Can. J. Math.Vol. **44** (4), 1992 pp. 824–842

CLASS NUMBERS OF REAL QUADRATIC FIELDS, CONTINUED FRACTIONS, REDUCED IDEALS, PRIME-PRODUCING QUADRATIC POLYNOMIALS AND QUADRATIC RESIDUE COVERS

S. LOUBOUTIN, R. A. MOLLIN AND H. C. WILLIAMS

ABSTRACT. In this paper we consider the relationship between real quadratic fields, their class numbers and the continued fraction expansion of related ideals, as well as the prime-producing capacity of certain canonical quadratic polynomials. This continues and extends work in [10]–[31] and is related to work in [3]–[4].

1. **Introduction.** The first objective of this paper is to classify those square-free positive integers d such that there are no split primes $p < \sqrt{\Delta}/2$ where Δ is the discriminant of $Q(\sqrt{d})$; i.e., all primes $p < \sqrt{\Delta}/2$ are inert or ramified. This continues and extends work begun in [10], [17]–[19] and [29]. In particular, [29, Theorem 1.3, p. 144] (which generalized [15, Theorem 1, p. 18], and [17, Theorem, p. 121]), classified all those square-free d for which *all* primes $p < \sqrt{\Delta}$ are inert. In fact the last two authors showed in [29] that having all primes less than $\sqrt{\Delta}/2$ inert forced d to be a very special type; i.e., $d = \ell^2 + r$ with $|r| \in \{1, 4\}$, called *narrow Richaud-Degert* (RD) types. In [22] the last two authors used the generalized Riemann hypothesis (GRH) to list all of these forms. Moreover this situation is intimately linked to the prime-producing capacity of a certain canonical quadratic polynomial $f_d(x)$ (see Remark 2.2) similar to the well-known Euler-Rabinowitsch polynomial (see Remark 3.3) which is related to the class number one problem for complex quadratic fields, (see the elucidation in [19] for example). Therefore, in [29] we were able to give a complete Rabinowitsch analogue for real quadratic fields. We say complete because if we require $f_d(x)$ to be prime for all x with $1 \leq x \leq \sqrt{\Delta}/2$ (as is the case for the Euler-Rabinowitsch polynomial) then having this tantamount to $h(d) = 1$ forces d to be of narrow RD type. In [23] the last two authors looked at other quadratic polynomials with large (not necessarily consecutive) prime-producing capacity which were related to the $h(d) = 1$ problem for *extended Richaud-Degert* (ERD)-types; i.e., those forms $d = \ell^2 + r$ with $4\ell \equiv 0 \pmod{r}$. Using the results of the second author in [18] and assuming the GRH the last two authors (in [23]) used the techniques similar to that of [29] to complete the task of determining *all* ERD-types with $h(d) = 1$, and left several conjectures pertaining to prime-producing quadratic polynomials, all but one of which were verified by the first author in [12]. Subsequent to [23] and [29] the last two authors were able to prove in [21], without the GRH

Received by the editors May 7, 1991 .
AMS subject classification: 11R11, 11R09, 11R29.

assumption, that the list in [23] and [29] is complete, with one possible exceptional value remaining which (given the proofs in [23] and [29]) would be a counterexample to the Riemann hypothesis. This line of work led the last two authors to explore further the connection between prime-producing quadratic polynomials and the class number one problem for real quadratic fields in [22], and [24]–[31] where they introduced new techniques based upon the triple connection between $h(d) = 1$, reduced ideals and the theory of continued fractions (see Theorem 2.8 below for example, and see [20] for a detailed elucidation). This new approach (also explored by the first author in [11]) led the last two authors to seek a general real quadratic field analogue of the Rabinowitsch condition for complex quadratic fields having class number one. They did so by looking for a precise prescription for the factorization (over the rational integers) of $f_d(x)$ investigated in [29]. They had success for small period lengths of ω (see Section 2) in [25], [27] and [31]. However in [31] they exhausted the algebraic techniques available and suggested therein that such a prescription would be extremely difficult to find in the completely general case. This problem remains open.

The wealth of results which came out of the above investigation (including a *new* record for prime-producing quadratic polynomials given in [26] which surpassed that of the celebrated Euler polynomial) led the authors to question what it would mean to allow ramified primes $p < \sqrt{\Delta}/2$ (but no split primes); i.e., to relax the restriction which the last two authors had so thoroughly investigated. This brings us back to the first main result of this paper which is the classification of such d in Theorem 3.1. It turns out that this situation also forces d to be of ERD-type but not necessarily of class number one. The machinery used to prove Theorem 3.1 is contained in the preliminary Lemmas 3.1–3.8. Some of these preliminary results are of interest in their own right, and two of them, Lemmas 3.5 and 3.7, generalize results of the first author in [10]. Moreover these lemmas investigate the link between prime-producing quadratic polynomials and the situation where there are no split primes less than $\sqrt{\Delta}/2$. We also settle a question of Halter-Koch raised in [4] which motivates the introduction of Lemmas 3.1–3.8. After the proof of Theorem 3.1 we discuss the phenomenon of prime-producing quadratic polynomials and the class number one problem for real quadratic fields as studied in [4], [12], [21] and [23]–[24]. This motivates the general question: What is the largest number of *consecutive* prime values that a quadratic polynomial can assume? Under the assumption of the "prime k-tuples conjecture" we prove that the answer is: Any number of consecutive prime values can be assumed.

In Section 4 we look at a refinement of a concept introduced by the last two authors in [32]; viz; quadratic residue covers for real quadratic fields. This is a new technique for investigating the class number one problem for real quadratic fields. We motivate the discussion by first citing the solution by the last two authors in [30] of the class number one problem for a sequence of Shanks, using quadratic residue covers. However, we are also able to prove that certain open conjectures for the forms $d = m^2 + 2$ and $d = m^2 - 8$ cannot be resolved by using these covers. Among the forms which can be approached using quadratic residue covers are those for which all the Q_i/Q_0's are powers of a single

integer in the continued fraction expansion of ω (see Section 2). In [22] the last two authors completely classified those positive square-free positive d's for which there are three or more Q_i/Q_0's in a row (as determined by the infrastructure of the principal class (see [36])) as powers of a single integer. Section 5 is devoted to providing a list of all positive square-free integers d such that $h(d) = 1$ and there are 3 or more Q_i/Q_0's in a row as powers of a single integer. Furthermore we prove that the list is complete with one possible exceptional value remaining.

This paper provides a meeting point for all the ideas explored in [10]–[31] and depicts the palatable results which can ensue from the interlinked use of theory of reduced ideals, continued fractions, prime-producing quadratic polynomials and quadratic residue covers when applied to class number problems for real quadratic fields.

We now turn to the next section which sets the stage with the machinery needed. We prove some results in Section 2 which are either not readily available in the literature or are folklore and deserve to see the light of print with elementary proofs such as Theorems 2.5 and 2.7.

2. **Notation and preliminaries.** Throughout d will denote a positive square-free integer, and $K = Q(\sqrt{d})$. We let O_K denote the maximal order in K, and the discriminant Δ, of K is $4d/\sigma^2$ where

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

Let $[\alpha, \beta]$ be the module $\{\alpha x + \beta y : x, y \in Z\}$, where Z denotes the rational integers. Then we note that $O_K = [1, \omega]$ where $\omega = (\sigma - 1 + \sqrt{d})/\sigma$, and $\Delta = (\omega - \bar{\omega})^2$ where $\bar{\omega}$ is the algebraic conjugate ω. The norm of $\alpha \in K$ is denoted $N(\alpha) = \alpha\bar{\alpha}$. Equivalence of two ideals I and J of O_K is denoted $I \sim J$, and a principal ideal generated by α is written (α). Also $\{I\}$ will denote the equivalence class of I in the class group C_K of K. It is well known that I is an ideal in O_K if and only if $I = [a, b + c\omega]$ where $a, b, c \in Z$ with $c|b$, $c|a$ and $ac|N(b+c\omega)$. Moreover, if $a > 0$ then a is unique and is the smallest positive rational integer in I, denoted by $a = L(I)$, and $N(I) = cL(I)$. Also, $\bar{I} = [a, b + c\bar{\omega}]$. If $c = 1$ then I is called a *primitive* ideal and $N(I) = L(I)$. Moreover, since $I = (c)[a/c, b/c + \omega]$, then we may restrict our attention to primitive ideals and we do so in what follows.

In the following we give an elucidation of the theory for reduced ideals. Proofs of these results and further details may be found in [39], (see also the description in [20]) and see [8]. A primitive ideal I is said to *reduced* if it does not contain any non-zero element α satisfying both $|\alpha| < N(I)$ and $|\bar{\alpha}| < N(I)$.

THEOREM 2.1. *(a) If I is any ideal of O_K then there exists a primitive ideal J such that $J \sim I$.*

(b) If I is any ideal of O_K then there exists an ideal J of O_K such that $J \sim I$ and J is reduced.

THEOREM 2.2. *I is a reduced ideal of O_K if and only if there exists some $\beta \in I$ such that $I = [N(I), \beta]$, $\beta > N(I)$ and $-N(I) < \bar{\beta} < 0$.*

THEOREM 2.3. *(a) If I is reduced then $N(I) < \sqrt{\Delta}$.*

https://doi.org/10.4153/CJM-1992-049-0 Published online by Cambridge University Press

(b) If I is a primitive ideal of O_K and $N(I) < \sqrt{\Delta}/2$ then I is reduced.

The following involves a Minkowski-like bound (see for example [1, Corollary 1, p. 135]).

THEOREM 2.4. *If I is a reduced ideal of O_K then there exists an ideal $J \sim I$ such that $N(J) < \sqrt{\Delta}/2$.*

Now we give an elucidation of the thoery of continued fractions as it pertains to the above. We will use these results extensively throughout the paper. Let $I = [N(I), b + \omega]$ be primitive and denote the continued fraction expansion of $(b + \omega)/N(I)$ by $\langle a, \overline{a_1, a_2, \ldots, a_\pi} \rangle$ where

$$(P_0, Q_0) = \big(\sigma b + \sigma - 1, \sigma N(I)\big).$$

and, (for $i \geq 0$),

$$d = P_{i+1}^2 + Q_i Q_{i+1},$$

$P_{i+1} = a_i Q_i - P_i$ where

$$a_i \lfloor (P_i + \sqrt{d})/Q_i \rfloor,$$

(with $\lfloor\ \rfloor$ being the greatest integer function). Therefore, $Q_i < 2\sqrt{d}$. For convenience we set $a = a_0$.

From the well-known results in [38] we get that the continued fraction expansion of $(b+\omega)/N(I)$ yields *all* the reduced ideals in O_K equivalent to I; i.e., $I = I_0 = [Q_0/\sigma, (P_0 + \sqrt{d})/\sigma] \sim I_1 = [Q_1/\sigma, (P_1 + \sqrt{d})/\sigma] \sim \cdots \sim I_{\pi-1} = [Q_{\pi-1}/\sigma, (P_{\pi-1} + \sqrt{d})/\sigma]$.

Moreover, since $Q_0 = Q_\pi$ and $P_0 \equiv P_\pi \pmod{Q_0}$ then by [38, Section 3, p. 140] we get $I_\pi = I$. Therefore the $(P_i + \sqrt{d})/Q_i$ are the complete quotients of $(b + \omega)/N(I)$. We call this expansion a *cycle* of reduced ideals and we note that the Q_i/σ's represent *norms* of *all* reduced ideals equivalent to I.

REMARK 2.1. The concept of *caliber* discussed in [9] is not new. In point of fact, from the above, we see that if $C_K = \bigcup_{i=1}^{h(d)} \{J_i\}$ and $\{J_i\}$ has t_i equivalent (distinct) reduced ideals then $\sum_{i=1}^{h(d)} t_i$ is the caliber.

The above development yields the following well-known result, which generalizes Proposition 2 of [10, p. 63] which was only proved for ambiguous ideals.

THEOREM 2.5. *Let $I = [N(I), b + \omega]$ be a reduced ideal of O_K.*

(a) If J is a reduced ideal of O_K and $I \sim J$ then $N(I) = Q_i/\sigma$ for some i with $1 \leq i \leq \pi$, where the Q_i's appear in the continued fraction expansion of $(b + \omega)/N(I)$.

(b) If J and $\bar{J}$ are the only ideals of norm $N(J)$, where J is reduced in O_K, and $N(J) = Q_i/\sigma$ for some i with $1 \leq i \leq \pi$ in the continued fraction expansion of $(b+\omega)/N(I)$ then either $J = I_i$ or $\bar{J} = I_i$.

REMARK 2.2. If J is primitive and either a product of ramified ideals, or a power of a split ideal then J and $\bar{J}$ are the only ideals of norm $N(J)$. In point of fact the above results

are special cases of the ideal-theoretic interpretation of the very old idea of reducing quadratic forms which is generally believed to have originated with Hermite (see [20]).

In what follows let

$$f_d(x) = \begin{cases} -x^2 + x + (d-1)/4 & \text{if } d \equiv 1 \pmod 4 \\ -x^2 + d & \text{if } d \equiv 2, 3 \pmod 4 \end{cases}$$

Observe that $f_d(x)$ is a canonical choice in that it is "norm-induced" as was the polynomial in Rabinowitsch's well-known Theorem for complex quadratic field ([33]–[34]) of which the following is a real quadratic field analogue. Although Theorem 2.6 was observed by the first author in [11, Theorem 4, p. 170], his proof requires adjustment. On page 170–171 of [11] one must replace "which is supposed ... generated by $w_0 - n_p$" by: "then P is one of the Q_i/Q_0's so P is principal."

THEOREM 2.6. *$h(d) = 1$ if and only if whenever $f_d(x) \equiv 0 \pmod p$ for any prime $p < \sqrt{\Delta}/2$ and any x with $1 \le x < \sqrt{\Delta}/2$, then $p = Q_i/Q_0$ for some i with $1 \le i \le \pi$ in the continued fraction expansion of ω.*

PROOF. If $h(d) = 1$, and $f_d(x) \equiv 0 \pmod p$ with $p < \sqrt{\Delta}/2$ and $0 \le x < \sqrt{\Delta}/2$ then the result follows from Theorem 2.3 and 2.5. Conversely, let $p < \sqrt{\Delta}/2$ divide $f_d(x)$. The result now follows from Theorem 2.5(b) and Remark 2.1. ∎

We also need the following well-known result which we prove for convenience's sake, and because an appropriate reference is not readily available.

THEOREM 2.7. *The class group C_K is generated by the non-inert primitive prime ideals J with $N(J) \le \sqrt{\Delta}/2$.*

PROOF. By Theorems 2.1–2.4, C_K is generated by $h(d)$ reduced ideals $I_1, \ldots, I_{h(d)}$ such that $N(I_i) \le \sqrt{\Delta}/2$ for $1 \le i \le h(d)$. Since a reduced ideal is, *a fortiori*, primitive, then any prime ideal $\mathcal{P}$ dividing I_i is not inert and satisfies $N(\mathcal{P}) \le N(I_i) \le \sqrt{\Delta}/2$. Now it is clear that the finite set of non-inert prime ideals dividing any I_i, for $1 \le i \le h(d)$, generates C_K. ∎

There are many well-known criteria for C_K to have class number equal to 1. We list some useful ones here.

THEOREM 2.8. *The following are equivalent, (where all Q_i's, refer to the continued fraction expansion of ω),*

(1) $h(d) = 1$

(2) $p = Q_i/Q_0$ *whenever* $p < \sqrt{\Delta}/2$ *and* p *divides* $f_d(x)$ *when* $1 \le x \le \sqrt{\Delta}/2$.

(3) $m = Q_i/Q_0$ *exactly* $\nu(m)$ *times for* $1 \le i \le \pi$ *and all* m *with* $1 \le m \sqrt{\Delta 15}$ *where* $\nu(m)$ *is the number of primitive ideals of norm* m.

(4) $p = Q_i/Q_0$ *for some* i *with* $1 \le i \le \pi - 1$ *whenever* p *is a non-inert prime less than* $\sqrt{\Delta}/2$.

(5) $\sum_{i=1}^{\pi} a_i + \theta = \lambda_1(d) + \lambda_2(d)$

https://doi.org/10.4153/CJM-1992-049-0 Published online by Cambridge University Press

where the a_i's are from the continued fraction expansion of ω, and $\lambda_1(d)$ is the number of solutions of $x^2+4yz=\Delta$ with $x,y,z\geq 0$, $\lambda_2(d)$ is the number of solutions of $x^2+4y^2=\Delta$ with $x,y\geq 0$, and

$$\theta=\begin{cases}0, & \text{if } d\equiv 1 \pmod 4,\ \pi=2n, a_n \text{ odd},\\ 1, & \text{if } d\equiv 1 \pmod 4,\ \pi=2n, a_n \text{ even},\\ 1, & \text{if } d\equiv 1 \pmod 4,\ \pi \text{ odd},\\ 1, & \text{if } d\equiv 2,3 \pmod 4,\ \pi=2n, a_n \text{ odd},\\ 2, & \text{if } d\equiv 2,3 \pmod 4,\ \pi=2n, a_n \text{ even},\\ 2, & \text{if } d\equiv 2,3 \pmod 4,\ \pi \text{ odd}.\end{cases}$$

PROOF. The equivalence of (1) and (2) is Theorem 2.6. The equivalence of (1) and (3) proceeds as follows. If $h(d)=1$ then since there always exists a primitive ideal I in each class, with norm $<\sqrt{\Delta/5}$, (e.g. see [2, Theorem 62, p. 79]), then *all* primitive ideals of norm m must occur as some Q_i/Q_0 by Theorem 2.5(a); i.e., $\nu(m)$ times. Conversely, since $N(I)=m<\sqrt{\Delta/5}<\sqrt{\Delta/4}$ implies that I is reduced then by Theorem 2.5 and the discussion before it we have all $\nu(m)$ ideals equivalent to I being principal; whence, $h(d)=1$. The equivalence of (1) and (4) is merely the observation that *all* non-inert primes $p<\sqrt{\Delta}/2$ divide $f_d(x)$, (see Lemma 3.1 below). The equivalence of (1) and (5) is [14, Theorem 2, p. 119]. ∎

For certain special forms of d we have results concerning $h(d)=1$ which will be useful to us later.

THEOREM 2.9. *(a) If $d=(2^n+3)^2-8$ then $h(d)=1$ if and only if p is inert for all odd primes $p<\sqrt{d}/2$.*

(b) If $d=m^2+r\equiv 1 \pmod 4$ where $|r|\in\{1,4\}$ then $h(d)=1$ if and only if p is inert for all primes $p<\sqrt{d}/2$.

PROOF. (a) It can be shown that for such forms Q_i is always a power of 2 (see [28]). The result now follows from Theorem 2.5

(b) This is proved in [29]. ∎

3. **Prime producing quadratic polynomials and class numbers.** The last two authors investigated criteria for a real quadratic field analogue of the well-known Euler-Rabinowitsch result for complex quadratic fields (see [23]–[25], [27] and [29]). As with the Euler polynomial, the prime-producing capacity of certain canonical polynomials was linked to the class number one problem. Although Theorem 2.6 is a well-known general criteria for a real quadratic field to have class number one in terms of the factorization of a "norm-induced" quadratic polynomial $f_d(x)$, the last two authors sought a more *precise* description of the factorization of that polynomial. They were able to do this in [25] and [27] by intimately linking the problem to the period length π of the continued fraction expansion of ω. The detailed description which this allowed, however, meant that the algebraic calisthenics necessary to be performed were extremely intricate, and

after solving the problem for $\pi \leq 5$ they had exhausted the algebraic techniques available. It is an open problem as to whether or not an algorithm exists for extending their algebraic techniques to the general case.

With the exhaustion of the techniques mentioned above the last two authors turned their attention to other polynomials in [23]–[24]. This allowed them to look at the class number one problem for the general ERD-types, which they began in [29] for narrow RD-types, (whose class number one was characterized therein by the (strictly) prime-producing capacity of $f_d(x)$). They left conjectures pertaining to the relationship between the class number one problem for ERD-types and these new polynomials in [23]–[24]. The first author investigated and solved all but one case of these conjectures in [12]. Now we examine 2 conjectures concerning these new prime-producing quadratic polynomials. In [4] Halter-Koch remarked that his result, [4, Theorem 3.1, p. 75], might only hold for ERD-types when d is positive. The following shows this to be false.

Consider the polynomial $f_p(x) = px^2 + px + (p-q)/4$ where $d = pq$ with $p \equiv q \equiv 3 \pmod 4$ and $p < q$. It follows from the Halter-Koch result that if $|f_p(x)|$ is 1 or prime for all integers x with $0 \leq x \leq 1/2(\sqrt{d/5} - 1)$ then $h(d) \leq 2$. (In fact from Gauss' genus theory it follows that $h(d) = 1$). Halter-Koch stated in [4, Remark, p. 76] that it is not known whether or not the above holds for non-ERD-types. Here is an example of a non-ERD-type for which the above *does* hold. Let $d = 341$, and $f_{11}(x) = 11x^2+11x-5 = px^2+px+(p-q)/4$ where $p = 11$ and $q = 31$. Then $|f_{11}(x)| = 5, 17, 61, 127$ for $x = 0, 1, 2, 3$ where $\lfloor(\sqrt{d/5} - 1)/2\rfloor = 3$ here. However d is *not* of ERD-type. Another example is $d = 917 = 7 \cdot 131$ which is not of ERD-type, but for which $f_7(x) = 7x^2 + 7x - 31$ and $|f_7(x)|$ is prime for $0 \leq x \leq 6$.

Now we prove a result (similar to the Halter-Koch result [*ibid.*]) which *does* yield an ERD-inference. In what follows $f_d(x)$ is as in Section 2. We first need some very useful and informative preliminary lemmas. Although some of these results are contained in [10] we include them here in order to make this paper as self-contained as possible. Moreover the proofs presented here are, for the most part, more elementary than those in [10]. Furthermore, some of these results are useful generalizations of results in [10] and [11] from the principal class to arbitrary classes. The reader will thereby be led in a step-wise fashion to the main result. Finally the results in the Lemmas are of interest in their own right. In what follows $(/)$ is the Kronecker symbol.

LEMMA 3.1. *Let $p < \sqrt{d}/2$ be prime, then $f_d(x) \equiv 0 \pmod p$ for some x with $1 \leq x < \sqrt{\Delta}/2$ if and only if $(d/p) \neq -1$; (i.e., all non-inert primes $p < \sqrt{\Delta}/2$ divide $f_d(x)$ and they are the* only *such prime divisors less than $\sqrt{\Delta}/2$).*

PROOF. If $d(p) \neq -1$ then there exists an integer y with $1 \leq y \leq p$ and $d \equiv y^2 \pmod p$. Hence, if $d \not\equiv 1 \pmod 4$ then setting $y = x$ yields the result. If $d \equiv 1 \pmod 4$ and $p > 2$ then we may assume that y is odd (since we may otherwise replace it by $p - y$). Thus setting $x = (y+1)/2$ yields the result. If $p = 2$ then $d \equiv 1 \pmod 8$ necessarily and $f_d(x)$ is clearly always even in this case.

Conversely, if $p < \sqrt{\Delta}/2$ and $f_d(x) \equiv 0 \pmod p$ for $1 \le x < \sqrt{\Delta}/2$ then, since $f_d(x) = -x^2 - 2x(\sigma-1)/\sigma + \big(d - (\sigma-1)\big)/\sigma^2$, we have $d \equiv (\sigma x + \sigma - 1)^2 \pmod p$; whence, p is not inert. ∎

In what follows R_K denotes the subgroup of C_K generated by the ramified prime ideals; (whence, R_K is of exponent 2 since $\mathcal{P} = \bar{\mathcal{P}}$ for all ramified primes).

LEMMA 3.2. *If $(d/p) \ne 1$ for all $p < \sqrt{\Delta}/2$ then $C_K = R_K$.*

PROOF. This follows immediately from Theorem 2.7. ∎

LEMMA 3.3. *The following are equivalent.*
(1) $(d/p) \ne 1$ for all $p < \sqrt{\Delta}/2$; (whence $C_K = R_K$).
(2) If $f_d(x) \equiv 0 \pmod p$ for some $p < \sqrt{\Delta}/2$ and $1 \le x < \sqrt{\Delta}/2$ then p divides Δ.

PROOF. The result is immediate from Lemmas 3.1–3.2 ∎

REMARK 3.1. Lemma 3.3 is also noted in [10, Proposition 13, p. 71] by different techniques.

LEMMA 3.4. *Let $\Delta = m^2 \pm 4r$ with $1 < r < m/2$; then Δ can be written in exactly one way;* viz. *$m = \lfloor\sqrt{\Delta}\rfloor$ in the case of the "+" sign and $m = \lfloor\sqrt{\Delta}\rfloor - 1$ for the "−" sign.*

PROOF. If $\Delta = m^2+4r$ and $1 < r < m/2$ then $m^2 < \Delta < m^2+2m < (m+1)^2$; whence $m = \lfloor\sqrt{\Delta}\rfloor$. If $\Delta = m^2-4r$ and $1 < r < m/2$ then $(m-1)^2 < m^2-4(m/2-1) \le \Delta < m^2$; whence, $m = \lfloor\sqrt{\Delta}\rfloor + 1$. ∎

The following generalizes [11, Lemma b, p. 172], and is also buried in [10, Proposition 7] in totally different terms. However we include it here to highlight it, to make the paper more self-contained, and to point out the more elementary techniques for achieving the result.

LEMMA 3.5. *Let $I = [N(I), b+\omega] \ne (1)$ be a reduced ambiguous ideal. Thus, if $Q_i/\sigma \ne N(I)$ then Q_i/σ is a square-free divisor of Δ in the continued fraction expansion of $(b+\omega)/N(I)$ if and only if $\pi = 2i$.*

PROOF. By [38, Theorem 7.4, p. 640] we get that $1 \ne N(I)$ is a square-free divisor of Δ. Let $\mathcal{S} = \{\text{primes } p : p|N(I)\}$, and let $\mathcal{P}_p$ be the primitive ideal over p. Since there is exactly one primitive ideal of norm $N(I)$ then $I = \prod_{p\in\mathcal{S}} \mathcal{P}_p$. Now set $J = \prod_{p\in\mathcal{S}'} \mathcal{P}_p$ where $\mathcal{S}' = \{p|d : p \notin \mathcal{S}\}$. We see that $\mathcal{S}' \ne \emptyset$, since otherwise $N(I) \ge d$ contradicting that I is reduced by Theorem 2.3. Thus $IJ = (\sqrt{d})$ unless possibly $2|N(I)$, $d \equiv 3 \pmod 4$ and $\mathcal{P}_2$ is not principal. In that case $IJ\mathcal{P}_2 \sim 1$, so we assume that $I_1 = J$ in the former case and $I_1 = J\mathcal{P}_2$ in the latter case. From [38, Theorem 7.3, p. 640] and the fact that there is exactly one primitive ideal of norm $N(I)$ we may assume that I_1 is reduced.

Thus, by Theorem 2.5(a), $N(I_1) = Q_i/\sigma$ for some i with $1 \le i \le \pi$ in the continued fraction expansion of $(b+\omega)/N(I)$. Also $N(I_1) \ne N(I)$ so in fact $0 < i < \pi$. Moreover by [38, Theorem 7.4, p. 640], $N(I_1)|\Delta$. Now, since $d = P_i^2 + Q_iQ_{i-1}$ then $Q_i|2P_i$. However, $2P_i/Q_i < (P_i+\sqrt{d})/Q_i < 2P_i/Q_i + 1$. Therefore $a_i = \lfloor(P_i+\sqrt{d})/Q_i\rfloor = 2P_i/Q_i$. Since

https://doi.org/10.4153/CJM-1992-049-0 Published online by Cambridge University Press

$P_{i+1} = a_iQ_i - P_i$ then $P_i = P_{i+1}$. Also $d = P_i^2 + Q_iQ_{i-1} = P_{i+1}^2 + Q_iQ_{i+1}$; whence, $Q_{i+1} = Q_{i-1}$. Furthermore, $a_{i+1} = \lfloor (P_{i+1} + \sqrt{d})/Q_{i+1} \rfloor = \lfloor (P_i + \sqrt{d})/Q_{i-1} \rfloor = \lfloor (a_{i-1}Q_{i-1} - P_{i-1} + \sqrt{d})/Q_{i-1} \rfloor = \lfloor a_{i-1} + (\sqrt{d} - P_{i-1})/Q_{i-1} \rfloor$.

However, $1 > (\sqrt{d} - P_{i-1})/Q_{i-1} > 0$; whence, $a_{i+1} = a_{i-1}$. Continuing in this fashion, and using the symmetry within the period we get $\pi = 2i$. ∎

REMARK 3.2. It is worth noting with regard to the above that if $I = I_0, I_1, \ldots, I_{\pi-1}$ is the complete cycle of reduced ideals equivalent to I (see Section 2), and I is a reduced ambiguous ideal then $\overline{(I_i)} = I_{\pi-i}$ (see [10, Lemma 4, p. 64]).

LEMMA 3.6. *Let $I = [N(I), b + \omega]$ be a reduced ideal. If $Q_i \geq \sqrt{d}$ in the continued fraction expansion of $(b + \omega)/N(I)$ then $a_i = 1$.*

PROOF. $2\sqrt{d} > P_i + \lfloor \sqrt{d} \rfloor \geq a_iQ_i \geq a_i\sqrt{d}$. ∎

The following improves upon [10, Proposition 14, p. 71].

LEMMA 3.7. *If $(d/p) \neq 1$ for all primes $p < \sqrt{d}/2$ and $I = [N(I), b + \omega]$ is a reduced ambiguous ideal then in the continued fraction expansion of $(b + \omega)/N(I)$, the period length π divides 4. Moreover, if $\pi = 1$ then $d = m^2 + 4$ or $d = 2$. If $\pi = 2$ then $\Delta = m^2 + 4r$ with $r > 1$ and $r|m$; and if $\pi = 4$ then $\Delta = m^2 - 4r$ with $r > 1$, and $r|m$.*

PROOF. If $I \neq (1)$ and $I^2 \neq (2)$ then by [37, Theorem 7.4, p. 640] we get that $1 \neq N(I)$ is a square-free divisor of Δ. However if $\pi = 1$, $d = P_1^2 + \sigma^2N(I)^2$, a contradiction. Thus if $\pi = 1$ then $I = (1)$ or $I^2 = (2)$. If $I = (1)$ then $d = P_1^2 + 4$ if $\sigma = 2$ or $d = P_1^2 + 1$ if $\sigma = 1$. However in the latter case any prime p divisor of P_1 satisfies $p < \sqrt{d}$ and $(d/p) = 1$, a contradiction; whence $d = 2$. If $I^2 = (2)$ then $\sigma = 1$ and $d = P_1^2 + 4$, a contradiction since $d \not\equiv 1 \pmod 4$, and d is square-free.

Now we assume that $\pi > 1$; i.e., $Q_1 \neq \sigma N(I)$.

CLAIM 1. If $\sigma \leq Q_1 < \sqrt{d}$ then Q_1/σ divides Δ and Q_1/σ is square-free, whence $\pi = 2$.

If a prime q divides Q_1/σ then q divides $f_d\big((P_1 - \sigma + 1)/\sigma\big)$, and so by Lemma 3.3 q divides $\Delta = 4d/\sigma^2 = \big(4P_1 + 4N(I)Q_1\sigma\big)/\sigma^2$. Therefore, if $q^2|(Q_1/\sigma)$ then $q^2|\Delta$. However, $q^2|\Delta$ if and only if $q^2 = 4$, in which case $\sigma = 1$ and $d = P_1^2 + N(I)Q_1$, which is a contradiction because the facts that $4|Q_1$ and that d is square-free together imply that $d \equiv 1 \pmod 4$. Therefore Q_1/σ is square-free and since I is a reduced ideal and $Q_1/\sigma \neq N(I)$ then $\pi = 2$. Moreover, $d = P_1^2 + \sigma N(I)Q_1$ with $\gcd\big(N(I), Q_1\big) = 1$ so $N(I)Q_1/\sigma$ divides P_i; i.e., $\Delta = m^2 + 4r$ with r dividing m and $r > 1$.

Now we assume that $Q_1 \geq \sqrt{d}$. By Lemma 3.6 we must have $a_1 = 1$. Therefore $P_2 = Q_1 - P_1$ and $Q_2 = 2P_1 + \sigma N(I) - Q_1$. Since $d = P_2^2 + Q_1Q_2$ then clearly $\sigma \leq Q_2 \leq \sqrt{d}$. Moreover, by the same argument as in Claim 1, Q_2/σ is square-free and divides Δ; whence, $\pi = 4$ by Lemma 3.5. In fact, $d = \big(P_1 + \sigma N(I)\big)^2 - \sigma N(I)\big(2P_1 + \sigma N(I) - Q_1\big)$; i.e., $d = m^2 - 4r$ where r divides m. ∎

Moreover we get [10, Lemma 9, p. 68],

COROLLARY 3.1. *Let I and J be reduced ambiguous ideals with $I \sim J$ and $N(I) = a$, $N(J) = b$. If $(d/p) \neq 1$ for all primes $p < \sqrt{\Delta}/2$ then $\Delta = m^2 \pm 4r$ with $r = ab$.*

PROOF. This is immediate from the proof of Lemma 3.7. ∎

LEMMA 3.8. *Let $\Delta = m^2 \pm 4r$ with r dividing m and $1 < r < m/2$. Let δ be a square-free integer dividing r. If $I \sim I_\delta$ (where I_δ is the unique reduced ambiguous ideal of norm δ) and $N(I) < \sqrt{\Delta}/2$ then $N(I)$ divides Δ.*

PROOF. For convenience sake and simplicity of notation we only prove the case where $\Delta = d \equiv 1 \pmod 4$ since the other case is essentially the same.

If $\Delta = m^2 + 4r$ then $I_\delta = [\delta, (m + \sqrt{\Delta})/2]$ and the continued fraction expansion of $(m + \sqrt{\Delta})/2\delta$ is

i:	0	1	2
P_i:	m	m	m
Q_i:	δ	r/δ	δ
a_i:	m/δ	$m\delta/r$	m/δ

If $\Delta = m^2 - 4r$ then $I_\delta[\delta, (m - 2\delta + \sqrt{\Delta})/2]$ and the continued fraction expansion of $(m - 2\delta + \sqrt{\Delta})/2\delta$ is

i:	0	1	2	3	4
P_i:	m	$m - 2\delta$	$m - 2r/\delta$	$m - 2r/\delta$	$m - 2\delta$
Q_i:	2δ	$2m - 2\delta - 2r/\delta$	$2r/\delta$	$2m - 2\delta - 2r/\delta$	2δ
a_i:	$m/\delta - 1$	1	$m\delta/r - 2$	1	$m/\delta - 1$

The result now follows from Theorems 2.3 and 2.5. (Observe that $2m - 2\delta - 2r/\delta \geq \sqrt{\Delta}$).

Now we prove the main result.

THEOREM 3.1. *The following are equivalent.*

(a) $(d/p) \neq 1$ for all primes $p < \sqrt{\Delta}/2$.

(b) If $f_d(x) \equiv 0 \pmod p$ for some $p < \sqrt{\Delta}/2$ and $1 \leq x < \sqrt{\Delta}/2$ then p divides Δ.

(c) One of the following statements holds.

(1) $d = m^2 + 4$ is prime and $h(d) = 1$.

(2) $d = m^2 - 1$ and either $m - 1$ or $m + 1$ is prime for $m > 1$, and $C_K = R_K$.

(3) $d = m^2 - 4$ and either $m - 2$ or $m + 2$ is prime for $m > 2$, and $C_K = R_K$.

(4) $d = m^2 + m$ with either m or $m + 1$ prime for $m > 0$ and $C_K = R_K$.

(5) $\Delta = m^2 \pm 4r$ with $1 < r < m/2$ and $r | m$. Moreover, $C_K = R_K$ and C_K is generated by the primes with norm dividing r. Finally if $\Delta \equiv 1 \pmod 4$ then Δ/r is prime, and if $\Delta \equiv 0 \pmod 4$ then the odd part of Δ/r is prime.

PROOF. The equivalence of (a) and (b) is Lemma 3.3. Now assume (a) and prove (c). By Lemma 3.2 we have $C_K = R_K$. By Theorem 2.7, C_K is generated by the non-inert primes of norm $< \sqrt{\Delta}/2$.

Let $I = [N(I), b + \omega]$ be a reduced prime ideal with $N(I) < \sqrt{\Delta}/2$. Consider the continued fraction expansion of $(b + \omega)/N(I)$. If $\pi = 1$ then by Lemma 3.7 either $d = 2$

https://doi.org/10.4153/CJM-1992-049-0 Published online by Cambridge University Press

which falls into case (4) or $d = m^2 + 4$ which is case (1). If d is not prime then using Lemma 3.7 again on one of the prime divisors we would get $\pi = 1$ for that continued fraction expansion, contradicting the existence of the prime, (since in that expansion $d = P_1^2 + 4p^2$ where p divides d). Moreover by Theorem 2.7, $h(d) = 1$ is forced.

Now assume $\pi = 2$. By Lemma 3.7, $\Delta = m^2 + 4r$ where $r|m$. If $r < m/2$ then we are in case (5). By Lemma 3.4, d can only be written in one such way. Therefore the continued fraction expansion for any ramified prime $\mathcal{P}$ with $N(\mathcal{P}) < \sqrt{\Delta}/2$ yields that $p|r$. By Theorem 2.7 then C_K is generated by the primes with norm dividing r. For case (5) it suffices to complete the case by showing that if $\Delta \equiv 1 \pmod 4$ then Δ/r is prime since the remainder is similar. If it were not prime then there exist $1 < d_1 < d_2$ such that $d/r = d_1 d_2$. Since $d/d_1 = rd_2 > d_2 > d_1$, the ideal of norm d_1 is reduced; so its norm d_1 divides r, a contradiction.

If $\pi = 2$ and we are not in case (5), then from the proof of Lemma 3.7 we have $N(I)Q_1 \geq P_1$. However by Lemma 3.5, $N(I)Q_1|2P_1$, so $2P_1 = N(I)Q_1\ell \geq P_1\ell$; whence $\ell = 1$ or 2. Now, if $\sigma = 1$ then $d = P_1^2 + 2P_1$ when $\ell = 1$ and $d = P_1^2 + P_1$ when $\ell = 2$. If $\sigma = 2$ then $d = P_1^2 + 4P_1$ when $\ell = 1$ and $d = P_1^2 + 2P_1 \not\equiv 1 \pmod 4$, a contradiction when $\ell = 2$. Thus we are in cases (2), (3) and (4).

It suffices to show the primality of one of the factors for any of the cases since they all have the same proof. We take $d = P_1^2 + 2P_1 = (P_1 + 1)^2 - 1$. If P_1 and $P_1 + 2$ have divisors $d_1 < \sqrt{P_1}$ and $d_2 < \sqrt{P_1 + 2}$ then the ideal with norm $d_1 d_2$ is reduced and so by Corollary 3.1, $d = m^2 \pm 4r$ with $d_1 d_2 | r$. However d can only be written thus in 3 ways; *viz.*, $d = (P_1 + 2)^2 - 2(P_1 + 2)$, $d = (P_1 + 1)^2 - 1$ and $d = (P_1 - 1)^2 + 2(P_1 - 1)$ so $d_1 d_2 | 2(P_1 + 2)$ or $2(P_1 - 1)$, a contradiction since $\gcd(P_1 + 2, d_1) = 1 = \gcd(P_1 - 1, d_1)$.

Finally the analysis for the case $\pi = 4$ is similar to that of $\pi = 2$ so we do not repeat it. Hence (a) $\Rightarrow$ (c).

To show that (c) $\Rightarrow$ (a) we only have to prove that (5) $\Rightarrow$ (a) since the other cases appear in [10]. We need to show that there are no split primes $\mathcal{P}$ of norm $N(\mathcal{P}) < \sqrt{\Delta}/2$. This follows from Theorems 2.3 and 2.5 together with Lemma 3.8. ∎

REMARK 3.2. Assuming a suitable Riemann hypothesis the first author showed in Theorem 18 of [10] that there are 60 real quadratic fields that satisfy any of the 3 equivalent conditions of Theorem 3.1 above. Concerning Halter-Koch's Remark [4, *op. cit.*], the first author clearly shows in [12] that when one chooses an upper bound less than $\sqrt{d}/4 - 1/2$ for x in the polynomial $px^2 + px + (p - q)/4$ then one gets a family strictly bigger than ERD-types. Moreover in [12, Lemma 11, p. 355] he explains how to determine this family. The interesting problem left open is to consider $d = pq \equiv 5 \pmod 8$ where $p \equiv q \equiv 3 \pmod 4$ and $p < q$ are primes, and determine the upper bound B in the set of consecutive integers x with $0 \leq x \leq B$ such that the polynomial $|px^2+px+(p-q)/4| = |f_p(x)|$ takes on only prime values (or 1). The first author managed to get this upper bound B in the case of imaginary quadratic fields (Theorem 2(b) of [13]). In fact, from [12], the first author conjectures that for such d of ERD-type, if $h(d) = 1$ then $|f_p(x)|$ is prime or 1 whenever $0 \leq x \leq \sqrt{d}/3 - 1$. He proves the converse in [12, Theorem 10, p. 333], (where we note here that the family $d = 4p^2s^2 + p$ should have been

excluded from consideration therein (and previously in [12, p. 330]) since $h(d) > 1$ for this family). The conjecture can be proved using the techniques of [23]–[24] to be true, with one possible exceptional value remaining. Given the techniques of [21], this exceptional value would be a counterexample to the Riemann hypothesis. However, proving the conjecture by algebraic means seems to be highly difficult since the upper bound in the conjecture is not a "Minkowksi-type" bound.

Given the above comments one might wonder about the more general question: What is the largest number of *consecutive* prime values that a quadratic polynomial can assume? There is reason to believe that the answer is: *Any* number of consecutive prime values may be assumed. We are indebted to Andrew Granville for the following elucidation which illustrates this contention.

Hardy and Littlewood considered a generalization of the twin prime conjecture. Essentially they reasoned as follows.

The consensus is that both p and $p+2$ are prime infinitely often, (where p is prime). Can we have $p, p+2$, and $p+4$ simultaneously prime infinitely often? For the following reasons the answer is no. Clearly $p \not\equiv 0 \pmod 3$. If $p \equiv -1 \pmod 3$ then $p+4 \equiv 0 \pmod 3$ and if $p \equiv 1 \pmod 3$ then $p+2 \equiv 0 \pmod 3$. A similar argument holds for $p, p+2, p+6, p+8, p+24$ to have one of them always divisible by 5. To generalize this idea, consider a finite set of positive integers $R = \{r_1, r_2, \dots r_k\}$. Clearly if q is a prime such that for each n, $1 \le n \le q$ we have $\prod_{i=1}^{k}(n+r_i) \equiv 0 \pmod q$, then there cannot exist infinitely many values p such that $\{p+r_i\}_{i=1}^{k}$ are all simultaneously prime. If such a prime q exists then R is called *inadmissable*. Otherwise R is *admissible*; i.e., R is admissable if and only if for all primes q there exists an integer a_q with $1 \le a_q \le q$ such that $\prod_{i=1}^{k}(a_q + r_i) \not\equiv 0 \pmod q$.

Hardy and Littlewood reasoned that if there is no good reason why $p+r_1, p+r_2, \dots, p+r_k$ cannot all be simultaneously prime infinitely often then they *should be*; or, more accurately,

THE PRIME k-TUPLES CONJECTURE (HARDY AND LITTLEWOOD (SEE [5]–[6])). If R is an admissable set then there are infinitely many integers n such that $n+r$ is prime for each $r \in R$. (The twin prime conjecture is then the case $R = \{0, 2\}$).

Now, with reference to the previous discussion, we have

THEOREM 3.3. *Suppose that the prime k-tuples conjecture is true. Then for any given integer $M > 0$ there exists a quadratic polynomial of the form $f(x) = x^2 + x + n$ such that $f(x)$ is prime for all integers x such that $1 \le x \le M$.*

PROOF. Let $r_j = f(j) = j^2 + j$ for $j = 1, 2, 3, \dots, M$.

CLAIM. The set $R = \{r_1, r_2, \dots, r_m\}$ is admissable.

If $q = 2$ then let $a_q = 1$. Now, each r_j is even so $\prod_{j=1}^{M}(r_j + 1)$ is odd. For each odd prime q let b_q be any quadratic non-residue modulo q, and set $a_q \equiv (1 - b_q)/4 \pmod q$. If $\prod_{j=1}^{M}(r_j + a_q) \equiv 0 \pmod q$ then $r_j + a_q \equiv 0 \pmod q$ for some j with $1 \le j \le M$; i.e., $r_j \equiv -a_q \pmod q$. Therefore, $(2j+1)^2 \equiv 4r_j + 1 \equiv 1 - 4a_q \equiv b_q \pmod q$. Thus we

https://doi.org/10.4153/CJM-1992-049-0 Published online by Cambridge University Press

achieve the contradiction that b_q is a quadratic residue modulo q. We have shown that $\prod_{j=1}^{M}(r_j + a_q) \not\equiv 0 \pmod{q}$; whence, the claim is secured.

Now, by the prime k-tuples conjecture we know that there exist arbitrarily large values of n for which $\{n + f_j\}_{j=1}^{M}$ are primes. Pick such an n and we see that $f(x) = x^2 + x + n$ is prime for $x = 1, 2, \ldots, M$. ∎

REMARK 3.3. From a non-theoretical (heuristic) point of view, it becomes an interesting question to see if we can find an n in Theorem 3.3 for $M = 50$ say. The largest number of known consecutive distinct (initial) prime values taken on by a quadratic polynomial is 45 (see [25] for such an example which supplants Euler's celebrated polynomial $x^2 - x + 41$ where $M = 40$). The methodology for doing this would be to pick n so that $1 - 4n$ is a quadratic non-residue for all primes $q < 200$ say. Then one can look at values of n is some residue classes modulo $\prod_{q<200} q$. Perhaps some sieve methods would provide us with a desired value of n. This is a problem for future investigation.

4. **Quadratic residue covers and quadratic polynomials.** First we refine the concept of a quadratic residue cover introduced by Mollin–Williams in [32].

DEFINITION 4.1. A finite set C of prime integers is called a *quadratic residue cover* of a family $\mathcal{F}$ of real quadratic fields whenever, for each field k of $\mathcal{F}$, there exists a prime p in C such that p splits in k, and such that the prime ideals above p are principal for only finitely many fields of $\mathcal{F}$, i.e., the prime ideals above p are not prinicpal "presque partout".

The last two authors proved in [30] that $(d/127) = 1$ whenever $d = (2^n + 3)^2 - 8$, and that the prime ideals above 127 are not principal whenever $127 < \sqrt{d}/2$. Thus, $C = \{127\}$ is a quadratic residue cover of the family $\mathcal{F} = \{Q(\sqrt{d}) : d = (2^n + 3)^2 - 8\}$. Using this fact they were able to prove in [29] their conjecture (posed in [28]), which now follows readily from Theorem 2.9 above.

THEOREM 4.1. *If* $d = (2^n + 3)^2 - 8$ *then* $h(d) = 1$ *if and only if* $d \in \{17, 41, 113, 353, 1217\}$.

REMARK 4.1. Theorem 4.1 is related to an investigation by Shanks of such forms d and their relationship to $h(d) = 1$.

In [28] the last two authors also conjectured that if $d = m^2 + 2$ then $h(d) = 1$ if and only if $d \in \{2, 3, 6, 11, 38, 83, 227\}$. Part (a) of Theorem 4.2 below shows that such a conjecture cannot be proved using quadratic residue covers. Indeed, for these fields 2 is ramified and the prime ideal above 2 is principal (since $N(m + \sqrt{d}) = -2$), so we can assume that any quadratic residue cover does not contain 2. Whenever $d = m^2 - 8$ then 2 splits, and the ideals above 2 are principal, (since $N\big((m + \sqrt{d})/2\big) = 2$). Therefore, again we can assume that any quadratic residue does not contain 2. Thus part (b) of Theorem 4.2 below shows that there does not exist any quadratic residue cover for this family. However, Theorem 4.1 shows that there exists one for a sub-family of this family.

THEOREM 4.2. *Let $\mathcal{C}$ be any finite set of odd prime integers. Then,*
(a) There exist infinitely many $d = m^2 + 2$ such that $(d/p) = -1$ for all $p \in \mathcal{C}$.
(b) There exist infinitely many $d = m^2 - 8$ such that $(d/p) = -1$ for all $p \in \mathcal{C}$.

Theorem 4.2 will be proved using the following.

THEOREM 4.3. *(a) Let $f(x) = ax^2 + bx + c$, $f(x) \not\equiv 0 \pmod 4$, where $a, b, c \in Z$, $a \neq 0$ and $\gcd(a, b, c)$ is square-free. Then there are infinitely many $n \in Z$ such that $f(n)$ is a square-free integer.*

(b) Let $f(x) = ax^2 + bx + c \in Z[x]$, $f(x) \not\equiv 0 \pmod 4$, $a > 0$ be with discriminant $D = b^2 - 4ac$ such that $\gcd(a, b, c)$ is square-free. Let $\mathcal{C}$ be any finite set of odd prime integers not dividing D. Then there exist infinitely many $n \in Z$ such that $f(n)$ is a square-free positive integer with $\big(f(n)/p\big) = -1$, and $p \in \mathcal{C}$, except when $p = 3 \in \mathcal{C}$, $a \equiv 2 \pmod 3$, and $D \equiv 1 \pmod 3$; in which case, $\big(f(n)/3\big) \neq -1$, $n \in Z$.

REMARK 4.2. Theorem 4.2 shows, for example, that there is no hope of ever finding any quadratic residue cover for the family $\mathcal{F} = \{Q(\sqrt{d}) : d = m^2 + r \equiv 5 \pmod 8\}$. For if we write $m = 2n + 1$ then $d = f(n)$ with $f(x) = 4x^2 + 4x + 5$ with $D = -2^6$. Since 2 is inert in the fields contained in $\mathcal{F}$, we may assume that any quadratic cover does not contain 2.

THEOREM 4.4. *Let p be an odd prime, $b \in F_p \setminus \{0\}$ and $\epsilon = \pm 1$. Then,*
(a) The set $\big\{x : x \in F_p, (x/p) = \epsilon$ and $\big((x+b)/p\big) = 1\big\}$ has $\frac{1}{4}\big(p - 2 - (b/p) - \epsilon\big(1 + (-b/p)\big)\big)$ elements.
(b) The set $\big\{x : x \in F_p, (x/p) = \epsilon$ and $\big((x+b)/p\big) \neq -1\big\}$ has $\frac{1}{4}\big(p - (b/p) - \epsilon\big(1 - (-b/p)\big)\big)$ elements. Thus, this set is non-empty except when $p = 3$, $b = 1$ and $\epsilon = 1$.

PROOF. (a) This follows from [7, Theorem 8.1], using the following expression for the number of elements of our set

$$1/4 \sum \big(1 + \epsilon(x/p)\big)\big(1 + (x+b)/p\big)\big)$$

where the sum ranges over all $b \in F_p$ and $x \neq 0, -b$.

(b) This follows from (a). ∎

PROOF OF THEOREM 4.3. (a) follows from [35]. For (b) we have that $f(x) = \frac{1}{4a}\{(2ax + b)^2 - \Delta\}$. If $p \in \mathcal{C}$ and p does not divide a then let a_p be such that $(a_p/p) = -(a/p)$ and such that $(a_p + \Delta/p) \neq -1$. Let b_p be such that $(2ab_p + b)^2 \equiv a_p + \Delta \pmod p$. If $p \in \mathcal{C}$ divides a, then p does not divide b, and we let b_p be such that $\big((bb_p + c)/p\big) = -1$. Let $b_{\mathcal{C}} \in Z$ such that $b_{\mathcal{C}} \equiv b_p \pmod p$, $p \in \mathcal{C}$. Hence $\big(f(b_{\mathcal{C}})/p\big) = -1$, $p \in \mathcal{C}$. Let $n = b_{\mathcal{C}} + kN_{\mathcal{C}}$, $k \in Z$ with $N_{\mathcal{C}} = \prod_{p \in \mathcal{C}} p$. Then $\big(f(n)/p\big) = -1$, $p \in \mathcal{C}$, and (a) gives us that there exist infinitely many $f(n)$ square-free. Indeed

$$f(n) = aN_{\mathcal{C}}^2 k^2 + f'(b_{\mathcal{C}})N_{\mathcal{C}}k + f(b)$$

and if p^2 divides $\gcd\left(aN_C^2, f'(b)N_C, f(b)\right)$ then p does not divide N_C (For if p divides N_C then p divides $f(b_C)$, which contradicts $\left(f(b_C)/p\right) = -1, p \in C$). Thus p^2 divides $\gcd\left(a, f'(b_C), f(b_C)\right) = \gcd(a, b, c)$ which is not possible. Hence (a) provides us with the result. ∎

In [31] Mollin and Williams introduced the concept of quadratic residue covers (refined at the beginning of this section) to study those forms d such that in the continued fraction expansion of ω, *all* Q_i/Q_0's are powers of a given prime p, and the relationship with $h(d) = 1$. As noted in [32], if $h(d) = 1$ then given all Q_i/Q_0's as powers of a single integer $a > 0$, a must in fact be prime. In particular they solved a conjecture for the case $p = 2$ as noted above. They also listed all $h(d) = 1$ when Q_i/Q_0's are all powers of p for $p \leq 19$, with one possible exception. They felt that this might be all possible values of d where $h(d) = 1$ and Q_i/Q_0's are p powers. The following section proves them to be correct.

5. **Consecutive powers of the Q_i/Q_0's and $h(d) = 1$.** Let

$$d = \left(\sigma\left(qa^n + (a^k - 1)/q\right)/2\right)^2 + \sigma^2 a^n$$

be square-free. In [21] we showed that if there are 3 or more Q_i/σ's (in the continued fraction expansion of ω) in a row as powers of a then d must be of the above form. The purpose of this section is to discover, (with one possible exception) all those values of d for which the class number $h(d)$ is 1.

We first note that if Q_i/σ is not a power of a, then $Q_i/\sigma > a^n$. This is very easy to show by the results on the continued fraction expansion of ω given in [22]. Thus if $a > 2$, we can never get a value of $Q_i/\sigma = 2$. If $d \not\equiv 5 \pmod 8$ there exists a prime ideal $\mathcal{P}$ lying over 2 such that $N(\mathcal{P}) = 2 < \sqrt{\Delta}/2$. Thus if $h(d) = 1$, $\mathcal{P}$ should be among the reduced principal ideals of K. Since this cannot be the case, we must have $h(d) > 1$ when $d \not\equiv 5 \pmod 8$ and $a \neq 2$. Hence we must have $\sigma = 2$ if $h(d) = 1$. Therefore in the sequel we will assume that $\sigma = 2$.

If a is composite, let p be any prime divisor of a. It follows that $(d/p) = 1$; hence, there exists a prime ideal $\mathcal{P}$ lying over p such that $N(\mathcal{P}) = p$ and $p \leq a/2 < \sqrt{\Delta}/2$. Hence $h(d) \neq 1$, as $\mathcal{P}$ cannot be among the reduced principal ideals of O_K. Thus, if $h(d) = 1$ we must have a being a prime. If $\gcd(n, k) > 1$ then by referring once again to the continued fraction expansion of ω given in [22] we see that no value of Q_i/σ can be a. If $h(d) = 1$ then a is a prime, $(d/a) = 1$ and $a < \sqrt{d}/2$, which means that some $Q_i/\sigma = 1$, a contradiction. We know from [22] that if all Q_i/σ are powers of a, then k divides n. Therefore if $h(d) = 1$ we must have $k = 1$ in this case.

Now we proceed to prove Conjecture 3.2 of [32]; i.e., that if $h(d) = 1$ and all Q_i/Q_0's are powers of p then $p \leq 19$ and the list given in [32] is complete; i.e.,

THEOREM 5.2. *Assume that in the continued fraction expansion of ω we have 3 or more Q_i/Q_0's in a row as powers of a single integer a; then $h(d) = 1$ if and only if $a = p$, a prime and either*

https://doi.org/10.4153/CJM-1992-049-0 Published online by Cambridge University Press

(a) $\pi = 1$ *and* $d \in \{2, 5, 13, 29, 53, 173, 293\}$

or

(b) $\pi > 1$ *and*

1) for $p = 2$, $d \in \{3, 6, 11, 17, 38, 41, 83, 113, 227, 353, 857, 1217\}$,

2) for $p = 3$, $d \in \{13, 21, 37, 61, 93, 157, 237, 397, 453, 7213\}$,

3) for $p = 5$, $d \in \{101, 461, 941\}$,

4) for $p = 7$, $d \in \{77, 197, 317, 557, 1253, 1877\}$,

5) for $p = 11$, $d \in \{773, 1133\}$,

6) for $p = 19$, $d = 437$,

with only one *possible value remaining, the existence of which would be a counterexample to the Riemann hypothesis.*

PROOF. From, [37] we have (with one possible exceptional value Δ remaining), that

$$L(1, \chi_\Delta) > .665\eta\Delta^{-\eta} \text{ for } 0 < \eta < 1/2 \text{ and } \Delta > \max\{e^{\frac{1}{\eta}}, e^{11.2}\}. \tag{1}$$

Also from the well known analytic class number formula we know that

$$2h(d)R = \sqrt{\Delta}L(1, \chi_\Delta), \tag{2}$$

and we let $d = \left(qa^n + (a^k - 1)/q\right)^2 + 4a^n$.

For our numbers we have $qa^n > a^k$ and $R < \left(\frac{k+n}{\gcd(n,k)}\right)\log\sqrt{\Delta}+1$ by Theorems 6.1–6.2 of [22]. Now $\sqrt{\Delta} > qa^n + (a^k - 1)/q > qa^n > a^n$ and since $qa^n > a^k$ we have $\sqrt{\Delta} > a^k$. It follows that

$$\max(k, n) < \log\sqrt{\Delta}/\log a \tag{3}$$

and

$$R < (\log\Delta)^2/(2\log a) + 1 \tag{4}$$

If we select $\eta = 1/\log\Delta + .001$, then $\eta > 1/\log\Delta$ and by (1), (2), (3), (4) we get

$$h(d) > \left(\frac{.24\Delta^{.499}}{(\log\Delta)^3/\log a + 2\log\Delta}\right) \geq g(\Delta) = \left(\frac{.24\Delta^{.499}}{(\log\Delta)^3/\log 2 + 2\log\Delta}\right)$$

Putting $\Delta = 10^{10}$, we see that $g(\Delta) > 1$. Since $g(\Delta)$ is an increasing function of Δ when $\Delta \geq 10^{10}$ we have $h(d) > 1$ whenever $d = \Delta > 10^{10}$ (with one possible exception).

In the special case of $k = 1$ we know by previous results [32] that we need only deal with values of $a \geq 13$ as all the values of d when $a \leq 11$ and $k = 1$ for $h(d) = 1$ are known.

Now,

$$R < \left(\frac{n+1}{2}\right)\log\Delta < \frac{1}{2}\left(\left(\frac{\log\Delta}{2\log a}\right) + 1\right)\log\Delta.$$

By (1) and (2) we get

$$h(d) > \left(\frac{.24\Delta^{.499}}{(\log\Delta)^3/2\log a + (\log\Delta)^2}\right)$$

when $\epsilon = .001$.

If $qa^n + (a-1)/q > 6000$, then $\Delta > 36,000,000$ and by using the above inequality we see that $h(d) > 1$. If $qa^n + (a-1)/q \leq 6000$ then there can only be a few possibilities for q, a and n. For each of these possibilities it is easy to check that the corresponding d value has either a small ($< \sqrt{\Delta}/2$) prime divisor or prime divisor ($\equiv 1 \pmod 4$) or there exists a small prime p ($< \sqrt{\Delta}/2$) such that $(\Delta/p) = 1$ and $p \neq a$. In each of these we cannot have $h(d) = 1$. Thus with one possible exception we know all the values of d such that $h(d) = 1$ when $k = 1$.

To deal with the remaining cases we need to prove the following claim.

CLAIM. If $k > 1$ and p is any prime such that $p < a^n$, $p \neq a$ and $(d/p) \neq -1$ then $h(d) > 1$.

Since $(d/p) \neq -1$ there must exist a prime ideal $\mathcal{P}$ lying over p such that $N(\mathcal{P}) = p < a^n$. Furthermore, since $k > 1$ we cannot have $h(d) = 1$ when all Q_i/σ values are powers of a. Thus we may assume the existence of some Q_i/σ which is not a power of a, and $p < a^n < Q_i/\sigma < \sqrt{d}/\sigma = \sqrt{\Delta}/2$. Thus if $h(d) = 1$ then p must be one of the Q_i/σ values, which, since $p \neq a$ is impossible. This completes the claim.

Now, if $h(d) = 1$ we must have $I(a,n,k,q) = qa^n + (a^k - 1)/q < 10^5$ and $a \geq 2$; whence $n \leq 16$. Also $a^{k-n} < q < 10^5/a^n$. Hence $a^k < 10^5$ and $k \leq 16$. Also $\gcd(n,k) = 1$. We can add some further restrictions by noting the identity

$$4d/\sigma^2 = \left(q_2^2 a^n + \left(\frac{a^{k/2}-1}{q_1}\right)^2\right)\left(q_1^2 a^n + \left(\frac{a^{k/2}-1}{q_2}\right)^2\right)$$

where $2|k$, $q = q_1 q_2$, $q_1 | a^{k/2} - 1$ and $q_2 | a^{k/2} + 1$. By putting $\sigma = 2$, $n = k$, $q_1 = q_2 = 1$ and $a = 1$, we see that this is a generalization of the well-known identity of Aurifeuille. Since $x^2 + y^2 \equiv 0, 1, 2 \pmod 4$ we see that $d \neq p$, $2p_1$, $p_1 p_2$ where p, p_1 and p_2 are primes and $p_1 \equiv p_2 \equiv -1 \pmod 4$ unless all of the following hold:

$$n \text{ is odd}, q \text{ is odd}, a \equiv -1 \pmod 4.$$

Thus if $h(d) = 1$ we must have all of these conditions above being true when $2|k$.

One case which is useful to eliminate is that of $n = 1$, $k = 2$. In this case

$$R < 3 \log \sqrt{\Delta} + 1$$

and

$$h(d) > \frac{.24\Delta^{.499}}{3(\log \Delta)^2 + 2 \log \Delta}.$$

If $\Delta > 13,000,000$, then $h(d) > 1$. Thus we need only consider

$$qa + (a^2 - 1)/q < 3606.$$

Since $qa > a^2$, this means that $a < 61$. We note that if $a \equiv -1 \pmod 3$ and $a \not\equiv -1 \pmod 9$ then

$$qa + (a^2 - 1)/q \not\equiv 0 \pmod 3.$$

https://doi.org/10.4153/CJM-1992-049-0 Published online by Cambridge University Press

Hence $d \equiv 0 \pmod 3$. Thus, if $a > 3$, then $h(d) > 1$, by the claim. Since $a \equiv -1 \pmod 4$, in order that $h(d) = 1$ we get $a \in \{3, 7, 19, 31, 43\}$. When $a = 3, 7, 31$ there is no odd divisor q of $a^2 - 1$ such that $q > a$. When $a = 19, 43$ there is only one possible divisor q of $a^2 - 1$ such that $q > a$ and $a < 3606/a$. Each of the resulting d values is divisible by a small prime $p < a$ ($p = 5$ when $a = 19$ and $p = 11$ when $a = 43$). Thus the case $n = 1$, $k = 2$ has been eliminated, (with one possible exception).

Since we have $k \neq 1$ and $n \geq 3$ when $k = 2$ and $qa^n > a^k$ we must have $a^3 < 10^5$ which means that since a must be a prime for $h(d) = 1$, we get $a \leq 43$.

By running a computer program on the remaining values of a, n, k, q we produced all the possible values of $I(a, n, k, q)$. If we found a prime $p < a^n$ such that

$$\left(\frac{I(a,n,k,q)^2 + 4a^n}{p}\right) \neq -1$$

then we eliminated the corresponding set of values of a, n, k, q from further consideration. This left us with a total of 14 square-free values of d for which $h(d)$ might be 1. Of these 9 are composite and have a prime factor congruent to 1 (mod 4); hence, $h(d) > 1$ for these. Of the 5 remaining numbers 857, 15641, 25301, 385661, 15280301 we found that $h(d) = 1, 3, 3$ and 7 for the first four. Also $15280301 \equiv 1 \pmod 7$ and 7 is not a value of any Q_i/σ in the continued fraction expansion of ω (where the period length is 15 for this number). Hence $h(d) > 1$ for this value. Thus the only new value of d for which $h(d) = 1$ beyond those computed earlier is $d = 857$ (where $a = 2, n = 2, k = 3, q = 7$). ∎

References

1. H. Cohn, *A second course in number theory*, John Wiley and Sons Inc., New York/London (1962).
2. L. E. Dickson, *Theory of Numbers*, Chelsea, NY (1957).
3. C. Friesen, *Legendre symbols and continued fractions*, Acta. Arith. **LIX**(1991), 365–379.
4. F. Halter-Koch, *Prime-producing quadratic polynomials and class numbers of quadratic orders*. In: Computational Number Theory, (A. Pethö, M. Pohst, H.C. Williams and H.G. Zimmer, eds.), Walter de Gruyter, Berlin (1991), 73–82.
5. G. H. Hardy and J. E. Littlewood, *Some problems of partitio numerorium; III: On the expression of a number as a sum of primes*, Acta. Math. (1924), 1–70.
6. D. Hensley and I. Richards, *On the incompatibility of two conjectures concerning primes*, Proc. Symp. in Pure Math., Analytic Number Theory (AMS) **24**(1973), 123–127.
7. L. K. Hua, *Introduction to number theory*, Springer-Verlag (1982).
8. P. Kaplan and K. S. Williams, *The distance between ideals in orders of real quadratic fields*, L'Enseignement Math. **36**(1990), 321–358.
9. G. Lauchaud, *Sur les corps quadratiques reëls principaux*, Seminaire de théorie de nombres; Paris 1984–85, Progress in Math. **63**, 165–175.
10. S. Louboutin, *Groupes des classes d'ideaux triviaux*, Acta. Arith, **LIV**(1989), 61–74.
11. ———, *Continued Fractions and Real Quadratic Fields*, J. Number Theory, **30**(1988), 167–176.
12. ———, *Prime producing quadratic polynomials and class numbers of real quadratic fields*, Canad. J. Math. **XLII**(1990), 315–341.
13. ———, *Extensions du Théorème de Frobenius-Rabinowitsch*, C.R. Acad. Sci. Paris I **312**(1991), 711–714.
14. H. Lu, *On the Class-Number of Real Quadratic Fields*, Sci. Sinica, (Special issue) **2**(1979), 118–130.
15. R. A. Mollin, *Necessary and Sufficient Conditions for the Class Number of a Real Quadratic Field to be One and a Conjecture of S. Chowla*, Proc. Amer. Math. Soc. **102**(1988), 17–21.
16. ———, *Lower Bounds for Class Numbers of Real Quadratic and Biquadratic Fields*, Proceed. Amer. Math. Soc. **101**(1987), 439–444.

17. ———, *Class Number One Criteria for Real Quadratic Fields I*, Proc. Japan Acad. (A) **63**(1987), 121–125.
18. ———, *Class Number One Criteria for Real Quadratic Fields II*, Proc. Japan Acad. (A) **63**(1987), 162–164.
19. ———, *On the Insolubility of a class diophantine equations and the non-triviality of the class number of related real quadratic fields of Richaud-Degert type*, Nagoya Math. J. **105**(1987), 39–47.
20. R. A. Mollin and H. C. Williams, *Computation of real quadratic fields with class number one*, Advances in the theory of computation and computational math., to appear.
21. ———, *Solution of the class number one problem for real quadratic fields of Richaud-Degert type (with one possible exception)*. In: Number Theory, Walter de Gruyter and Co., Berlin, (1990), (R. A. Mollin, ed.), 417–425.
22. ———, *Consecutive powers in continued fractions*, Acta. Arith., to appear.
23. ———, *Prime-producing polynomials and real quadratic fields of class number one*. In: Number Theory, (C. Levesque and J. M. DeKoninck (eds.)), Walter de Gruyter and Co., (1989), 654–663.
24. ———, *Class Number one for real quadratic fields, continued fractions, and reduced ideals*. In: Number Theory and Applications, (R. A. Mollin, ed.) NATO ASI, **C265**(1989), 481–496.
25. ———, *Period four and real quadratic fields of class number one*, Proc. Japan Acad. (A) **65**(1989), 89–93.
26. ———, *Class number problems for real quadratic fields*. In: Number Theory and Cryptography, London Math. Soc. Lecture Note Series, **154**(1990), 177–195.
27. ———, *Real quadratic fields of class number one and continued faction period less than six*, C.R. Math. Rep. Acad. Sci. Canada **XI**(1989), 51–56.
28. ———, *Powers of two, continued fractions, and real quadratic fields of class number one*, Memorial volume to C. F. Gauss (G. Rassias (ed.)), to appear.
29. ———, *On prime valued polynomials and class numbers of real quadratic fields*, Nagoya Math. J. **112** (1988), 143–151.
30. ———, *Affirmative solution of a conjecture related to a sequence of Shanks*, Proc. Japan Acad. (A) **67**(1991), 70–72.
31. ———, *Continued fractions of period five and real quadratic fields of class number one*, Acta. Arth. **LVI**(1990), 55–63,
32. ———, *Quadratic Residue Covers for Real Quadratic Fields*, to appear.
33. G. Rabinowitsch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratishen Zahlkorpern*, Proc. Fifth Internat. Congress Math. (Cambridge) (1913), 418–421.
34. ———, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratishen Zahlkorpern*, J. Rein. Angew. Math. **142**(1913), 153–164.
35. G. Ricci, *Ricerche arithmetiche sui polinomi*, Rend. Circ. Math. Palermo **57**(1933), 433–475.
36. D. Shanks, *The infrastructure of real quadratic fields and its applications*, Proc. 1972 number theory Conf., Boulder, CO (1973), 217–224.
37. T. Tatuzawa, *On a theorem of Siegel*, Japan J. Math. **21**(1951), 163–178.
38. H. C. Williams, *Continued fractions and number theoretic computations*, Rocky Mtn. J. Math. **15**(1985), 621–655.
39. 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.

University of Caen
France

University of Calgary
Canada

University of Manitoba
Canada