ACTA ARITHMETICA
LXXXV.4 (1998)

Jacobi symbols, ambiguous ideals, and continued fractions

by

R. A. Mollin (Calgary, Alta.)

The purpose of this paper is to generalize some seminal results in the literature concerning the interrelationships between Legendre symbols and continued fractions. We introduce the power of ideal theory into the arena. This allows significant improvements over the existing results via the infrastructure of real quadratic fields.

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

$$\omega_0 = (\sigma_0 - 1 + \sqrt{D_0})/\sigma_0 \quad \text{and} \quad \Delta_0 = (\omega_0 - \omega_0')^2 = 4D_0/\sigma_0^2,$$

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.

1991 *Mathematics Subject Classification*: Primary 11R11; Secondary 11D09, 11R29, 11R65.

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

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

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 $0\le b<a$. 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 $-a\le b<a$.

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

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

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

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):

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

and (for $i \geq 0$),

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

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

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

where $\lfloor x \rfloor$ is the greatest integer less than or equal to x, i.e. the *floor* of x. Therefore, $\gamma = \langle a_0; a_1, \ldots, a_i, \ldots \rangle$ 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 $\gamma = \langle a_0; \overline{a_1, a_2, \ldots, a_l} \rangle = \langle \overline{a_0; a_1, a_2, \ldots, a_{l-1}} \rangle$. 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 $\mathcal{O}_\Delta$. The following is fundamental to the discussion (see [4, Theorem 2.1.2, pp. 44–47]). The following relationship between the ideals and continued fractions was dubbed the *infrastructure* of a real quadratic field by Dan Shanks.

Theorem 1.2 (The Continued Fraction Algorithm). *Let $\Delta > 0$ be a discriminant, and let $I = I_1 = [a, b + \omega_\Delta]$ be a primitive ideal in the order $\mathcal{O}_\Delta$. Set $P = P_0$ and $Q = Q_0$, as defined in* (1.1), *and let P_i and Q_i for $i > 0$ be defined by* (1.2)–(1.4) *in the simple continued fraction expansion of*

$\gamma = \gamma_0 = (P + \sqrt{D})/Q$. If $I_i = [Q_{i-1}/\sigma, (P_{i-1} + \sqrt{D})/\sigma]$, then $I_1 \sim I_i$ for all $i \geq 1$. Also, there exists a least value $m \geq 1$ such that I_{m+i} is reduced for all $i \geq 0$.

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

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

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

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

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

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

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

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

Also, if we define the *alternating sum* for $\sqrt{D}$ as

$$\Sigma = \sum_{j=1}^{l} (-1)^{l-j} a_j,$$

then by [3, (3.3), p. 369], if l is even,

$$\begin{aligned} \Sigma \equiv l + 2 + a_{l/2} + 2B_{l/2-2} + 2B_{l/2-1} + 2A_{l/2-2} \\ + 2A_{l/2-1} + 2A_{l/2-1}B_{l/2-2} \pmod 4, \end{aligned} \tag{1.9}$$

and by [3, (4.1), p. 370],

$$(-1)^{l/2} a_{l/2} Q_{l/2} + 2(A_{l/2-1}A_{l/2-2} - DB_{l/2-1}B_{l/2-2}) = 0. \tag{1.10}$$

If $l(\sqrt{D}) = l$ is odd, then by [4, Exercise 2.1.13(a), p. 58], $a_j = a_{l-j}$ whenever $1 \leq j < l$. Thus, in this case

$$\Sigma = 2a_0. \tag{1.11}$$

The reader is cautioned that our notation is in conflict with that of Friesen [3]. Our notation is consistent with that of [4].

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

Theorem 1.3. *Suppose that $D > 0$ is a radicand, and $l(\sqrt{D}) = l$ with the Q_j defined for the simple continued fraction expansion of $\sqrt{D}$ as in* (1.1)–(1.4). *Then $Q_j \mid 2D$ with $Q_j > 1$ if and only if $j = l/2$. Furthermore, if D is even, then $Q_j \mid D$ with $Q_j > 1$ if and only if $j = l/2$. In either case, $a_{l/2} = 2P_{l/2}/Q_{l/2}$.*

Proof. See [4, Theorem 6.1.4, p. 193]. ■

REMARK 1.2. Theorem 1.3 is applicable to a special set of ideals, which will be the dominant candidates of study in the sequel. If I is an $\mathcal{O}_\Delta$-ideal such that $I = I'$, then I is called *ambiguous.* Ambiguous ideals are necessarily divisors of Δ, and so are of order 1 or 2 in $\mathcal{C}_\Delta$ (see [4, Exercise 1.2.5, p. 13]). Since Theorem 1.2 tells us that the Q_j are the norms of all the principal reduced $\mathcal{O}_\Delta$-ideals via the simple continued fraction expansion of $\sqrt{D}$, Theorem 1.3 tells us that there is a principal reduced ideal of norm $Q_{l/2}$ in the simple continued fraction expansion of $\sqrt{D}$. Observe as well the important fact that since we are going to be considering only simple continued fraction expansions of $\sqrt{D}$ in the sequel, it follows that $\Delta = 4D$, even when $D \equiv 1 \pmod 4$. In the latter case we are not in the maximal order. In any case, $\sigma = 1$ henceforth.

Finally, there is a classical result due to Gauss that we will need, so we present it here for the convenience of the reader. First, we need to define the following concepts. The elementary abelian 2-subgroup of $\mathcal{O}_\Delta$ is denoted by $\mathcal{C}_{\Delta,2}$ with order $h_{\Delta,2}$.

THEOREM 1.4. *If Δ is a fundamental discriminant divisible by exactly $n \in \mathbb{N}$ distinct primes, then the following each hold.*

1. *$\mathcal{C}_{\Delta,2}$ has order $h_{\Delta,2} = 2^{t_\Delta}$, where $t_\Delta = n - 2$ if $\Delta > 0$ and there is a prime $p \mid \Delta$ with $p \equiv 3 \pmod 4$, and $t_\Delta = n - 1$ otherwise.*
2. *If $\Delta > 0$ is divisible by a prime $p \equiv 3 \pmod 4$, then $\mathcal{C}_{\Delta,2}$ is generated by classes represented by ambiguous ideals.*

Proof. For part 1, see [4, Theorem 1.3.3, p. 16], and for part 2 see [4, Exercise 1.3.7(d), p. 19]. ■

2. Results. At the beginning of [3, Section 7, p. 377], Friesen states: "The cases considered in this paper, namely where N is the product of two distinct primes or where N is twice such a product, are, in some sense, both the most general cases and also the simplest ones, for which we can hope to arrive at relationships between the Legendre symbols, the alternating sum, Σ, and the period of the continued fraction expansion of $\sqrt{N}$. One can expect more complications (and many more separate cases to examine) when N has 3 or more odd prime factors." In this section, we show that this view is not entirely correct when viewed from the perspective of ideal theory. We show that there can be an *unbounded* number of prime factors in the discriminant if the analogous situation to the simple cases covered in [1], [3], and [5] is assumed (see Corollaries 2.1 and 2.4 below). Furthermore, we need not even restrict attention to fundamental discriminants. For instance, our first result generalizes one of the main results of [3] by exploiting some classical ideal-theoretic facts seemingly overlooked by the aforementioned authors.

Theorem 2.1. *Suppose that $\Delta = 4D$ is a discriminant with radicand $D = ab \equiv 1 \pmod 4$, with $a \equiv 3 \pmod 4$, $a, b \in \mathbb{N}$. Then $l(\sqrt{D}) = l$ is even. Furthermore, if $a = Q_{l/2}$ in the simple continued fraction expansion of $\sqrt{D}$, then the following Jacobi symbol equalities hold*:

$$\left(\frac{a}{b}\right) = (-1)^{l/2} \quad \textit{and} \quad \left(\frac{b}{a}\right) = (-1)^{l/2+1}.$$

Proof. By (1.8),

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

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

$$A_{l/2-1}^2 - DB_{l/2-1}^2 = (-1)^{l/2} Q_{l/2}. \tag{2.12}$$

Now we show that $Q_{l/2} \mid A_{l/2-1}$. By (1.10), $Q_{l/2} \mid A_{l/2-1}A_{l/2-2}$, since $Q_{l/2} = a \mid D$. However, by (2.12) any prime that divides $Q_{l/2}$ must divide $A_{l/2-1}$, so by (1.7), $Q_{l/2} \mid A_{l/2-1}$. By setting $x = A_{l/2-1}/a$ and $y = B_{l/2-1}$, we get

$$ax^2 - by^2 = (-1)^{l/2}. \tag{2.13}$$

Hence,

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

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

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

where the last equality follows since $a \equiv 3 \pmod 4$. ■

Remark 2.1. The reader may wonder why we did not need to assume that $\gcd(a, b) = 1$ in the hypothesis of Theorem 2.1. However, the condition $a = Q_{l/2}$ is strong enough to ensure that this is the case. To see this we merely look at (2.13) in the above proof.

Remark 2.2. The hypothesis of Theorem 2.1 (and that of Theorem 2.2 below) relies upon the fact that we are assuming the existence of a principal ideal I with $1 < N(I) < \sqrt{D}$. By Theorem 1.1, this means that I is reduced, so by the continued fraction algorithm, Theorem 1.2, $N(I) = Q_j$ for some natural number j with $1 < j < l$ in the simple continued fraction expansion of $\sqrt{D}$. However, if $N(I) \mid 2D$, then by Theorem 1.3, we must have $N(I) = Q_{l/2}$, since there is exactly one non-trivial reduced ideal in the principal class of $\mathcal{C}_\Delta$ by Theorem 1.3. This is what underlies the following result, which Theorem 2.1 generalizes.

Corollary 2.1 (Friesen [3, Theorem 2, p. 372]). *If* $D = pq$, $p \equiv q \equiv 3 \pmod 4$, $p < q$ *primes*, *then the following Legendre symbol equalities hold*:

$$\left(\frac{p}{q}\right) = (-1)^{l/2} \quad \textit{and} \quad \left(\frac{q}{p}\right) = (-1)^{l/2+1}.$$

Proof. By part 1 of Theorem 1.4, $\mathcal{C}_{\Delta,2} = 1$, since $t_\Delta = 0 = n - 2$ therein. In other words, h_Δ is odd. Hence, the $\mathcal{O}_\Delta$-ideal $\mathcal{P}$ above p must be principal, given that it is an ambiguous ideal (see Remark 1.2). Since $p < q$ forces $p < \sqrt{D} = \sqrt{\Delta}/2$, it follows from Theorem 1.1 that $\mathcal{P}$ is reduced. Therefore, we may invoke Theorems 1.2–1.3 to conclude that $p = Q_{l/2}$, since $\mathcal{P} \sim 1$. Hence, the hypothesis of Theorem 2.1 holds, and the result follows. ∎

Example 2.1. If $D = 3 \cdot 11 = 33$, then $\sqrt{D} = \langle 5; \overline{1, 2, 1, 10}\rangle$, $l = 4$,

$$\left(\frac{3}{11}\right) = 1 = \left(\frac{-1}{11}\right)^{l/2} \quad \text{and} \quad \left(\frac{11}{3}\right) = -1 = \left(\frac{-1}{11}\right)^{l/2+1}.$$

For an example of a non-fundamental radicand, we have the following.

Example 2.2. Let $D = 3549 = 3 \cdot 7 \cdot 13^2 = ab = 3 \cdot 1183$. Then

$$\sqrt{D} = \langle 59; \overline{1, 1, 2, 1, 9, 4, 1, 1, 1, 29, 6, 1, 38, 1, 6, 29, 1, 1, 1, 4, 9, 1, 2, 1, 1, 118}\rangle,$$

so $l = 26$, and $Q_{l/2} = Q_{13} = 3$. Therefore,

$$\left(\frac{a}{b}\right) = \left(\frac{3}{1183}\right) = -1 = (-1)^{l/2},$$
$$\left(\frac{b}{a}\right) = \left(\frac{1183}{3}\right) = 1 = (-1)^{l/2+1}.$$

The hypothesis of Theorem 2.1 may seem difficult to check in general. However, we can cite entire classes of radicands which, by their very nature, must satisfy the criterion. For instance, we have the following.

Corollary 2.2. *Suppose that D satisfies the first statement of Theorem 2.1. Suppose further that*

$$D = (at)^2 - a \qquad \textit{for some } t \in \mathbb{N},\ t > 1.$$

Then the following Jacobi symbol equalities hold:

$$\left(\frac{a}{b}\right) = (-1)^{l/2} \quad \textit{and} \quad \left(\frac{b}{a}\right) = (-1)^{l/2+1}.$$

Proof. We have the $\mathcal{O}_D$-ideal

$$\mathcal{A} = [a, at + \sqrt{D}] = (at + \sqrt{D}) \sim 1$$

since $N(I) = (at)^2 - D = a$. Also, since $t > 1$, we have $a < \sqrt{D}$. Therefore, by the continued fraction algorithm Theorem 1.2, $a = Q_{l/2}$. The result now follows from Theorem 2.1. ∎

Radicands of the type in Corollary 2.2 are examples of *Extended Richaud–Degert* (*ERD*) *types*, which have been extensively studied. See [4, pp. 77 ff] for complete details.

EXAMPLE 2.3. Let $D = 210^2 - 15 = 44085 = ab = 15 \cdot 2939$. Then

$$\sqrt{D} = \langle 209; \overline{1, 26, 1, 418} \rangle,$$

so $l = 4$,

$$\begin{aligned} \left(\frac{a}{b}\right) &= \left(\frac{15}{2939}\right) = 1 = (-1)^{l/2}, \\ \left(\frac{b}{a}\right) &= \left(\frac{2939}{15}\right) = -1 = (-1)^{l/2+1}. \end{aligned}$$

Other ERD-types fit into the pattern as well.

COROLLARY 2.3. *Let D satisfy the first statement of Theorem* 2.1. *Furthermore*, *assume that*

$$D = (at)^2 \pm 4a \qquad \textit{for some } t \in \mathbb{N}.$$

Then the following Jacobi symbol equalities hold:

$$\left(\frac{a}{b}\right) = (-1)^{l/2} \quad \textit{and} \quad \left(\frac{b}{a}\right) = (-1)^{l/2+1}.$$

Proof. The ideal $[4a, at + \sqrt{D}]$ is principal in $\mathcal{O}_{4D}$ since $|N(at + \sqrt{D})| = 4a$. However, by [4, Exercise 1.5.3(a), p. 28],

$$[4a, at + \sqrt{D}] = [a, at + \sqrt{D}][4, at + \sqrt{D}],$$

and $[4, at + \sqrt{D}] \sim 1$, since $[4, at + \sqrt{D}] = [2, at + \sqrt{D}]^2 \sim 1$, given that $[2, at + \sqrt{D}]$ is an ambiguous $\mathcal{O}_{4D}$-ideal. Hence, $[a, at + \sqrt{D}] \sim 1$. Since $a < \sqrt{D}$, by the continued fraction algorithm we have $Q_{l/2} = a$, so the result follows from Theorem 2.1. ∎

EXAMPLE 2.4. Let $D = 182301 = 427^2 - 28 = 3 \cdot 7 \cdot 8681 = ab = 7 \cdot 26043$. Then

$$\sqrt{D} = \langle 426; \overline{1, 29, 2, 212, 1, 120, 1, 212, 2, 29, 1, 852} \rangle,$$

so $l = 12$. Therefore,

$$\begin{aligned} \left(\frac{a}{b}\right) &= \left(\frac{7}{26043}\right) = 1 = (-1)^{l/2}, \\ \left(\frac{b}{a}\right) &= \left(\frac{26043}{7}\right) = -1 = (-1)^{l/2+1}. \end{aligned}$$

However, if the hypothesis of Theorem 2.1 is violated, then the conclusion cannot be guaranteed.

Example 2.5. Let $D = 210^2+15 = 44115 = 3\cdot5\cdot17\cdot173 = ab = 15\cdot2941$. We have $\langle 210; \overline{28, 420}\rangle$, so $l = 2$, and $Q_{l/2} = Q_1 = 15$. However,

$$\left(\frac{15}{2941}\right) = 1 \neq (-1)^{l/2} = -1.$$

Here $D \equiv 3 \pmod 4$.

Theorem 2.1 also has a disguised test for principality of ambiguous ideals built into it. It is not always easy to check whether a given ideal is principal without, for example, constructing the continued fraction expansion of $\sqrt{D}$ and sifting through the values of the Q_j's via the continued fraction algorithm. However, all we need to know via Theorem 2.1 is the value of $l(\sqrt{D}) = l$.

Example 2.6. If $D = 3\cdot5\cdot7\cdot13 = 1365$, then

$$\sqrt{D} = \langle 36; \overline{1, 17, 2, 17, 1, 72}\rangle,$$

so $l = 6$. We have

$$\left(\frac{3}{455}\right) = 1 \neq (-1)^{l/2} = -1, \quad \text{hence} \quad \mathcal{P}_3 \not\sim 1, \ \ \mathcal{P}_3 \mid 3.$$

Also,

$$\left(\frac{7}{195}\right) = 1 \neq (-1)^{l/2} = -1, \quad \text{hence} \quad \mathcal{P}_7 \not\sim 1, \ \ \mathcal{P}_7 \mid 7,$$

$$\left(\frac{3\cdot13}{35}\right) = 1 \neq (-1)^{l/2} = -1, \quad \text{hence} \quad \mathcal{P}_3\mathcal{P}_{13} \not\sim 1, \ \ \mathcal{P}_{13}|13,$$

and

$$\left(\frac{7\cdot13}{15}\right) = 1 \neq (-1)^{l/2} = -1, \quad \text{hence} \quad \mathcal{P}_7\mathcal{P}_{13} \not\sim 1.$$

Since $h_D = h_{D,2} = 4$ by part 1 of Theorem 1.4, we cannot have all combinations of $\mathcal{P}_j$ for $j = 3, 7, 13$ non-principal, so the only possibility is that $\mathcal{P}_3\mathcal{P}_7 \sim 1$. Hence, we have shown that

$$\mathcal{C}_D = \langle\mathcal{P}_3\rangle \times \langle\mathcal{P}_{13}\rangle = \langle\mathcal{P}_7\rangle \times \langle\mathcal{P}_{13}\rangle.$$

Example (2.6) shows the power of Theorem 2.1 in determining the elementary abelian 2-group structure via Jacobi symbols.

Thus far, we have considered only radicands $D \equiv 1 \pmod 4$. We now turn to the other case covered in [3].

Theorem 2.2. *Let $D = 2ab \equiv 2 \pmod 4$, $a, b \in \mathbb{N}$, be a radicand where $a \equiv 3 \pmod 4$ and $b \equiv 7 \pmod 8$. Then $l(\sqrt{D}) = l$ is even. If $Q_{l/2} = 2a$, then the following Jacobi symbol equalities hold*:

$$\left(\frac{a}{b}\right) = (-1)^{l/2} \quad \textit{and} \quad \left(\frac{b}{a}\right) = (-1)^{l/2+1}.$$

Proof. This follows in the same fashion as Theorem 2.1. ■

Corollary 2.4 (Friesen [3, Theorem 5, p. 374].) *If* $p \equiv 3 \pmod 8$ *and* $q \equiv 7 \pmod 8$ *are primes and* $D = 2pq$, *then* l *is even and*

$$\left(\frac{p}{q}\right) = \begin{cases} (-1)^{l/2} & \text{if } 2p < q, \\ (-1)^{l/2+1} & \text{if } 2p > q. \end{cases}$$

Proof. As in the proof of Theorem 2.1, l is even, and

$$A_{l/2-1}^2 - DB_{l/2-1}^2 = (-1)^{l/2} Q_{l/2}.$$

Checking this equation modulo 8, one sees that $Q_{l/2} \neq 2, p$. If $2p < q$, then by the continued fraction algorithm and Theorem 1.4, $Q_{l/2} = 2p$, so the result follows from Theorem 2.2. ■

Remark 2.3. If one compares the latter proof with that given in [3, Theorem 5, pp. 374–375], where five separate cases are considered, then the superiority of the infrastructure method becomes evident.

Corollary 2.5. *Suppose that* D *satisfies the first statement of Theorem 2.2. Suppose further that* $D = n^2 \pm r$, *where* $r \mid n$, $r, n \in \mathbb{N}$, *and* $r \equiv 6 \pmod 8$, *where* $n > r$ *if* $D = n^2 - r$. *Then the following Jacobi symbol equalities hold*:

$$\left(\frac{r/2}{D/r}\right) = (-1)^{l/2} \quad \text{and} \quad \left(\frac{D/r}{r/2}\right) = (-1)^{l/2+1}.$$

Proof. This is proved exactly as in the proof of Corollary 2.2. ■

Example 2.7. Let $D = 2 \cdot 3 \cdot 7 = 42 = 6^2 + 6 = n^2 + r$. Then

$$\sqrt{42} = \langle 6; \overline{2, 12} \rangle,$$

so $l = 2$, and

$$\left(\frac{r/2}{D/r}\right) = \left(\frac{3}{7}\right) = -1 = (-1)^{l/2},$$
$$\left(\frac{D/r}{r/2}\right) = \left(\frac{7}{3}\right) = 1 = (-1)^{l/2+1}.$$

In view of Remark 2.2, what is hidden in the above is the following relationship between solvability of Diophantine equations and the principality of certain ideals.

Theorem 2.3. *Suppose that* $\Delta = 4D$ *is a discriminant with associated radicand* D, $I \sim 1$ *is an* $\mathcal{O}_\Delta$*-ideal with* $1 < N(I) < \sqrt{D}$, *and* $N(I) \mid 2D$. *If* $D = ab$ *for some* $a, b \in \mathbb{N}$ *with* $a < b$, *then the Diophantine equation*

$$|ax^2 - by^2| = 1 \tag{2.14}$$

has a solution $x, y \in \mathbb{Z}$ *if and only if* $a = N(I) = Q_{l/2}$ *in the simple continued fraction expansion of* $\sqrt{D}$.

Proof. Suppose that equation (2.14) has a solution $x, y \in \mathbb{Z}$. Since $a < b$, we have $a < \sqrt{D}$. Set

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

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

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

Therefore, the $\mathcal{O}_D$-ideal $I = (\alpha)$ is principal with $|N(I)| = a$ dividing D. By Theorems 1.1–1.3, $a = Q_{l/2} = N(I)$.

Conversely, if $a = N(I) = Q_{l/2} \mid D$, then $I = (\alpha)$ is principal, so there are $x, y \in \mathbb{Z}$ such that $\alpha = x + y\sqrt{D}$, and $N(\alpha) = \pm a$. Therefore, $x^2 - y^2D = \pm a$, so

$$|a(x/a)^2 - by^2| = 1,$$

as required. ■

Remark 2.4. Notice that in the proof of Corollary 2.1, the classical result from ideal theory is basically what underlies the phenomenon explored by the aforementioned authors. The link between the solvability of certain Diophantine equations and the principality of certain related ideals, as displayed in Theorem 2.3, is the backbone of all the arguments presented herein, but not explicitly present in the papers [1]–[3] and [5].

We now turn to a generalization of results from [1]–[3] and [5] involving the alternating sum Σ. First we generalize a result from [3] as a preparatory lemma.

Lemma 2.1. *If $D \equiv 2 \pmod 4$ is a radicand, where $D > 0$, and $l(\sqrt{D}) = l$ is even, then*

$$\Sigma \equiv l + 2 + A_{l/2-1} \pmod 4 \qquad \text{if } Q_{l/2} \text{ is even}, \tag{2.15}$$

and

$$\Sigma \equiv l + 2B_{l/2-1} \pmod 4 \qquad \text{if } Q_{l/2} \text{ is odd.} \tag{2.16}$$

Proof. First assume that $Q_{l/2}$ is even. Since $Q_{l/2} \mid D$ by Theorem 1.3, we have $Q_{l/2} \equiv 2 \pmod 4$. Thus, by (1.8), $A_{l/2-1}$ is even and $B_{l/2-1}$ is odd. By (1.2), $P_{l/2}$ is even, so by Theorem 1.3, $a_{l/2}$ is even. By (1.7), $A_{l/2-2}$ is odd, and by (1.10), $B_{l/2-2}$ is even. Therefore, using (1.10), $a_{l/2} \equiv \pm A_{l/2-1} \pmod 4$. Hence, by putting all of this information into (1.9), we get

$$\Sigma \equiv l + 2 \pm A_{l/2-1} + 2B_{l/2-1} + 2A_{l/2-2} \equiv l \pm A_{l/2-1} + 2 \pmod 4,$$

and since $l \equiv -l \pmod 4$ and $-2 \equiv 2 \pmod 4$, we obtain

$$\Sigma \equiv l + A_{l/2-1} + 2 \pmod 4,$$

as required.

Now we assume that $Q_{l/2}$ is odd. Thus, by (1.8), $A_{l/2-1}$ is odd, and by Theorem 1.3, $a_{l/2}$ is even. Therefore, by (1.10),

$$a_{l/2}+2A_{l/2-2}\equiv 0 \pmod 4.$$

Hence, from (1.9),

$$\begin{aligned}\Sigma &\equiv l+2+2B_{l/2-2}+2B_{l/2-1}+2A_{l/2-1}+2A_{l/2-1}B_{l/2-2} \pmod 4\\ &\equiv l+2(1+A_{l/2-1})+2B_{l/2-2}(1+A_{l/2-1})+2B_{l/2-1} \pmod 4\\ &\equiv l+2B_{l/2-1} \pmod 4,\end{aligned}$$

as required. ■

Corollary 2.6 (Friesen [3, Lemma (4.2)–(4.3), p. 370]). *If $D=2pq$ where p, q are odd primes and if $l(\sqrt{D})$ is even, then*

$$\Sigma\equiv\begin{cases} l+A_{l/2-1}+2 \pmod 4 & \text{if } Q_{l/2} \text{ is even,}\\ l+2B_{l/2-1} & \text{if } Q_{l/2} \text{ is odd.}\end{cases}$$

Example 2.8. Let $D=2\cdot 7=14$. Then $\sqrt{D}=\langle 3;\overline{1,2,1,6}\rangle$, so $l=4$. Also, $A_{l/2-1}+A_1=4$, so $l+2+A_{l/2-1}=10$. Since $\Sigma=-1+2-1+6=6$, we get

$$\Sigma\equiv l+2+A_{l/2-1} \pmod 4,$$

where $Q_{l/2}=Q_2=2$.

Example 2.9. Let $D=2\cdot 7\cdot 31=434$. Then $\sqrt{D}=\langle 20;\overline{1,4,1,40}\rangle$, so $l=4$. Also, $B_{l/2-1}=B_1=1$, so $l+2B_{l/2-1}=8$. Since $\Sigma=-1+4-1+40=42$, we get

$$\Sigma\equiv l+2B_{l/2-1} \pmod 4,$$

where $Q_{l/2}=Q_2=7$.

Example 2.10. Let $D=2\cdot 3\cdot 5\cdot 13\cdot 17=6630$. Then

$$\sqrt{D}=\langle 81;\overline{2,2,1,4,1,2,2,162}\rangle,$$

so $l=8$. Also, $A_{l/2-1}=A_3=570$, so $l+2+A_{l/2-1}=580$.

Since $\Sigma=-2+2-1+4-1+2-2+162=164$, we get

$$\Sigma\equiv l+2+A_{l/2-1} \pmod 4,$$

where $Q_{l/2}=Q_4=30$.

We may now state the first main result on the alternating sum Σ.

Theorem 2.4. *Let $D=2ab$ be a radicand with $a,b\in\mathbb{N}$, where*

$$a\equiv 5 \pmod 8 \quad \text{and} \quad b\equiv 3 \pmod 4.$$

Then l is even. Suppose that in the simple continued fraction expansion of $\sqrt{D}$, we have $Q_{l/2} \in \{a, b, 2a, 2b\}$. Then

$$\Sigma \equiv \left(\frac{a}{b}\right) + 1 \pmod 4.$$

Proof. By (1.8) and Theorem 1.3,

$$Q_{l/2}(A_{l/2-1}/Q_{l/2})^2 - (D/Q_{l/2})B_{l/2-1}^2 = (-1)^{l/2},$$

where $Q_{l/2} \mid A_{l/2-1}$ by the same techniques as used in the proof of Theorem 2.1. Thus, by setting $x = A_{l/2-1}/Q_{l/2}$ and $y = B_{l/2-1}$, we get

$$Q_{l/2}x^2 - (D/Q_{l/2})y^2 = (-1)^{l/2}. \tag{2.17}$$

Suppose that $Q_{l/2} = 2b$. By (2.17), x is odd and $l/2$ is even, so $A_{l/2-1} \equiv 2 \pmod 4$. Therefore, by (2.15) in Lemma 2.1,

$$\Sigma \equiv 0 \pmod 4.$$

Also, from (2.17) we get

$$\left(\frac{a}{b}\right) = -\left(\frac{-ay^2}{b}\right) = -\left(\frac{2bx^2 - ay^2}{b}\right) = -\left(\frac{(-1)^{l/2}}{b}\right) = -\left(\frac{1}{b}\right) = -1,$$

so the result follows.

Suppose that $Q_{l/2} = 2a$. Then by (2.17),

$$2ax^2 - by^2 = (-1)^{l/2},$$

so $B_{l/2-1}$ is odd. Thus,

$$2x^2 + 1 \equiv (-1)^{l/2} \pmod 4.$$

Therefore, x and $l/2$ have the same parity, so

$$A_{l/2-1} = 2ax \equiv 2x \equiv l \pmod 4.$$

By (2.15), $\Sigma \equiv 2 \pmod 4$. Also, by (2.17) and quadratic reciprocity,

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

The result follows.

Suppose that $Q_{l/2} = a$. Then by (2.17),

$$ax^2 - 2by^2 = (-1)^{l/2},$$

so

$$5 - 6y^2 \equiv (-1)^{l/2} \pmod 8.$$

Hence, all of $l/2$, x, and $B_{l/2-1}$ are odd. Thus, by (2.16) in Lemma 2.1, $\Sigma \equiv 0 \pmod 4$. Also,

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

so the result follows.

Finally, suppose that $Q_{l/2} = b$. By (2.17),

$$bx^2 - 2ay^2 = (-1)^{l/2},$$

so both x and $A_{l/2-1}$ are odd. Thus,

$$3 - 2y^2 \equiv (-1)^{l/2} \pmod 4.$$

Therefore,

$$B_{l/2-1} \equiv l/2 + 1 \pmod 2.$$

By (2.16), $\Sigma \equiv 2 \pmod 4$. Also,

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) = \left(\frac{bx^2 - 2ay^2}{a}\right) = \left(\frac{-1}{a}\right)^{l/2} = 1.$$

Hence, the full result is proved. ∎

To check that the hypothesis on the $Q_{l/2}$ holds in Theorem 2.4, we merely note that $D = cQ_{l/2}$ for some $c \in \mathbb{N}$. This is easily determined for ERD-types.

Corollary 2.7. *Suppose that $D = n^2 + a$ is a radicand, $a \mid n$, where $a, n \in \mathbb{N}$, $a \equiv 5 \pmod 8$, n odd, and $b = D/(2a) \equiv 3 \pmod 4$. Then*

$$\Sigma \equiv \left(\frac{a}{b}\right) + 1 \pmod 4.$$

Proof. By [4, Theorem 3.2.1, p. 78], $Q_{l/2} = a$, so the result follows from Theorem 2.4. ∎

Example 2.11. Let $D = 230 = 15^2 + 5 = 2ab = 2 \cdot 5 \cdot 23$. Then $\sqrt{D} = \langle 15; \overline{6, 30}\rangle$, $Q_{l/2} = Q_1 = 5$, and

$$\left(\frac{a}{b}\right) = \left(\frac{5}{23}\right) = -1.$$

Since $\Sigma = -6 + 30 = 24$, we get

$$\Sigma \equiv 0 \equiv \left(\frac{a}{b}\right) + 1 \pmod 4.$$

Example 2.12. Let $D = 105^2 + 21 = 11046 = 2ab = 2 \cdot 21 \cdot 263$. Then $\sqrt{D} = \langle 105; \overline{10, 210}\rangle$, and $Q_{l/2} = 21$. Also,

$$\left(\frac{a}{b}\right) = \left(\frac{21}{263}\right) = -1.$$

Since $\Sigma = -10 + 210 = 200$, we get

$$\Sigma \equiv 0 \equiv \left(\frac{a}{b}\right) + 1 \pmod 4.$$

Other ERD-types are also easy to check under the purview of Theorem 2.4.

Corollary 2.8. *If* $D = n^2 \pm 2a$ *is a radicand where* $2a \mid n \in \mathbb{N}$, $a \equiv 5 \pmod 8$, $b = D/(2a) \equiv 3 \pmod 4$, *then*

$$\Sigma \equiv \left(\frac{a}{b}\right) + 1 \pmod 4.$$

Proof. By [4, Theorem 3.2.1, p. 78], $Q_{l/2} = 2a$. The result now follows from Theorem 2.4. ∎

Example 2.13. Let $D = 476238 = 690^2 + 138 = 2ab = 2 \cdot 69 \cdot 3451$. Then $\sqrt{D} = \langle 690; \overline{10, 1380}\rangle$, $Q_{l/2} = Q_1 = 138 = 2a$, and

$$\left(\frac{a}{b}\right) = \left(\frac{69}{3451}\right) = 1.$$

Since $\Sigma = -10 + 1380 = 1370$, we get

$$\Sigma \equiv 2 \equiv \left(\frac{a}{b}\right) + 1 \pmod 4.$$

However, when the hypothesis of Corollary 2.8 fails, then we cannot guarantee the conclusion.

Example 2.14. Let $D = 475962 = 690^2 - 138 = 2ab = 2 \cdot 69 \cdot 3449$. Then $\sqrt{D} = \langle 689; \overline{1, 8, 1, 1378}\rangle$, $Q_{l/2} = Q_2 = 138 = 2a$, and

$$\left(\frac{a}{b}\right) = \left(\frac{69}{3449}\right) = 1.$$

Since $\Sigma = -1 + 8 - 1 + 1378 = 1384 \equiv 0 \pmod 4$, we get

$$\Sigma \not\equiv 2 \equiv \left(\frac{a}{b}\right) + 1 \pmod 4.$$

Here, $b \equiv 1 \pmod 4$.

We now generalize some results from [3] on alternating sums in order to complete the picture. This will allow us to formulate a table of values that generalizes tables in [3].

Theorem 2.5. *Suppose that* $D > 0$ *is a radicand, no prime* $p \equiv 3 \pmod 4$ *divides* D, *and* $\sqrt{D} = \langle a_0; \overline{a_1, a_2, \ldots, a_l}\rangle$. *If* $Q_{l/2}$ *is square-free, then*

$$\Sigma \equiv 2a_0 l \pmod 4.$$

Proof. If l is odd, then by (1.11), $\Sigma = 2a_0$, so the result trivially follows. Assume that l is even. By Theorem 1.3, $Q_{l/2} \mid D$, so $Q_{l/2} \equiv 2 \pmod 8$ or $Q_{l/2} \equiv 1 \pmod 4$.

If $Q_{l/2} \equiv 2 \pmod 8$, then (1.8) implies that

$$2(A_{l/2-1}/Q_{l/2})^2 - B_{l/2-1}^2 \equiv (-1)^{l/2} \pmod 4$$

since $Q_{l/2}$ is square-free. Thus, $A_{l/2-1} \equiv l+2 \pmod 4$. By (2.15) in Lemma 2.1,

$$\Sigma \equiv 0 \equiv 2a_0 l \pmod 4.$$

If $Q_{l/2} \equiv 1 \pmod 4$ and $D \equiv 2 \pmod 4$, then by (1.8), $A_{l/2-1}$ is odd and $B_{l/2-1} \equiv l/2 \pmod 2$. Therefore, by (2.16) in Lemma 2.1,

$$\Sigma \equiv 0 \equiv 2a_0 l \pmod 4.$$

If $Q_{l/2} \equiv 1 \pmod 4$ and $D \equiv 1 \pmod 4$, then by Theorem 1.3,

$$a_{l/2} = 2P_{l/2}/Q_{l/2},$$

so $a_{l/2}$ is even.

If $l/2$ is even, then by (1.8), $A_{l/2-1}$ is odd and $B_{l/2-1}$ is even. By (1.10),

$$a_{l/2} \equiv 2A_{l/2-2} \pmod 4.$$

Hence, putting the above into (1.9) yields $\Sigma \equiv 0 \equiv 2a_0 l \pmod 4$.

If $l/2$ is odd, then by (1.8), $A_{l/2-1}$ is even and $B_{l/2-1}$ is odd. By (1.7), $A_{l/2-2}$ is odd and by (1.10),

$$a_{l/2} \equiv 2B_{l/2-2} \pmod 4.$$

Finally, putting the above into (1.9) yields $\Sigma \equiv 0 \equiv 2a_0 l \pmod 4$. ■

Corollary 2.9 (Friesen [3, Theorem 1, p. 371]). *Let $p \equiv q \equiv 1 \pmod 4$ be distinct primes, and let $D = pq$. Then*

$$\Sigma \equiv 2a_0 l \pmod 4.$$

Corollary 2.10 (Friesen [3, Theorem 4, p. 373]). *Let $p \equiv q \equiv 1 \pmod 4$ be distinct primes, and let $D = 2pq$. Then*

$$\Sigma \equiv 2a_0 l \pmod 4.$$

The above allows us to generalize tables in [3].

In Table 2.1, we assume that $D = ab$, $a, b \in \mathbb{N}$, is a radicand. Also, in the columns for $a \equiv 1, 5 \pmod 8$, we assume that D is not divisible by any prime $p \equiv 3 \pmod 4$, and $Q_{l/2}$ is square-free. In the columns where $a \equiv 3, 7 \pmod 8$, we assume that $Q_{l/2} = a$.

Table 2.1

	$a \equiv 1 \pmod 8$	$a \equiv 3 \pmod 8$
$b \equiv 1 \pmod 8$	$\Sigma \equiv 2a_0l \pmod 4$	
$b \equiv 3 \pmod 8$		$(\frac{a}{b}) = (-1)^{l/2}$
$b \equiv 5 \pmod 8$	$\Sigma \equiv 2a_0l \pmod 4$	
$b \equiv 7 \pmod 8$		$(\frac{a}{b}) = (-1)^{l/2}$

	$a \equiv 5 \pmod 8$	$a \equiv 7 \pmod 8$
$b \equiv 1 \pmod 8$	$\Sigma \equiv 2a_0l \pmod 4$	
$b \equiv 3 \pmod 8$		$(\frac{a}{b}) = (-1)^{l/2}$
$b \equiv 5 \pmod 8$	$\Sigma \equiv 2a_0l \pmod 4$	
$b \equiv 7 \pmod 8$		$(\frac{a}{b}) = (-1)^{l/2}$

Next, we observe that if $a, b \in \mathbb{N}$ are odd and relatively prime, then

$$\left(\frac{a}{b}\right) = (-1)^{\Sigma/2+1} \quad \text{if and only if} \quad \Sigma \equiv \left(\frac{a}{b}\right) + 1 \pmod 4.$$

Hence, we achieve the following generalization of [3, Table 2, p. 366] via Theorem 2.4.

In Table 2.2, we assume that $D = 2ab$, for $a, b \in \mathbb{N}$, is a radicand. Also, in the columns for $a \equiv 1, 5 \pmod 8$, we assume that D is not divisible by any prime $p \equiv 3 \pmod 4$ and $Q_{l/2}$ is square-free. In the columns where $a \equiv 3, 7 \pmod 8$, we assume that $Q_{l/2} \in \{a, b, 2a, 2b\}$. Furthermore, in the column where $a \equiv 3 \pmod 8$ and $b \equiv 7 \pmod 8$, we assume that $Q_{l/2} = 2a$, and in the column where $a \equiv 7 \pmod 8$ and $b \equiv 3 \pmod 8$, we assume $Q_{l/2} = 2b$.

Table 2.2

	$a \equiv 1 \pmod 8$	$a \equiv 3 \pmod 8$
$b \equiv 1 \pmod 8$	$\Sigma \equiv 2a_0l \pmod 4$	
$b \equiv 3 \pmod 8$		
$b \equiv 5 \pmod 8$	$\Sigma \equiv 2a_0l \pmod 4$	$(\frac{b}{a}) = (-1)^{\Sigma/2+1}$
$b \equiv 7 \pmod 8$		$(\frac{a}{b}) = (-1)^{l/2}$

	$a \equiv 5 \pmod 8$	$a \equiv 7 \pmod 8$
$b \equiv 1 \pmod 8$	$\Sigma \equiv 2a_0l \pmod 4$	
$b \equiv 3 \pmod 8$	$(\frac{a}{b}) = (-1)^{\Sigma/2+1}$	$(\frac{b}{a}) = (-1)^{l/2}$
$b \equiv 5 \pmod 8$	$\Sigma \equiv 2a_0l \pmod 4$	$(\frac{b}{a}) = (-1)^{\Sigma/2+1}$
$b \equiv 7 \pmod 8$	$(\frac{a}{b}) = (-1)^{\Sigma/2+1}$	

Finally, we observe that, with the above generalizations of the results from [3], we may state the following.

THEOREM 2.6. *Let $D = ab$, $a, b \in \mathbb{N}$, be a radicand with $a \equiv 3 \pmod 8$ and $b \equiv 7 \pmod 8$. Then l is even. If $Q_{l/2} \in \{2a, b\}$, then*

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

where $T + U\sqrt{D}$ is the fundamental unit of $\mathcal{O}_{4D}$.

Proof. This goes exactly as in the proof of [3, Theorem 7, p. 377], with the more general results above being referenced rather than the narrower results proved therein. ■

COROLLARY 2.11 (Friesen [3, Theorem 7, p. 377]). *Let $p \equiv 3 \pmod 8$ and $q \equiv 7 \pmod 8$ be primes and let $D = 2pq$. Then the following Legendre symbol equality holds*:

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

where $T + U\sqrt{D}$ is the fundamental unit of $\mathbb{Q}(\sqrt{D})$.

Again, ERD-types are special candidates.

COROLLARY 2.12. *If $D = (4at)^2 - a$, where $a \mid n$, $a \equiv 3 \pmod 8$, and $b = D/a \equiv 7 \pmod 8$, then*

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

Proof. By [4, Theorem 3.2.1, p. 78], $Q_{l/2} = 2a$, so the result follows. ■

EXAMPLE 2.15. Let $D = 141 = 12^2 - 3 = ab = 3 \cdot 47$. Then

$$T + U\sqrt{D} = 95 + 8\sqrt{141} \quad \text{and} \quad \left(\frac{a}{b}\right) = \left(\frac{3}{47}\right) = 1 = (-1)^{U/2}.$$

We conclude with an illustration of Corollary 2.12 that shows the power over the narrower scope in Corollary 2.11. We use a non-fundamental discriminant and composite a and b.

EXAMPLE 2.16. Let $D = 324^2 - 27 = 104949 = 3^3 \cdot 13^2 \cdot 23 = ab = 27 \cdot 3887$. Then the fundamental unit of $\mathcal{O}_{4D} = [1, \sqrt{104949}]$ is

$$T + U\sqrt{D} = 7775 + 24\sqrt{D}.$$

Hence,

$$\left(\frac{a}{b}\right) = \left(\frac{27}{3887}\right) = 1 = (-1)^{U/2}.$$

Acknowledgments. The author thanks the referee for comments that led to a clarification of the presentation in the paper.

References

[1] P. Chowla and S. Chowla, *Problems on periodic simple continued fractions*, Proc. Nat. Acad. Sci. U.S.A. 69 (1972), 3745.

[2] H. Cohn, *A Second Course in Number Theory*, Wiley, New York, 1962.

[3] C. Friesen, *Legendre symbols and continued fractions*, Acta Arith. 59 (1991), 365–379.

[4] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, 1995.

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

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

Received on 30.7.1997
and in revised form on 15.12.1997 (3237)