MATHEMATICS OF COMPUTATION, VOLUME 28, NUMBER 125, JANUARY, 1974

Applications of a Continued Fraction Algorithm to Some Class Number Problems

By M. D. Hendy

Abstract. We make extensive use of Lagrange's algorithm for the evaluation of the quotients in the continued fraction expansion of the quadratic surd ω, where $\omega = \sqrt{d}$ for $d \equiv 2, 3 \pmod 4$ and $(\sqrt{d} - 1)/2$ for $d \equiv 1 \pmod 4$. The recursively generated terms Q_n in his algorithm lead to all norms of primitive algebraic integers of $Q(\sqrt{d})$ less than $\sqrt{(D/4)}$, D being the discriminant. By ensuring that the values Q_n contain at most one small prime, we are able to generate sequences of determinants d of real quadratic fields whose genera usually contain more than one ideal class. Formulae for their fundamental units are given.

1. Norms of Principal Ideals. Let $Q(\sqrt{d})$ be a real quadratic field with discriminant D, fundamental unit ϵ, and let ω be the algebraic integer

$$\begin{aligned} \omega &= (\sqrt{d} - 1)/2, \qquad d \equiv 1 \pmod 4, \\ &= \sqrt{d}, \qquad\qquad d \not\equiv 1 \pmod 4. \end{aligned} \tag{1.1}$$

We can expand ω as an infinite continued fraction

$$\omega = [a_0, a_1, \cdots, a_n, \cdots], \tag{1.2}$$

and calculate the nth convergent p_n/q_n from the quotients a_n in the standard way. It is shown (e.g. [1, Chapter 33]) that the set $\{\pm p_n \pm \omega q_n\}$ includes all the primitive (i.e., no rational divisors other than ± 1) algebraic integers of $Q(\sqrt{d})$ with norm less than $\sqrt{(D/4)}$. We adopt from [1] an algorithm due mainly to Lagrange for calculating the quotients a_n. Recursively, with $[x]$ meaning the largest integer $\leqq x$,

$$a_n = [(P_n + \sqrt{d})/Q_n], \tag{1.3}$$

where

$$P_n = a_{n-1}Q_{n-1} - P_{n-1} \quad \text{and} \tag{1.4}$$

$$Q_n = (d - P_n^2)/Q_{n-1} \tag{1.5}$$

and with initial values $(P_0, Q_0) = (-1, 2)$ or $(0, 1)$ depending on whether $d \equiv 1 \pmod 4$ or not. The sequences of integers, a_n, P_n, Q_n are each periodic, of period l, commencing with $n = 1$. If we set

$$\alpha_n = p_n + \omega q_n, \tag{1.6}$$

we find that $\alpha_{l-1} = \epsilon$, α_{n+l} is an associate of α_n, and

Received June 27, 1972.

AMS (MOS) subject classifications (1970). Primary 12A25, 12A45, 12A50.

Key words and phrases. Principal ideals, real quadratic field, fundamental unit, infinite continued fraction, Lagrange algorithm, class number, genera, Shanks sequence S_n.

$$Q_n = (-1)^n Q_0 N(\alpha_{n-1}) > 0. \tag{1.7}$$

The period l, therefore, is the smallest positive integer n for which $Q_n = Q_0$. The cycles are reflective with

$$P_n = P_{l-n+1}, \tag{1.8}$$

$$Q_n = Q_{l-n} \quad \text{and} \tag{1.9}$$

$$a_n = a_{l-n}, \qquad 0 < n < l. \tag{1.10}$$

Hence, we find the sequence (Q_n/Q_0), $n = 1, 2, \cdots, l$ includes the norms of all principal ideals over $Q(\sqrt{d})$ with norm $< \sqrt{(D/4)}$.

2. Estimates of Class Number. Let $\nu(m)$ be the number of primitive ideals over $Q(\sqrt{d})$ of norm $m \geqq 1$. It is well known that if p is prime

$$\nu(p) = (1 + (D/p)), \tag{2.1}$$

where (D/p) is the Legendre symbol. From elementary considerations, we can show that ν is multiplicative, and, for $r > 1$,

$$\nu(p^r) = (D/p)(1 + (D/p)). \tag{2.2}$$

It is also well known that each ideal class over $Q(\sqrt{d})$ contains at least one primitive ideal with norm less than $\sqrt{(D/5)}$. By comparing $\nu(m)$ with the number of appearances of m in the sequence (Q_n/Q_0), $n = 1, 2, \cdots, l$, for each positive integer $m < \sqrt{(D/5)}$, we can obtain some estimate of the number of classes $h(d)$ of ideals over $Q(\sqrt{d})$. For example, $h = 1$ if and only if m appears in the sequence $\nu(m)$ times, for each m in the interval.

Suppose the ideals over $Q(\sqrt{d})$ lie in g genera with f classes in each genus so that

$$h(d) = fg. \tag{2.3}$$

Suppose p is a prime for which none of its powers p^i, $i \geqq 1$, appear in the sequence (Q_n/Q_0), and for which $(D/p) = 1$. Let A be an ideal of norm p.

Suppose A belongs to the principal genus. As the set of classes of the principal genus is a group of order f, the fth power of A, A^f, must belong to the identity element, i.e., the principal class, and A^f is principal. Alternatively, if A does not belong to the principal genus, A^2 does, so that A^{2f} is a principal ideal. No power of p occurs in the sequence, so

$$p^{2f} > \sqrt{(D/4)}, \tag{2.4}$$

i.e.,

$$2f > (\log_p(D/4))/2. \tag{2.5}$$

(The value $2f$ can be replaced by f if we know A is in the principal genus, and, in particular, if $g = 1$.)

We can also give an upper bound to f by finding a limit to the number of classes in the principal genus. An ideal of norm m is in the principal genus if and only if the Jacobi symbol $(m/a) = 0$ or 1 for each divisor $a \equiv 1 \pmod 4$ of D. When m has this property, we define $\mu(m) = \nu(m)$, otherwise let $\mu(m) = 0$. Let $\sigma(m)$ be the number

of appearances of m in (Q_n/Q_0), $n = 1, 2, \cdots, l$. Then

$$f \leqq 1 + \sum_{m=2}^{[\sqrt{(D/5)}]} (\mu(m) - \sigma(m)). \tag{2.6}$$

For many values of d, the bounds (2.5) and (2.6) are sufficient to determine f, and hence h, precisely.

The occurrence of values d for which $f > 1$ is relatively low. The first such value is $f = 3$ for $d = 79$. In the range $1 < d < 2025$, only 213 (17.4%) of the 1227 square-free values of d have $f > 1$ [2]. Kloss [3] reported that of the primes $p \equiv 1 \pmod 4$ in the range $5 \leqq p \leqq 105269$ about 80% of the fields $Q(\sqrt{p})$ have $f\,(=h) = 1$. The proportion in smaller intervals was relatively stable.

In order to find values of d for which $f > 1$, we need to locate values of d for which a relatively small prime p ($p < (D/4)^{1/4}$) can occur in Eq. (2.5). For each odd prime p, approximately $(p - 1)/2p \doteq \frac{1}{2}$ of the numbers in a given large (in comparison to p) interval are quadratic residues (mod p). Hence, one would expect heuristically that the proportion of numbers in such an interval which are not quadratic residues for at least one of the first n odd primes to be of the order of 2^{-n}.

If we can generate values of d for which the sequence (Q_n/Q_0) contains at most one small prime, then the greater the value of d, the larger, in general, the value of f. We do this in two ways: firstly by generating all values of d for which the period $l \leqq 4$, and secondly by finding values of d for which the corresponding sequence (Q_n/Q_0) contains only one integer c and its powers.

3. Fields with Small Periods. If the period of $Q(\sqrt{d})$, $l \equiv 0 \pmod 2$, then it can be shown by elementary means that the principal ideal $(\alpha_{l/2})$ is ambiguous, and its norm $Q_{l/2}/Q_0$ is a divisor of D. Also, as $(\alpha_l) = (1)$, the only nonambiguous principal ideals occur for $l \leqq 4$, when $l = 3$; (α_1) and (α_2) and when $l = 4$; (α_1) and (α_3). These are conjugate ideals, of the same norm, hence, although (α_1^2) is also principal, its norm is not represented in the sequence (Q_n/Q_0), $n = 1, \cdots, 4$. Hence, $(Q_1/Q_0)^2 > \sqrt{(D/4)}$, so that

$$Q_1/Q_0 > (D/4)^{1/4}. \tag{3.1}$$

The same result holds for both values of l. Hence, the only numbers in the sequence $1 < (Q_n/Q_0) < (D/4)^{1/4}$ are Q_1/Q_0 when $l = 2$, and Q_2/Q_0 when $l = 4$; so, for $l \leqq 4$, (Q_n/Q_0) can contain at most one small prime.

In order to generate such values of $d = a^2 + b$, with $b \leqq 2a$, it is convenient to consider three cases separately. These will be: (i) $d \not\equiv 1 \pmod 4$, (ii) $d \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$, (iii) $d \equiv 1 \pmod 4$, $b \equiv 1 \pmod 4$. By considering the reflective properties (1.8), (1.9) and (1.10) of the algorithm (1.3)–(1.5), we can, subject to some bounds and modular constraints, specify the first $[(l + 4)/4]$ values of a_n, and the first $[(l + 2)/4]$ values of P_n. With these values nominated, d is then uniquely determined. However, in case (iii), we find necessarily that $a_1 = 1$, reducing the number of parameters in this case. Hence, for cases (i) and (ii), d is specified by $[(l + 2)/2]$ parameters, and, in case (iii), by $[l/2]$ parameters.

For example, to find all the values of $d = a^2 + b$ in case (iii) with length 3, we have $d \equiv b \equiv 1 \pmod 4$ and $a \equiv 0 \pmod 2$ as it is case (iii). From Eqs. (1.3)–(1.5), we can calculate the first few values of P_n, Q_n, a_n. These are given in Table I.

TABLE I

n	0	1	2
P_n	-1	$a - 1$	$(b + 1)/2$
Q_n	2	$a + (b - 1)/2$	$a - (b - 1)/2$
a_n	$(a - 2)/2$	1	$\cdots$ etc.

By Eq. (1.9), $Q_1 = Q_2$, so $b = 1$, $d = a^2 + 1 = (2r)^2 + 1$, with $2r = a$. For sufficiency, we expand $d = (2r)^2 + 1$, again using Eqs. (1.3)–(1.5) to ensure that we will always get $l = 3$. This expansion is given in Table II.

TABLE II

n	0	1	2	3
P_n	-1	$2r - 1$	1	$2r - 1$
Q_n	2	$2r$	$2r$	2
a_n	$r - 1$	1	1	

Hence, $d = (2r)^2 + 1$ is of length 3 provided $r > 1$. No modular constraints need be placed as all values are integral.

In a similar way, we calculate the eleven other cases. Their expansions corresponding to Table II will be given as an appendix. We summarise the results in Theorem 1.

THEOREM 1. *The periods $l \leqq 4$ occur precisely for the values of d listed in Table* III.

TABLE III

$l = 1$:

(i) $d = (2r - 1)^2 + 1$, $r \geqq 1$.

(ii) $d = (2r - 1)^2 + 4$, $r \geqq 2$.

(iii) $d = 5$. (In this case, as $\omega < 1$, we expand $1 + \omega$.)

$l = 2$:

(i) $d = (rs)^2/4 + r \not\equiv 1 \pmod 4$, $rs \equiv 0 \pmod 2$, $r, s \geqq 2$.

(ii) $d = (rs)^2 + 4r$, $rs \equiv 1 \pmod 2$, $r, s \geqq 3$.

(iii) $d = (2r + 1)^2 - 4$, $r \geqq 2$.

$l = 3$:

(i) $d = (r(4rs + 1) + s)^2 + 4rs + 1$, $r \not\equiv s \pmod 2$, $r, s \geqq 1$.

(ii) $d = (r(rs + 1) + s)^2 + 4(rs + 1)$, $(r - 1)(s - 1) \equiv 0 \pmod 2$, $r, s \geqq 1$.

(iii) $d = (2r)^2 + 1$, $r \geqq 2$.

$l = 4$:

(i) $d = (rs + t)^2/4 + r \not\equiv 1 \pmod 4$, $rs \equiv t \pmod 2$ { $rs \equiv t \pmod{(st + 1)}$,

(ii) $d = (rs + t)^2 + 4r$, $rs \not\equiv t \pmod 2$ { and $r > t \geqq 1$, $st \geqq 2$.

(iii) $d = (rs)^2 - 4r$, $rs \equiv 1 \pmod 2$, $r, s \geqq 3$.

From the appendix, we can extract the values of the sequence (Q_n/Q_0), $n_l = 1, 2, \cdots, l$. These are given in Table IV.

TABLE IV

l	(i)	(ii)	(iii)
1	1	1	1
2	r, 1	r, 1	$2r - 1$, 1
3	$4rs + 1$, $4rs + 1$, 1	$rs + 1$, $rs + 1$, 1	r, r, 1
4	r, $st + 1$, r, 1	r, $st + 1$, r, 1	r, $rs - r - 1$, r, 1

The above tables do not include squares nor multiples of 4, but contain many numbers with square factors. As our interest lies in fields $Q(\sqrt{d})$ where d is square-free, we will restrict our reference to only square-free values of d in the above tables.

From an examination of the values of f and a comparison with l in the interval $1000 < d < 2000$ [2], we find a general trend for the values of $f > 1$ to be associated with small values of l. For example, over 60% of the values of d with $l \leqq 4$ have $f > 1$, while less than 10% of the values of d with $l > 4$ have $f > 1$. The most extreme case against this trend is $d = 1171$ with $l = 26$ and $f = 3$. Its exceptional nature can be accounted for from the fact that 1171 is a quadratic residue for each of the first six odd primes. (Cf. Table I in [4], where values of $N_p \equiv 1 \pmod 8$ are listed, N_p being the smallest integer which is a quadratic residue for 3, 5, 7, $\cdots$, p. $N_{17} = 18001$.)

Also, from Table III, we can construct sequences of values of d, which, provided they are square-free, will give an increasing sequence of values of f by Eq. (2.5). For example, if we consider the sequence

$$d_n = (6n - 3)^2 + 1, \tag{3.2}$$

we find $(d_n/3) = 1$. If d_n is square-free, then, by Eq. (2.5),

$$f > (\log_3(2n - 1))/2, \tag{3.3}$$

which is unbounded as n increases. It seems likely from the Hardy-Littlewood conjectures (e.g., see [5]) that an infinite number of the d_n are prime, and even more likely, that an infinite number are square-free. Similar results can be constructed from other sequences from Theorem 1.

4. Generalisation of Shanks' Sequence. The second method outlined in Section 2 is to find values of d for which the sequence (Q_n/Q_0) contains only powers of one integer c. For example, Daniel Shanks in [6] introduces the sequence

$$S_n = (2^n + 3)^2 - 8. \tag{4.1}$$

For values of S_n that are square-free, the sequence (Q_n/Q_0), $n = 1, 2, \cdots, l$, where $l = 2n + 1$, takes the values

$$2^n, 2, 2^{n-1}, 2^2, \cdots, 2^{n-1}, 2, 2^n, 1 \tag{4.2}$$

so that

$$Q_{2r} = 2^r Q_0, \qquad Q_{2r+1} = 2^{n-r} Q_0. \tag{4.3}$$

We will consider the more general problem of constructing values of d so that the corresponding sequence (Q_n/Q_0) is

$$Q_{2r} = c^r Q_0, \qquad Q_{2r+1} = c^{n-r} Q_0, \tag{4.4}$$

for integers $c > 1$.

From Eq. (1.5), we can derive, for each $r \geqq 1$,

$$Q_{2r}Q_{2r+1} = c^n Q_0 = d - P_{2r+1}^2 \quad \text{and} \tag{4.5}$$

$$Q_{2r-1}Q_{2r} = c^{n+1}Q_0 = d - P_{2r}^2. \tag{4.6}$$

Hence, ${P_{2r+1}}^2 = d - c^n Q_0 = {P_1}^2$, ${P_{2r}}^2 = d - c^{n+1}Q_0 = {P_2}^2$, $P_1 > P_2$ and ${P_1}^2 - {P_2}^2 = c^n Q_0(c-1) \equiv 0 \pmod 2$, for $n \geqq 1$. Hence, let $P = (P_1 + P_2)/2$ and $k = P - P_2$. Thus, we obtain

$$P_{2r+1} = P + k, \qquad P_{2r} = P - k, \tag{4.7}$$

with $k > 0$. From Eq. (1.4), we can show that $Q_{s+1} = Q_{s-1} + a_s(P_s - P_{s+1})$; so, for each $r \geqq 1$,

$$Q_0 c^{r+1} = Q_0 c^r + 2k a_{2r+1} \quad \text{and} \tag{4.8}$$

$$Q_0 c^{n-r} = Q_0 c^{n-r+1} - 2k a_{2r}. \tag{4.9}$$

Hence,

$$2k a_{2r+1} = c^r(c-1)Q_0 \quad \text{and} \tag{4.10}$$

$$2k a_{2r} = c^{n-r}(c-1)Q_0. \tag{4.11}$$

Equations (4.10) and (4.11) hold for each value of $r \geqq 1$, hence $2k \mid (c-1)Q_0$. Suppose

$$2km = Q_0(c-1), \tag{4.12}$$

so that, for $r \geqq 1$,

$$a_{2r} = mc^{n-r}, \qquad a_{2r+1} = mc^r. \tag{4.13}$$

Using Eq. (1.5), we can show that

$$4Pk = P_1^2 - P_2^2 = c^n(c-1)Q_0 = 2kmc^n Q_0, \tag{4.14}$$

and hence

$$P = (Q_0 mc^n)/2. \tag{4.15}$$

From Eq. (1.5), we also find

$$d = ((Q_0 mc^n)/2 + k)^2 + Q_0^2 b^n. \tag{4.16}$$

We now consider two cases, depending on whether or not $d \equiv 1 \pmod 4$.

Case A. $d \not\equiv 1 \pmod 4$. Thus $Q_0 = 1$ and, by Eq. (4.15), $c \equiv 1 \pmod 2 \Rightarrow m \equiv 0 \pmod 2$, as P is integral. Let $m = 2q$, so that Eq. (4.12) becomes

$$4qk = c - 1, \tag{4.17}$$

so $c \equiv 1 \pmod 4$. $d = (qc^n + k)^2 + c^n \equiv (q+k)^2 + 1 \not\equiv 1 \pmod 4$. Hence $q + k \equiv 1 \pmod 2$, so $qk \equiv 0 \pmod 2$, and Eq. (4.17) gives $c \equiv 1 \pmod 8$.

Thus, in Case A, the values of d given by Eq. (4.16) are

$$d = (qc^n + k)^2 + c^n, \tag{4.18}$$

with $c \equiv 1 \pmod 8$ and $qk = (c - 1)/4$. All the values of d given by Eq. (4.18) give rise to the sequence (4.4). For example, with $(c, k, q) = (9, 2, 1)$, we obtain the sequence

$$d_n = (9^n + 2)^2 + 9^n. \tag{4.19}$$

In particular, $d_3 = 535090$ which has, for the first seven values of Q_n, Q_1 to Q_7: 729, 9, 81, 81, 9, 729, 1.

Case B. $d \equiv 1 \pmod 4$, in which case $Q_0 = 2$ and, by Eq. (4.12),

$$km = c - 1. \tag{4.20}$$

From Eq. (4.16) with $d \equiv 1 \pmod 4$ and Eq. (4.20), we find

$$d = (mc^n + k)^2 + 4c^n, \tag{4.21}$$

with $c = mk + 1$. To ensure $d \equiv 1 \pmod 4$, we require $mc^n + k \equiv mc + k \equiv 1 \pmod 2$. However, by Eq. (4.20), this means $(mk + 1)m + k \equiv mk + m + k \equiv 1 \pmod 2$, so that

$$(m + 1)(k + 1) \equiv 0 \pmod 2, \tag{4.22}$$

i.e., one of m, k must be odd. Provided this condition is met, we can obtain the sequence (4.4). For example, with $(c, k, m) = (2, 1, 1)$, we obtain Shanks' sequence

$$d = S_n = (2^n + 1)^2 + 4 \cdot 2^n = (2^n + 3)^2 - 8. \tag{4.23}$$

Other examples will be given in the appendix.

5. Fundamental Units. Having obtained the quotients a_n from Eq. (1.3), we can readily calculate the fundamental unit α_{l-1} from Eq. (1.6). From Eq. (1.7), we note

$$N(\epsilon) = (-1)^l. \tag{5.1}$$

Corresponding to each field extracted from the values of d in Table III, we can set up a table of their fundamental units (see Table V).

TABLE V

d	ϵ
$(2r - 1)^2 + 1$	$(2r - 1) + \sqrt{d}$
$(2r - 1)^2 + 4$	$((2r - 1) + \sqrt{d})/2$
5	$(1 + \sqrt{d})/2$
$(rs)^2/4 + r$	$(rs^2 + 2)/2 + s\sqrt{d}$
$(rs)^2 + 4r$	$(rs^2 + 2 + s\sqrt{d})/2$
$(2r + 1)^2 - 4$	$(2r + 1) + \sqrt{d}$
$(r(4rs + 1) + s)^2 + 4rs + 1$	$((4r^2 + 1)^2 s + r(4r^2 + 3)) + (4r^2 + 1)\sqrt{d}$
$(r(rs + 1) + s)^2 + 4(rs + 1)$	$((r^2 + 1)^2 s + r(r^2 + 3) + (r^2 + 1)\sqrt{d})/2$
$(2r)^2 + 1$	$2r + \sqrt{d}$
$(rs + t)^2/4 + r$	$((rs + st + 1)^2 + 2s(rs - t) + s(rs + st + 1)\sqrt{d})/2(st + 1)$
$(rs + t)^2 + 4r$	$((rs + st + 2)^2 - 2(st + 1) + s(rs + st + 1)\sqrt{d})/2(st + 1)$
$(rs)^2 - 4r$	$(rs^2 - 2 + s\sqrt{d})/2$

For the sequences of Section 4, we obtain by Eq. (4.13) the sequence $(a_n) = a_0, m, mc^{n-1}, mc, mc^{n-2}, mc^2, \cdots$. From this, we can calculate the coefficients p_r, q_r recursively. Less calculation is involved in finding q_r, than in finding p_r, and as $l = 2n + 1$ is odd, we can obtain the coefficients u, v of $\epsilon = u + v\sqrt{d}$ from

$$v = q_{2n}, \tag{5.2}$$

$$u = (dq_{2n}^2 - Q_0^2)^{1/2}. \tag{5.3}$$

We find by induction that

$$q_{2r} = 1 + \sum_{s=1}^{r}\left(\sum_{t=0}^{r-s}\binom{r-t}{s}\binom{s+t-1}{s-1}c^{s(n-1)-t}\right)m^{2s}, \tag{5.4}$$

and

$$q_{2r+1} = \sum_{s=0}^{r}\left(\sum_{t=0}^{r-s}\binom{r-t}{s}\binom{s+t}{s}c^{sn+t}\right)m^{2s+1}, \tag{5.5}$$

hence

$$v = 1 + \sum_{s=1}^{n}\left(\sum_{t=0}^{n-s}\binom{n-t}{s}\binom{s+t-1}{s-1}c^{s(n-1)-t}\right)m^{2s}. \tag{5.6}$$

For example, in the case $d = (9^3 + 2)^2 + 9^3 = 535090$, we find by Eq. (5.6) that $v = 34\,351529$. Rather than use Eq. (5.3) directly, computation is shortened by noting the approximation

$$u \doteq v\sqrt{d}. \tag{5.7}$$

In this case, $v\sqrt{d} = 25128\,090632.99997$. Taking u as 25128 090633, we find $u^2 = dv^2 - 1 = 631\,420938\,860262\,340689$.

As n increases, so does the complexity of calculation in Eq. (5.6), and in fact, for $n > 15$, multiprecision arithmetical subroutines are needed to compute v. However, if only approximate values of u, v etc. are required, we can rearrange Eq. (5.6) to isolate the leading terms.

For example, in the case of Shanks' sequence $d_n = (2^n + 3)^2 - 8$, with $c = 2$, $m = 1$ (Eq. (4.23)), we can rearrange Eq. (5.6) to give

$$v = 1 + \sum_{q=1}^{n}\left(\sum_{r=1}^{q}\binom{n-r+1}{n-q+1}\binom{n+r-q-1}{n-q}2^{q-r}\right)2^{n(n-q)} \tag{5.8}$$

whose leading terms give the approximation

$$\begin{aligned} v = 2^{n^2-n}(1 &+ (3n-1)2^{-n} + (\tfrac{9}{2}n^2 - \tfrac{19}{2}n + 5)2^{-2n} \\ &+ (\tfrac{9}{2}n^3 - 24n^2 + \tfrac{85}{2}n - 25)2^{-3n} + O(n^4 2^{-4n})). \end{aligned} \tag{5.9}$$

Using the approximation $\sqrt{d} = 2^n(1 + 3.2^{-n} - 4.2^{-2n} + 12.2^{-3n} + O(2^{-4n}))$ in Eq. (5.7), we obtain

$$\begin{aligned} u = 2^{n^2}(1 &+ (3n+2)2^{-n} + (\tfrac{9}{2}n^2 - \tfrac{1}{2}n - 2)2^{-2n} \\ &+ (\tfrac{9}{2}n^3 - \tfrac{21}{2}n^2 + 2n + 6)2^{-3n} + O(n^4 2^{-4n})), \end{aligned} \tag{5.10}$$

and use $\epsilon \doteq 2u$ for an approximation for ϵ.

In a recent paper [7], Shanks required an asymptotic value for $\log \epsilon^2$ in the computation of the class number $h(S_n)$. He quotes from a paper, yet to be published [8], the result

$$\log(\epsilon^2) = 2n^2 \log 2 + O(n2^{-n}). \tag{5.11}$$

Using Eq. (5.10) and the log series, we can refine Eq. (5.11) to

$$\begin{aligned}\log(\epsilon^2) = {} & (2n^2 + 2)\log 2 + (6n + 4)2^{-n} \\ & - (13n + 8)2^{-2n} + (42n + \tfrac{76}{3})2^{-3n} + O(n^4 2^{-4n}).\end{aligned} \tag{5.12}$$

However, for other than relatively small values of n, we can use the approximation of $(2n^2 + 2)\log 2$. In the case $n = 19$ quoted by Shanks, (5.12) gives 501.838653, with the remainder terms after $(2n^2 + 2)\log 2$ contributing only 0.000225. (Cf. (5.11) giving 500.452134.)

6. Conclusion. In his algorithm for calculating class numbers of real quadratic fields, Shanks [7] notes that the efficiency of computation is greatly enhanced by knowing a priori the fundamental unit of the field, and in the cases listed above with only a small number of easily recognised primitive principal ideals, other problems in his algorithm are reduced.

Obviously, it would be possible to classify all fields of any given period, by extending the processes of Section 3. However, the current method has a practical barrier to indefinite extension in the sheer mass of algebraic manipulation with increasing numbers of parameters being required. There may well be other more fruitful approaches to the problem.

7. Appendix.

$l = 1$:

	$d = (2r-1)^2 + 1$		$d = (2r-1)^2 + 4$		$d = 5$	
n	0	1	0	1	0	1
P_n	0	$2r-1$	-1	$2r-1$	1	1
Q_n	1	1	2	2	2	2
a_n	$2r-1$		$r-1$		1	

$l = 2$:

	$d = (rs)^2/4 + r$			$d = (rs)^2 + 4r$			$d = (2r+1)^2 - 4$		
n	0	1	2	0	1	2	0	1	2
P_n	0	$\frac{rs}{2}$	$\frac{rs}{2}$	-1	rs	rs	-1	$2r-1$	$2r-1$
Q_n	1	r	1	2	$2r$	2	2	$4r-2$	2
a_n	$\frac{rs}{2}$	s		$\frac{rs-1}{2}$	s		r	1	

$l = 3$:

$$d = (r(4rs + 1) + s)^2 + 4rs + 1$$

n	0	1	2	3
P_n	0	$r(4rs+1)+s$	$r(4rs+1)-s$	$r(4rs+1)-s$
Q_n	1	$4rs+1$	$4rs+1$	1
a_n	$r(4rs+1)+s$	$2r$	$2r$	

$d = (r(rs+1)+s)^2 + 4(rs+1)$ $\qquad$ $d=(2r)^2+1$

n	0	1	2	3	0	1	2	3
P_n	-1	$r(rs+1)+s$	$r(rs+1)-s$	$r(rs+1)+s$	-1	$2r-1$	1	$2r-1$
Q_n	2	$2(rs+1)$	$2(rs+1)$	2	2	$2r$	$2r$	2
a_n	$\frac{r(rs+1)+s-1}{2}$	r	r		$r-1$	1	1	

$l = 4$:

$d=(rs+t)^2/4+r$ $\qquad$ $d=(rs+t)^2+4r$

n	0	1	2	3	4	0	1	2	3	4
P_n	0	$\frac{rs+t}{2}$	$\frac{rs-t}{2}$	$\frac{rs-t}{2}$	$\frac{rs+t}{2}$	-1	$rs+t$	$rs-t$	$rs-t$	$rs+t$
Q_n	1	r	$1+st$	r	1	2	$2r$	$2(st+1)$	$2r$	2
a_n	$\frac{rs+t}{2}$	s	$\frac{rs-t}{1+st}$	s		$\frac{rs+t-1}{2}$	s	$\frac{rs-t}{1+st}$	s	

$d = (rs)^2 - 4r$

n	0	1	2	3	4
P_n	-1	$rs-2$	$rs-2r$	$rs-2r$	$rs-2$
Q_n	2	$2(rs-r-1)$	$2r$	$2(rs-r-1)$	2
a_n	$\frac{rs-3}{2}$	1	$s-2$	1	

$d \not\equiv 1 \pmod 4$		$d \equiv 1 \pmod 4$	
(c, k, q)	d	(c, k, m)	d
(9, 1, 2)	$(2.9^n+1)^2+9^n$	(2, 1, 1)	$(1.2^n+1)^2+4.2^n$
(9, 2, 1)	$(1.9^n+2)^2+9^n$	(3, 1, 2)	$(2.3^n+1)^2+4.3^n$
(17, 1, 4)	$(4.17^n+1)^2+17^n$	(3, 2, 1)	$(1.3^n+2)^2+4.3^n$
(17, 4, 1)	$(1.17^n+4)^2+17^n$	(4, 1, 3)	$(3.4^n+1)^2+4.4^n$
(25, 1, 6)	$(6.25^n+1)^2+25^n$	(4, 3, 1)	$(1.4^n+3)^2+4.4^n$
(25, 2, 3)	$(3.25^n+2)^2+25^n$	(5, 1, 4)	$(4.5^n+1)^2+4.5^n$
(25, 3, 2)	$(2.25^n+3)^2+25^n$	(5, 4, 1)	$(1.5^n+4)^2+4.5^n$
(25, 6, 1)	$(1.25^n+6)^2+25^n$	(6, 1, 5)	$(5.6^n+1)^2+4.6^n$

etc.

The University of New England
Mathematics Department
Armidale, N.S.W. 2351, Australia

1. G. CHRYSTAL, *Algebra.* Part II, 2nd ed., A. and C. Black Ltd., London, 1931.
2. E. L. INCE, *Cycles of Reduced Ideals in Quadratic Fields*, Mathematical Tables, vol. IV, British Association for the advancement of Science, London, 1934.
3. K. E. KLOSS, "Some number theoretic calculations," *J. Res. Nat. Bur. Standards Sect. B*, v. 69B, 1965, p. 335–336. MR **32** #7473.
4. D. H. LEHMER, EMMA LEHMER & DANIEL SHANKS, "Integer sequences having prescribed quadratic character," *Math. Comp.*, v. 24, 1970, pp. 433–451. MR **42** #5889.
5. DANIEL SHANKS, "On the conjecture of Hardy and Littlewood concerning the number of primes of the form n^2+a," *Math. Comp.*, v. 14, 1960, pp. 320–332. MR **22** #10960.
6. DANIEL SHANKS, "On Gauss's class number problems," *Math. Comp.*, v. 23, 1969, pp. 151–163. MR **41** #6814.
7. DANIEL SHANKS, "Class number, a theory of factorisation and genera," *Proc. Sympos. Pure Math.*, vol. 20, Amer. Math. Soc., Providence, R.I., 1971, pp. 415–440.
8. DANIEL SHANKS, "An interesting sequence: S_n." (To appear.)