd^* \text{ is not a square.} \tag{1}$$

For $d = 1$, this is Pell's equation, while the general equation (1) is sometimes called antipellian. Multiplication of (1) with d implies (with $X = dx$, $Y = dy$ and $D = dd^*$) the norm equation

$$X^2 - DY^2 = \pm d, \quad \text{where } d \mid D \quad \text{and} \quad (X, Y) = 1. \tag{2}$$

Conversely, if d is squarefree, then (2) implies (1). The solubility of (2) can be rephrased in the language of binary quadratic forms. Explicitly, this was done by G. Pall in [15], where the following

E-mail address: franz.halterkoch@aon.at.

doi:10.1016/j.jnt.2011.02.005

result was stated and essentially attributed to C.F. Gauss (see the English Edition [2]). A special case was later rediscovered by H.F. Trotter [17].

Theorem A. *Let $\Delta > 0$ be a discriminant of binary quadratic forms. Then precisely two divisors of Δ can be properly represented by the principal class of discriminant Δ.*

The special case of (1) where $D = dd^*$ is squarefree was frequently investigated in the literature, using different methods. In this case, the result reads as follows.

Theorem B. *Let $D \in \mathbb{N}$ be a squarefree positive integer, and*

$$D^* = \begin{cases} 2D & \text{if } D \equiv 3 \bmod 4, \\ D & \text{if } D \not\equiv 3 \bmod 4. \end{cases}$$

Then there is exactly one $1 < m \mid D^*$ such that the diophantine equation

$$x^2 - Dy^2 = m$$

has a solution $(x, y) \in \mathbb{Z}^2$.

An elementary proof of Theorem B, only using the theory of Pell's equation, was given in [8], a proof within the theory of continued fractions is in [4], and a proof using the theory of quadratic number fields can be found in [7].

Partial results in the general case (also addressing the connection with ideal theory, continued fractions and Jacobi symbols) were obtained only recently by various authors, see [12,10,14,1,18,3].

There is a significant overlap with R.A. Mollin's paper [13]. There he investigates antipellian equations within the theory of continued fractions, however ignoring the structural point of view taken in the main Theorems 4.3 and 4.4 of the present paper. Nevertheless, some of his explicit results there are more general than the applications given in our Section 5 below.

The basic tools for the present investigations are the theory of ambiguous ideals in quadratic number fields as developed in [5] and their connection with continued fractions. This interrelation is principally known and republished several times (I refer to R. Mollin's book [11] and to the article [9]). Unfortunately, the terminology on these subjects is far from being standardized. Thus I decided to give an overview of the necessary basic result, at least to fix the notation. This will be done in Sections 2 and 3.

Section 4 contains the main results concerning Eq. (1) and their connection with ideal theory, continued fractions and Jacobi symbols. By the way, it turns out that it is natural to consider the more general equations $dx^2 - d^*y^2 = \pm t$, where $t \in \{1, 2\}$ if $\Delta \equiv 12 \bmod 16$, and $t \in \{1, 4\}$ if $\Delta \equiv 1 \bmod 4$. Finally, Section 5 contains several applications for small discriminants.

2. Quadratic orders

A non-square integer $\Delta \in \mathbb{Z}$ is called a *discriminant* if $\Delta \equiv 0$ or $1 \bmod 4$, and we set

$$\sigma_\Delta = \begin{cases} 0 & \text{if } \Delta \equiv 0 \bmod 4, \\ 1 & \text{if } \Delta \equiv 1 \bmod 4, \end{cases} \qquad \omega_\Delta = \frac{\sigma_\Delta + \sqrt{\Delta}}{2}$$

and

$$\mathcal{O}_\Delta = \mathbb{Z}[\omega_\Delta] = \left\{ \frac{a + b\sqrt{\Delta}}{2} \;\middle|\; a, b \in \mathbb{Z},\ a \equiv b\Delta \bmod 2 \right\}.$$

We call ω_Δ the *basis number* and $\mathcal{O}_\Delta$ the *order* of discriminant Δ. A quadratic discriminant Δ is called a *fundamental discriminant* if it admits no factorization $\Delta = \Delta_1 m^2$ such that Δ_1 is a discriminant and $m \in \mathbb{N}_{\geqslant 2}$. Every discriminant Δ has a unique factorization $\Delta = \Delta_0 f^2$, where Δ_0 is a fundamental discriminant and $f \in \mathbb{N}$. In this factorization, $\Delta_0 = \Delta_K$ is the field discriminant of the quadratic number field $K = \mathbb{Q}(\sqrt{\Delta})$, $\mathcal{O}_{\Delta_0} = \mathcal{O}_K$ is its maximal order, and $f = (\mathcal{O}_K : \mathcal{O}_\Delta)$. We denote by $(\xi \mapsto \xi')$ the non-trivial automorphism of K, and for a subset $X \subset K$, we set $X' = \{\xi' \mid \xi \in X\}$. For $\xi \in K$, we call ξ' its *conjugate* and $\mathcal{N}(\xi) = \xi\xi' \in \mathbb{Q}$ its *norm*.

If Δ is a quadratic discriminant, then the unit group $\mathcal{O}_\Delta^\times$ of $\mathcal{O}_\Delta$ is given by

$$\mathcal{O}_\Delta^\times = \{\varepsilon \in \mathcal{O}_\Delta \mid |\mathcal{N}(\varepsilon)| = 1\} = \left\{\frac{a + b\sqrt{\Delta}}{2} \;\middle|\; a, b \in \mathbb{Z},\ |a^2 - b^2\Delta| = 4\right\},$$

and, if $\Delta > 0$, then $\mathcal{O}_\Delta = \langle -1, \varepsilon_\Delta \rangle$, where $\varepsilon_\Delta = \min(\mathcal{O}_\Delta \cap \mathbb{R}_{>1})$ is the *fundamental unit* of discriminant Δ (see [6, §16.4]).

An algebraic number $\xi \in \mathbb{C}$ of degree 2 is called a *quadratic irrational*. For an integer $D \in \mathbb{Z}$, we normalize its square root by $\sqrt{D} \geqslant 0$ if $D \geqslant 0$, and $\Im\sqrt{D} \geqslant 0$ if $D < 0$. Then every quadratic irrational $\xi \in \mathbb{C}$ has a unique representation

$$\xi = \frac{b + \sqrt{b^2 - 4ac}}{2a}, \quad \text{where } a, b, c \in \mathbb{Z} \text{ and } (a, b, c) = 1.$$

In this representation, the triple $(a, b, c) \in \mathbb{Z}^3$ is called the *type* and $\Delta = b^2 - 4ac$ is called the *discriminant* of ξ. If $\Delta \in \mathbb{Z}$ is any discriminant, then $\Delta = 4D + \sigma_\Delta$, where $D \in \mathbb{Z}$, and the basis number ω_Δ is a quadratic irrational of type $(1, \sigma_\Delta, -D)$ and discriminant Δ.

Two irrational numbers $\xi, \xi_1 \in \mathbb{C} \setminus \mathbb{Q}$ are called *equivalent* if

$$\xi_1 = \frac{\alpha\xi + \beta}{\gamma\xi + \delta} \quad \text{for some } \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}).$$

It is easily checked that equivalent quadratic irrationals have the same discriminant.

Let K be a quadratic number field. For $n \in \mathbb{N}$ and $\alpha_1, \ldots, \alpha_n \in K$, we denote by $[\alpha_1, \ldots, \alpha_n] = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n \subset K$ the $\mathbb{Z}$-module generated by $\alpha_1, \ldots, \alpha_n$. A free $\mathbb{Z}$-submodule $\mathfrak{a} \subset K$ of rank 2 is called a *lattice* in K, and $\mathcal{R}(\mathfrak{a}) = \{\lambda \in K \mid \lambda\mathfrak{a} \subset \mathfrak{a}\}$ is called its *ring of multipliers*. If (ω_1, ω_2) is a basis of $\mathfrak{a}$, then $\mathfrak{a} = [\omega_1, \omega_2]$. In particular, for every discriminant Δ we have

$$\mathcal{O}_\Delta = [1, \omega_\Delta] = \left\{\frac{a + b\sqrt{\Delta}}{2} \;\middle|\; a, b \in \mathbb{Z},\ a \equiv b\Delta \bmod 2\right\}.$$

In a different terminology, the following Propositions 2.1, 2.2 and 2.3 can be found in [5, Propositions 1 and 3].

Proposition 2.1 *(Structure of lattices). Let K be a quadratic number field and $\mathfrak{a} \subset K$ a lattice. Then $\mathfrak{a} = m[1, \xi]$, where $m = \min(\mathfrak{a} \cap \mathbb{Q}_{>0})$ and $\xi \in K$. If ξ is a quadratic irrational of type (a, b, c) and discriminant Δ, then $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_\Delta$, and $\mathfrak{a}\mathfrak{a}' = m^2 a^{-1}\mathcal{O}_\Delta$. In particular, $\mathfrak{a}$ is an invertible fractional ideal of $\mathcal{O}_\Delta$.*

Proof. Observe first that $\mathfrak{a} \cap \mathbb{Q} \neq \{0\}$. Indeed, $\mathfrak{a}'$ and $\mathcal{R}(\mathfrak{a}')$ are lattices as well, and it $0 \neq \alpha \in \mathfrak{a}$, then there is some $q \in \mathbb{N}$ such that $q\alpha \in \mathcal{R}(\mathfrak{a}')$, which implies that $0 \neq q\mathcal{N}(\alpha) = q\alpha\alpha' \in \mathfrak{a} \cap \mathbb{Q}$. Now $\mathfrak{a} \cap Q$ is a finitely generated non-zero subgroup of $\mathbb{Q}$, and therefore $\mathfrak{a} \cap Q = m\mathbb{Z}$, where $m = \min(\mathfrak{a} \cap \mathbb{Q}_{>0})$. Let (ω_1, ω_2) be a basis of $\mathfrak{a}$ and $m = c_1\omega_1 + c_2\omega_2$, where $c_1, c_2 \in \mathbb{Z}$. Then $(c_1, c_2) = 1$ by the minimal choice of m, and there exist $u_1, u_2 \in \mathbb{Z}$ such that $c_1u_2 - c_2u_1 = 1$. If $\xi_1 = u_1\omega_1 + u_2\omega_2$, then

$$\begin{pmatrix} m \\ \xi_1 \end{pmatrix} = \begin{pmatrix} c_1 & c_2 \\ u_1 & u_2 \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \quad \text{and} \quad \big(\mathfrak{a} : [m, \xi_1]\big) = |c_1u_2 - c_2u_1| = 1.$$

Hence $\mathfrak{a} = [m, \xi_1] = m[1, \xi]$, where $\xi = m^{-1}\xi_1$.

Assume now that ξ if of type (a, b, c) and discriminant $\Delta = b^2 - 4ac$. We shall prove that $\mathcal{O}_\Delta\mathfrak{a} \subset \mathfrak{a}$ and $m^{-2}\mathfrak{a}\mathfrak{a}' = \mathcal{O}_\Delta$. Then it follows that

$$\mathcal{O}_\Delta \subset \mathcal{R}(\mathfrak{a}) = \mathcal{R}(\mathfrak{a})\mathcal{O}_\Delta = m^{-2}\mathfrak{a}\mathfrak{a}'\mathcal{R}(\mathfrak{a}) \subset m^{-2}\mathfrak{a}\mathfrak{a}' = \mathcal{O}_\Delta,$$

and therefore equality holds. Since

$$\omega_\Delta = \frac{\sigma_\Delta - b}{2} + a\frac{b + \sqrt{\Delta}}{2a} \in [1, \xi] \quad \text{and} \quad \omega_\Delta\xi = -c + \frac{\sigma_\Delta + b}{2}\frac{b + \sqrt{\Delta}}{2a} \in [1, \xi],$$

we obtain $\mathcal{O}_\Delta\mathfrak{a} = m[1, \omega_\Delta][1, \xi] = m[1, \xi, \omega_\Delta, \omega_\Delta\xi] \subset \mathfrak{a}$. On the other hand, as $b \equiv \sigma_\Delta \bmod 2$,

$$m^{-2}\mathfrak{a}\mathfrak{a}' = [a, a\xi]\big[1, \xi'\big] = \left[a, b, c, \frac{b + \sqrt{\Delta}}{2}\right] = \left[1, \frac{b + \sqrt{\Delta}}{2}\right] = [1, \omega_\Delta] = \mathcal{O}_\Delta. \qquad \square$$

Proposition 2.2 *(Equivalence of lattices). Let K be a quadratic number field and $\xi, \xi_1 \in K \setminus \mathbb{Q}$.*

1. *Let $\theta \in K^\times$ be such that $[1, \xi] = \theta[1, \xi_1]$. Then there exists some matrix*

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \quad \textit{such that } \xi_1 = \frac{\alpha\xi + \beta}{\gamma\xi + \delta} \textit{ and } \theta = \gamma\xi + \delta.$$

2. *Suppose that*

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \quad \textit{and} \quad \xi_1 = \frac{\alpha\xi + \beta}{\gamma\xi + \delta}. \quad \textit{Then } [1, \xi_1] = \frac{1}{\gamma\xi + \delta}[1, \xi].$$

Proof. 1. If $[1, \xi] = [\theta, \theta\xi_1]$, then

$$\begin{pmatrix} \theta\xi_1 \\ \theta \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \xi \\ 1 \end{pmatrix} \quad \text{for some } \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}),$$

and consequently

$$\theta = \gamma\xi + \delta \quad \text{and} \quad \xi_1 = \frac{\theta\xi_1}{\theta} = \frac{\alpha\xi + \beta}{\gamma\xi + \delta}.$$

2. By assumption, we have

$$[1, \xi_1] = \frac{1}{\gamma\xi + \delta}[\gamma\xi + \delta, \alpha\xi + \beta] = \frac{1}{\gamma\xi + \delta}[1, \xi]. \qquad \square$$

Next we investigate ideals. Let Δ be a discriminant and $K = \mathbb{Q}(\sqrt{\Delta})$. Every non-zero fractional ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ is a lattice in K, and by Proposition 2.1 it is invertible if and only if $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_\Delta$.

An ideal $\mathfrak{a} \subset \mathcal{O}_\Delta$ is called $\mathcal{O}_\Delta$-*primitive* if $e^{-1}\mathfrak{a} \not\subset \mathcal{O}_\Delta$ for all $e \in \mathbb{N}_{\geqslant 2}$, and it is called $\mathcal{O}_\Delta$-*regular* if it is $\mathcal{O}_\Delta$-primitive and $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_\Delta$. Consequently, every $\mathcal{O}_\Delta$-regular ideal is invertible, and the product of two $\mathcal{O}_\Delta$-regular ideals is again $\mathcal{O}_\Delta$-regular. A lattice $\mathfrak{c} \subset K$ is an invertible fractional ideal of $\mathcal{O}_\Delta$ if and only if $\mathfrak{c} = m^{-1}\mathfrak{a}$ for some $\mathcal{O}_\Delta$-regular ideal $\mathfrak{a} \subset \mathcal{O}_\Delta$ and $m \in \mathbb{N}$.

Two $\mathcal{O}_\Delta$-regular ideals $\mathfrak{a}, \mathfrak{a}_1$ are called *equivalent* if $\mathfrak{a}_1 = \lambda\mathfrak{a}$ for some $\lambda \in K^\times$. For an $\mathcal{O}_\Delta$ regular ideal $\mathfrak{a} \subset \mathcal{O}_\Delta$, we denote by $[\mathfrak{a}]$ its equivalence class and by $\mathfrak{N}_\Delta(\mathfrak{a}) = (\mathcal{O}_\Delta : \mathfrak{a}) \in \mathbb{N}$ its *absolute norm*. The set $\mathcal{C}_\Delta$ of all ideal classes $[\mathfrak{a}]$ built by $\mathcal{O}_\Delta$-regular ideals $\mathfrak{a} \subset \mathcal{O}_\Delta$ is a finite abelian group under the composition $[\mathfrak{a}][\mathfrak{a}_1] = [\mathfrak{a}\mathfrak{a}_1]$. Its unit element is the *principal class* $[\mathcal{O}_\Delta]$ which consists of all primitive principal ideals of $\mathcal{O}_\Delta$. Up to isomorphisms, $\mathcal{C}_\Delta = \mathrm{Pic}(\mathcal{O}_\Delta)$ is the factor group of invertible fractional ideals modulo fractional principal ideals of $\mathcal{O}_\Delta$.

Next we describe the fundamental connection between quadratic irrationals and ideals. For a quadratic irrational $\xi \in \mathbb{C}$ of type (a, b, c) and discriminant Δ, we define the lattice

$$I(\xi) = \left[a, \frac{b+\sqrt{\Delta}}{2}\right] = |a|[1, \xi] \subset \mathcal{O}_\Delta.$$

Clearly, $I(\xi) = I(-\xi)$, $I(\xi') = I(\xi)'$, and $\mathcal{O}_\Delta = I(\omega_\Delta)$. If ξ, ξ_1 are quadratic irrationals, then it is easily checked that $I(\xi) = I(\xi_1)$ if and only if $\xi_1 = \varepsilon\xi + n$ for some $\varepsilon \in \{\pm 1\}$ and $n \in \mathbb{Z}$.

Proposition 2.3 *(Structure of regular ideals). Let Δ be a discriminant.*

1. *A subset $\mathfrak{a} \subset \mathbb{Q}(\sqrt{\Delta})$ is an $\mathcal{O}_\Delta$-regular ideal if and only if $\mathfrak{a} = I(\xi)$ for some quadratic irrational ξ of discriminant Δ. Moreover, if ξ is of type (a, b, c), then $\mathfrak{N}_\Delta(\mathfrak{a}) = |a|$.*
2. *Let ξ, ξ_1 be quadratic irrationals of discriminant Δ. Then ξ and ξ_1 are equivalent if and only if $[I(\xi)] = [I(\xi_1)] \in \mathcal{C}_\Delta$.*

Proof. 1. By definition, $I(\xi) \subset \mathcal{O}_\Delta$ is a lattice, $e^{-1}I(\xi) \not\subset \mathcal{O}_\Delta$ for all $e \in \mathbb{N}_{\geqslant 2}$, and $\mathcal{R}(I(\xi)) = \mathcal{O}_\Delta$ by Proposition 2.1. Hence $I(\xi)$ is an $\mathcal{O}_\Delta$-regular ideal.

Let now $\mathfrak{a} \subset \mathcal{O}_\Delta$ be an $\mathcal{O}_\Delta$-regular ideal. By Proposition 2.1, $\mathfrak{a} = m[1, \xi]$, where $m = \min(\mathfrak{a} \cap \mathbb{Q}_{>0})$ and ξ is a quadratic irrational, say of type (a, b, c) and discriminant $\Delta' = b^2 - 4ac$. Since $\mathcal{O}_{\Delta'} = \mathcal{R}(\mathfrak{a}) = \mathcal{O}_\Delta$, it follows that $\Delta = \Delta'$, and as $\mathfrak{a} \cap \mathbb{Q}_{>0} \subset \mathbb{N}$, we obtain $m \in \mathbb{N}$. Now $m\xi \in \mathfrak{a} \subset \mathcal{O}_\Delta$ implies $a \mid m$, say $m = ae$ for some $e \in \mathbb{Z}$. Hence

$$\mathfrak{a} = m\left[1, \frac{b+\sqrt{\Delta}}{2a}\right] = e\left[a, \frac{b+\sqrt{\Delta}}{2}\right] = |e|\left[|a|, \frac{b+\sqrt{\Delta}}{2}\right],$$

and $|e|^{-1}\mathfrak{a} \subset \mathcal{O}_\Delta$ implies $|e| = 1$ and $\mathfrak{a} = I(\xi)$. Since

$$\begin{pmatrix} |a| \\ \frac{b+\sqrt{\Delta}}{2} \end{pmatrix} = \begin{pmatrix} |a| & 0 \\ \frac{b-\sigma_\Delta}{2} & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \omega_\Delta \end{pmatrix},$$

it follows that $\mathfrak{N}_\Delta(\mathfrak{a}) = |a|$.

2. By Proposition 2.2. $\square$

From now on we consider positive discriminants and real quadratic irrationals.

Definition 2.4.

1. Let $\xi \in \mathbb{R}$ be a quadratic irrational. Then the quadratic irrational

$$\xi^+ = \frac{1}{\xi - \lfloor \xi \rfloor}$$

is called the *successor* of ξ. ξ is called:

   - *reduced* if $\xi > 1$ and $-1 < \xi' < 0$;
   - *ambiguous* if $\xi + \xi' \in \mathbb{Z}$.
2. Let $\Delta > 0$ be a discriminant. An $\mathcal{O}_\Delta$-regular ideal $\mathfrak{a} \subset \mathcal{O}_\Delta$ is called:
   - *reduced* if $\mathfrak{a} = I(\xi)$ for some reduced quadratic irrational ξ;
   - *ambiguous* if $\mathfrak{a}' = \mathfrak{a}$.

Proposition 2.5. *Let $\xi \in \mathbb{R}$ be a quadratic irrational of type (a, b, c) and discriminant Δ.*

1. *ξ is reduced if and only if $0 < \sqrt{\Delta} - b < 2a < \sqrt{\Delta} + b$. In particular, if ξ is reduced, then $0 < a < \sqrt{\Delta}$, $0 < b < \sqrt{\Delta}$, $0 < -c < \sqrt{\Delta}$, and ξ^+ is also reduced.*
2. *ξ is ambiguous if and only if $a \mid b$, and $I(\xi)$ is ambiguous if and only if ξ is ambiguous.*
3. *If $\xi^+ = -\xi'^{-1}$, then ξ is ambiguous, and if ξ is reduced and ambiguous, then $\xi^+ = -\xi'^{-1}$.*
4. *If ξ and $\xi_1 \in \mathbb{R}$ are reduced quadratic irrationals and $I(\xi) = I(\xi_1)$, then $\xi = \xi_1$.*

Proof. All assertions are easily checked (and in fact well known). □

It is easily checked that ξ is ambiguous if and only if $I(\xi)' = I(\xi)$, and in this case the $\mathcal{O}_\Delta$-regular ideal $\mathfrak{a} = I(\xi)$ is also called *ambiguous*.

If ξ is reduced, then ξ is ambiguous if and only if $\xi^+ = -\xi'^{-1}$. Indeed, if $\xi^+ = -\xi'^{-1}$, then $\xi' = \lfloor \xi \rfloor - \xi$, and therefore $\xi + \xi' \in \mathbb{Z}$. Conversely, if ξ is reduced and ambiguous, then $\xi - 1 < \xi + \xi' < \xi$, hence $\lfloor \xi \rfloor = \xi + \xi'$ and $\xi^+ = (\xi - \lfloor \xi \rfloor)^{-1} = -\xi'^{-1}$.

If $\Delta > 0$ is a discriminant, then an $\mathcal{O}_\Delta$-regular ideal $\mathfrak{a} \subset \mathcal{O}_\Delta$ is called *reduced* if $\mathfrak{a} = I(\xi)$ for some reduced quadratic irrational $\xi \in \mathbb{R}$. If $\xi \in \mathbb{R}$ is any quadratic irrational, then $I(\xi)$ is reduced if and only if $\xi + \lfloor -\xi' \rfloor > 1$ (see [5, Lemma 2]). In particular, the unit ideal $\mathcal{O}_\Delta = I(\omega_\Delta)$ is reduced.

3. Continued fractions and reduction

Our main reference for the classical theory of continued fractions is Perron's book [16]. It is well known that every $\xi \in \mathbb{R} \setminus \mathbb{Q}$ has a unique (simple) continued fraction

$$\xi = [u_0, u_1, \ldots] = \lim_{n \to \infty} [u_0, u_1, \ldots, u_n],$$

where $u_0 \in \mathbb{Z}$, $u_i \in \mathbb{N}$ for all $i \geqslant 1$, and

$$[u_0, u_1, \ldots, u_n] = u_0 + \cfrac{1}{u_1 + \cfrac{1}{u_2 + \cfrac{1}{\ddots + \cfrac{1}{u_{n-1} + \cfrac{1}{u_n}}}}} = \frac{p_n}{q_n},$$

such that $p_n \in \mathbb{Z}$, $q_n \in \mathbb{N}$ and $(p_n, q_n) = 1$. The sequences $(p_n)_{n \geqslant -2}$ of *partial numerators* of ξ and $(q_n)_{n \geqslant -2}$ of *partial denominators* of ξ satisfy the recursion

$$p_{-2} = 0, \qquad p_{-1} = 1, \quad \text{and} \quad p_i = u_i p_{i-1} + p_{i-2} \quad \text{for all } i \geqslant 0,$$

$$q_{-2} = 1, \qquad q_{-1} = 0, \quad \text{and} \quad q_i = u_i q_{i-1} + q_{i-2} \quad \text{for all } i \geqslant 0.$$

The numbers $\xi_n = [u_n, u_{n+1}, \ldots]$ are called the *complete quotients* of ξ. They are equivalent to ξ and satisfy the recursion formulas $\xi_0 = \xi$ and $\xi_{n+1} = \xi_n^+$ for all $n \geqslant 0$.

A sequence $(x_n)_{n\geqslant 0}$ is called *ultimately periodic* with *period length* $l\geqslant 1$ and *pre-period length* $k\geqslant 0$ if $x_{n+l}=x_n$ for all $n\geqslant k$, and k and l are minimal with this property. In this case, we write

$$(x_n)_{n\geqslant 0}=(x_0,x_1,\dots)=(x_0,x_1,\dots,x_{k-1},\overline{x_k,x_{k+1},\dots,x_{k+l-1}}).$$

If $k=0$, then the sequence is called *purely periodic*.

Proposition 3.1 *(Periodicity Theorem). Let $\xi\in\mathbb{R}\setminus\mathbb{Q}$, $\xi=[u_0,u_1,\dots]$ its continued fraction and $(\xi_n)_{n\geqslant 0}$ its sequence of complete quotients.*

1. *For $k\geqslant 0$ and $l\geqslant 1$ the following assertions are equivalent*:
   (a) *The sequence $(u_n)_{n\geqslant 0}$ is ultimately periodic with pre-period length k and period length l.*
   (b) *The sequence $(\xi_n)_{n\geqslant 0}$ is ultimately periodic with pre-period length k and period length l.*
   (c) *The numbers $\xi=\xi_0,\xi_1,\dots,\xi_{k+l-1}$ are distinct, and $\xi_{k+l}=\xi_k$.*
2. *The sequence $(u_n)_{n\geqslant 0}$ is ultimately periodic if and only if ξ is a quadratic irrational, and it is purely periodic if and only if ξ is a reduced quadratic irrational.*
3. *Let ξ be a quadratic irrational, and suppose that $(\xi_n)_{n\geqslant 0}$ has pre-period length k and period length l. Then $\{\xi_k,\xi_{k+1},\dots,\xi_{k+l-1}\}$ is the set of all reduced quadratic irrationals which are equivalent to ξ.*
   We call $l=l(\xi)$ the *period length* and $(\xi_k,\xi_{k+1},\dots,\xi_{k+l-1})$ the *period* of ξ.

Proof. [16, §17 and Chapter III]. □

Corollary 3.2. *Let $\Delta>0$ be a discriminant, $\xi\in\mathbb{R}$ a quadratic irrational of discriminant Δ, $l=l(\xi)$ and $(\eta_1,\dots,\eta_l)$ the period of ξ. Then $I(\eta_1),\dots,I(\eta_l)$ are distinct, and $\{I(\eta_1),\dots,I(\eta_l)\}$ is the set of all reduced ideals in the ideal class $[I(\xi)]\in\mathcal{C}_\Delta$.*

Proof. A subset $\mathfrak{a}\subset K$ is an $\mathcal{O}_\Delta$-regular ideal lying in the ideal class $[I(\xi)]$ if and only if $\mathfrak{a}=I(\eta)$ for some reduced quadratic irrational η equivalent to ξ. Hence the assertion follows by Propositions 3.1 and 2.5. □

Theorem 3.3. *Let $\Delta=4D+\sigma_\Delta>0$ be a discriminant, $\omega_\Delta=[u_0,u_1,\dots]$ the continued fraction of its basis number and $l=l(\omega_\Delta)$. Then $u_n=u_{n+l}$ for all $n\geqslant 1$, $u_l=2u_0-\sigma_\Delta$, $u_{l-i}=u_i$ for all $i\in[1,l-1]$, and therefore*

$$\omega_\Delta=\frac{\sigma+\sqrt{\Delta}}{2}=[u_0,\overline{u_1,u_2,\dots,u_2,u_1,2u_0-\sigma_\Delta}].$$

Let $(p_n)_{n\geqslant -2}$ be the sequence of partial numerators, $(q_n)_{n\geqslant -2}$ the sequence of partial denominators and $(\xi_n)_{n\geqslant 0}$ the sequence of complete quotients of ω_Δ. For $n\geqslant 0$, ξ_n is of type (a_n,b_n,c_n), where $a_n\geqslant 1$ and $b_n=2B_n-\sigma_\Delta$ for some $B_n\in\mathbb{Z}$.

$(\xi_1,\dots,\xi_l)$ is the period of ω_Δ, and $\{I(\xi_1),\dots,I(\xi_l)\}$ is the set of all reduced principal ideals of $\mathcal{O}_\Delta$. In particular,

$$\xi_l=[\overline{2u_0-\sigma_\Delta,u_1,u_2,\dots,u_2,u_1}]=\omega_\Delta+u_0-\sigma,\quad \textit{and}\quad I(\xi_l)=I(\omega_\Delta)=\mathcal{O}_\Delta.$$

If ε_Δ denotes the fundamental unit of discriminant Δ, then $\mathcal{N}(\varepsilon_\Delta)=(-1)^l$, and

$$\varepsilon_\Delta^m=\left(p_{l-1}-q_{l-1}\omega_\Delta'\right)^m=p_{ml-1}-q_{ml-1}\omega_\Delta'\quad \textit{for all } m\in\mathbb{N}_0.$$

If Δ has a prime divisor $q\equiv 3 \bmod 4$, then l is even and $\mathcal{N}(\varepsilon_\Delta)=1$.

1. *For all $n \geqslant 0$, the following relations hold*:
   (a) $B_n + B_{n+1} = a_n u_n + \sigma_\Delta$.
   (b) $p_{n-1} = B_n q_{n-1} + a_n q_{n-2}$.
   (c) $Dq_{n-1} = (B_n - \sigma_\Delta)p_{n-1} + a_n p_{n-2}$.
   (d) $4(-1)^n a_n = (2p_{n-1} - \sigma_\Delta q_{n-1})^2 - \Delta q_{n-1}^2 = 4\mathcal{N}(p_{n-1} - q_{n-1}\omega_\Delta)$.
   (e) $(-1)^n a_n = p_{n-1}^2 - \sigma_\Delta p_{n-1}q_{n-1} - Dq_{n-1}^2$.
2. *If $i \geqslant -1$ and $n \geqslant 0$, then $p_{i+nl} - q_{i+nl}\omega'_\Delta = (p_i - q_i\omega'_\Delta)(p_{l-1} - q_{l-1}\omega'_\Delta)^n$.*
3. *If l is odd, then ξ_l is the only ambiguous number in the period of ω_Δ, and $\mathcal{O}_\Delta$ is the only reduced ambiguous principal ideal of $\mathcal{O}_\Delta$.*
4. *Let $l = 2k$ be even. Then ξ_k and ξ_l are the only ambiguous numbers in the period of ω_Δ, $(p_{k-1} - q_{k-1}\omega'_\Delta)^2 = a_k\varepsilon_\Delta$, $2B_k = a_k u_k + \sigma_\Delta$,*

$$a_k \mid (2p_{k-1} - q_{k-1}, \Delta) \quad \textit{if } \sigma_\Delta = 1, \quad \textit{and} \quad a_k \mid 2(p_{k-1}, D) \quad \textit{if } \sigma_\Delta = 0.$$

In particular, $\mathcal{O}_\Delta$ and $I(\xi_k)$ are the only reduced ambiguous principal ideals of $\mathcal{O}_\Delta$.

Proof. We prove 3 and 4. The other assertions can be either found in [16, §20, §27 and §30] or easily derived from the investigations there. The assertion concerning reduced principal ideals follows by Corollary 3.2.

If $i \in [1, l]$, then

$$\xi_i = [\overline{u_i, u_{i+1}, \ldots, u_l, u_1, \ldots, u_{i-1}}] = [\overline{u_{l-i+1}, \ldots, u_l, u_1, \ldots, u_{l-i}}] = \xi_{l-i+1}$$

(see [16, §23]), and by Proposition 2.5.3 it follows that ξ_i is ambiguous if and only if $\xi_{i+1} = \xi_i^+ = -\xi_i'^{-1} = \xi_{l-i+1}$. In particular, ξ_l is ambiguous. If $i \in [1, l-1]$, then ξ_i is ambiguous if and only if $i + 1 = l - i + 1$, that is, if and only if $l = 2i$. This proves 3 and the first assertion of 4.

Assume now that $l = 2k$. Then $\xi_{k+1} = -\xi_i'^{-1}$, and therefore

$$-1 = \xi_{k+1}\xi_k' = \frac{b_{k+1} + \sqrt{\Delta}}{a_{k+1}}\frac{b_k - \sqrt{\Delta}}{a_k} = \frac{b_k b_{k+1} - \Delta + (b_k - b_{k+1})\sqrt{\Delta}}{4a_k a_{k+1}},$$

which implies that $b_k = b_{k+1}$, hence $B_k = B_{k+1}$ and $2B_k = a_k u_k + \sigma_\Delta$. By 1(b) we obtain $2p_{k-1} - \sigma_\Delta q_{k-1} = 2B_k q_{k-1} + 2a_k q_{k-2} - \sigma_\Delta q_{k-1} = (2B_k - \sigma_\Delta)q_{k-1} + 2a_k q_{k-2}$, and as $a_k \mid 2B_k - \sigma_\Delta$, it follows that $a_k \mid 2p_{k-1} - \sigma_\Delta q_{k-1}$ and therefore $a_k \mid \Delta q_{k-1}^2$ by 1(d). By 1(e), $(a_k, q_{k-1}) \mid p_{k-1}$, hence $(a_k, q_{k-1}) = 1$ and $a_k \mid \Delta$. Consequently, $a_k \mid (2p_{k-1} - q_{k-1}, \Delta)$ if $\sigma_\Delta = 1$. If $\sigma_\Delta = 0$, then $a_k \mid 2p_{k-1}$, hence $a_k \mid 2D$ by 1(e), and therefore $a_k \mid 2(p_{k-1}, D)$.

It remains to prove that $(p_{k-1} - q_{k-1}\omega'_\Delta)^2 = a_k\varepsilon_\Delta = a_k(p_{l-1} - q_{l-1}\omega'_\Delta)$. Since $\omega_\Delta'^2 = D + \sigma_\Delta\omega'_\Delta$ and $(1, \omega'_\Delta)$ is linearly independent, we must prove that

$$a_k p_{l-1} = p_{k-1}^2 + Dq_{k-1}^2 \quad \text{and} \quad a_k q_{l-1} = q_{k-1}(2p_{k-1} - \sigma_\Delta q_{k-1}).$$

From the matrix equation

$$\begin{pmatrix} p_{l-1} & p_{l-2} \\ q_{l-l} & q_{l-2} \end{pmatrix} = \prod_{\nu=0}^{l-1}\begin{pmatrix} u_\nu & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix}\prod_{\nu=k}^{l-1}\begin{pmatrix} u_\nu & 1 \\ 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix}\prod_{\nu=k}^{l-1}\begin{pmatrix} u_{l-\nu} & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \left(\prod_{\nu=0}^{k} \begin{pmatrix} u_\nu & 1 \\ 1 & 0 \end{pmatrix} \right)^{\mathrm{t}} \begin{pmatrix} 0 & 1 \\ 1 & -u_0 \end{pmatrix}$$

$$= \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \begin{pmatrix} p_k & q_k \\ p_{k-1} & q_{k-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -u_0 \end{pmatrix}$$

$$= \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \begin{pmatrix} q_k & p_k - u_0 q_k \\ q_{k-1} & p_{k-1} - u_0 q_{k-1} \end{pmatrix}$$

it follows that $p_{l-1} = p_{k-1}q_k + p_{k-2}q_{k-1}$ and $q_{l-1} = q_{k-1}(q_k + q_{k-2})$. By 1(c),

$$\begin{aligned} a_k p_{l-1} &= a_k p_{k-1} q_k + a_k p_{k-2} q_{k-1} = a_k p_{k-1} q_k + D q_{k-1}^2 - (B_k - \sigma_\Delta) p_{k-1} q_{k-1} \\ &= p_{k-1}\big[a_k u_k q_{k-1} + a_k q_{k-2} - (B_k - \sigma_\Delta) q_{k-1}\big] + D q_{k-1}^2 \\ &= p_{k-1}(B_k q_{k-1} + a_k q_{k-2}) + D q_{k-1}^2 = p_{k-1}^2 + D q_{k-1}^2. \end{aligned}$$

By 1(b),

$$\begin{aligned} 2p_{k-1} - \sigma_\Delta q_{k-1} &= 2B_k q_{k-1} + 2a_k q_{k-2} - \sigma_\Delta q_{k-1} = (B_k + B_{k+1} - \sigma_\Delta) q_{k-1} + 2a_k q_{k-2} \\ &= a_k(u_k q_{k-1} + 2q_{k-2}) = a_k(q_k + q_{k-2}), \end{aligned}$$

and therefore $q_{k-1}(2p_{k-1} - \sigma_\Delta q_{k-1}) = a_k q_{k-1}(a_k + q_{k-2}) = a_k q_{l-1}$. $\square$

4. Main results

Theorem 4.1. *Let $\Delta \in \mathbb{N}$ be a discriminant.*

1. *Suppose that $\Delta = 4D$,*
   - *$c \in \{1, 2\}$ if $8 \mid D$, and $c = 1$ if $8 \nmid D$;*
   - *$t \in \{1, 2\}$ if $D \equiv 3 \bmod 4$, and $t = 1$ if $D \not\equiv 3 \bmod 4$;*
   - *$D = c^2 d d^*$, where $d, d^* \in \mathbb{N}$ and $(d, d^*) = 1$,*

   and set

$$\mathfrak{j} = \begin{cases} [d, \sqrt{D}\,] & \text{if } ct = 1, \\ [2d, d + \sqrt{D}\,] & \text{if } t = 2, \\ [4d, 2d + \sqrt{D}\,] & \text{if } c = 2. \end{cases}$$

   (a) *$\mathfrak{j}$ is an $\mathcal{O}_\Delta$-regular ambiguous ideal of $\mathcal{O}_\Delta$ satisfying $\mathfrak{N}_\Delta(\mathfrak{j}) = c^2 dt$, and every $\mathcal{O}_\Delta$-regular ambiguous ideal of $\mathcal{O}_\Delta$ is of this form.*
   $\mathfrak{j}$ is reduced if and only if $d < d^*$, and $\mathfrak{j}$ is a principal ideal of $\mathcal{O}_\Delta$ if and only if there exist $x, y \in \mathbb{Z}$ such that

$$\left| dx^2 - d^* y^2 \right| = t \quad \textit{and} \quad (c, xy) = 1.$$

   (b) *Let $x, y \in \mathbb{Z}$ be such that $|dx^2 - d^* y^2| = t$ and $(c, xy) = 1$. Then*

$$\mathfrak{j} = (cdx + y\sqrt{D}\,)\mathcal{O}_\Delta.$$

2. *Suppose that* $\Delta \equiv 1 \bmod 4$ *and* $\Delta = dd^*$, *where* $d, d^* \in \mathbb{N}$ *and* $(d, d^*) = 1$, *and set*

$$\mathfrak{j} = \left[d, \frac{d+\sqrt{\Delta}}{2}\right].$$

(a) $\mathfrak{j}$ *is an* $\mathcal{O}_\Delta$*-regular ambiguous ideal of* $\mathcal{O}_\Delta$ *satisfying* $\mathfrak{N}_\Delta(\mathfrak{j}) = d$, *and every* $\mathcal{O}_\Delta$*-regular ambiguous ideal of* $\mathcal{O}_\Delta$ *is of this form.*
$\mathfrak{j}$ *is reduced if and only if* $d < d^*$, *and* $\mathfrak{j}$ *is a principal ideal of* $\mathcal{O}_\Delta$ *if and only if there exist* $x, y \in \mathbb{Z}$ *such that* $|dx^2 - d^*y^2| = 4$.

(b) *Let* $x, y \in \mathbb{Z}$ *such that* $|dx^2 - d^*y^2| = 4$. *Then*

$$\mathfrak{j} = \frac{dx + y\sqrt{\Delta}}{2}\mathcal{O}_\Delta.$$

Proof. 1. (a) By [5, Proposition 1] it follows that $\mathfrak{j} \subset \mathcal{O}_\Delta$ is an $\mathcal{O}_\Delta$-regular ambiguous ideal, every $\mathcal{O}_\Delta$-regular ambiguous ideal is of this form, and $\mathfrak{j}$ is reduced if and only if $d < d^*$. By Proposition 2.3.1, $\mathfrak{N}_\Delta(\mathfrak{j}) = c^2dt$.

Let now $\mathfrak{j}$ be principal, say $\mathfrak{j} = (u + y\sqrt{D})\mathcal{O}_\Delta$, where $u, y \in \mathbb{Z}$ and $(u, y) = 1$.

If $ct = 1$, then $D = dd^*$, and $u + y\sqrt{D} \in [d, \sqrt{D}]$ implies $u = dx$ for some $x \in \mathbb{Z}$. Since $d = \mathfrak{N}_\Delta(\mathfrak{j}) = |\mathcal{N}(dx + y\sqrt{D})| = |d^2x^2 - dd^*y^2|$, it follows that $|dx^2 - d^*y^2| = 1$.

If $t = 2$, then $u + y\sqrt{D} \in [2d, d + \sqrt{D}]$ implies $u + y\sqrt{D} = 2dv + (d + \sqrt{D})w$ for some $v, w \in \mathbb{Z}$, and if $x = 2v + w$, then $u = dx$ and $y = w$. Since $D = dd^*$, it follows that $2d = \mathfrak{N}_\Delta(\mathfrak{j}) = |\mathcal{N}(dx + y\sqrt{D})| = |d^2x^2 - dd^*y^2|$, which implies $|dx^2 - d^*y^2| = 2$.

If $c = 2$, then $u + y\sqrt{D} \in [4d, 2d + \sqrt{D}]$ implies that there exist $v, w \in \mathbb{Z}$ such that $u + y\sqrt{D} = 4dv + (2d + \sqrt{D})w$. If $x = 2v + w$, then $u = 2dx$, $y = w$, and $2 \nmid xy$. Since $D = 4dd^*$, it follows that $4d = \mathfrak{N}_\Delta(\mathfrak{j}) = |\mathcal{N}(2dx + y\sqrt{D})| = |4d^2x^2 - 4dd^*y^2|$, which implies $|dx^2 - d^*y^2| = 1$.

The converse follows by (b).

(b) If $ct = 1$, then obviously $dx + y\sqrt{D} \in \mathfrak{j}$, hence $(dx + y\sqrt{D})\mathcal{O}_\Delta \subset \mathfrak{j}$, and equality holds, since

$$\mathfrak{N}_\Delta\big((dx + y\sqrt{D})\mathcal{O}_\Delta\big) = \big|\mathcal{N}(dx + y\sqrt{D})\big| = \big|d^2x^2 - dd^*y^2\big| = d = \mathfrak{N}_\Delta(\mathfrak{j}).$$

If $t = 2$, then $D = dd^* \equiv 3 \bmod 4$, hence $2 \nmid xy$, and $x - y = 2u$ for some $u \in \mathbb{Z}$. Now we obtain $dx + y\sqrt{D} = 2du + (d + \sqrt{D})y \in \mathfrak{j}$, hence $(dx + y\sqrt{D})\mathcal{O}_\Delta \subset \mathfrak{j}$, and equality holds, since

$$\mathfrak{N}_\Delta\big((dx + y\sqrt{D})\mathcal{O}_\Delta\big) = \big|\mathcal{N}(dx + y\sqrt{D})\big| = \big|d^2x^2 - dd^*y^2\big| = 2d = \mathfrak{N}_\Delta(\mathfrak{j}).$$

If $c = 2$ and $2 \nmid xy$, then $D = 4dd^*$ and $x - y = 2u$ for some $u \in \mathbb{Z}$, which implies $2dx + y\sqrt{D} = 4du + (2d + \sqrt{D})y \in \mathfrak{j}$. Hence we obtain $(dx + y\sqrt{D})\mathcal{O}_\Delta \subset \mathfrak{j}$, and equality holds, since

$$\mathfrak{N}_\Delta\big((2dx + y\sqrt{D})\mathcal{O}_\Delta\big) = \big|\mathcal{N}(2dx + y\sqrt{D})\big| = \big|4d^2x^2 - 4dd^*y^2\big| = 4d = \mathfrak{N}_{4D}(\mathfrak{j}).$$

2. (a) By [5, Proposition 1] it follows that $\mathfrak{j} \subset \mathcal{O}_\Delta$ is an $\mathcal{O}_\Delta$-regular ambiguous ideal, every $\mathcal{O}_\Delta$-regular ambiguous ideal is of this form, and $\mathfrak{j}$ is reduced if and only if $d < d^*$. By Proposition 2.3.1, $\mathfrak{N}_\Delta(\mathfrak{j}) = d$.

Let now $\mathfrak{j}$ be principal, say $\mathfrak{j} = \frac{u+y\sqrt{\Delta}}{2}\mathcal{O}_\Delta$, where $u, y \in \mathbb{Z}$ and $u \equiv y \bmod 2$. Then $\frac{u+y\sqrt{\Delta}}{2} \in \mathfrak{j}$ implies $\frac{u+y\sqrt{\Delta}}{2} = dv + \frac{d+\sqrt{\Delta}}{2}w$ for some $v, w \in \mathbb{Z}$. Hence it follows that $u = dx$, where $x = 2v + w$, $w = y$, $\mathfrak{j} = \frac{dx+y\sqrt{\Delta}}{2}$, $d = \mathfrak{N}_\Delta(\mathfrak{j}) = \frac{|d^2x^2 - dd^*y^2|}{4}$, and therefore $|d^2x^2 - dd^*y^2| = 4$.

(b) If $|dx^2 - d^*y^2| = 4$, then $x \equiv y \bmod 2$, $\frac{dx+y\sqrt{\Delta}}{2} = d\frac{x-y}{2} + \frac{d+\sqrt{\Delta}}{2}y \in \mathfrak{j}$, hence $\frac{dx+y\sqrt{\Delta}}{2}\mathcal{O}_\Delta \subset \mathfrak{j}$, and equality holds, since

$$\mathfrak{N}_\Delta\left(\frac{dx+y\sqrt{\Delta}}{2}\mathcal{O}_\Delta\right) = \left|\mathcal{N}\left(\frac{dx+y\sqrt{\Delta}}{2}\right)\right| = \frac{|d^2x^2 - dd^*y^2|}{4} = d = \mathfrak{N}_\Delta(\mathfrak{j}). \qquad \square$$

The following remark addresses the diophantine equation $|dx^2 - d^*y^2| = 1$ if $c = 2$ and $2 \mid xy$.

Remark 4.2. Let $D \in \mathbb{N}$ be not a square, $8 \mid D$ and $D = 4dd^*$, where $d, d^* \in \mathbb{N}$ and $(d, d^*) = 1$. Let $x, y \in \mathbb{Z}$ be such that $|dx^2 - d^*y^2| = 1$.

1. If $2 \mid x$, then $(2dx + y\sqrt{D})\mathcal{O}_{4D} = [4d, \sqrt{D}\,]$.
   Indeed, if $x = 2x_1$, where $x_1 \in \mathbb{Z}$, then $|4dx_1^2 - d^*y^2| = 1$ and $D = (4d)d^*$. Hence the assertion follows by Theorem 4.1.2(a).
2. If $2 \mid y$ and $y = 2y_1$, then $(dx + y_1\sqrt{D})\mathcal{O}_{4D} = [d, \sqrt{D}\,]$.
   Indeed, in this case $|dx^2 - 4d^*y_1^2| = 1$ and $D = d(4d^*)$. Hence again the assertion follows by Theorem 4.1.2(a).

Theorem 4.3. *Let $D \in \mathbb{N}$ be not a square and $l = l(\sqrt{D}\,)$ the period length of $\sqrt{D}$. Let $\mathcal{L}(D)$ be the set of all quadruples $(d, d^*, t, \sigma_\Delta)$, where*

- *$d, d^* \in \mathbb{N}$ and $(d, d^*) = 1$;*
- *$D = c^2dd^*$, where $c \in \{1, 2\}$ if $8 \mid D$, and $c = 1$ if $8 \nmid D$;*
- *$t \in \{1, 2\}$ if $D \equiv 3 \bmod 4$, and $t = 1$ if $D \not\equiv 3 \bmod 4$;*
- *$\sigma \in \{\pm 1\}$;*
- *there exist $x, y \in \mathbb{Z}$ such that $dx^2 - d^*y^2 = \sigma t$ and $(c, xy) = 1$.*

Then $|\mathcal{L}(D)| = 4$, and the structure of $\mathcal{L}(D)$ is as follows.

1. *If l is odd, then $\mathcal{L}(D) = \{(1, D, 1, \pm 1), (D, 1, 1, \pm 1)\}$.*
2. *If $l = 2k$ is even, then*

$$\mathcal{L}(D) = \bigl\{(1, D, 1, 1), (D, 1, 1, -1), \bigl(d, d^*, t, \sigma\bigr), \bigl(d^*, d, t, -\sigma\bigr)\bigr\},$$

   where $1 \leqslant d < d^*$ and $cdt \neq 1$.
3. *Let $l = 2k$ be even and $(d, d^*, t, \sigma) \in \mathcal{L}(D)$ such that $1 \leqslant d < d^*$ and $cdt \neq 1$. Then $\sigma = (-1)^k$. If $(p_n)_{n \geqslant -2}$ denotes the sequence of partial numerators and $(q_n)_{n \geqslant -2}$ the sequence of partial denominators of $\sqrt{D}$, then*

$$p_{k-1}^2 - Dq_{k-1}^2 = (-1)^k c^2dt, \qquad c^2dt\varepsilon_{4D} = (p_{k-1} + q_{k-1}\sqrt{D}\,)^2,$$
$$c^2dt \mid 2p_{k-1} \quad \textit{and} \quad \varepsilon_{4D} = (-1)^k + \frac{2d^*}{t}q_{k-1}^2 + \frac{2p_{k-1}q_{k-1}}{c^2dt}\sqrt{D}.$$

Proof. Note that $(d, d^*, t, \sigma) \in \mathcal{L}(D)$ holds if and only if $(d^*, d, t, -\sigma) \in \mathcal{L}(D)$.

1. If l is odd, then Theorem 3.3 implies that $\mathcal{N}(\varepsilon_{4D}) = -1$, and $\mathcal{O}_{4D}$ is the only reduced ambiguous principal ideal in $\mathcal{O}_{4D}$. Hence we obtain $\mathcal{N}(\mathcal{O}_{4D}^\times) = \{\pm 1\}$, $\{(1, D, 1, \pm 1), (D, 1, 1, \pm 1)\} \subset \mathcal{L}(D)$, $D \not\equiv 3 \bmod 4$ and $t = 1$. Assume now that there exists some $(d, d^*, 1, \sigma) \in \mathcal{L}(D)$ such that $1 \leqslant d < d^*$ and $cd > 1$. Then Theorem 4.1.1 implies the existence of some reduced ambiguous principal ideal $\mathfrak{j} \subset \mathcal{O}_{4D}$ such that $\mathfrak{N}_{4D}(\mathfrak{j}) = c^2d > 1$, a contradiction.

2. Let $l = 2k$ be even. Then Theorem 3.3 implies $\mathcal{N}(\varepsilon_\Delta) = 1$ and therefore $\mathcal{N}(\mathcal{O}_{4D}^\times) = \{1\}$. We prove first:

A. If $(d, d^*, t, \sigma) \in \mathcal{L}(D)$, then $(d, d^*, t, -\sigma) \notin \mathcal{L}(D)$.

Proof of A. Assume to the contrary that there is some $(d, d^*, t, \sigma) \in \mathcal{L}(D)$ such that $(d, d^*, t, -\sigma) \in \mathcal{L}(D)$, and let $x, y, x_1, y_1 \in \mathbb{Z}$ be such that $dx^2 - d^*y^2 = \sigma t$, $dx_1^2 - d^*y_1^2 = -\sigma t$ and $(c, xy) = (c, x_1y_1) = 1$. By Theorem 4.1.1(b) it follows that $(cdx + y\sqrt{D})\mathcal{O}_{4D} = (cdx_1 + y_1\sqrt{D})\mathcal{O}_{4D}$, and therefore $cdx_1 + y_1\sqrt{D} = \varepsilon(cdx + y\sqrt{D})$ for some $\varepsilon \in \mathcal{O}_{4D}^\times$. Taking norms, we obtain

$$-c^2d\sigma t = \mathcal{N}(cdx_1 + y_1\sqrt{D}) = \mathcal{N}(\varepsilon)\mathcal{N}(cdx + y\sqrt{D}) = \mathcal{N}(\varepsilon)c^2d\sigma t,$$

and therefore $\mathcal{N}(\varepsilon) = -1$, a contradiction. □

By Theorem 3.3.4, $\mathcal{O}_{4D}$ contains precisely one reduced ambiguous principal ideal $\mathfrak{j}$ distinct from the unit ideal, and by Theorem 4.1.1 this ideal gives rise to an equation $|dx^2 - d^*y^2| = t$, where $d, d^* \in \mathbb{N}$ and $x, y \in \mathbb{Z}$ are such that $1 \leqslant d < d^*$, $(d, d^*) = 1$, $D = c^2dd^*$, $cdt > 1$ and $(c, xy) = 1$. Hence there exists some $\sigma \in \{\pm 1\}$ such that $(d, d^*, t, \sigma) \in \mathcal{L}(D)$. To prove uniqueness, we must show:

B. If $(d_1, d_1^*, t_1, \sigma_1), (d_2, d_2^*, t_2, \sigma_2) \in \mathcal{L}(D)$, $1 \leqslant d_1 < d_1^*$, $c_1t_1d_1 > 1$, and $1 \leqslant d_2 < d_2^*$, $c_2t_2d_2 > 1$, then $(d_1, d_1^*, t_1, \sigma_1) = (d_2, d_2^*, t_2, \sigma_2)$.

Proof of B. For $i \in \{1, 2\}$, suppose that $(d_i, d_i^*, t_i, \sigma_i) \in \mathcal{L}(D)$, $1 \leqslant d_i < d_i^*$ and $c_it_id_i > 1$, where $c_i \in \{1, 2\}$ are such that $D = c_i^2d_id_i^*$. By Theorem 4.1 there exist $x_i, y_i \in \mathbb{Z}$ such that $(c_i, x_iy_i) = 1$, and

$$\mathfrak{j}_i = (c_id_ix_i + y_i\sqrt{D})\mathcal{O}_{4D} = \begin{cases} [d_i, \sqrt{D}\,] & \text{if } c_it_i = 1, \\ [2d_i, d_i + \sqrt{D}\,] & \text{if } t_i = 2, \\ [4d_i, 2d_i + \sqrt{D}\,] & \text{if } c_i = 2 \end{cases}$$

is a reduced ambiguous ideal distinct from the unit ideal in the principal class of $\mathcal{O}_{4D}$. Hence it follows that $\mathfrak{j}_1 = \mathfrak{j}_2$, and in particular $\mathfrak{N}_{4D}(\mathfrak{j}_1) = \mathfrak{N}_{4D}(\mathfrak{j}_2)$, which implies $c_1^2t_1d_1 = c_2^2t_2d_2$.

If $t_1 = 2$, then $D \equiv 3 \mod 4$, hence $c_1 = c_2 = 1$. Since $2d_1 = t_2d_2$ and d_2 is odd, it follows that $t_2 = 2$, $d_1 = d_2$, $d_1^* = d_2^*$, and A implies $\sigma_1 = \sigma_2$. By symmetry, we may now assume that $t_1 = t_2 = 1$.

Assume now that $c_1 \neq c_2$, say $c_1 = 2$ and $c_2 = 1$. Then we obtain $4d_1 = d_2$ and $[4d_1, 2d_1 + \sqrt{D}\,] = [d_2, \sqrt{D}\,] = [4d_1, \sqrt{D}\,]$, a contradiction. Hence it follows that $c_1 = c_2$, $d_1 = d_2$, $d_1^* = d_2^*$, and A implies $\sigma_1 = \sigma_2$. □

3. Let again $l = 2k$ be even and $(d, d^*, t, \sigma) \in \mathcal{L}(D)$, where $1 \leqslant d < d^*$ and $ctd > 1$. Let $x, y \in \mathbb{Z}$ be such that $dx^2 - d^*y^2 = \sigma t$. Then $\mathfrak{j} = (cdx + y\sqrt{D})\mathcal{O}_{4D}$ is a reduced principal ideal of $\mathcal{O}_{4D}$ such that $\mathfrak{N}_{4D}(\mathfrak{j}) = c^2dt$ by Theorem 4.1.1.

Let $(\xi_n)_{n \geqslant 0}$ be the sequence of complete quotients of $\sqrt{D} = \omega_{4D}$, and for $n \geqslant 0$ let (a_n, b_n, c_n) be the type of ξ_n. By Theorem 3.3, $I(\xi_l) = \mathcal{O}_{4D}$ and $I(\xi_k)$ are the only reduced ambiguous principal ideals of $\mathcal{O}_{4D}$. Hence it follows that $\mathfrak{j} = I(\xi_k)$, and $\mathfrak{N}_{4D}(\mathfrak{j}) = |\mathcal{N}(\xi_k)| = c^2dt = a_k$. By Theorem 3.3 we obtain

$$\mathcal{N}(\xi_k) = p_{k-1}^2 - c^2dd^*q_{k-1}^2 = (-1)^kc^2dt, \qquad c^2dt\varepsilon_{4D} = (p_{k-1} + q_{k-1}\sqrt{D})^2$$

and

$$\varepsilon_{4D} = \frac{p_{k-1}^2 + q_{k-1}^2D + 2p_{k-1}q_{k-1}\sqrt{D}}{c^2dt} = (-1)^k + \frac{2d^*}{t}q_{k-1}^2 + \frac{2p_{k-1}q_{k-1}}{c^2dt}\sqrt{D}$$

(note that $c^2dt \mid 2p_{k-1}$ by Theorem 3.3). It remains to prove that $\sigma = (-1)^k$.

Case 1. $c=2$. Then $8 \mid D$, $t=1$, $a_k = 4d \mid 2p_{k-1}$, and therefore $p_{k-1} = 2dx_1$, where $x_1 \in \mathbb{Z}$. If $y_1 = q_{k-1}$, then $(p_{k-1}, q_{k-1}) = 1$ implies $2 \nmid y_1$, and it follows that $dx_1^2 - d^*y_1^2 = (-1)^k$. If $2 \nmid x_1$, then $(d, d^*, 1, (-1)^k) \in \mathcal{L}(D)$, hence $\sigma = (-1)^k$, and we are done.

We assert that the case $2 \mid x_1$ cannot occur. Indeed, if $2 \mid x_1$, then $x_1 = 2x_2$, where $x_2 \in \mathbb{Z}$, and $4dx_2^2 - d^*y_1^2 = (-1)^k$. But this implies that $(4d, d^*, 1, (-1)^k) \in \mathcal{L}(D)$, hence either $(4d, d^*, 1, (-1)^k) = (d, d^*, 1, \sigma)$ or $(4d, d^*, 1, (-1)^k) = (d^*, 4d, 1, -\sigma)$, and both relations are impossible.

Case 2. $c=1$ and $2 \nmid d$ (in particular, this occurs if $D \equiv 3 \bmod 4$). As $a_k = td \mid 2p_{k-1}$, it follows that $d \mid p_{k-1}$, say $p_{k-1} = dx_1$, where $x_1 \in \mathbb{Z}$. If $y_1 = q_{k-1}$, then $dx_1^2 - d^*y_1^2 = (-1)^k t$, hence $(d, d^*, t, (-1)^k) \in \mathcal{L}(D)$ and therefore $\sigma = (-1)^k$.

Case 3. $ct = 1$ and $d = 2d_0$, where $d_0 \in \mathbb{N}$ and $2 \nmid d_0$. Since $a_k = 2d_0 \mid 2p_{k-1}$, we obtain $p_{k-1} = d_0x_1$, where $x_1 \in \mathbb{Z}$. If $y_1 = q_{k-1}$, then $d_0x_1^2 - 2d^*y_1^2 = 2(-1)^k$, which implies that $2 \mid x_1$. If $x_1 = 2x_2$, where $x_2 \in \mathbb{Z}$, then $dx_2^2 - d^*y_1^2 = (-1)^k$, hence $(d, d^*, 1, (-1)^k) \in \mathcal{L}(D)$ and therefore $\sigma = (-1)^k$.

Case 4. $ct = 1$ and $d = 4^e d_0$, where $e, d_0 \in \mathbb{N}$ and $4 \nmid d_0$. If $D_0 = d_0 d^*$, then $\sigma = dx^2 - d^*y^2 = d_0(2^e x)^2 - d^*y^2$ implies that $(d_0, d^*, 1, \sigma) \in \mathcal{L}(D_0)$. Since $a_k = 4^e d_0 \mid 2p_{k-1}$, it follows that $2^e d_0 \mid 2^{2e-1} d_0 \mid p_{k-1}$, and we set $p_{k-1} = 2^e d_0 x_1$, where $x_1 \in \mathbb{Z}$. If $y_1 = q_{k-1}$, then $(p_{k-1}, q_{k-1}) = 1$ implies $2 \nmid y_1$. It follows that $d_0x_1^2 - d^*y_1^2 = (-1)^k$, and therefore $(d_0, d^*, 1, (-1)^k) \in \mathcal{L}(D_0)$. If $d_0 > 1$, then $l(\sqrt{D_0})$ is even, and B (applied with D_0 instead of D) yields $\sigma = (-1)^k$. If $d_0 = 1$, then $\sigma \equiv -d^* \bmod 4$. Since $2 \nmid d^*y_1^2$, it follows that $2 \mid x_1$, hence $(-1)^k \equiv -d^* \bmod 4$, and thus again $\sigma = (-1)^k$. $\square$

Theorem 4.4. *Let $\Delta \in \mathbb{N}$ be not a square, $\Delta \equiv 1 \bmod 4$, $l = l(\omega_\Delta)$ the period length of ω_Δ and $l^* = l(\sqrt{\Delta})$ the period length of $\sqrt{\Delta}$. Let $\mathcal{L}_0(\Delta)$ be the set of all triples (d, d^*, σ) such that*

$$d, d^* \in \mathbb{N},\ \bigl(d, d^*\bigr) = 1,\ \Delta = dd^*,\ \sigma \in \{\pm 1\},\ \text{and there exist } x, y \in \mathbb{Z} \text{ such that } dx^2 - d^*y^2 = 4\sigma.$$

Then $|\mathcal{L}_0(\Delta)| = 4$, and the structure of $\mathcal{L}_0(\Delta)$ is as follows.

1. *If l is odd, then $\mathcal{L}_0(\Delta) = \{(1, \Delta, \pm 1), (\Delta, 1, \pm 1)\}$.*
2. *If $l = 2k$ is even, then*

$$\mathcal{L}_0(\Delta) = \bigl\{(1, \Delta, 1), (\Delta, 1, -1), \bigl(d, d^*, \sigma\bigr), \bigl(d^*, d, -\sigma\bigr)\bigr\},$$

   where $(d, d^*, \sigma) \notin \{(1, \Delta, -1), (\Delta, 1, 1)\}$.
3. *Let $l = 2k$ be even and $(d, d^*, \sigma) \in \mathcal{L}_0(\Delta)$ such that $1 < d < d^*$. Then $\sigma = (-1)^k$. Let $(p_n)_{n \geqslant -2}$ be the sequence of partial numerators and $(q_n)_{n \geqslant -2}$ the sequence of partial denominators of ω_Δ. Then $d \mid 2p_{k-1} - q_{k-1}$, and if $2p_{k-1} - q_{k-1} = ds_k$, then*

$$ds_k^2 - d^*q_{k-1}^2 = 4(-1)^k, \qquad d\varepsilon_\Delta = \left(\frac{ds_k + q_{k-1}\sqrt{\Delta}}{2}\right)^2,$$

   and

$$\varepsilon_\Delta = (-1)^k + \frac{d^*q_{k-1}^2 + q_{k-1}s_k\sqrt{\Delta}}{2}.$$

   Moreover, ε_Δ has half-integral coordinates if and only if there exist $x, y \in \mathbb{Z}$ such that $|dx^2 - d^*y^2| = 4$ and $(x, y) = 1$.
4. *If $(d, d^*, \sigma) \in \mathcal{L}_0(\Delta)$, then there exist $x_1, y_1 \in \mathbb{Z}$ such that $dx_1^2 - d^*y_1^2 = \sigma$. In particular, if l is even, then $l \equiv l^* \bmod 4$.*

Proof. Note that $(d, d^*, \sigma) \in \mathcal{L}_0(\Delta)$ holds if and only if $(d^*, d, -\sigma) \in \mathcal{L}_0(\Delta)$.

1. If l is odd, then Theorem 3.3 implies that $\mathcal{N}(\varepsilon_\Delta) = -1$, and $\mathcal{O}_\Delta$ is the only reduced ambiguous principal ideal in $\mathcal{O}_\Delta$. Hence $\mathcal{N}(\mathcal{O}_\Delta^\times) = \{\pm 1\}$, and therefore $\{(1, \Delta, \pm 1), (\Delta, 1, \pm 1)\} \subset \mathcal{L}_0(\Delta)$. Assume that there is some $(d, d^*, \sigma) \in \mathcal{L}_0(\Delta)$ such that $1 < d < d^*$. Then Theorem 4.1.2 implies the existence of some reduced ambiguous principal ideal $\mathfrak{j} \subset \mathcal{O}_{4D}$ such that $\mathfrak{N}_{4D}(\mathfrak{j}) = d > 1$, a contradiction.

2. Let $l = 2k$ be even. Then Theorem 3.3 implies $\mathcal{N}(\mathcal{O}_\Delta^\times) = \{1\}$. We prove first:

A. If $(d, d^*, \sigma) \in \mathcal{L}_0(\Delta)$, then $(d, d^*, -\sigma) \notin \mathcal{L}_0(\Delta)$.

Proof of A. Assume to the contrary that there is some $(d, d^*, \sigma) \in \mathcal{L}_0(\Delta)$ such that $(d, d^*, -\sigma) \in \mathcal{L}_0(\Delta)$, and let $x, y, x_1, y_1 \in \mathbb{Z}$ be such that $dx^2 - d^* y^2 = 4\sigma$ and $dx_1^2 - d^* y_1^2 = -4\sigma$. By Theorem 4.1.2 it follows that

$$\left[d, \frac{d + \sqrt{\Delta}}{2}\right] = \frac{dx + y\sqrt{\Delta}}{2}\mathcal{O}_\Delta = \frac{dx_1 + y_1\sqrt{\Delta}}{2}\mathcal{O}_\Delta$$

and therefore $dx_1 + y_1\sqrt{\Delta} = \varepsilon(dx + y\sqrt{\Delta})$ for some $\varepsilon \in \mathcal{O}_\Delta^\times$. Taking norms, we obtain $-4d\sigma = \mathcal{N}(dx_1 + y_1\sqrt{\Delta}) = \mathcal{N}(\varepsilon)\mathcal{N}(dx + y\sqrt{\Delta}) = 4\mathcal{N}(\varepsilon)d\sigma$ and therefore $\mathcal{N}(\varepsilon) = -1$, a contradiction. $\square$

By Theorem 3.3.4, $\mathcal{O}_{4D}$ contains precisely one reduced ambiguous principal ideal $\mathfrak{j}$ distinct from the unit ideal, and by Theorem 4.1.2 this ideal gives rise to an equation $|dx^2 - d^* y^2| = 4$, where $d, d^* \in \mathbb{N}$, $1 < d < d^*$, $(d, d^*) = 1$, $\Delta = dd^*$ and $x, y \in \mathbb{Z}$. Hence there exists some $\sigma \in \{\pm 1\}$ such that $(d, d^*, \sigma) \in \mathcal{L}_0(D)$. To prove uniqueness, we must show:

B. If $(d_1, d_1^*, \sigma_1), (d_2, d_2^*, \sigma_2) \in \mathcal{L}_0(\Delta)$, $1 < d_1 < d_1^*$ and $1 < d_2 < d_2^*$, then $(d_1, d_1^*, \sigma_1) = (d_2, d_2^*, \sigma_2)$.

Proof of B. For $i \in \{1, 2\}$, suppose that $(d_i, d_i^*, \sigma_i) \in \mathcal{L}_0(\Delta)$. By Theorem 4.1.2 there exist $x_i, y_i \in \mathbb{Z}$ such that

$$\mathfrak{j}_i = \frac{d_i x_i + y_i\sqrt{\Delta}}{2}\mathcal{O}_\Delta = \left[d_i, \frac{d_i + \sqrt{\Delta}}{2}\right]$$

is a reduced ambiguous principal ideal distinct from the unit ideal of $\mathcal{O}_\Delta$. Therefore it follows that $\mathfrak{j}_1 = \mathfrak{j}_2$, in particular $d_1 = d_2$, hence $d_1^* = d_2^*$, and A implies $\sigma_1 = \sigma_2$. $\square$

3. Let again $l = 2k$ be even and $(d, d^*, \sigma) \in \mathcal{L}_0(\Delta)$, where $1 < d < d^*$. Let $x, y \in \mathbb{Z}$ be such that $dx^2 - d^* y^2 = 4\sigma$. Then

$$\mathfrak{j} = \left(\frac{dx + y\sqrt{\Delta}}{2}\right)\mathcal{O}_\Delta = \left[d, \frac{d + \sqrt{\Delta}}{2}\right]$$

is a reduced principal ideal of $\mathcal{O}_\Delta$ such that $\mathfrak{N}(\mathfrak{j}) = d$ by Theorem 4.1.2.

Let $(\xi_n)_{n \geqslant 0}$ be the sequence of complete quotients of ω_Δ, and for $n \geqslant 0$ let (a_n, b_n, c_n) be the type of ξ_n. By Theorem 3.3, $I(\xi_l) = \mathcal{O}_\Delta$ and $I(\xi_k)$ are the only reduced ambiguous principal ideals of $\mathcal{O}_{4D}$. Hence it follows that $\mathfrak{j} = I(\xi_k)$ and $\mathfrak{N}_\Delta(\mathfrak{j}) = |\mathcal{N}(\xi_k)| = d = a_k$. Since $a_k \mid (2p_{k-1} - q_{k-1}, \Delta)$ by Theorem 3.3, there exists some $s_k \in \mathbb{Z}$ such that $2p_{k-1} - q_{k-1} = ds_k$, and then $4(-1)^k d = d^2 s_k^2 - dd^* q_{k-1}^2$, which implies $ds_k^2 - d^* q_{k-1}^2 = 4(-1)^k$. Moreover,

$$d\varepsilon_\Delta = \left(\frac{ds_k + q_{k-1}\sqrt{\Delta}}{2}\right)^2 \quad \text{and} \quad \varepsilon_\Delta = (-1)^k + \frac{d^* q_{k-1}^2 + q_{k-1} s_k \sqrt{\Delta}}{2}.$$

In particular, $(d, d^*, (-1)^k) \in \mathcal{L}_0(\Delta)$, and by A it follows that $(d, d^*, \sigma) \in \mathcal{L}_0(\Delta)$ if and only if $\sigma = (-1)^k$.

The above formulas show that ε_Δ has half-integral coordinates if and only if $2 \nmid q_{k-1}$, and in this case the diophantine equation $|dx^2 - d^*y^2| = 4$ has a solution $(x, y) \in \mathbb{Z}^2$ such that $(x, y) = 1$, namely $(x, y) = (s_k, q_{k-1})$. Assume now that there exist $x, y \in \mathbb{Z}$ such that $(x, y) = 1$ and $dx^2 - d^*y^2 = \sigma \in \{\pm 1\}$. Then

$$\varepsilon = \frac{2\sigma + d^*y^2 + xy\sqrt{\Delta}}{2} \in \mathcal{O}_\Delta$$

is half-integral, and $\mathcal{N}(\varepsilon) = 1$, which implies that $\varepsilon \in \mathcal{O}_\Delta^\times \setminus \mathcal{O}_{4\Delta}^\times$. Since $\mathcal{O}_\Delta^\times \neq \mathcal{O}_{4\Delta}^\times$ if and only if ε_Δ has half-integral coordinates, it follows that ε_Δ has half-integral coordinates.

4. Suppose that $(d, d^*, \sigma) \in \mathcal{L}_0(\Delta)$, and let $x, y \in \mathbb{Z}$ be such that $dx^2 - d^*y^2 = 4\sigma$. If $x \equiv y \equiv 0 \bmod 2$, we set $x = 2x_1$, $y = 2y_1$, and we obtain $dx_1^2 - d^*y_1^2 = \sigma$. Thus assume now that $x \equiv y \equiv 1 \bmod 2$. Then we set

$$x_1 = \frac{(dx^2 - 3\sigma)x}{2} \quad \text{and} \quad y_1 = \frac{(dx^2 - \sigma)y}{2},$$

and we assert that $dx_1^2 - d^*y_1^2 = \sigma$. For the proof, we start with the identity

$$64\sigma d^3 = \left(d^2x^2 - \Delta y^2\right)^3 = \left[dx\left(d^2x^2 + 3\Delta y^2\right)\right]^2 - \Delta\left[y\left(3d^2x^2 + \Delta y^2\right)\right]^2.$$

Now we find

$$\begin{aligned} dx\left(d^2x^2 + 3\Delta y^2\right) &= dx\left[4d^2x^2 - 3\left(d^2x^2 - \Delta y^2\right)\right] = dx\left(4d^2x^2 - 12d\sigma\right) \\ &= 4d^2x\left(dx^2 - 3\sigma\right) = 8d^2x_1 \end{aligned}$$

and

$$\begin{aligned} y\left(3d^2x^2 + \Delta y^2\right) &= y\left[4d^2x^2 - \left(d^2x^2 - \Delta y^2\right)\right] = y\left(4d^2x^2 - 4d\sigma\right) \\ &= 4dy\left(dx^2 - \sigma\right) = 8dy_1. \end{aligned}$$

Hence it follows that $64\sigma d^3 = 64d^4x_1^2 - 64d^2y_1^2\Delta$, and therefore $\sigma = dx_1^2 - d^*y_1^2$.

Suppose now that l is even. Then there exists some $(d, d^*, \sigma) \in \mathcal{L}_0(\Delta)$ such that $1 < d < d^*$, and, as we have just proved, this implies that $(d, d^*, 1, \sigma) \in \mathcal{L}(\Delta)$. By Theorem 4.3 it follows that l^* is even, and if $l^* = 2k^*$, then $\sigma = (-1)^k = (-1)^{k^*}$, which implies $l \equiv l^* \bmod 4$. $\square$

Remark 4.5. Theorems 4.3 and 4.4 are closely connected with the results of R.A. Mollin in [13], in particular with his Theorems 3 and 9. There he derives a close connection between the fundamental solutions of pellian and antipellian equations in terms of continued fractions.

5. Applications

Theorem 5.1. *(Compare [13, Theorem 5 and corollaries].) Let* $q \equiv 3 \bmod 4$ *be a prime and* $\Delta = 4q^r$ *for some odd* $r \in \mathbb{N}$.

1. *Then* $l(\sqrt{q}) = 2k$ *is even,* $l(\sqrt{q^r}) \equiv l(\sqrt{q}) \bmod 4$, *and there exists exactly one* $\sigma \in \{\pm 1\}$ *such that the diophantine equation*

$$x^2 - q^r y^2 = 2\sigma \textit{ is solvable, namely } \sigma = (-1)^k = \begin{cases} 1 & \textit{if } q \equiv 7 \bmod 8, \\ -1 & \textit{if } q \equiv 3 \bmod 8. \end{cases}$$

2. *If* $\varepsilon_\Delta = u + v\sqrt{q^r}$, *where* $u, v \in \mathbb{N}$, *then* $2 \mid u$ *and* $\mathcal{N}(\varepsilon_\Delta) = 1$.

Proof. 1. By Theorem 3.3, $\mathcal{N}(\varepsilon_\Delta) = 1$ and $l(\sqrt{q^r}) = 2k$ is even. By Theorem 4.3, applied with $D = q^r$, there exists a unique $\sigma \in \{\pm 1\}$ such that the diophantine equation $x^2 - q^r y^2 = 2\sigma$ has a solution $(x, y) \in \mathbb{Z}^2$, namely $\sigma = (-1)^k$. Hence

$$1 = \left(\frac{2(-1)^k}{q}\right) = (-1)^k \left(\frac{2}{q}\right), \quad \text{and} \quad \sigma = (-1)^k = \begin{cases} 1 & \text{if } q \equiv 7 \bmod 8, \\ -1 & \text{if } q \equiv 3 \bmod 8. \end{cases}$$

Therefore the parity of k does not depend on r.

2. Let $(p_n)_{n \geqslant -2}$ the sequence of partial numerators and $(q_n)_{n \geqslant -2}$ the sequence of partial denominators of $\sqrt{q^r}$. Since $(1, q^r, 2, (-1)^k) \in \mathcal{L}(q^r)$, it follows that $p_{k-1}^2 - q^r q_{k-1}^2 = 2(-1)^k$, hence $2 \nmid q_{k-1}$, and $\varepsilon_\Delta = (-1)^k + q^r q_{k-1}^2 + p_{k-1} q_{k-1} \sqrt{D}$, which implies $u = (-1)^k + q^r q_{k-1}^2 \equiv 0 \bmod 2$. □

Theorem 5.2. *Let* $q \equiv 3 \bmod 4$ *be a prime and* $r \in \mathbb{N}$. *Then* $l(\sqrt{2q}) = 2k$ *is even,* $l(\sqrt{2q^r}) \equiv l(\sqrt{2q}) \bmod 4$, *and there exists exactly one* $\sigma \in \{\pm 1\}$ *such that the diophantine equation*

$$2x^2 - q^r y^2 = \sigma \textit{ is solvable, namely } \sigma = (-1)^k = \begin{cases} 1 & \textit{if } q \equiv 7 \bmod 8, \\ -1 & \textit{if } q \equiv 3 \bmod 8. \end{cases}$$

Proof. Note that $l(\sqrt{2q^r}) = 2k$ is even by Theorem 3.3. By Theorem 4.3, applied with $D = 2q^r$, there exists a unique $\sigma \in \{\pm 1\}$ such that the diophantine equation $2x^2 - q^r y^2 = \sigma$ has a solution $(x, y) \in \mathbb{Z}^2$, namely $\sigma = (-1)^k$. Hence

$$1 = \left(\frac{2(-1)^k}{q}\right) = (-1)^k \left(\frac{2}{q}\right), \quad \text{and} \quad \sigma = (-1)^k = \begin{cases} 1 & \text{if } q \equiv 7 \bmod 8, \\ -1 & \text{if } q \equiv 3 \bmod 8. \end{cases}$$

In particular, the parity of k does not depend on r. □

Theorem 5.3. *(Compare [13, Theorem 10].) Let* q *and* q *be odd primes and* $\Delta = 4p^r q^s$ *for some odd* $r, s \in \mathbb{N}$ *such that* $p^r < q^s$.

1. *If* $\mathcal{N}(\varepsilon_\Delta) = -1$, *then the diophantine equation* $|p^r x^2 - q^s y^2| = 1$ *is unsolvable.*
2. *Suppose that* $\mathcal{N}(\varepsilon_\Delta) = 1$ *and* $l(\sqrt{p^r q^s}) = 2k$. *Then there exists precisely one* $\sigma \in \{\pm 1\}$ *such that the diophantine equation* $p^r x^2 - q^s y^2 = \sigma$ *is solvable, namely* $\sigma = (-1)^k$. *In particular,*

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

Proof. By Theorem 4.3, applied with $D = p^r q^s$. □

Theorem 5.4. *Let* p *and* q *be primes and* $\Delta = 8p^r q^s$ *for some odd* $r, s \in \mathbb{N}$. *If* $\mathcal{N}(\varepsilon_\Delta) = 1$, *we set* $l(\sqrt{2p^r q^s}) = 2k$.

1. *Let* $p \equiv 1 \bmod 8$ *and* $q \equiv 5 \bmod 8$.

(a) *The diophantine equations* $|2x^2 - p^r q^s y^2| = 1$ *and* $|2p^r x^2 - q^s y^2| = 1$ *are unsolvable.*
(b) *If* $\mathcal{N}(\varepsilon_\Delta) = 1$*, then there exists precisely one* $\sigma \in \{\pm 1\}$ *such that the diophantine equation* $p^r x^2 - 2q^s y^2 = \sigma$ *is solvable, namely*

$$\sigma = \begin{cases} (-1)^k & \text{if } p^r < 2q^s, \\ (-1)^{k+1} & \text{if } p^r > 2q^s, \end{cases} \quad \text{and} \quad \left(\frac{p}{q}\right) = 1.$$

(c) *If* $\mathcal{N}(\varepsilon_\Delta) = -1$*, then the diophantine equation* $|p^r x^2 - 2q^s y^2| = 1$ *is unsolvable.*

2. *Let* $p \equiv 3 \bmod 8$ *and* $q \equiv 5 \bmod 8$ (*then* $\mathcal{N}(\varepsilon_\Delta) = 1$).
(a) *The diophantine equation* $|2x^2 - p^r q^s y^2| = 1$ *is unsolvable.*
(b) *Exactly one of the two diophantine equations*

$$2p^r x^2 - q^s y^2 = -\left(\frac{p}{q}\right) \quad \text{and} \quad p^r x^2 - 2q^s y^2 = \left(\frac{p}{q}\right)$$

is solvable, while the two diophantine equations

$$2p^r x^2 - q^s y^2 = \left(\frac{p}{q}\right) \quad \text{and} \quad p^r x^2 - 2q^s y^2 = -\left(\frac{p}{q}\right)$$

are both unsolvable.

3. *Let* $p \equiv 3 \bmod 8$ *and* $q \equiv 7 \bmod 8$ (*then* $\mathcal{N}(\varepsilon_\Delta) = 1$).
(a) *The diophantine equations* $|2x^2 - p^r q^s y^2| = 1$ *and* $|p^r x^2 - 2q^s y^2| = 1$ *are both unsolvable.*
(b) *There exists precisely one* $\sigma \in \{\pm 1\}$ *such that the diophantine equation* $2p^r x^2 - q^s y^2 = \sigma$ *is solvable, namely*

$$\sigma = \begin{cases} (-1)^k & \text{if } 2p^r < q^s, \\ (-1)^{k+1} & \text{if } 2p^r > q^s, \end{cases} \quad \text{and} \quad (-1)^k \left(\frac{p}{q}\right)(q^s - 2p^r) > 0.$$

(c) *(Compare [13, Corollary 10].) If* $\varepsilon_\Delta = u + v\sqrt{2p^r q^s}$*, then* v *is even, and*

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

Proof. We apply Theorem 4.3 with $D = 2p^r q^s$. If $\mathcal{N}(\varepsilon_\Delta) = 1$, then exactly one of the six diophantine equations

$$\text{(I)} \quad 2x^2 - p^r q^s y^2 = \pm 1, \qquad \text{(II)} \quad 2p^r x^2 - q^s y^2 = \pm 1, \qquad \text{(III)} \quad p^r x^2 - 2q^s y^2 = \pm 1$$

is solvable. Otherwise, if $\mathcal{N}(\varepsilon_\Delta) = -1$, then $p \equiv q \equiv 1 \bmod 4$, and all these diophantine equations are unsolvable.

1. (a) If $x, y \in \mathbb{Z}$ are such that $2x^2 - p^r q^s y^2 = \sigma \in \{\pm 1\}$, then $2x^2 \equiv \sigma \bmod q$, and therefore

$$1 = \left(\frac{\sigma}{q}\right) = \left(\frac{2}{q}\right),$$

a contradiction.

If $x, y \in \mathbb{Z}$ are such that $2p^r x^2 - q^s y^2 = \sigma \in \{\pm 1\}$, then the congruences $2p^r x^2 \equiv \sigma \bmod q$ and $q^s y^2 \equiv \sigma \bmod p$ imply that

$$1=\left(\frac{\sigma}{q}\right)=\left(\frac{2p}{q}\right)=-\left(\frac{p}{q}\right)\quad\text{and}\quad 1=\left(\frac{\sigma}{p}\right)=\left(\frac{q}{p}\right),$$

which contradicts the quadratic reciprocity law.

(b) By (a) and Theorem 4.3, there exists exactly one $\sigma\in\{\pm 1\}$ such that the diophantine equation $p^rx^2-2q^sy^2=\sigma$ is solvable, and $\sigma=(-1)^k$ if and only if $p^r<2q^s$. In particular, it follows that

$$1=\left(\frac{\sigma}{q}\right)=\left(\frac{p}{q}\right).$$

(c) By the preliminary remark.

2. (a) As in 1(a), since ± 2 is a quadratic non-residue modulo q.

(b) By the preliminary remark, exactly one of the four diophantine equations $2p^rx^2-q^sy^2=\pm 1$ and $p^rx^2-2q^sy^2=\pm 1$ is solvable. Let $x,y\in\mathbb{Z}$ and $\sigma\in\{\pm 1\}$. If $2p^rx^2-q^sy^2=\sigma$, then $\sigma\equiv -q^sy^2 \bmod p$ and therefore

$$\sigma=\left(\frac{\sigma}{p}\right)=-\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right).$$

If $p^rx^2-2q^sy^2=\sigma$, then $\sigma\equiv -2q^sy^2 \bmod p$ and therefore

$$\sigma=\left(\frac{\sigma}{p}\right)=\left(\frac{-2q}{p}\right)=\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right).$$

3. (a) If $x,y\in\mathbb{Z}$ are such that $2x^2-p^rq^sy^2=\sigma\in\{\pm 1\}$, then $2x^2\equiv\sigma \bmod p$ and $2x^2\equiv\sigma \bmod q$, which implies

$$-1=\left(\frac{2}{p}\right)=\left(\frac{\sigma}{p}\right)=\left(\frac{\sigma}{q}\right)=\left(\frac{2}{q}\right)=1,\quad\text{a contradiction.}$$

If $x,y\in\mathbb{Z}$ are such that $p^rx^2-2q^sy^2=\sigma\in\{\pm 1\}$, then $p^rx^2\equiv\sigma \bmod q$ and $-2q^sy^2\equiv\sigma \bmod p$, which implies

$$\sigma=\left(\frac{\sigma}{p}\right)=\left(\frac{-2q}{p}\right)=\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)=-\left(\frac{\sigma}{q}\right)=-\sigma,\quad\text{a contradiction.}$$

(b) By (a) and the preliminary remark, there is exactly one $\sigma\in\{\pm 1\}$ for which the diophantine equation $2p^rx^2-q^sy^2=\sigma$ is solvable, and by Theorem 4.3 we obtain $\sigma=(-1)^k$ if and only if $2p^r<q^s$. If $x,y\in\mathbb{Z}$ are such that $2p^rx^2-q^sy^2=\sigma$, then $2p^rx^2\equiv\sigma \bmod q$, and therefore

$$\sigma=\left(\frac{\sigma}{q}\right)=\left(\frac{2p}{q}\right)=\left(\frac{p}{q}\right),\quad\text{which implies}\quad (-1)^k\left(\frac{p}{q}\right)\left(q^s-2p^r\right)>0.$$

(c) Let $(p_n)_{n\geqslant -2}$ the sequence of partial numerators and $(q_n)_{n\geqslant -2}$ the sequence of partial denominators of $\sqrt{2p^rq^s}$. For $g\in\mathbb{Z}$, we denote by $\mathrm{v}_2(g)$ the 2-adic exponent of g.

Assume first that $2p^r<q^s$. Then $(2p^r,q^s,1,(-1)^k)\in\mathcal{L}(2p^rq^s)$, and it follows that $p_{k-1}^2-2p^rq^sq_{k-1}^2=(-1)^k2p^r$, $2\mid p_{k-1}$, $2\nmid q_{k-1}$, and

$$\varepsilon_\Delta=(-1)^k+2q^sq_{k-1}^2+\frac{p_{k-1}q_{k-1}}{p^r}\sqrt{2p^rq^s},\quad\text{which implies}\quad v=\frac{p_{k-1}q_{k-1}}{p^r}$$

and $\mathsf{v}_2(v) = \mathsf{v}_2(p_{k-1}) \geqslant 1$. Since

$$p_{k-1}^2 = 2p^r\big[(-1)^k + q^s q_{k-1}^2\big] \equiv 2\big[1-(-1)^k\big] \mod 8,$$

it follows that $4 \mid p_{k-1}$ (and thus $4 \mid v$) if and only if $2 \mid k$, and therefore

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

Assume now that $q^s < 2p^r$. Then $(q^s, 2p^r, 1, (-1)^k) \in \mathcal{L}(2p^r q^s)$, and it follows that $p_{k-1}^2 - 2p^r q^s q_{k-1}^2 = (-1)^k q^s$, hence $2 \nmid p_{k-1}$, and

$$\varepsilon_\Delta = (-1)^k + 4p^r q_{k-1}^2 + \frac{2p_{k-1}q_{k-1}}{q^s}\sqrt{2p^r q^s}, \quad \text{which implies} \quad v = \frac{2p_{k-1}q_{k-1}}{q^s}$$

and $\mathsf{v}_2(v) = \mathsf{v}_2(q_{k-1}) + 1 \geqslant 1$. Since

$$p_{k-1}^2 = q^s\big[2p^r q_{k-1}^2 + (-1)^k\big] \equiv 2q_{k-1}^2 - (-1)^k \mod 8,$$

it follows that $2q_{k-1}^2 \equiv 1 + (-1)^k \mod 8$. Hence $2 \mid q_{k-1}$ (and thus $4 \mid v$) if and only if $2 \nmid k$, and therefore

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

References

[1] C. Friesen, Legendre symbols and continued fractions, Acta Arith. 59 (1991) 365–379.
[2] C.F. Gauss, Disquisitiones Arithmeticae, Springer, 1966.
[3] B. Goddard, K. Cheng, R.A. Mollin, The diophantine equatione $ax^2 - by^2 = c$ solved via continued fractions, Acta Math. Univ. Comenian. 71 (2002) 121–138.
[4] F. Halter-Koch, Über Pell'sche Gleichungen und Kettenbrüche, Arch. Math. 49 (1987) 29–37.
[5] F. Halter-Koch, P. Kaplan, K.S. Williams, Y. Yamamoto, Infrastructure des classes ambiges d'ideaux des ordres des corps quadratiques réels, Enseign. Math. 37 (1991) 263–292.
[6] H. Hasse, Vorlesungen über Zahlentheorie, Springer, 1950.
[7] H. Hasse, Number Theory, Springer, 1980.
[8] P. Kaplan, A propos des équations antipelliennes, Enseign. Math. 29 (1983) 323–328.
[9] P. Kaplan, K.S. Williams, The distance between ideals in the orders of a real quadratic field, Enseign. Math. 36 (3) (1990) 321–358.
[10] R.A. Mollin, All solutions of the Diophantine equation $x^2 - dy^2 = n$, Far East J. Math. Special Volume III (1998) 257–293.
[11] R.A. Mollin, Quadratics, CRC Press, 1996.
[12] R.A. Mollin, Jacobi symbols, ambiguous ideals, and continued fractions, Acta Arith. 85 (1998) 331–349.
[13] R.A. Mollin, A continued fraction approach to the Diophantine equation $ax^2 - by^2 = \pm 1$, JP J. Algebra Number Theory Appl. 4 (2004) 565–571.
[14] R.A. Mollin, A.J. van der Poorten, Continued fractions, Jacobi symbols, and quadratic diophantine equations, Canad. Math. Bull. 43 (2000) 218–225.
[15] G. Pall, Discriminantal divisors of binary quadratic forms, J. Number Theory 1 (1969) 525–533.
[16] O. Perron, Die Lehre von den Kettenbrüchen, B.G. Teubner, 1989.
[17] H.F. Trotter, On the norms of units in quadratic fields, Proc. Amer. Math. Soc. 22 (1969) 198–201.
[18] A.J. van der Poorten, P.G. Walsh, A note on Jacobi symbols and continued fractions, Amer. Math. Monthly 106 (1999) 52–56.