MATHEMATICS OF COMPUTATION
VOLUME 62, NUMBER 206
APRIL 1994, PAGES 885–897

QUADRATIC RESIDUE COVERS FOR CERTAIN REAL QUADRATIC FIELDS

R. A. MOLLIN AND H. C. WILLIAMS

ABSTRACT. Let $\Delta_n(a, b) = (ba^n+(a-1)/b)^2+4a^n$ with $n \geq 1$ and $b \mid a-1$. If $\mathscr{C}$ is a finite set of primes such that for each $n \geq 1$ there exists some $q \in \mathscr{C}$ for which the Legendre symbol $(\Delta_n(a, b)/q) \neq -1$, we call $\mathscr{C}$ a quadratic residue cover (QRC) for the quadratic fields $K_n(a, b) = Q(\sqrt{\Delta_n(a, b)})$. It is shown how the existence of a QRC for any a, b can be used to determine lower bounds on the class number of $K_n(a, b)$ when $\Delta_n(a, b)$ is the discriminant of $K_n(a, b)$. Also, QRCs are computed for all $1 \leq a, b \leq 10000$.

1. INTRODUCTION

In [11] Shanks introduced the interesting sequence $S_n = (2^n + 3)^2 - 8 = (2^n+1)^2+2^{n+2}$. Shanks discovered this sequence by tabulating the class number h of the quadratic fields $\mathbf{Q}(\sqrt{d_k})$, where $d_k = k^2 - 8 < 10^4$, $k \geq 1$, and d_k is prime. He noticed that the only value of d_k in his table such that $h \neq 1$ is $d_k = 4481$. On further analysis he deduced that the class number h_n of the quadratic fields $\mathbf{Q}(\sqrt{S_n})$ $(4481 = S_6)$ for prime values of S_n tend to be large as n increases. For example, if $n = 1, 2, 3, 4, 5$, the class number of $\mathbf{Q}(\sqrt{S_n})$ is 1, but Shanks was unable to find another value of n for which this is true; in fact, $h_8 = 3$, $h_{10} = 9$, $h_{11} = 11$, $h_{12} = 27$. Also, since S_7, S_9 are odd, composite and squarefree, their corresponding class numbers must be divisible by 2 (see Theorem 3.1 below).

Recently, Mollin and Williams [8] were able to prove that $h_n = 1$ for squarefree S_n only for $n = 1, 2, 3, 4, 5$. The proof was elementary and depended upon the easily established fact that the Legendre symbol $(S_n/127) = 1$ for all $n \geq 0$. We point out here that the proof could also be made to work if we had used any finite set of primes $\mathscr{C}$ such that for any $n \geq 0$, we have $(S_n/q) = 1$ for some $q \in \mathscr{C}$. We used $\mathscr{C} = \{127\}$, but it is easy to show that if $\mathscr{C} = \{5, 7, 13, 17, 241\}$, then for any $n \geq 0$ we get $(S_n/q) = 1$ for some $q \in \mathscr{C}$. This is because $(S_n/5) = 1$ when $n \equiv 2 \pmod 4$; $(S_n/7) = 1$ when $n \equiv 0 \pmod 3$; $(S_n/13) = 1$ when $n \equiv 1, 11 \pmod{12}$; $(S_n/17) = 1$ when $n \equiv 0, 1, 4, 7 \pmod 8$; and $(S_n/241) = 1$ when $n \equiv 5, 19 \pmod{24}$. Notice that the integers are completely covered by the various congruences modulo 4, 3, 12, 8, 24; that is, for any integer n, one of these congruences must hold.

Received by the editor September 5, 1992 and, in revised form, April 22, 1993.
1991 *Mathematics Subject Classification.* Primary 11R11, 11R29, 11Y40, 05B40.
The first author's research is supported by NSERC of Canada Research Grant #A8484; that of the second author is supported by NSERC of Canada Research Grant #A7649.

0025-5718/94 $1.00 + $.25 per page

If, for some function f such that $f\colon \mathbf{Z}^{\geq 0} \to \mathbf{Z}^{\geq 0}$, we have a finite set of primes $\mathscr{C}$ such that for any $n \in \mathbf{Z}^{\geq 0}$ we get

$$(f(n)/q) \neq -1$$

for some $q \in \mathscr{C}$, we call $\mathscr{C}$ a *quadratic residue cover* (QRC) for f. If $K_n = \mathbf{Q}(\sqrt{f(n)})$ and $\mathscr{C}$ is a QRC for f, we will say that $\mathscr{C}$ is a QRC for the fields K_n $(n = 0, 1, 2, \ldots)$. Thus, we have seen that either $\{127\}$ or $\{5, 7, 13, 17, 241\}$ is a QRC for the fields $\mathbf{Q}(\sqrt{S_n})$ $(n = 0, 1, 2, \ldots)$. The purpose of this paper is to generalize Shanks's sequence and show how a computer can be enlisted to search for quadratic residue covers for such sequences. It will also be shown that in certain cases these covers can be used to establish a *lower* bound on the growth of the class number of the real quadratic fields corresponding to these sequences. In order to do this, we must first provide a review of some of the properties of real quadratic fields.

2. Real quadratic fields

The results given here concerning real quadratic fields are well known. They can be found, for example, in Williams and Wunderlich [13] and Cohn [1]. Let d be a squarefree positive integer and $\omega = (\sigma - 1 + \sqrt{d})/\sigma$, where

$$\sigma = \begin{cases} 1 & \text{when } d \equiv 2, 3 \pmod 4, \\ 2 & \text{when } d \equiv 1 \pmod 4. \end{cases}$$

The discriminant Δ of $\mathbf{K} = \mathbf{Q}(\sqrt{d})$ is given by $\Delta = (2/\sigma)^2 d$, and if $[\alpha, \beta]$ denotes the module $\{\alpha x + \beta y \mid x, y \in \mathbf{Z}\}$, then the maximal order $\mathbf{O_K}$ of $\mathbf{K}$ is given by $\mathbf{O_K} = [1, \omega]$. If $\alpha \in \mathbf{K}$, we use $\bar{\alpha}$ to denote the conjugate of α, and $N(\alpha)$ to denote the value of $\alpha\bar{\alpha}$, the *norm* of α.

An *ideal* of $\mathbf{O_K}$ can be written as $\mathbf{a} = [a, b + c\omega]$, where $a, b, c \in \mathbf{Z}$ with $a, c > 0$, $c \mid b$, $c \mid a$, and $ac \mid N(b + c\omega)$. Furthermore, if $a, b, c \in \mathbf{Z}$ with $c \mid b$, $c \mid a$, and $ac \mid N(b + \omega)$, then $[a, b + c\omega]$ is an ideal of $\mathbf{O_K}$. For an ideal $\mathbf{a} = [a, b + c\omega]$ with $a, c > 0$, the *norm* of $\mathbf{a}$, $N(\mathbf{a})$, is given by $N(\mathbf{a}) = ac > 0$. If $c = 1$, then $\mathbf{a}$ is said to be a *primitive* ideal.

A primitive ideal $\mathbf{a}$ is said to be *reduced* if it does *not* contain any nonzero element α such that $|\alpha| < N(\mathbf{a})$ and $|\bar{\alpha}| < N(\mathbf{a})$.

Theorem 2.1. *If* $\mathbf{a}$ *is a reduced ideal of* $\mathbf{O_K}$, *then* $N(\mathbf{a}) < \sqrt{\Delta}$. *If* $\mathbf{a}$ *is a primitive ideal of* $\mathbf{O_K}$ *such that* $N(\mathbf{a}) < \sqrt{\Delta}/2$, *then* $\mathbf{a}$ *is a reduced ideal of* $\mathbf{O_K}$. □

At this point it is convenient to introduce continued fractions into our discussion. Let $\alpha \in \mathbf{K}$; we can write $\alpha = (P_0 + \sqrt{d})/Q_0$, where $P_0, Q_0 \in \mathbf{Z}$. If we put $q_0 = \lfloor \alpha \rfloor$ and define

$$P_{i+1} = q_i Q_i - P_i, \qquad Q_i Q_{i+1} = d - P_{i+1}^2,$$
$$q_{i+1} = \left\lfloor \frac{P_{i+1} + \sqrt{d}}{Q_{i+1}} \right\rfloor \qquad (i = 0, 1, 2, \ldots),$$

then

$$\alpha = \langle q_0, q_1, q_2, \ldots, q_i, \ldots \rangle$$

is the continued fraction expansion of α. One of the important uses for continued fractions in the theory of real quadratic fields is illustrated in

Theorem 2.2. *Let* $\mathbf{a}_1 = \mathbf{a} = [a, b+\omega]$ *be a reduced ideal of* $\mathbf{O}_\mathbf{K}$. *If we put* $\alpha = (b+\omega)/a$, *then all of the reduced ideals in the same equivalence class as* $\mathbf{a}$, *and only these, are given by*

$$\mathbf{a}_m = [Q_{m-1}/\sigma, (P_{m-1}+\sqrt{d})/\sigma] \qquad (i = 1, 2, 3, \ldots),$$

where the values of the P_i*'s and* Q_i*'s are found by expanding* α *into a continued fraction.* □

Since by Theorem 2.1 there can only be a finite number of reduced ideals of $\mathbf{Q}_\mathbf{K}$, and since all the $\mathbf{a}_m$ are reduced, we see that the sequence of reduced ideals $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \ldots, \mathbf{a}_m, \ldots$ produced by the continued fraction expansion must be purely periodic; that is, there must exist a minimal $k \in \mathbf{Z}^{>0}$ such that $\mathbf{a}_{k+1} = \mathbf{a}_1$. We call k the period length of the continued fraction expansion of α. In the case of the principal ideal class, we can put $\mathbf{a}_1 = \mathbf{O}_\mathbf{K} = [1, \omega]$ and use π to denote this period length. If ε_0 is the fundamental unit of $\mathbf{K}$ and R $(= \log \varepsilon_0)$ is the regulator of K, then by a result of Pen and Skubenko [9], we have $R > k \log \phi$, where $\phi = (1+\sqrt{5})/2$. Thus, if h is the class number of $\mathbf{K}$, we see that if C is the total number of reduced ideals in $\mathbf{K}$, then

$$C < Rh/\log \phi. \tag{2.1}$$

We should also mention that if p is any odd rational prime, we have

$$(p) = \mathbf{p}_1^2 \quad \text{when } p \mid \Delta,$$
$$(p) = \mathbf{p}_1\mathbf{p}_2 \quad \text{when } (\Delta/p) = 1,$$
$$(p) = \mathbf{p} \quad \text{when } (\Delta/p) = -1,$$

where (p) is the ideal $[p, p\omega]$ and $\mathbf{p}$, $\mathbf{p}_1$, $\mathbf{p}_2$ denote prime ideals such that $N(\mathbf{p}_1) = N(\mathbf{p}_2) = p$ and $N(\mathbf{p}) = p^2$. If $p = 2$, then

$$(2) = \mathbf{p}_1^2 \quad \text{when } 2 \mid \Delta,$$
$$(2) = \mathbf{p}_1\mathbf{p}_2 \quad \text{when } \Delta \equiv 1 \pmod 8,$$
$$(2) = \mathbf{p} \quad \text{when } \Delta \equiv 5 \pmod 8.$$

The following theorem is also useful.

Theorem 2.3. *The class number of* $\mathbf{Q}(\sqrt{d})$ *is odd if and only if* $d = 2, p, 2p_1, p_1p_2$, *where* p, p_1, p_2 *denote primes and* $p_1 \equiv p_2 \equiv -1 \pmod 4$. □

3. Quadratic residue covers

In the case of $d = 4481$, Shanks noticed that all of the reduced ideals (Shanks used the language of quadratic forms rather than that of ideals) in the principal ideal class have norms which are powers of 2 only. It was this property of 4481 that he used to produce his sequence S_n. More recently, Mollin [6] has shown that when $\pi \geq 3$, all the reduced principal ideals of $\mathbf{O}_\mathbf{K}$ have norms which are powers of a single integer a (> 1) if and only if

$$\Delta = (ba^n + (a-1)/b)^2 + 4a^n,$$

where $b \mid a-1$ and $n > 0$. In this case, $\pi = 2n+1$, and the continued fraction expansion of ω is given by

$$P_{2j} = \sigma(ba^n - (a-1)/b)/2, \qquad Q_{2j} = \sigma a^j, q_{2j} = ba^{n-j} \qquad (j \geq 1)$$

and

$$P_{2j+1} = \sigma(ba^n + (a-1)/b)/2, \quad Q_{2j+1} = \sigma a^{n-j}, \quad q_{2j+1} = ba^j \qquad (j \geq 0).$$

Also from Halter-Koch [2], the value of ε_0 is given by

$$\varepsilon_0 = \alpha\beta^n, \tag{3.1}$$

where

$$\alpha = (\sigma(ba^n + (a-1)/b) + 2\sqrt{\Delta})/(2\sigma),$$
$$\beta = (\sigma(ba^n + a + 1) + 2b\sqrt{\Delta})/(2\sigma a).$$

In the case of these values for Δ, suppose that $p < \sqrt{\Delta}/2$ is a prime such that $p \neq a$ and $(\Delta/p) = 0, 1$. If $\mathbf{p}$ is a prime ideal divisor of (p), we get $N(\mathbf{p}) = p$. It follows that since $\mathbf{p}$ is a primitive ideal, $\mathbf{p}$ must be reduced by Theorem 2.1. If $h = 1$, then $\mathbf{p}$ must be principal; but, since all the reduced principal ideals must have norms which are powers of a, this is impossible. For $\Delta = S_n$, we see that if $127 < \sqrt{\Delta}/2$, then $h_n > 1$. Since $S_n > (2 \cdot 127)^2 = 64516$ for $n \geq 8$, S_7 is composite, and $h_6 = 3$, we get $h_n > 1$ for all squarefree S_n with $n \geq 6$. Notice that we could also use our other $\mathscr{C}$ here because we know that there always exists some prime $p \leq 241$ such that $(S_n/p) = 1$; hence, $h_n > 1$ whenever $\sqrt{S_n}/2 > 241$, which occurs when $n \geq 9$. This illustrates how QRCs can be used to establish this kind of class number result.

Let

$$\Delta_n(a, b) = (ba^n + (a-1)/b)^2 + 4a^n,$$

and let $\mathscr{C}(a, b)$ denote a QRC for the fields $\mathbf{K}_n(a, b) = \mathbf{Q}(\sqrt{\Delta_n(a, b)})$. If $\Delta_n(a, b)$ is composite, we have the following simple result.

Theorem 3.1. *If* $\Delta_n(a, b) = (ba^n + (a-1)/b)^2 + 4a^n$ *is the discriminant of* $\mathbf{K}_n(a, b)$, *then* $2 \mid h_n(a, b)$ *whenever* $\Delta_n(a, b)$ *is composite.*

Proof. Suppose n is even. In this case, $\Delta_n(a, b)$ is a sum of two squares, and consequently, if p denotes any odd prime divisor of $\Delta_n(a, b)$, we get $p \equiv 1 \pmod 4$. If n is odd and $p \mid \Delta_n(a, b)$, we see that $(-4a/p) = (-a/p) = 1$. We also note, however, that

$$b^2\Delta_n(a, b) = (b^2a^n + a + 1)^2 - 4a; \tag{3.2}$$

thus, if $p \mid \Delta_n(a, b)$, we get $(4a/p) = (a/p) = 1$. Since $(-a/p) = 1 = (a/p)$, we must have $(-1/p) = 1$ and $p \equiv 1 \pmod 4$. By Theorem 2.3 it is clear that $2 \mid h_n(a, b)$ whenever $\Delta_n(a, b)$ is composite. □

Thus, the only possibility for $h_n(a, b)$ to be 1 occurs when $\Delta_n(a, b)$ is a prime.

If we consider the case of a being composite, let q be any prime divisor of a such that $q^2 \leq a$. It is clear in this case that $\{q\}$ is a QRC for the fields $\mathbf{K}_n(a, b)$. We will use the notation $\mathscr{C}(a, b) = \mathscr{S}$, where $\mathscr{S}$ is some set, to denote that $\mathscr{S}$ is a QRC for $\mathbf{K}_n(a, b)$; no uniqueness is to be attributed, then, to the use of the symbol $\mathscr{C}(a, b)$, as several different sets could qualify for a $\mathscr{C}(a, b)$. We have already seen in the case of S_n that $\mathscr{C}(2, 1) = \{127\}$ or $\{5, 7, 13, 17, 241\}$. Thus we see that $\mathscr{C}(a, b) = \{q\}$ if $q \mid a$ and $q^2 \leq a$. If a is a prime and $a \notin \mathscr{C}(a, b)$, then because of the finiteness condition on $\mathscr{C}(a, b)$, there must exist some minimal $l \in \mathbf{Z}^{>0}$ such that $a^l \equiv 1 \pmod q$

for all $q \in \mathscr{C}$. We call such a QRC an l-QRC and denote it by $\mathscr{C}_l(a, b)$. The following theorem shows why it is useful to try to find a $\mathscr{C}_l(a, b)$ with a minimal l.

We first point out, however, that all of our results concerning the class number of $\mathbf{K}_n(a, b)$ are contingent upon the discriminant $\mathbf{K}_n(a, b)$ being $\Delta_n(a, b)$. To this end, we define $h_n(a, b)$ only when $\Delta_n(a, b)$ is odd and squarefree, or $\Delta_n(a, b) \equiv 0 \pmod 4$ and $\Delta_n(a, b)/4$ is squarefree.

Theorem 3.2. *Let q be any prime such that $(d/q) = 1$. If no power of q appears as the norm of a reduced principal ideal of $Q(\sqrt{d})$, then $h > \log\Delta/(2\log q)$.*

Proof. Since $(d/q) = 1$, there must exist some prime ideal $\mathbf{q}$ which divides (q) such that $N(\mathbf{q}) = q$. Since $\mathbf{q}^h$ is a primitive, principal ideal and $N(\mathbf{q}^h) = q^h$, we cannot have $\mathbf{q}^h$ as a reduced principal ideal; hence, by Theorem 2.1 we have $2q^h > \sqrt{\Delta}$. □

Corollary 3.2.1. *If $\mathscr{C}_l(a, b)$ is an l-QRC for the fields $\mathbf{K}_n(a, b)$, and no element of $\mathscr{C}_l(a, b)$ divides $\Delta_n(a, b)$ for any $n \geq l$, then*

$$h_n(a, b) > (n - 1)/l.$$

Proof. Put $h = h_n(a, b)$ and let $q \in \mathscr{C}_l(a, b)$. Since $a^l > q$ and $q \nmid a\Delta_n(a, b)$, by the theorem we must have

$$a^{lh} > q^h > \sqrt{\Delta_n(a, b)}/2 > ba^n/2 \geq a^{n-1}. \quad \square$$

Corollary 3.2.2. *If a is composite, then*

$$h_n(a, b) > 2n - 1.$$

Proof. For $\mathscr{C}(a, b) = \{q\}$ as above, we get

$$2q^h > \sqrt{\Delta_n(a, b)} > a^n > q^{2n} \geq 2q^{2n-1}.$$

Hence $h_n(a, b) > 2n - 1$. □

Notice that in this case, since $n \geq 1$, we always have $h > 1$ when $\pi \geq 3$.

To illustrate further the importance of the existence of QRCs, we consider the case of $\pi < 3$. We need only look at those d-values such that $d \equiv 5 \pmod 8$; for, otherwise, either $\Delta = 4d$ or $\Delta \equiv 1 \pmod 8$ and $\{2\}$ is a QRC in either case. If $\pi = 1$, then it is easy to show that $d = (2n + 1)^2 + 4$; if $\pi = 2$, then $d = a^2(2n + 1)^2 + 4a$, where a (> 1) is odd and squarefree. But, by Theorem 4.3 of Louboutin, Mollin, and Williams [5], we see that for any prime value of a or $a = 1$, we can *never* have a QRC for $\mathbf{K}_n = \mathbf{Q}(\sqrt{a^2(2n + 1)^2 + 4a})$.

Also, we have seen that in the case of Shanks's sequence S_n, we can very easily show that $h_n > 1$ for $n \geq 6$ when S_n is squarefree. That is, we have a simple, parametric family of fields for which we know all the squarefree members with $h = 1$. There are many cases of parametric families of fields for which this is very difficult to determine. Consider, for example, $d_n = (2n + 1)^2 + 4$. By using results of Kim, Leu, and Ono [3], we can only assert that we know all the values of n $(0, 1, 2, 3, 6, 8)$ such that $h = 1$ for this family, with the possible exception of one other value. The existence of this other value n, however, would violate the Extended Riemann Hypothesis. Many other results

of this type can be found in Mollin and Williams [7], and this same kind of analysis can be used on our $\mathbf{K}_n(a, b)$ fields.

We make use of the analytic class number formula

$$2hR = \sqrt{\Delta}L(1, \chi), \tag{3.3}$$

where

$$L(1, \chi) = \lim_{s \to 1} L(s, \chi), \qquad L(s, \chi) = \sum_{n=1}^{\infty} \left(\frac{\Delta}{n}\right) n^{-s},$$

and $(\cdot/n)$ is the Kronecker symbol. By Tatuzawa [12], we know that, if $0 < \eta < \frac{1}{2}$ and $\Delta > \max\{e^{11 \cdot 2}, e^{1/\eta}\}$, then

$$L(1, \chi) > .655\eta\Delta^{-\eta}$$

with at most one exceptional value of Δ possible. In fact, Tatuzawa knew that the existence of this exceptional value of Δ would violate the Riemann Hypothesis on $L(s, \chi)$.

We can now prove

Theorem 3.3. *Let a, b be fixed. If $\Delta_n(a, b) > B > 73131$, then*

$$h_n(a, b) > .24\sqrt{B}/(\log B)^3 \qquad (n \geq 2)$$

with at most one exceptional value of n possible.

Proof. Put $\eta = 1/\log B$. Since $\Delta_n(a, b) > \max\{e^{11 \cdot 2}, e^{1/\eta}\}$, we get

$$L(1, \chi) > .655\eta\Delta_n^{-\eta}(a, b)$$

with one possible exceptional value of $\Delta_n(a, b)$. Now by (3.3) we have

$$h > .655\sqrt{\Delta_n(a, b)}\eta\Delta_n^{-\eta}(a, b)/(2R). \tag{3.4}$$

Also, by (3.1) it is easy to see that the regulator R of $\mathbf{K}_n(a, b)$ satisfies

$$R < (n+1)\log\sqrt{\Delta_n(a, b)}. \tag{3.5}$$

Since

$$\sqrt{\Delta_n(a, b)} > ba^n \geq a^n,$$

and $a \geq 2$, we get

$$n < \log\sqrt{\Delta_n(a, b)}/\log a < \log\Delta_n(a, b) - 1.$$

Hence, by (3.4) and (3.5),

$$\begin{aligned} h_n(a, b) &> \frac{.655\eta(\Delta_n(a, b))^{1/2-\eta}}{(\log\Delta_n(a, b))^2} > \frac{.655\eta B^{1/2-\eta}}{(\log B)^2} \\ &= \frac{.655\sqrt{B}}{e(\log B)^3} > \frac{.24\sqrt{B}}{(\log B)^3}. \quad \square \end{aligned}$$

The result of Theorem 3.3 is certainly better than that of Corollary 3.2.1, but it is a conditional result only and depends upon deep analytic results. Corollary 3.2.1, on the other hand, is not conditional (given a certain $\mathscr{C}_l(a, b)$) and is elementary. As an example, we point out that for S_n we have a cover

$C_7(2, 1) = \{127\}$ and $h_n > (n-1)/7$. Thus, if $n \geq 70001$, we know that $h_n > 10000$ unconditionally. By Theorem 3.3 we would get $h_n > 10000$ for $n \geq 32$, with one possible exception. In §5 we will show how to use the computer to narrow this gap between 70001 and 32.

4. A SEARCH TECHNIQUE FOR QRCs AND NUMERICAL RESULTS

We first point out that if we are attempting to find a $\mathscr{C}_l(a, b)$ for $\mathbf{K}_n(a, b)$, we may assume that $b^2 \leq a - 1$. This follows from

Theorem 4.1. *If $\mathscr{C}$ is an l-QRC for the fields $\mathbf{K}_n(a, b)$, then it is also an l-QRL for the fields $\mathbf{K}_n(a, (a-1)/b)$.*

Proof. Put $\Delta'_n(a, b) = \Delta(a, (a-1)/b)$, so that

$$a^{-2n}\Delta'_n(a, b) = (ba^{-n} + (a-1)/b)^2 + 4a^{-n}.$$

Putting $m \equiv -n \pmod{l}$, $m \geq 0$, we get

$$a^{-2n}\Delta'_n(a, b) \equiv \Delta_m(a, b) \pmod{q}$$

for any $q \in \mathscr{C}$. Since $(\Delta_m(a, b)/q') \neq -1$ for some $q' \in \mathscr{C}$, we get $(\Delta'_n/q') \neq -1$. □

While we are not able to provide a proof that for some l a $\mathscr{C}_l(a, b)$ always exists for $\mathbf{K}_n(a, b)$, we can provide a simple heuristic reason for believing that this is the case. Let $d(m)$ denote the number of divisors of m, and let $\mathscr{N}_k$ denote the set $\{0, 1, 2, 3, \ldots, k-1\}$. It is a well-known result of Sylvester that if $\mathscr{Q}_k$ is the set of distinct prime factors of $a^k - 1$, then $|\mathscr{Q}_k| \geq d(k) - 1$. Also, if $q \in \mathscr{Q}_k$, the distinct values for $\Delta_n(a, b)$ modulo q can occur only for $n \in \mathscr{N}_k$. Now for any prime $q \in \mathscr{Q}_k$, it seems reasonable to assume that the probability that $(\Delta_n(a, b)/q) \neq -1$ is about $\frac{1}{2}$. Thus, we would expect that if $\nu_k = |\mathscr{Q}_k|$ and 2^{ν_k} is much larger than k $(= |\mathscr{N}_k|)$, then $\mathscr{Q}_k$ is likely to be a possibility for $\mathscr{C}_l(a, b)$ with $l = k$. Notice that if $k = 2^\mu\kappa$, where κ is an odd prime, we have $d(k) = 2\mu + 2$. In this case, the ratio

$$2^{\nu_k}/k \geq 2^{2\mu+2-1}/2^\mu\kappa = 2^{\mu+1}/\kappa.$$

Thus, if $\kappa = 3$ (say), we would not expect to have a large value for μ before we found a $\mathscr{C}_l(a, b)$ with $l = 3 \cdot 2^\mu$. In fact, in a preliminary computer run we found that for all prime values of $a \leq 200$, there exists a $\mathscr{C}_l(a, b)$ for each b which divides $a - 1$ with $l = 2^\mu$ or $3 \cdot 2^\mu$ and $\mu \leq 4$. Also, for these covers the maximum value of $|\mathscr{C}_l(a, b)|$ is 6.

Encouraged by the success of this preliminary run, we ran a second program which attempted to find covers $\mathscr{C}_l(a, b)$ with smaller l values. For a given pair (a, b) and a value of k, the program first determined $\mathscr{Q}_k$ and $\mathscr{N}_k$. For each prime $q \in \mathscr{Q}_k$ the values of m such that $(\Delta_m(a, b)/q) \neq -1$ were determined and deleted from those in $\mathscr{N}_k$. When a q-value caused elements to be deleted from $\mathscr{N}_k$, it was added to a set $\mathscr{C}_k$, previously initialized to $\varnothing$. If, at some point, $\mathscr{N}_k = \varnothing$, then $\mathscr{C}_k$ is a k-QRC for $\mathbf{K}_n(a, b)$. The program attempted to find k-QRCs for $k = 1, 2^i, 2^i\kappa$, where κ is an odd prime. For values of k of the form 2^i or $2^i\kappa$, the program would initialize k to either 2 or κ and then continue to double k until either a cover was found or $|\mathscr{C}_k| > 8$. This value of 8 was chosen in order to terminate what might otherwise be a long and

TABLE 4.1

l	Number of Covers
1	6582
2	1988
3	403
5	226
6	187
7	56
10	51
11	12
12	28
13	3
14	2
17	2
19	1
20	2
22	1
	total 9544

likely fruitless attempt to find a cover with a small value of l. Our previous experience indicated that if an l-QRC exists for $\mathbf{K}_n(a, b)$, then $|\mathscr{C}_l(a, b)|$ tends to be small. The smallest value of k of the forms mentioned above such that $\mathscr{C}_k$ is a cover was recorded, and then the program tried to reduce the number of elements in $\mathscr{C}_k$ by testing every possible subset of it in order to find one with the minimal number of elements which was still a cover. This minimal cover was used for $\mathscr{C}_l(a, b)$.

The program was written in MAPLE and tested on $\Delta_n(a, b)$ for all prime values of a such that $2 \leq a \leq 10{,}000$ and all values of b such that $b \mid a-1$, $b \geq 1$, $b^2 \leq a-1$. No attempt was made to eliminate values of $\Delta_n(a, b)$ which have square factors. In under a week of run time in background on a SUN-4 computer, a cover was found for $\mathbf{K}_n(a, b)$ for every possible pair (a, b) under consideration. Curiously, the largest value of l which was found is 22 for

$$\mathscr{C}_{22}(7, 1) = \{23, 1123, 293459, 10746341\}.$$

In Table 4.1 we give the number of covers found for the various values of l recorded by the program.
The largest value of $|\mathscr{C}_l(a, b)|$ found in our run is 5 for

$$\mathscr{C}_{12}(4253, 4) = \{5, 7, 13, 31, 769\}.$$

The largest element in any of our covers is

$$q = 8915483434116700294079244744 1$$

TABLE 4.2

l	Number of Covers
1	5628
2	2032
3	692
5	459
6	332
7	136
10	139
11	29
12	73
13	6
14	6
17	3
19	1
20	5
22	2
28	1
	total 9544

in $\mathscr{C}_{11}(1873, 1) = \{67, 89, q\}$. One of the more interesting covers is that for $l = 19$; this is

$$\mathscr{C}_{19}(43, 6) = \{229, 4219, 46399, 2137444528747943\}.$$

The remarkable feature of this run is that a cover was always found, and found for a relatively small value of l. Furthermore, there was no tendency for the value of l to increase with increasing values of a (as one would tend to expect by our heuristic). Indeed, some of the covers with large l-value such as

$$\mathscr{C}_{20}(5, 1), \mathscr{C}_{22}(7, 1), \mathscr{C}_{13}(17, 2), \mathscr{C}_{17}(43, 3), \mathscr{C}_{19}(43, 6)$$

occurred when a is relatively small.

In view of Corollary 3.2.1 it is also of some interest to investigate the possible existence of *strict* QRCs or SQRCs. These are quadratic residue covers $\mathscr{C}(a, b)$ such that for any $n \geq 0$ there must exist some $p \in \mathscr{C}(a, b)$ for which $(\Delta_n(a, b)/p) = 1$. The argument used above also suggests that an l-SQRC should always exist for any $\mathbf{K}_n(a, b)$. We modified our program to search for l-SQRCs for $\mathbf{K}_n(a, b)$ for a, b in the same range as before. In under two weeks of background run time we found an l-SQRC for every possible pair (a, b) in our range. Once again the l-values did not get very large, the largest being 28 for $\mathscr{C}_{28}(3, 1)$. We summarize these results in Table 4.2. The largest value for $|\mathscr{C}_l(a, b)|$ in this run is once again 5, but it occurred for 5 different covers. Also, as observed earlier, there was no tendency for l to increase with increasing values of a.

Given these phenomena and our heuristic, it does not seem unreasonable to make the following

Conjecture. *For any prime value of* a *and any* b *such that* $b \mid a-1$ *and* $b \geq 1$, *there always exists for some* l *an* l*-QRC for* $\mathbf{K}_n(a, b)$.

We have already found all of the squarefree elements of Shanks's sequence S_n for which $h_n = 1$. We can now go somewhat further, as we can bound from below the value of $h_n(a, b)$. In fact, we can easily establish the following result.

Theorem 4.2. *If* d *is a positive squarefree integer such that all the reduced principal ideals in* $\mathbf{Q}(\sqrt{d})$ *have norms which are powers of an odd prime* $p > 2$, $\pi \geq 3$, *and* $h = 1$, *then*

$$d \in \{37, 61, 157, 397, 7213\} \quad \text{when } p = 3,$$
$$d \in \{101, 461, 941\} \quad \text{when } p = 5,$$
$$d \in \{197, 317, 557, 1877\} \quad \text{when } p = 7,$$
$$d \in \{773\} \quad \text{when } p = 11.$$

Proof. By using the l-values determined by our program and the bound of Corollary 3.2.1, we can easily establish an upper bound on d for h to be 1. Most of the d-values below this bound can be easily eliminated by finding a small prime q such that $q \neq p$, $q < \sqrt{d}/2$, and $(d/q) = 0, 1$. The few remaining numbers can be tested by evaluating h for $\mathbf{Q}(\sqrt{d})$. □

5. A REFINEMENT

As pointed out in §3, the result of Corollary 3.2.1 gives us an unconditional lower bound on $h_n(a, b)$, but the bound is not a very good one. In this section we will discuss a method by which this bound can be improved. Our technique is elementary, unconditional, and can easily be implemented on a computer.

Suppose that we have a set of primes $\mathbf{P} = \{p_1, p_2, \ldots, p_k\}$ such that if $p_i \in \mathbf{P}$, then $p_i \leq \sqrt{\Delta}/2$ and $(\Delta/p_i) = 1$. Consider the set $\mathbf{N}$ made up of integers $n \leq \sqrt{\Delta}/2$ such that each distinct prime divisor of n is in $\mathbf{P}$. We can prove

Theorem 5.1. *If* d *is a positive squarefree integer,* $\mathbf{K} = \mathbf{Q}(\sqrt{d})$, h *is the class number, and* R *is the regulator of* $\mathbf{K}$, *then*

$$\frac{Rh}{\log \phi} > |N| \geq \frac{1}{k!} \prod_{i=1}^{k} \frac{\log(\sqrt{\Delta}/2)}{\log p_i}.$$

Proof. By (2.1) we know that $Rh/\log\phi > C$, where C is the total number of reduced ideals in $\mathbf{K}$. If $p_i \in \mathbf{P}$, then $(p_i) = \mathbf{p}_{1i}\mathbf{p}_{2i}$. Let $\mathbf{p}_i$ be either of these. If

$$r = \prod_{i=1}^{k} \mathbf{p}_i^{b_i},$$

then $\mathbf{r}$ is reduced if $N(\mathbf{r}) < \sqrt{\Delta}/2$. This occurs when $\sum_{i=1}^{k} b_i \log p_i < \log(\sqrt{\Delta}/2)$.

If $B, w_1, w_2, w_3, \ldots, w_k \in \mathbf{R}^+$, $\vec{w} = (w_1, w_2, \ldots, w_k)$ and

$$\mathscr{T}_k(B) = \{\vec{x} \mid \vec{x} \in (\mathbf{Z}^{\geq 0})^k, \vec{x} \cdot \vec{w} < B\},$$

then by a result of Lehmer [4] (see also Rosser [10]) we have

$$|\mathscr{T}_R(B)| > (B^k + kW_kB/2^{k-1})/(k!V_k), \tag{5.1}$$

where $W_k = \sum_{i=1}^{k} w_i$, $V_k = \prod_{i=1}^{k} w_i$. If $B = \log(\sqrt{\Delta}/2)$ and $w_i = \log p_i$ $(i = 1, 2, \ldots, k)$, then $C \geq |N| = |\mathscr{T}_k(B)| > B^k/(k!V_k)$, and our result follows. □

We can improve Theorem 5.1 by considering

$$\mathbf{r} = \prod_{i=1}^{k} \mathbf{p}_i^{e_i} \mathbf{p}_i^{f_i},$$

where $e_i f_i = 0$ and $e_i, f_i \geq 0$ $(i = 1, 2, 3, \ldots, k)$. If

$$N(\mathbf{r}) = \prod_{i=1}^{k} p^{e_i + f_i} < \sqrt{\Delta}/2,$$

then $\mathbf{r}$ is a reduced ideal of $\mathbf{O}_k$. Thus, there are at least as many distinct reduced ideals as there are sets of pairs (e_i, f_i) $(i = 1, 2, \ldots, k)$ such that

(1) $\sum_{i=1}^{k} (e_i + f_i) \log p_i \leq \log(\sqrt{\Delta}/2)$,
(2) $e_i f_i = 0$,
(3) $e_i + f_i \geq 0$.

Define the set

$$\mathscr{S}_k(B) = \{\vec{\mathbf{x}} \mid \vec{\mathbf{x}} \in (\mathbf{Z}^{\geq 1})^k, \vec{x} \cdot \vec{w} < B\}.$$

If $\vec{\mathbf{x}} \in \mathscr{S}_k(B)$, then

$$\vec{x} - \vec{1} \in \mathscr{T}(B - W_k) \quad (\vec{1} = (1, 1, 1, \ldots, 1)).$$

Hence,

$$|\mathscr{S}_k(B)| \geq |\mathscr{T}_k(B - W_k)|.$$

Let $\vec{x} = (e_1 + f_1, e_2 + f_2, \ldots, e_k + f_k)$, where e_i and f_i $(i = 1, 2, \ldots, k)$ satisfy (1) and (2) above and $e_i + f_i \geq 1$. If $B = \log(\sqrt{\Delta}/2)$, then $\vec{x} \in \mathscr{S}_k(B)$. Thus, the total number of sets of pairs (e_i, f_i) $(i = 1, 2, \ldots, k)$ satisfying (1), (2) and $e_i + f_i \geq 1$ is given by $2^k |\mathscr{S}_k(B)|$. If we were to allow the jth component of $\vec{x}$ to be such that $e_j + f_j = 0$, then the number of sets of pairs (e_i, f_i) $(i = 1, 2, \ldots, k)$ satisfying (1), (2) and $e_i + f_i \geq 1$ $(i \neq j)$, $e_j = f_j = 0$, is given by

$$2^{k-1} |\mathscr{T}_{k-1}(B - (W_k - w_j))|.$$

It follows that the total number of sets of pairs (e_i, f_i) $(i = 1, 2, \ldots, k)$ satisfying (1), (2), and (3) must exceed

$$2^k |\mathscr{T}_k(B - W_k)| + 2^{k-1} \sum_{j=1}^{k} |\mathscr{T}_{r-1}(B - (W_k - w_j))|$$

$$> \frac{2^k}{k!V_k} (B - W_k)^{k-1} (B + (k-1)W_k)$$

by (5.1).

We have shown, then, that

$$C > \frac{2^k}{k!V_k} (B - W_k)^{k-1} (B + (k-1)W_k).$$

Thus, by using (2.1), we can prove

Theorem 5.2. *Let d be a squarefree positive integer, $\mathbf{K} = \mathbf{Q}(\sqrt{d})$, h be the class number of $\mathbf{K}$, and R be the regulator of $\mathbf{K}$. If $p_1, p_2, \ldots, p_k$ are distinct primes such that the Kronecker symbol $(\Delta/p_i) = 1$ $(i = 1, 2, \ldots, k)$, then*

$$h > \frac{2^k \log \phi}{k! V_k R}(B - W_k)^{k-1}(B + (k-1)W_k),$$

where

$$B = \log(\sqrt{\Delta}/2), \quad V_k = \prod_{i=1}^{k} \log p_i, \quad W_k = \sum_{i=1}^{k} \log p_i. \quad \square$$

We will now apply this result to our fields $\mathbf{K}_n(a, b)$. By (3.2) we get

$$\sqrt{\Delta_n(a, b)} < (b^2 a^n + a + 1)/b < a^{n+1};$$

thus, from (3.5) we find that

$$R < (n+1)^2 \log a. \tag{5.2}$$

Also,

$$\log(\sqrt{\Delta}/2) > n \log a + \log b - \log 2 \geq (n-1) \log a.$$

Hence, by Theorem 5.2 we have

$$h_n(a, b) > \frac{2^k \log \phi}{k! V_k (n+1)^2 \log a}((n-1)\log a - W_k)^{k-1}((n-1)\log a + (k-1)W_k).$$

Since, for $a > x > y > 0$, we get

$$(a-y)^n(a+ny) > (a-x)^n(a+nx),$$

we see that if we have values A, B such that $W_k \leq A$, $V_k \leq B$, then

$$h_n(a, b) > \frac{2^k \log \phi}{k! B (n+1)^2 \log a}((n-1)\log a - A)^{k-1}((n-1)\log a + (k-1)A). \tag{5.3}$$

We now illustrate how (5.3) can be used to improve a bound given by Theorem 3.1. As we mentioned in §3, $h_n = h_n(2, 1) > 10000$ for $n \geq 70001$. By a simple computer search it is easy to establish that for each n such that $0 \leq n \leq 70000$, there exist 6 distinct primes ≤ 163 such that $(S_n/p) = 1$ for any of these 6 primes p. Since we know that $(S_n/2) = (S_n/127) = 1$, we may assume that $k = 6$,

$$A = \log(2 \cdot 127 \cdot 149 \cdot 151 \cdot 157 \cdot 163),$$

$$B = \log 2 \log 127 \log 149 \log 151 \log 157 \log 163.$$

Thus, by (5.3), we find that $h_n > 10000$ for $n \geq 257$. Now for each n such that $0 \leq n \leq 256$, there exist 8 distinct primes ≤ 131 such that $(S_n/p) = 1$ for any of these 8 primes; thus, we can put $k = 8$,

$$A = \log(2 \cdot 101 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 127 \cdot 131),$$

$$B = \log 2 \log 101 \log 103 \log 107 \log 109 \log 113 \log 127 \log 131,$$

and we get from (5.3) $h_n > 10000$ for $n \geq 145$, a considerable improvement over the 70001 bound given in §3.

6. Acknowledgments

The authors gratefully acknowledge the assistance provided by Mike Jacobson in obtaining the computer results in this paper. They would also like to thank an anonymous referee for several valuable suggestions for improving this paper.

BIBLIOGRAPHY

1. H. Cohn, *A second course in number theory*, Wiley, New York, 1962.
2. F. Halter-Koch, *Einige periodische Kettenbruchentwicklungen und Grundeinheiten quadratischer Ordnungen*, Abh. Math. Sem. Univ. Hamburg **59** (1989), 157–169.
3. H. K. Kim, M.-G. Leu, and T. Ono, *On two conjectures on real quadratic fields*, Proc. Japan Acad. Ser. A Math. Sci. **63** (1987), 222–224.
4. D. H. Lehmer, *The lattice points of an n-dimensional tetrahedron*, Duke Math. J. **7** (1940), 341–353.
5. S. Louboutin, R. A. Mollin, and H. C. Williams, *Class numbers of real quadratic fields, continued fractions, reduced ideals, prime producing quadratic polynomials and quadratic covers*, Canad. J. Math. **44** (1992), 824–842.
6. R. A. Mollin, *Powers in continued fractions and class numbers of real quadratic fields*, Utilitas Math. **42** (1992), 25–30.
7. R. A. Mollin and H. C. Williams, *On a determination of real quadratic fields of class number one and related continued fraction period length less than* 25, Proc. Japan Acad. Ser. A Math. Sci. **67** (1991), 20–25.
8. ———, *Affirmative solution of a conjecture related to a sequence of Shanks*, Proc. Japan Acad. Ser. A Math. Sci. **67** (1991), 70–72.
9. A. S. Pen and B. F. Skubenko, *Estimation from above of the period of a quadratic irrationality*, Math. Notes Acad. Sci. USSR **5** (1969), 247–250.
10. B. Rosser, *On the first case of Fermat's last theorem*, Bull. Amer. Math. Soc. **45** (1939), 636–640.
11. D. Shanks, *On Gauss's class number problems*, Math. Comp. **23** (1969), 151–163.
12. T. Tatuzawa, *On a theorem of Siegel*, Japan J. Math. **21** (1951), 163-178.
13. H. C. Williams and M. C. Wunderlich, *On the parallel generation of the residues for the continued fraction factoring algorithm*, Math. Comp. **48** (1987), 405–423.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF CALGARY, CALGARY, ALBERTA, CANADA T2N 1N4

E-mail address: ramollin@acs.ucalgary.ca

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF MANITOBA, WINNIPEG, MANITOBA, CANADA R3T 2N2

E-mail address: Hugh_Williams@csmail.cs.umanitoba.ca