

A LOWER BOUND FOR THE CLASS NUMBER OF A REAL QUADRATIC FIELD OF ERD-TYPE

R. A. MOLLIN, L.-C. ZHANG AND PAULA KEMP

ABSTRACT. In this paper, we use the Lagrange neighbour and our equivalence theorem for primitive ideals to obtain lower bounds which are sharper than those given in the literature for class numbers of real quadratic fields $Q(\sqrt{d})$ in general, but applied to greatest advantage when d is of ERD type.

1. Notation and preliminaries. Throughout the paper d is a positive square-free integer, $K = Q(\sqrt{d})$, $h(d)$ is the class number of K and τ is the divisor function.

The Z -module $\{\alpha x + \beta y : x, y \in Z\}$ is denoted by $[\alpha, \beta]$. Therefore, the maximal order (or the ring of algebraic integers) O_K of K is $[1, \omega]$ where we define ω as $\omega = (\sigma - 1 + \sqrt{d})/\sigma$ and $\sigma = 1$ if $d \equiv 2, 3 \pmod{4}$, $\sigma = 2$ if $d \equiv 1 \pmod{4}$. Moreover, the discriminant of K is then $\Delta = (\omega - \bar{\omega})^2$ where $\bar{\omega}$ is the algebraic conjugate of ω . The norm of $\alpha \in K$ is $N(\alpha) = \alpha\bar{\alpha}$.

It is well-known (cf. [12]) that I is an ideal of O_K if and only if I has a representation as $I = [a, b + c\omega]$ where $a > 0$, $b > 0$, $c \mid b$, $c \mid a$ and $ac \mid N(b + c\omega)$. In fact, for a given I , the integers c and a are uniquely determined, where a is the least positive integer in I . If $c = 1$, the ideal I is called *primitive* and moreover, in this case $a = N(I) =$ norm of I . An ideal I is said to be *reduced* if I is primitive and there does not exist a non-zero element α in I with both $|\alpha| < N(I)$ and $|\bar{\alpha}| < N(I)$.

It has recently been proved (see [1] and [3]) that if $d = a^2 + 1$ where a is an odd integer greater than one, then

$$(1.1) \quad h(d) \geq 2\tau(a) - 2.$$

This is a sharp bound for some d . For example, $h(82) = 4 = 2\tau(9) - 2$. On the other hand, this bound is not very good for other d 's. In particular, if $d = q^2 + 1$, where q is an odd prime, then $2\tau(q) - 2 = 2$, and the bound becomes trivial.

Moreover, from the genus theory of Gauss, one can see that

$$(1.2) \quad h(d) \geq 2^{s-1},$$

where s is the number of distinct prime divisors of d , excluding one prime congruent to 3 modulo 4 (if such primes divide d). However when $d = a^2 + 1 = 2p$, where $p \equiv 1 \pmod{4}$ is a prime, then (1.2) only gives a trivial bound $h(d) \geq 2^{s-1} = 2$.

Received by the editors May 14, 1992; revised April 7, 1993 and October 12, 1993.

AMS subject classification: 11R11, 11R09, 11R29.

Key words and phrases: class number, primitive ideal, divisor function, Lagrange neighbour, ERD-type, quadratic fields.

© Canadian Mathematical Society 1994.

Also in [1] and [3] it is shown that if $d = a^2 + 4$, $a > 1$, and a odd, then

$$(1.3) \quad h(d) \geq \tau(a) - 1.$$

Again this bound is sharp for some d . For example $h(229) = 3 = \tau(15) - 1$. On the other hand, if $d = q^2 + 4$, where q is an odd prime then $\tau(q) - 1 = 1$ gives the trivial bound.

The forms of d above are special cases of more general forms called *Extended Richard-Degert-types* (or simply ERD-types); i.e., those of the form $d = a^2 + r$ where $r \mid 4a$. In this paper, our general bounds for class numbers of real quadratic fields are best applied to ERD-types and give better bounds than those in (1.1)–(1.3) above, as well as those in [2] and elsewhere.

First, for completeness we state the following theorem which is proved by Mollin and Zhang in [11].

THEOREM 1.1. *If $I_1 = [a_1, b_1 + \omega]$ and $I_2 = [a_2, b_2 + \omega]$ are primitive ideals in $O_K = [1, \omega]$, then I_1 is equivalent to I_2 if and only if there exist coprime rational integers x, y satisfying the following three conditions:*

$$(1.4) \quad |(\sigma a_1 x + (\sigma b_1 + \sigma - 1)y)^2 - dy^2| = \sigma^2 a_1 a_2$$

$$(1.5) \quad a_2 \mid (a_1 x + (b_1 + b_2 + \sigma - 1)y)$$

$$(1.6) \quad \sigma^2 a_1 a_2 \mid (\sigma^2 a_2 (b_2 - b_1)x + (d - (\sigma b_1 + \sigma - 1)^2)y).$$

We also remind the reader of the following from [11].

DEFINITION 1.1. *If $I = [a, b + \omega]$ is a primitive ideal in O_K , then the *Lagrange neighbour* $I^+ = [a^+, b^+ + \omega]$ is defined by $b^+ = -b + a \lfloor (b + \omega)/a \rfloor$ and $a^+ = -N(b^+ + \omega)/a$, where $\lfloor \cdot \rfloor$ denotes the greatest integer function.*

2. Main results. We first need some preliminary results.

LEMMA 2.1. *Let $I = [m, b + \omega]$ be a primitive ideal in O_K with $1 < m < -N(b + \omega)$ and $|b| < (\sqrt{\Delta} - \sigma + 1)/2$. If $N(b + \omega)$ has no proper divisor $c > 1$ which is a norm of a principal reduced ideal in O_K then I is not principal. In fact, $I \sim I^+$ and I^+ is reduced and not principal.*

PROOF. If I is reduced then I cannot be principal since m divides $N(b + \omega)$. Therefore, we may assume that I is not reduced; whence, $m > \sqrt{\Delta}/2$ by Corollary 4.2 of [11].

CLAIM. $\lfloor (b + \omega)/m \rfloor = 0$.

If $b < 0$ then $\lfloor (b + \omega)/m \rfloor \leq (b + \omega)/m \leq (\omega - 1)/m < 1$. If $b \geq 0$ and $m < \sqrt{\Delta}$ then the fact that $b < (\sqrt{\Delta} - \sigma + 1)/2$ allows us to invoke Corollary 4.3 of [11] which says that $m - \omega > b$; i.e., $\sigma m - \sigma + 1 - \sqrt{d} > \sigma b$ from which it follows that $1 > (\sigma b + \sigma - 1 + \sqrt{d})/\sigma m = (b + \omega)/m$. If $b \geq 0$ and $m > \sqrt{\Delta}$, then in order that

$b + \omega \geq m > \sqrt{\Delta}$ we must have $b > (\sqrt{\Delta} - \sigma + 1)/2$, a contradiction which secures the claim.

We may now display the Lagrange neighbour I^+ of I explicitly as $I^+ = [-N(b + \omega)/m, -b + \omega]$ which is reduced since $1 < -N(b + \omega)/m < \sqrt{\Delta}/2$. Thus $I^+ \not\sim (1)$ since $-N(b + \omega)/m$ is a proper divisor of $N(b + \omega)$. Since $I^+ \sim I$, this secures the result. ■

We now turn to consequences of Lemma 2.1 for ERD-types (defined below).

DEFINITION 2.1. $d = a^2 + r$ is said to be of *Extended Richaud-Degert type* (or ERD-type) if $r \mid 4a$.

DEFINITION 2.2. Let $d = a^2 + r$ and set

$$A = \begin{cases} 2a + r - 1 & \text{if } \sigma = 1 \text{ and } r < 0, \\ a/2 + (r - 1)/4 & \text{if } \sigma = 2 \text{ and } r \text{ is odd,} \\ a + r/4 - 1 & \text{if } \sigma = 2 \text{ and } r < 0 \text{ is even,} \\ 1 & \text{otherwise,} \end{cases}$$

$$B = \begin{cases} |r|/\sigma^2 & \text{if } \sigma = 2 \text{ and } r \text{ is even,} \\ |r| & \text{otherwise,} \end{cases}$$

and

$$C = \begin{cases} a/2 - (r - 1)/4 & \text{if } \sigma = 2 \text{ and } r > 0 \text{ is odd,} \\ 1 & \text{otherwise,} \end{cases}$$

and let

$$S = \{n > 1 \text{ integer} \mid n = A, B \text{ or } C\}.$$

COROLLARY 2.1. Let $d = a^2 + r$ where $r \mid 4a$ and $|r| < 2a$. Moreover, let $I = [m, b + \omega]$ be a primitive ideal in O_K with $1 < m < -N(b + \omega)$ and $|b| < (\sqrt{\Delta} - \sigma + 1)/2$. If no proper divisor $n > 1$ of $N(b + \omega)$ is in the set S then I is not principal.

PROOF. We need only look at a list of continued fraction expansions of ω for each ERD-type (which we have given in the proof of Corollary 3.3. of [11]) to see that the only possible norms of principal reduced ideals are those in S (together with 1). By Lemma 2.1, the result follows. ■

EXAMPLE 2.1. Let $d = 226 = 15^2 + 1 = 2 \cdot 113$ and $I = [63, 10 + \sqrt{226}]$ with $1 < m = 63 < -N(10 + \sqrt{226}) = 126$. Then $I \sim I^+ = [2, -10 + \sqrt{226}] = [2, \sqrt{226}]$, I^+ is clearly reduced and I^+ is not principal since the continued fraction expansion of $\omega = \sqrt{226}$ has period 1 and (1) is the only principal reduced ideal. On the other hand, $J = [63, 17 + \sqrt{226}] = (17 + \sqrt{226})$ is a principal ideal with norm = 63 which is a proper divisor of $N(10 + \sqrt{226})$. Note that S is vacuous.

LEMMA 2.2. If $[ca_1, b + \omega] \sim [ca_2, b + \omega]$ are primitive ideals in O_K , then $[a_1, b + \omega] \sim [a_2, b + \omega]$.

PROOF. Since $[ca_1, b + \omega] \sim [ca_2, b + \omega]$, by Theorem 1.1 there exist coprime integers x and y satisfying the conditions

$$(2.1) \quad |(\sigma ca_1 x + (\sigma b + \sigma - 1)y)^2 - dy^2| = \sigma^2 c^2 a_1 a_2$$

$$(2.2) \quad ca_2 \mid (ca_1x + (2b + \sigma - 1)y)$$

$$(2.3) \quad \sigma^2c^2a_1a_2 \mid (d - (\sigma b + \sigma - 1)^2)y.$$

From (2.2) we get that

$$(2.4) \quad c \mid (2b + \sigma - 1)y.$$

CLAIM. $c \mid y$.

If there is a power of a prime, p^e , dividing c but not dividing y , then from (2.3) $p^2 \mid d - (\sigma b + \sigma - 1)^2$. If $p = 2$ then clearly $\sigma = 2$ and so by (2.4) $2 \mid (2b + \sigma - 1)$, a contradiction. Hence $p > 2$ and from (2.2) we get that $p^2 \mid (\sigma b + \sigma - 1)^2$; whence, $p^2 \mid d$, contradicting that d is square-free. Therefore the claim is established.

Now we set $y' = y/c$ and so from (2.1)–(2.3) we get

$$\begin{aligned} |(\sigma a_1x + (\sigma b + \sigma - 1)y')^2 - dy'^2| &= \sigma^2a_1a_2 \\ a_2 \mid (a_1x + (2b + \sigma - 1)y') \\ \sigma^2a_1a_2 \mid (d - (\sigma b + \sigma - 1)^2)y'. \end{aligned}$$

By Theorem 1.1 the result now follows. ■

DEFINITION 2.3. If $d = a^2 + r$ where $r \mid 4a$, then set

$$M = \begin{cases} 2(a - 1) & \text{if } r = -1 \\ 2a/\sigma^2 & \text{if } r = 1 \text{ and } d \neq 5, \\ a & \text{if } r = 4, \\ a - 2 & \text{if } r = -4, \\ 2(a - 2) & \text{if } r = -2a, \\ a/3 & \text{if } r = -4a/3, \\ a - 4 & \text{if } r = -4a, \\ |r|/\sigma^2 & \text{if } r \notin \{\pm 1, \pm 4, -2a, -4a/3, -4a\}. \end{cases}$$

DEFINITION 2.4. Let $t > 0$ be any integer and suppose that (u, v) is a rational integral solution of $x^2 - dy^2 = \pm\sigma^2t$. We say that (u, v) is a *trivial solution* when $t = m^2$ and m divides both u and v . Otherwise (u, v) is called *nontrivial*.

REMARK 2.1. For the sake of completeness, and in order to make the paper more self-contained we now generalize [4, Theorem 1.1, p. 41] from ordinary RD-types (*i.e.*, those $d = a^2 + r$ with $r \mid 4a$ and $-a < r \leq a$) to the more general ERD-types defined in Definition 2.1.

LEMMA 2.3. Let $d = a^2 + r$ be of ERD-type and let t be any positive integer. If $x^2 - dy^2 = \pm\sigma^2t$ has a nontrivial solution, then $t \geq M$ where M is defined in Definition 2.3.

PROOF. Upon examination of the proof of [4, Theorem 1.1, p. 41] we see that it holds for all $r \mid 4a$ except for $r \in \{-2a, -4a/3, -4a\}$. If $r = -2a$, then $d = a^2 - 2a = (a - 1)^2 - 1$, and we may invoke [4, *ibid.*] with $r = -2a$ replaced by $r = -1$ in which case M becomes $2(a - 2)$. If $r = -4a$ then $d = a^2 - 4a = (a - 2)^2 - 4$, and so we may invoke [4, *op. cit.*] with $r = -4a$ replaced by $r = -4$ in which case M becomes $a - 4$. If $r = -4a/3$ then by [4, Lemma 1.1, p. 40] we must have $t \geq a/3 - 4/9$ which secures the proof. ■

LEMMA 2.4. Let $d = a^2 + r$ with r dividing $4a$ and let $I_i = [a_i, b + \omega]$ for $i = 1, 2$ be two primitive ideals in O_K with $a_1 \neq a_2$. If $a_i = ga'_i$ for $i = 1, 2$ where $g = \gcd(a_1, a_2)$ and $1 < a'_1 a'_2 < M$ where M is given by Definition 2.3, then $I_1 \not\sim I_2$.

PROOF. Without loss of generality we may assume that $a'_2 > a'_1$. If $J_1 = [a'_1, b + \omega] \not\sim [a'_2, b + \omega] = J_2$ then it follows from Lemma 2.2 that $I_1 \not\sim I_2$ so we prove only the former. Assume that $J_1 \sim J_2$; then by Theorem 1.1 there exist coprime integers x and y such that

$$(2.5) \quad |(\sigma a'_1 x + (\sigma b + \sigma - 1)y)^2 - dy^2| = \sigma^2 a'_1 a'_2$$

$$(2.6) \quad a'_2 \mid (a'_1 x + (2b + \sigma - 1)y)$$

$$(2.7) \quad \sigma^2 a'_1 a'_2 \mid (d - (\sigma b + \sigma - 1)^2)y.$$

By Lemma 2.3, (2.5) is only possible if $a'_1 a'_2 = t^2$ for some t dividing both y and $\sigma a'_1 x + (\sigma b + \sigma - 1)y$; whence t divides both $\sigma a'_1 x$ and y . Since $\gcd(a'_1, a'_2) = 1$, set $a'_1 = t_1^2$ and $a'_2 = t_2^2$ with $\gcd(t_1, t_2) = 1$. From (2.6) we get

$$t_2^2 \mid (t_1^2 x + (2b + \sigma - 1)y);$$

whence, $t_2 \mid x$. However, $t_2 > 1$ and t_2 also divides y , a contradiction. ■

We are now in a position to prove the main result.

THEOREM 2.1. Let $d = a^2 + r$ with $r \mid 4a$ and set $-N(b + \omega) = mn$ where $|b| < (\sqrt{\Delta} - \sigma + 1)/2$ and $m < M$ (with M defined as in Definition 2.3). If mn has no proper divisor ℓ with $\ell \in \mathcal{S}$ (with \mathcal{S} defined as in Definition 2.2), then

$$h(d) \geq \max\{\tau(m), \tau(m) + d(n) - 1\}$$

where $d(n)$ denotes the number of prime (not necessarily distinct) divisors of n .

PROOF. Let $1 = a_1 < a_2 < \dots < a_t = m$ be all the divisors of m and set $t = \tau(m)$. By Lemma 2.3, $[a_i, b + \omega] \not\sim [a_j, b + \omega]$ for any $i \neq j$; whence, $h(d) \geq \tau(m)$. (Observe that since $m < M$, no proper divisor of m is in \mathcal{S}).

Let $n = p_1 \dots p_r$ (not necessarily distinct primes). Since no proper divisor of $-N(b + \omega) = mn$ is in \mathcal{S} , invoking Corollary 2.1 and Lemma 2.2 for $1 \leq i, j \leq r - 1 = d(n) - 1$, we find that $[mp_1 \dots p_i, b + \omega] \not\sim [mp_1 \dots p_j, b + \omega]$ and for $1 \leq i \leq t$, $1 \leq j \leq r - 1$, we find that $[mp_1 \dots p_j, b + \omega] \not\sim [a_i, b + \omega]$. Therefore, $h(d) \geq t + r - 1 = \tau(m) + d(n) - 1$. ■

REMARK 2.2. We note that in Theorem 2.1 the assumption that $N(b + \omega)$ has no proper divisor in \mathcal{S} is always satisfied for $d = a^2 + \sigma^2$, where a is odd, because \mathcal{S} is vacuous in that case.

REMARK 2.3. Theorem 2.1 actually shows that, for example, if $d = a^2 + r$ with $|r| \in \{1, 4\}$ and $h(d) = 1$, then all primes $p < M$ must be inert in K . This was shown in [7, Lemma 2.3, p. 148] where Mollin and Williams listed all such d 's with $h(d) = 1$ (under a suitable Riemann hypothesis). Later they were able to remove the Riemann

hypothesis assumption in [8] where they proved that the list is complete, with one possible exceptional value of d remaining whose existence would be a counterexample to the Riemann hypothesis. They extended these techniques in [9] where they listed all d 's with $h(d) = 1$ (with one possible exception) where $k \leq 24$ (k is the period length of the continued fraction expansion of ω (observe that $k \leq 4$ when d is of ERD-type)). Then in [10] Mollin and Williams concluded with some algebraic and computational advances which allowed them to effectively compute all d 's (with one possible exception) where $h(d) = 2$ and $k \leq 24$.

REMARK 2.4. Theorem 2.1 also shows that if $d \not\equiv 1 \pmod{4}$ is of ERD-type and $|r| > 2$ then $h(d) > 1$. This was proved in [5, Theorem 1, p. 162]. Also, if $d = a^2 + 1$ with a odd then $h(d) = 1$ if and only if $d = 2$. Moreover, if $d \equiv 1 \pmod{8}$ is of ERD-type then either $d = 33$ or $h(d) > 1$.

REMARK 2.5. We note that Theorem 2.1 gives better bounds than those found in [2]. For example, in [2] the bound for $h(d)$ where $d = 4097$ is given as $h(d) \geq 5$, whereas if we consider $-N(15 + \omega) = 2^4 \cdot 7^2$ and take $m = 2^4$ and $n = 7^2$ then $h(d) \geq 6$ is our bound from Theorem 2.1. Also for $d = (13^2)^2 - 4 = 28557$ the bound given in [2] is $h(d) \geq 3$. However, we note that $N(4 + \omega) = 3^2 \cdot 13 \cdot 61$ and taking $m = 3^2 \cdot 13$, $n = 61$, one can see that our bound is $h(d) \geq 6$. Similarly, we improve upon other bounds in [2].

To see that the bounds we found are better for some d than the bounds given in (1.1)–(1.3) and elsewhere, we provide the following examples.

EXAMPLE 2.2. Let $d = 170 = 13^2 + 1$. From (1.1), $h(170) \geq 2\tau(13) - 2 = 2$. By Theorem 2.1, choosing $b = 4$, $d - b^2 = 154 = 2 \cdot 7 \cdot 11$ and $m = 14$, we find that $h(170) \geq 4$. Actually, $h(170) = 4$.

EXAMPLE 2.3. Let $d = 442 = 21^2 + 1 = 2 \cdot 13 \cdot 17$. The bound from (1.1) is $2\tau(21) - 2 = 6$. The bound from (1.2) is $2^{3-1} = 4$. By Theorem 2.1, choosing $b = 8$, $d - b^2 = 378 = 2 \cdot 3^3 \cdot 7$, and $m = 2 \cdot 3^2$, we have $h(442) \geq 7$. Actually, $h(442) = 8$.

EXAMPLE 2.4. Let $d = 226 = 15^2 + 1 = 2 \cdot 113$. From (1.1), $h(226) \geq 2\tau(15) - 2 = 6$. The bound from (1.2) is clearly 2 because $s = 2$. By Theorem 2.1, choosing $b = 8$, $d - b^2 = 162 = 2 \cdot 3^4$ and $m = 18$ we have that $h(d) \geq 7$. In fact, $h(226) = 8$.

EXAMPLE 2.5. Let $d = 1373 = 37^2 + 4$. The bound from (1.3), is $\tau(37) - 1 = 1$. Noting that $-N(b + \omega) = 343 = 7^3$ where $b = 0$. Taking $m = 7$ and $n = 7^2$, by Theorem 2.1 we find that $h(1373) \geq 3$. Actually, $h(1373) = 3$.

EXAMPLE 2.6. Let $d = 3485 = 59^2 + 4$. The bound from (1.3) is $\tau(59) - 1 = 1$. However, $-N(b + \omega) = 715 = 5 \cdot 11 \cdot 13$ with $b = 12$. Taking $m = 5 \cdot 11 = 55$, by Theorem 2.1 we find that $h(3485) \geq 4$. Actually, $h(3485) = 4$.

EXAMPLE 2.7. Let $d = 2405 = 49^2 + 4$. The bound from (1.3) is $\tau(49) - 1 = 2$. However, $-N(b + \omega) = 595 = 5 \cdot 7 \cdot 17$, with $b = 2$. Taking $m = 5 \cdot 7 = 35$, by Theorem 2.1 we find that $h(2405) \geq 4$. Actually, $h(2405) = 4$.

EXAMPLE 2.8. Let $d = 25935 = 161^2 + 4$. The bound from (1.3) is $\tau(161) - 1 = 3$. Taking $N(\omega) = 25935 = 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19$ and $m = 3 \cdot 5 \cdot 7$ and $n = 13 \cdot 19$, we get $h(d) \geq 9$. Actually, $h(25935) = 16$.

EXAMPLE 2.9. Let $d = 14^2 + 7 = 203$. Then $-N(9 + \omega) = 2 \cdot 61$. Taking $m = 2$ and $n = 61$ we have $h(d) \geq \tau(m) + d(n) - 1 = 2$. In fact, $h(d) = 2$.

ACKNOWLEDGEMENTS. The first author's research is supported by NSERC Canada grant #A8484. Moreover, the authors wish to thank the referee for a suggestion which led to the paper being more self-contained.

REFERENCES

1. F. Halter-Koch, *Quadratische Ordnungen mit grosser Klassenzahl*, J. Number Theory **34**(1990), 82–94.
2. ———, *Quadratische Ordnungen mit grosser Klassenzahl, II*, J. Number Theory **44**(1993), 166–171.
3. R. A. Mollin, *On the divisor function and class numbers of real quadratic fields I*, Proc. Japan Acad. Ser. A **6**(1990), 109–111.
4. ———, *On the insolubility of a class of diophantine equations and the nontriviality of the class numbers of related real quadratic fields of Richard-Degert type*, Nagoya Math. J. **105**(1987), 39–47.
5. ———, *Class number one criteria for real quadratic fields II*, Proc. Japan Acad. **63**(1987), 162–164.
6. R. A. Mollin and H. C. Williams, *Class Number Problems for real Quadratic Fields*, Number Theory and Cryptography, (ed. J. H. Loxton), London Lecture Note series **154**, 1990, 77–105.
7. ———, *On prime valued polynomials and class numbers of real quadratic fields*, Nagoya Math. J. **112** (1988), 143–151.
8. ———, *Solution of the class number one problem for real quadratic fields of extended Richard-Degert type (with one possible exception)*, Number Theory (ed. R. A. Mollin), Walter de Gruyter, Berlin-New York, 1990, 417–425.
9. ———, *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 **67**(1991), 20–25.
10. ———, *On real quadratic fields of class number two*, Math. Comp. **59**(1992), 625–632.
11. R. A. Mollin and L.-C. Zhang, *Reduced ideals, the divisor function, continued fractions and class numbers of real quadratic fields*, Publ. Math. Debrecen, to appear.
12. H. C. Williams and M. C. Wunderlich, *On the parallel generation of the residues for the continued fraction factoring algorithm*, Math. Comp. **177**(1987), 405–423.

Mathematics Department
University of Calgary
Calgary, Alberta
T2N 1N4
e-mail: ramollin@acs.ucalgary.ca

Mathematics Department
Southwest Missouri State University
Springfield, Missouri 65804
U.S.A.
e-mail: liz917f@smsvm.bitnet