Canad. Math. Bull. Vol. **43** (2), 2000 pp. 218–225

Continued Fractions, Jacobi Symbols, and Quadratic Diophantine Equations

R. A. Mollin and A. J. van der Poorten

Abstract. The results herein continue observations on norm form equations and continued fractions begun and continued in the works [1]–[3], and [5]–[6].

1 Notation and Preliminaries

Let $D_0 > 1$ be a square-free positive integer and set: $\sigma_0 = \begin{cases} 2 & \text{if } D_0 \equiv 1 \pmod 4, \\ 1 & \text{otherwise.} \end{cases}$

Define

$$\omega_0 = (\sigma_0 - 1 + \sqrt{D_0})/\sigma_0,$$

and

$$\Delta_0 = (\omega_0 - \omega_0')^2 = 4D_0/\sigma_0^2,$$

where ω_0' is the *algebraic conjugate* of ω_0, namely $\omega_0' = (\sigma_0 - 1 - \sqrt{D_0})/\sigma_0$. The value Δ_0 is called a *fundamental discriminant* or *field discriminant* with associated *radicand* D_0, and ω_0 is called the *principal fundamental surd associated with* Δ_0. Let

$$\Delta = f_\Delta^2 \Delta_0$$

for some $f_\Delta \in \mathbb{N}$. If we set $g = \gcd(f_\Delta, \sigma_0)$, $\sigma = \sigma_0/g$,

$$D = (f_\Delta/g)^2 D_0,$$

and

$$\Delta = 4D/\sigma^2,$$

then Δ is called a *discriminant* with associated *radicand* D. Furthermore, if we let

$$\omega_\Delta = (\sigma - 1 + \sqrt{D})/\sigma = f_\Delta \omega_0 + h$$

for some $h \in \mathbb{Z}$, then ω_Δ is called the *principal surd* associated with the discriminant $\Delta = (\omega_\Delta - \omega_\Delta')^2$. This will provide the canonical basis element for certain rings that we now define.

Let $[\alpha, \beta] = \alpha\mathbb{Z} + \beta\mathbb{Z}$ be a $\mathbb{Z}$-module. Then

$$\mathcal{O}_\Delta = [1, \omega_\Delta],$$

Received by the editors April 15, 1998; revised October 1, 1998.
AMS subject classification: Primary: 11R11; secondary: 11D09, 11R29, 11R65.

is an *order* in $K = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{D_0})$ with conductor f_Δ. If $f_\Delta = 1$, then $\mathcal{O}_\Delta$ is called the *maximal order in* K.

Now we bring ideal theory into the picture. Let $I = [a, b + c\omega_\Delta]$, with $a > 0$. The following tells us when such a module is an ideal (see [4, Exercise 1.2.1(a), p. 12]).

Proposition 1.1 **(Ideal Criterion)** *Let Δ be a discriminant, and let $I \neq (0)$ be a $\mathbb{Z}$-submodule of $\mathcal{O}_\Delta$. Then I has a representation of the form*

$$I = [a, b + c\omega_\Delta],$$

where $a, c \in \mathbb{N}$ and $b \in \mathbb{Z}$ with $0 \leq b < a$. Furthermore, I is an ideal of $\mathcal{O}_\Delta$ if and only if this representation satisfies $c \mid a$, $c \mid b$, and $ac \mid N(b + c\omega_\Delta)$. (For convenience, we call I an $\mathcal{O}_\Delta$-ideal.) If $c = 1$, then I is called primitive*, and I has a canonical representation as*

$$I = [a, (b + \sqrt{\Delta})/2],$$

with $-a \leq b < a$.

If $I = [a, b + \omega_\Delta]$ is a primitive $\mathcal{O}_\Delta$-ideal, then a is the least positive rational integer in I, denoted $N(I) = a$ called the *norm of* I.

An $\mathcal{O}_\Delta$-ideal I is called *reduced* if there does *not* exist any element $\alpha \in I$ such that both $|\alpha| < N(I)$ and $|\alpha'| < N(I)$, where α' denotes the *algebraic conjugate* of $\alpha \in \mathcal{O}_\Delta$, namely if $\alpha = (x + y\sqrt{\Delta})/2$, then $\alpha' = (x - y\sqrt{\Delta})/2$. On the other hand, the conjugate of the ideal I is $I' = [a, b + \omega'_\Delta]$.

It is convenient to have easily verified conditions for reduction (see [4, Corollaries 1.4.2–1.4.4, p. 19]).

Theorem 1.1 *Suppose that $\Delta > 0$ is a discriminant and $I = [a, b + \omega_\Delta]$ is an $\mathcal{O}_\Delta$-ideal. Then each of the following hold.*

1. *If $N(I) < \sqrt{\Delta}/2$, then I is reduced.*
2. *If I is reduced, then $N(I) < \sqrt{\Delta}$.*
3. *If $0 \leq b < a < \sqrt{\Delta}$ and $a > \sqrt{\Delta}/2$, then I is reduced if and only if*

$$a - \omega_\Delta < b < -\omega'_\Delta.$$

Now we give an elucidation of the theory of continued fractions as it pertains to the above. Continued fraction expansions will be denoted by

$$\langle a_0; a_1, a_2, \ldots, a_l, \ldots \rangle,$$

where $a_i \in \mathbb{R}$ are called the *partial quotients* of the continued fraction expansion. If $a_i \in \mathbb{Z}$, and $a_i > 0$ for all $i > 0$, then the continued fraction is called an *infinite simple continued fraction* (which is equivalent to being an irrational number), whereas if the expression terminates, then it is called a *finite simple continued fraction* (which is equivalent to being a rational number).

We will be discussing *quadratic irrationals* which are real numbers γ associated with a radicand D such that γ can be written in the form

$$\gamma = (P + \sqrt{D})/Q,$$

where $P, Q, D \in \mathbb{Z}$, $D > 0$, $Q \neq 0$, and $P^2 \equiv D \pmod{Q}$. The following is a setup for our discussion of the continued fraction algorithm.

Suppose that $I = [a, b + \omega_\Delta]$ is a primitive ideal in $\mathcal{O}_\Delta$, then we define the following for the quadratic irrational $\gamma = (b + \omega_\Delta)/a$ (where g and h are defined above):

$$(P_0, Q_0) = \Big(\big(\sigma_0 b + f_\Delta(\sigma_0 - 1) + h\sigma_0\big)/g, a\sigma_0/g\Big), \tag{1.1}$$

and (for $i \geq 0$),

$$D = P_{i+1}^2 + Q_i Q_{i+1}, \tag{1.2}$$

$$P_{i+1} = a_i Q_i - P_i, \tag{1.3}$$

and

$$a_i = \lfloor (P_i + \sqrt{D})/Q_i \rfloor, \tag{1.4}$$

where $\lfloor x \rfloor$ is the greatest integer less than or equal to x, *i.e.*, the *floor* of x. Therefore, $\gamma = \langle a_0; a_1, \dots, a_i, \dots \rangle$ is the simple continued fraction expansion of γ.

Remark 1.1 The *simple* continued fraction expansion of a quadratic irrational γ is called *purely periodic* provided that there is an integer $l \in \mathbb{N}$ such that $\gamma = \langle a_0; \overline{a_1, a_2, \dots, a_l} \rangle = \langle \overline{a_0; a_1, a_2, \dots, a_{l-1}} \rangle$. The value $l = l(\gamma)$ is called the *period length* of the simple continued fraction expansion of γ. Furthermore, quadratic irrationals are purely periodic if and only if they are *reduced*, *i.e.*, a quadratic irrational γ is purely periodic if and only if $\gamma > 1$ and $-1 < \gamma' < 0$.

In what follows we need the notion of equivalence of ideals. Two ideals I and J of $\mathcal{O}_\Delta$ are *equivalent* (denoted by $I \sim J$) if there exist non-zero $\alpha, \beta \in \mathcal{O}_\Delta$ such that $(\alpha)I = (\beta)J$ (where (x) denotes the principal ideal generated by x). For a discriminant Δ, the *class group* of $\mathcal{O}_\Delta$ determined by these equivalence classes is denoted by $\mathcal{C}_\Delta$, with order h_Δ, the *class number* of $\mathcal{O}_\Delta$.

In the next section the methods of proof require results on the following well-known pair of sequences. For a quadratic irrational $\gamma = \langle a_0; a_1, \dots \rangle$, define two sequences of integers $\{A_i\}$ and $\{B_i\}$ inductively by:

$$A_{-2} = 0,\ A_{-1} = 1,\ A_i = a_i A_{i-1} + A_{i-2} \quad (\text{for } i \geq 0), \tag{1.5}$$

$$B_{-2} = 1,\ B_{-1} = 0,\ B_i = a_i B_{i-1} + B_{i-2} \quad (\text{for } i \geq 0). \tag{1.6}$$

The first result for these sequences comes from [4, Exercise 2.1.2(c), p. 54],

$$A_k B_{k-1} - A_{k-1} B_k = (-1)^{k-1}, \tag{1.7}$$

https://doi.org/10.4153/CMB-2000-029-8 Published online by Cambridge University Press

for any $k \in \mathbb{N}$.

If $\gamma = \sqrt{D}$, and $\ell = \ell(\sqrt{D})$, where $D > 0$ is a radicand, then by [4, Exercise 2.1.2(g)(iv), p. 55],

$$A_{k-1}^2 - B_{k-1}^2 D = (-1)^k Q_k. \tag{1.8}$$

There is also another useful fact that we will exploit in the next section.

Theorem 1.2 *Suppose that $D > 0$ is a radicand, and $\ell(\sqrt{D}) = \ell$ with the Q_j defined for the simple continued fraction expansion of $\sqrt{D}$ as in Equations* (1.1)–(1.4). *Then $Q_j \mid 2D$ with $Q_j > 1$ if and only if $j = \ell/2$. Furthermore, if D is even, then $Q_j \mid D$ with $Q_j > 1$ if and only if $j = \ell/2$. In either case, $a_{\ell/2} = 2P_{\ell/2}/Q_{\ell/2}$. Furthermore, if I is a principal, reduced $\mathcal{O}_\Delta$-ideal, then $N(I) = Q_k$ for some natural number $k \leq \ell$.*

Proof See [4, Theorem 6.1.4, p. 193], and [4, Theorem 2.1.2, pp. 44–47]. ■

2 Results

In this section, we generalize some notions developed in [3], which in turn generalized the results in [1]–[2], and [6]. In particular, the main feature that underlies the results of [3] is generalized in the following.

Theorem 2.1 *Suppose that $\Delta = 4D$ is a discriminant with associated odd radicand D, $I \sim 1$ is a primitive $\mathcal{O}_\Delta$-ideal with $1 < N(I) < \sqrt{\Delta}$, and $N(I) \mid \Delta$. If $D = ab$ for some $a, b \in \mathbb{N}$, with $ac < b$, then the Diophantine equation*

$$|ax^2 - by^2| = c, \tag{2.1}$$

where $c \in \{1, 2, 4\}$, has a solution $x, y \in \mathbb{Z}$ with $\gcd(x, y) = 1$ if and only if $ac = N(I) = Q_{\frac{1}{2}\ell}$ for $c = 1, 2$, and $4a = N(I) = Q_f$ where f is roughly a sixth of the way along the period in the simple continued fraction expansion of $\sqrt{D}$ (see Example 2.2 following Theorem 2.3).

Proof Suppose that Equation (2.1) has a solution $x, y \in \mathbb{Z}$. Since $ac < b$, then $a < \sqrt{\Delta}$. Set

$$\alpha = ax + y\sqrt{D}.$$

Then $\alpha \in \mathcal{O}_\Delta$, and

$$|N(\alpha)| = |a^2x^2 - y^2 D| = a|ax^2 - by^2| = ac.$$

Therefore, the $\mathcal{O}_D$-ideal $I = (\alpha)$ is principal and primitive, since $\gcd(ax, y) = \gcd(x, y) = 1$, given that D is odd. Also, $|N(I)| = ac$ divides Δ. By Theorems 1.1–1.2, $ac = Q_{\ell/2} = N(I)$, if $c = 1, 2$, and $N(I) = 4a = Q_f$ for some $f < \ell$.

Conversely, suppose that I is a primitive ideal with $ac = N(I) = Q_k \mid \Delta$, where $k = \ell/2$ if $c = 1, 2$, and $k = f$ if $c = 4$. Then $I = (\alpha)$ is principal, so there are $z, y \in \mathbb{Z}$ with $\gcd(z, y) = 1$ such that $\alpha = z + y\sqrt{D}$, and $N(\alpha) = \pm ac$. Therefore, $z^2 - y^2 D = \pm ac$, so

$$|a(z/a)^2 - by^2| = |ax^2 - by^2| = c,$$

with $\gcd(x, y) = 1$, as required. ■

https://doi.org/10.4153/CMB-2000-029-8 Published online by Cambridge University Press

Theorem 2.2 *Suppose that* $\Delta = 4D$ *is a discriminant with radicand* $D = ab$, *with* $b \equiv 3 \pmod 4$, $a, b \in \mathbb{N}$. *Then* $\ell(\sqrt{D}) = \ell$ *is even. Furthermore, if* $2a = Q_{\frac{1}{2}\ell}$ *in the simple continued fraction expansion of* $\sqrt{D}$, *then the following Jacobi symbol equality holds:*

$$\left(\frac{2a}{b}\right) = (-1)^{\frac{1}{2}\ell}.$$

Proof By Equation (1.8),

$$A_{\ell-1}^2 - B_{\ell-1}^2 D = (-1)^{\ell}.$$

If ℓ is odd, then $A_{\ell-1}^2 \equiv -1 \pmod b$, a contradiction since $b \equiv 3 \pmod 4$. Thus, ℓ is even. From Equation (1.8) again,

$$A_{\ell/2-1}^2 - DB_{\ell/2-1}^2 = (-1)^{\ell/2} Q_{\ell/2}. \tag{2.2}$$

Now we show that $Q_{\ell/2} \mid A_{\ell/2-1}$. By Equation (2.2), $Q_{\ell/2} \mid A_{\ell/2-1}A_{\ell/2-2}$, since $Q_{\ell/2} = a \mid D$. However, by Equation (2.2) any prime that divides $Q_{\ell/2}$ must divide $A_{\ell/2-1}$, so by Equation (1.7), $Q_{\ell/2} \mid A_{\ell/2-1}$. By setting $x = A_{\ell/2-1}/a$ and $y = B_{\ell/2-1}$, we get

$$ax^2 - by^2 = (-1)^{\ell/2}. \tag{2.3}$$

Hence,

$$\left(\frac{a}{b}\right) = \left(\frac{ax^2}{b}\right) = \left(\frac{ax^2 - by^2}{b}\right) = \left(\frac{(-1)^{\ell/2}}{b}\right) = \left(\frac{-1}{b}\right)^{\ell/2} = (-1)^{\ell/2},$$

where the last equality follows from the fact that $b \equiv 3 \pmod 4$. ■

Example 2.1 Let $D = 1891 = 31 \cdot 61 = a \cdot b$. Then $\ell = 36$, and $Q_{\ell/2} = 2 \cdot a = 62$, and $(\frac{-1}{b}) = (\frac{-1}{61})^{\ell/2} = 1$.

Theorem 2.3 *Let* $\Delta = 4ab$ *be a discriminant with associated odd radicand* $D = ab$. *Then if*

$$ax^2 - by^2 = \pm 4 \tag{2.4}$$

has a solution $x, y \in \mathbb{Z}$ *with* $\gcd(x, y) = 1$,

$$aX^2 - bY^2 = \pm 1 \tag{2.5}$$

also has a solution $X, Y \in \mathbb{Z}$, *with* $\gcd(X, Y) = 1$. *Moreover, if Equation* (2.4) *has a solution, and* $4a < b$, *then* $Q_f = 4a$ *for some natural number* $f < \ell/2$ *where* ℓ *is the period length of the simple continued fraction expansion of* $\sqrt{D}$. *If Equation* (2.5) *has a solution, and* $a < b$, *then* $Q_{\frac{1}{2}\ell} = a$. *Hence,*

$$\left(\frac{-1}{b}\right)^f = \left(\frac{a}{b}\right) = \left(\frac{-1}{b}\right)^{\frac{1}{2}\ell}.$$

https://doi.org/10.4153/CMB-2000-029-8 Published online by Cambridge University Press

Proof Assume that Equation (2.4) has a solution in integers x, y. Set

$$X = \frac{(ax^2 \mp 3)x}{2}, \quad \text{and} \quad Y = \frac{(ax^2 \mp 1)y}{2}.$$

Claim 2.1

$$aX^2 - bY^2 = \pm 1.$$

Let $z = ax$. Then

$$(z^2 - Dy^2)^3 = \big(z(z^2 + 3Dy^2)\big)^2 - D\big(y(3z^2 + Dy^2)\big)^2 = \pm 64a^3.$$

But

$$z(z^2 + 3Dy^2) = z\big(4z^2 - 3(z^2 - Dy^2)\big) = z(4z^2 \mp 12a) = 8a^2X.$$

Thus,

$$y(3z^2 + Dy^2) = y\big(4z^2 - (z^2 - Dy^2)\big) = y(4z^2 \mp 4a) = 8aY.$$

In other words,

$$64a^4X^2 - 64a^2DY^2 = \pm 64a^3,$$

which implies that

$$aX^2 - bY^2 = \pm 1,$$

which is Claim 2.1.

Since $\gcd(x, y) = 1$, then it follows that $\gcd(X, Y) = 1$.

If Equation (2.4) is solvable, then $(ax)^2 - Dy^2 = \pm 4a$. Since $4a < b$, then the primitive, principal ideal $(ax + y\sqrt{D})$ is reduced, since its norm is less than $\sqrt{\Delta}/2$. Hence, by Theorem 1.2, $Q_f = 4a$ for some $f \in \mathbb{N}$ with $f < \ell$. Hence,

$$A_{f-1}^2 - B_{f-1}^2 D = (-1)^f 4a.$$

Therefore, $a \mid A_{f-1}$ so by setting $z = A_{f-1}/a$ and $w = B_{f-1}$, we get

$$az^2 - bw^2 = (-1)^f 4.$$

Thus,

$$\left(\frac{a}{b}\right) = \left(\frac{(-1)^f 4}{b}\right) = \left(\frac{-1}{b}\right)^f.$$

On the other hand, as in [3], if Equation (2.5) is solvable, then

$$\left(\frac{a}{b}\right) = \left(\frac{-1}{b}\right)^{\frac{1}{2}\ell}.$$

Hence,

$$\left(\frac{-1}{b}\right)^{\frac{1}{2}\ell} = \left(\frac{-1}{b}\right)^f,$$

so f and $\frac{1}{2}\ell$ have the same parity. ∎

https://doi.org/10.4153/CMB-2000-029-8 Published online by Cambridge University Press

Example 2.2 Let $\Delta = 4 \cdot 805 = 2^2 \cdot 5 \cdot 7 \cdot 23$. Then

$$5x^2 - 161y^2 = -4,$$

has the solution $x = 17$ and $y = 3$. Here $a = 5$, and $b = 161$ with $\ell = 18$, and

$$Q_{\frac{1}{2}\ell} = a = 5 = Q_9, \quad Q_f = 4a = 20 = Q_3,$$

where $f = \frac{1}{6}\ell$, as predicted in Theorem 2.1. Also, we observe that $Q_6 = 4$, and Q_6 is *roughly* (see Remark 2.1 following this example) a third of the way along the period. It is necessarily the case that when we encounter $Q_k = 4$, then we are a "third" of the way along the period and this signals the fundamental unit of the maximal order. To see this, note that by Equation (1.8),

$$A_5^2 - B_5^2 \cdot 805 = 1447^2 - 51^2 \cdot 805 = 4 = Q_6,$$

and indeed

$$(1447 + 51\sqrt{805})/2$$

is the fundamental unit of $\mathbb{Z}[(1 + \sqrt{805})/2]$. Furthermore,

$$\left(\frac{-1}{b}\right)^f = \left(\frac{-1}{161}\right)^3 = 1 = \left(\frac{a}{b}\right) = \left(\frac{5}{161}\right) = \left(\frac{-1}{b}\right)^{\frac{1}{2}\ell} = \left(\frac{-1}{b}\right)^9.$$

Remark 2.1 Unfortunately Example 2.2 gives us *exactly* a sixth of the way along for Q_f. However, in general this is not the case, at least in terms of ℓ. What we mean specifically is the following. The ideal $[Q_6, P_6 + \sqrt{D}] = [4, 25 + \sqrt{805}]$, when cubed, becomes $[1, \sqrt{D}]$, namely $[4, 25 + \sqrt{805}]^3 = (8)[1, \sqrt{D}] \sim \mathcal{O}_\Delta$. In a similar spirit, $[Q_f, P_f + \sqrt{D}]^6 = [20, 15 + \sqrt{805}]^6 \sim \mathcal{O}_\Delta$. Similarly, $[Q_{\frac{1}{2}\ell}, P_{\frac{1}{2}\ell} + \sqrt{D}] \sim \mathcal{O}_\Delta$, but unfortunately, for cube or sixth roots, the position of the ideal in the cycle is a little more blurred. Namely it may not sit *exactly* in the one-sixth or one-third position in terms of ℓ, but nonetheless sits at a third or a sixth in terms of raising it to a power as just described. Also, our paper [5] describes the notion of "halfway" along the period in a similar "blurred" fashion.

Remark 2.2 The interested reader will note that $Q_j = 4$ for some natural number $j < \ell$ in the simple continued fraction expansion of $\sqrt{D_0}$ for a fundamental radicand $D_0 \equiv 1 \pmod 4$ if and only if the ideal $I = [4, 1 + \sqrt{D_0}]$ is principal in $\mathcal{O}_\Delta$ where $\Delta = 4D_0$ (see [4, Exercise 2.1.16, p. 61]). In turn, the principality of I is tantamount to the solvability of Equation (2.1) with $c = 4$, and $D_0 = ab$. This is related to a problem of Eisenstein, who looked for a criterion for the solvability of the aforementioned equation when $N(\varepsilon_{D_0}) = -1$ and $D_0 \equiv 5 \pmod 8$, where ε_{D_0} is the fundamental unit of $\mathcal{O}_{D_0} = [1, (1 + \sqrt{D_0})/2]$. Equation (2.1) is known to be solvable for $c = 4$, and $ab = D_0 \equiv 5 \pmod 8$ if and only if ε_{D_0} is *not* in $\mathbb{Z}[\sqrt{D_0}] = \mathcal{O}_{4D_0} = \mathcal{O}_\Delta$, which is the *non*-maximal order in the maximal order $\mathcal{O}_{D_0}$, which is the ring of integers of $\mathbb{Q}(\sqrt{D_0})$. For further information see [4, Exercises 2.1.14–2.1.16].

Acknowledgments The second author's research is supported, in part, by a grant from the Australian Research Council, and the first author's research is supported by NSERC Canada grant #A8484.

References

[1] P. Chowla and S. Chowla, *Problems on periodic simple continued fractions*. Proc. Nat. Acad. Sci. U.S.A. **69**(1972), 37–45.

[2] C. Friesen, *Legendre symbols and continued fractions*. Acta Arith. **LIX**(1991), 365–379.

[3] R. A. Mollin, *Jacobi symbols, ambiguous ideals, and continued fractions*. Acta Arith. (4) **LXXXV**(1998), 331–349.

[4] ———, *Quadratics*. CRC Press, Boca Raton-New York-London, 1996.

[5] R. A. Mollin, A. J. van der Poorten, and H. C. Williams, *Halfway to a solution of* $x^2 - Dy^2 = -3$. J. Théorie Nombres, Bordeaux **6**(1994), 421–459.

[6] A. Schinzel, *On two conjectures of P. Chowla and S. Chowla concerning continued fractions*, Ann. Mat. Appl. **98**(1974), 111–117.

Mathematics Department
University of Calgary
Calgary, Alberta
T2N 1N4
website: http://www.math.ucalgary.ca/˜ramollin/
e-mail: ramollin@math.ucalgary.ca

School of MPCE
Macquarie University Sydney
Sydney, N.S.W. 2109
Australia
website: http://www.mpce.mq.edu.au/alf
e-mail: alf@mpce.mq.edu.au