MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 355-360

AMBIGUOUS CLASSES IN QUADRATIC FIELDS

R. A. MOLLIN

Dedicated to the memory of D. H. Lehmer

ABSTRACT. We provide sufficient conditions for the class group of a quadratic field (with positive or negative discriminant) to be generated by ambiguous ideals. This investigation was motivated by a recent result of F. Halter-Koch, which we show is false.

1. INTRODUCTION

The principal result is the provision of sufficient conditions for the class group of quadratic fields to be generated by certain prescribed ambiguous ideals in terms of certain canonical quadratic polynomials. We were motivated by the principal result of [1], which contains a serious error. We therefore provide a counterexample to Theorem 3.1 of [1], which motivates the discussion. Although the aforementioned result is false, we provide a list (which we conjecture to be complete) of all the polynomials which satisfy the prime producing hypothesis (but not necessarily the conclusion) of [1]. We maintain that this is of interest in its own right.

2. NOTATION AND PRELIMINARIES

Let $Q(\sqrt{d})$ be a quadratic field, where d is a (positive or negative) squarefree integer, and let $\Delta = 4d/\sigma^2$ be its *discriminant*, where $\sigma = 2$ if $d \equiv 1 \pmod 4$ and $\sigma = 1$ otherwise. Thus the *radicand* d is the squarefree kernel of Δ.

Let $[\alpha, \beta] = \alpha\mathbb{Z} \oplus \beta\mathbb{Z}$; then the maximal order $\mathcal{O}_\Delta$ of $Q(\sqrt{d})$ is $[1, \omega_\Delta]$, where $\omega_\Delta = (\sigma - 1 + \sqrt{d})/\sigma$. It is well known that I is a nonzero ideal in $\mathcal{O}_\Delta$ if and only if $I = [a, b + c\omega_\Delta]$, where a, b, $c \in \mathbb{Z}$ with $c|b$, $c|a$ and $ac|N(b+c\omega_\Delta)$, where N is the norm, i.e., $N(\alpha) = \alpha\overline{\alpha}$, where $\overline{\alpha}$ is the algebraic conjugate of α. The ideal I is called *primitive* if $c = 1$ and $a > 0$. In this case, a is the smallest positive integer in I and $a = N(I) = (\mathcal{O}_\Delta : I)$. Let C_Δ denote the class group of $\mathcal{O}_\Delta$. Equivalence in C_Δ is denoted by $I \sim J$ (by which we mean that there are nonzero elements α_1 and α_2 of $\mathcal{O}_\Delta$ with $\alpha_1 I = \alpha_2 J$). We denote the order of C_Δ by h_Δ, the *class number* of $\mathcal{O}_\Delta$. Principal ideals (generated by a single element α) are denoted by (α). The following is well known.

Received by the editor May 19, 1992 and, in revised form, September 10, 1992.
1991 *Mathematics Subject Classification.* Primary 11R11, 11R29, 11Y40.
Key words and phrases. Ambiguous ideal, quadratic field, class number, exponent.

Theorem 2.1. *Every class of C_Δ contains a primitive ideal I with $N(I) < M_\Delta$, where*

$$M_\Delta = \begin{cases} \sqrt{-\Delta/3} & \text{if } \Delta < 0, \\ \sqrt{\Delta/5} & \text{if } \Delta > 0. \end{cases}$$

Based upon the above, the following improves upon Theorem 2.7 of [2].

Theorem 2.2. *The class group C_Δ is generated by the primitive prime ideals $\mathscr{P}$ with $N(\mathscr{P}) < M_\Delta$.*

Proof. By Theorem 2.1 there is an ideal I in each class with $N(I) < M_\Delta$. Each such ideal is divisible by a primitive prime ideal $\mathscr{P}$, and $N(\mathscr{P}) \leq N(I) < M_\Delta$. The result now follows. □

Throughout the paper, if q is a positive squarefree divisor of Δ, then $\mathscr{Q}_q$ denotes the unique $\mathscr{O}_\Delta$-prime ideal above q, or simply $\mathscr{Q}$ if no confusion with other divisors of Δ arises.

3. Prime quadratics

As mentioned above, we begin with a counterexample to Theorem 3.1 of [1], which motivates the discussion leading to criteria for C_Δ to be generated by ambiguous ideals (given in terms of certain local primality conditions for the polynomials which we now define).

Definition 3.1. Let q be a positive squarefree divisor of a discriminant Δ; then

$$F_{\Delta,q}(x) = qx^2 + (\alpha - 1)qx + \frac{1}{4q}((\alpha - 1)q^2 - \Delta),$$

where $\alpha = 1$ if $4q$ divides Δ and $\alpha = 2$ otherwise. Also, set $A_\Delta = \lfloor \frac{1}{2}(M_\Delta - 1) \rfloor$.

Example 3.1. The claim of [1, Theorem 3.1, p. 75] is that if, under the assumption of Definition 3.1, we have that $|F_{\Delta,q}(x)|$ is 1 or prime for all integers x with $0 \leq x \leq A_\Delta$, then $C_K = \{1, \mathscr{Q}\}$. The following example contradicts this assertion. Let $\Delta = 285 = 3 \cdot 5 \cdot 19 = 17^2 - 4$ and $q = 15$; then $F_{\Delta,q}(x) = 15x^2 + 15x - 1$. Here, $\lfloor M_\Delta \rfloor = 7$ and $A_\Delta = 3$, so $|F_{\Delta,q}(x)| = 1, 29, 89$ and 179 for $x = 0, 1, 2$, and 3, respectively. However, $C_\Delta \neq \{1, \mathscr{Q}_{15}\}$. In fact $\mathscr{Q}_{15} \sim 1$ and $C_\Delta = \langle \mathscr{Q}_3 \rangle = \langle \mathscr{Q}_5 \rangle$, where $\langle x \rangle$ denotes the cyclic group generated by x.

Remark 3.1. For the interested reader the error in the proof of [1, Theorem 3.1, p. 75] lies in the assumption that (in Halter-Koch's notation) $\mathscr{I}\mathscr{J}_q$ is primitive. (For instance, in Example 3.1, $\mathscr{J}_q = \mathscr{Q}_{15}$ and $\mathscr{Q}_3 = \mathscr{J}$; whence, $\mathscr{I}\mathscr{J}_q = \mathscr{Q}_3^2\mathscr{Q}_5$ is definitely not primitive.)

We have compiled in Table 3.1 a list of all positive radicands for which $|F_{\Delta,q}(x)|$ is 1 or prime for all integers x with $0 \leq x \leq A_\Delta$. Therein, the radicands 1085, 1965 and 2085 are also counterexamples to [1, Theorem 3.1].

Now we prove a result which gives sufficient conditions for C_Δ to be generated by ambiguous ideals. First we need a preliminary result which generalizes [2, Lemma 3.1, p. 7].

Lemma 3.1. *Let $q \geq 1$ be a squarefree divisor of a discriminant Δ. If p is a prime, then $F_{\Delta,q}(x) \equiv 0 \pmod{p}$ for some integer $x \geq 0$ if and only if $(\Delta/p) \neq -1$ and p does not divide q.*

Proof. If $(\Delta/p) \neq -1$ and $p = 2$ does not divide q, then choose $x = 0$ if $(q^2(\alpha - 1) - \Delta)4q$ is even, and $x = 1$ otherwise. Now assume $p > 2$. Thus, there is an integer y such that $\Delta/q \equiv qy^2 \pmod{p}$. By replacing y by $p - y$ if necessary, we may assume that $y \equiv \alpha - 1 \pmod{2}$. Setting $y = 2x + \alpha - 1$, we get that $\Delta/q \equiv q(2x + \alpha - 1)^2 \pmod{p}$, i.e.,

$$F_{\Delta,q}(x) = qx^2 + qx(\alpha - 1) + \frac{1}{4q}((\alpha - 1)q^2 - \Delta) \equiv 0 \pmod{p}.$$

Conversely, if $F_{\Delta,q}(x) \equiv 0 \pmod{p}$, then $\Delta \equiv [q(2x + \alpha - 1)]^2 \pmod{p}$, whence $(\Delta/p) \neq -1$. Moreover, if p divides q, then p^2 divides Δ, whence $p = 2$. Therefore, $\Delta \equiv 0 \pmod{4}$. If $\Delta \equiv 8 \pmod{16}$, then $qx^2 - \Delta/4q$ is odd for all $x \geq 0$, a contradiction. Therefore, $\Delta \equiv 12 \pmod{16}$, in which case $(q^2 - \Delta)/4q$ must be even (since $\alpha = 2$ and q is even in this case). Therefore, $q^2 \equiv \Delta \pmod{16}$, whence $(q/2)^2 \equiv 3 \pmod{4}$, which is absurd. □

Theorem 3.1. *Let $q_i \geq 1$ for $1 \leq i \leq n$ be pairwise relatively prime, squarefree divisors of a discriminant Δ. If, for each prime $p < M_\Delta$ with $(\Delta/p) \neq -1$ and $p \neq q_i$ for any positive $i \leq n$ there exists a $q = \prod_{i \in \mathcal{S}} q_i$ for some $\mathcal{S} \subseteq \{1, 2, \ldots, n\}$ such that $|F_{\Delta,q}(x)| = p$ for some nonnegative integer x, then*

$$C_\Delta = \{1, \mathcal{Q}_1, \ldots, \mathcal{Q}_n\}.$$

Proof. By Theorem 2.2, C_Δ is generated by the primitive prime ideals $\mathcal{P}$ with $N(\mathcal{P}) = p < M_\Delta$ and $(\Delta/p) \neq -1$. If $p \neq q_i$ for any positive $i \leq n$, then by hypothesis, $|F_{\Delta,q}(x)| = p$ for some integer $x \geq 0$ (with q as above). Therefore, $\frac{1}{4}(q(2x + \alpha - 1)^2 - \Delta/q) = p$. Thus, $\frac{1}{4}[(q(2x + \alpha - 1))^2 - \Delta] = pq$. Now set

$$b = \begin{cases} qx & \text{if } \alpha = 1, \\ qx + (q-1)/2 & \text{if } \alpha = 2 \text{ and } q \text{ is odd}, \\ q(2x+1)/2 & \text{if } \alpha = 2 \text{ and } q \text{ is even}. \end{cases}$$

Hence, $\mathcal{P}\mathcal{Q} = [pq, b + \omega_\Delta]$ is primitive with $N(b + \omega_\Delta) = pq$, i.e., $\mathcal{P}\mathcal{Q} \sim 1$ (since, in fact, $\mathcal{P}\mathcal{Q} = (b + \omega_\Delta))$, whence $\mathcal{P} \sim \mathcal{Q}$, and the result follows. □

Remark 3.2. The case where $n = 1$ in Theorem 3.1 provides a correct version of Theorem 3.1 of [1]. We note that the radicand 285 in Example 3.1 does not allow us to choose $q = 15$ because neither $|F_{\Delta,1}(x)|$ nor $|F_{\Delta,q}(x)|$ yields the value 3 or 5 for any nonnegative integer $x \leq A_\Delta = 3$. However, if we choose $q = 3$ or $q = 5$, then the hypothesis of Theorem 3.1 is satisfied, since $|F_{\Delta,3}(2)| = 5$ and $|F_{\Delta,5}(1)| = 3$, with the observation that 3 and 5 are the only noninert primes less than M_Δ. Therefore, we arrive at the correct conclusion, i.e., $C_{285} = \langle \mathcal{Q}_3 \rangle = \langle \mathcal{Q}_5 \rangle$.

Remark 3.3. Theorem 3.1 of [1] becomes correct under the assumption $q = 1$ or q prime, $q | D_0$, $q \nmid f$.

Now we give a sequence of examples to illustrate Theorem 3.1.

Example 3.2. Let $\Delta = 1157 = 13 \cdot 89 = 34^2 + 1$ and set $q = 13$. Since $\lfloor M_\Delta \rfloor = 15$ and the only noninert prime $p < M_\Delta$ with $p \neq 13$ is $p = 7$, then the fact that $F_{\Delta,13}(1) = 7$ implies that the hypothesis of Theorem 3.1 holds. Thus, $C_\Delta = \langle \mathscr{Q}_{13} \rangle$.

Example 3.3. Let $\Delta = 4 \cdot 195 = 4 \cdot 3 \cdot 5 \cdot 13$; then $\lfloor M_\Delta \rfloor = 12$ and $A_\Delta = 6$. Let $q_1 = 3$ and $q_2 = 5$. Since $F_{\Delta,15}(1) = 2$, which is the only prime $p < M_\Delta$, $p \neq 2$ with p noninert, then by Theorem 3.1

$$C_\Delta = \langle \mathscr{Q}_3 \rangle \times \langle \mathscr{Q}_5 \rangle .$$

Example 3.4. Let $\Delta = 4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 4 \cdot 1155$; then $\lfloor M_\Delta \rfloor = 30$ and $A_\Delta = 14$. If $q_1 = 3$, $q_2 = 5$ and $q_3 = 7$, then the only noninert primes $p < M_\Delta$ with $p \neq q_i$ for $i = 1, 2, 3$ are 2, 11, 17 and 29. Since $F_{\Delta,35}(1) = 2$, $F_{\Delta,105}(0) = 11$, $F_{\Delta,15}(2) = 17$ and $F_{\Delta,21}(2) = 29$, then by Theorem 3.1

$$C_\Delta = \langle \mathscr{Q}_3 \rangle \times \langle \mathscr{Q}_5 \rangle \times \langle \mathscr{Q}_7 \rangle .$$

The following consequences of Theorem 3.1 show its high degree of applicability to results in the literature.

Corollary 3.1 [3, Theorem 1, p. 655]. *If* $\Delta = 4(4l^2 \pm 2) > 8$ *and* $|F_{\Delta,2}(x)| = |2x^2 - d/2|$ *is* 1 *or prime for all integers* x *with* $0 \le x < \sqrt{d}/2$, *then* $h_\Delta = 1$.

Proof. By Theorem 3.1 and Lemma 3.1, $C_\Delta = \{1, \mathscr{Q}_2\}$. However, $\mathscr{Q}_2 \sim 1$, since $|N((2l \pm 2 + \sqrt{\Delta})/2)| = 2$. □

Corollary 3.2 [3, Theorem 2, p. 656]. *If* $\Delta = 4((2l+1)^2 \pm 2)$ *with* $l > 0$ *and* $|F_{\Delta,2}(x)| = |2x^2 + 2x + (1 - \Delta)/2|$ *is* 1 *or prime for all integers* x *with* $0 < x < (\sqrt{\Delta} + 1)/2$, *then* $h_\Delta = 1$.

Proof. By Theorem 3.1 and Lemma 3.1, $C_\Delta = \{1, \mathscr{Q}_2\}$. However, $\mathscr{Q}_2 \sim 1$, since $|N(2l + 1 + \sqrt{\Delta})| = 2$. □

The following is [3, Conjecture 2, p. 658].

Corollary 3.3. *Let* $\Delta = l^2 - q \equiv 5 \pmod 8$, *where* q *is an odd prime dividing* l. *If* $|F_{\Delta,q}(x)| = |qx^2 + qx + (q^2 - \Delta)/4q|$ *is* 1 *or prime for all integers* x *with* $0 \le x < \sqrt{d-1}/4 - \frac{1}{2}$, *then* $h_\Delta = 1$.

Proof. By Theorem 3.1 and Lemma 3.1, $C_\Delta = \{1, \mathscr{Q}_q\}$. However, $\mathscr{Q}_q \sim 1$, since $N(l + \sqrt{\Delta}) = q$. □

The following is [3, Conjecture 4, p. 659].

Corollary 3.4. *Let* $\Delta = l^2 \pm 4q$, *where* q *is an odd prime dividing* l. *If* $|qx^2 + qx + (q^2 - \Delta)/4q|$ *is* 1 *or prime for all integers* x *with* $0 \le x < (\sqrt{\Delta - 1} + 1)/2$, *then* $h_\Delta = 1$.

Proof. Since $|N((l + \sqrt{\Delta})/2)| = q$, then the result follows as above. □

Remark 3.4. The types of forms in Corollaries 3.1–3.4 are called extended *Richaud-Degert* (ERD)*-types*, i.e., those of the form $d = \Delta/\sigma^2 = l^2 + r$, where r divides $4l$. In [3, 4] we found all such Δ's with $h_\Delta = 1$ under the assumption of a suitable Riemann hypothesis, and in [5] we were able to eliminate the Riemann hypothesis and show that our list is complete (with one possible exceptional value of Δ, whose existence would be a counterexample to that Riemann hypothesis). The following answers a question about ERD types posed in [1, Remark, p. 76].

TABLE 3.1. This table lists all radicands $0 < d < 10^6$ such that $|F_{\Delta,q}(x)|$ is 1 or prime for all nonnegative integers $x \leq A_\Delta$, where q is a positive squarefree divisor of the discriminant Δ.

d	q	d	q	d	q	d	q
2	1	26	2	93	3	402	6
2	2	26	13	102	6	413	7
3	1	29	1	110	10	437	1
3	2	29	29	110	22	437	23
3	3	30	6	122	2	453	3
5	1	30	10	138	6	573	3
5	5	30	30	141	3	645	15
6	2	33	3	165	3	678	6
6	3	33	11	165	5	717	3
6	6	35	5	173	1	917	7
7	1	35	7	182	14	957	3
7	7	38	2	182	26	965	5
10	2	38	38	213	3	1077	3
10	5	42	6	222	6	1085	5
10	10	42	14	230	10	1085	7
11	1	42	42	237	3	1085	35
11	11	53	1	258	6	1133	11
13	1	53	53	285	5	1245	15
13	13	62	2	285	15	1253	7
14	2	66	6	293	1	1293	3
14	7	69	3	318	6	1685	5
14	14	77	7	341	11	1757	7
15	3	77	11	357	3	1965	15
15	5	77	77	357	7	2085	15
21	1	78	6	362	2	2373	21
21	3	85	5	365	5	2397	3
21	21	85	17	398	2	4245	15

Example 3.5. Let $\Delta = 917 = 7 \cdot 131$; then $\lfloor M_\Delta \rfloor = 13$, $A_\Delta = 6$. The only noninert prime $p < 13$, $p \neq 7$, is $p = 11$ and $F_{\Delta,7}(2) = 11$, so by Theorem 3.1, $C_\Delta = \langle \mathscr{C}_7 \rangle$. We note that 917 is not an ERD-type. The only other non-ERD type appearing in Table 3.1 is $\Delta = 341$. (Note that since $|F_{341,11}(0)| = 5$, the only noninert prime $p < M_{341}$ (with $p \neq 11$), then $C_{341} = \langle \mathscr{C}_{11} \rangle$).

Although the principal result of [1] has been shown to be false herein, it is still of interest in its own right to determine all those positive Δ's and q's such that $F_{\Delta,q}(x)$ is 1 or prime for $0 \leq x \leq A_\Delta$.

Some serious computational evidence leads us to pose:

Conjecture 3.1. *Table* 3.1 *is complete, i.e., if* $d > 4245$, *then* $|F_{\Delta,q}(x)|$ *is composite for some nonnegative* $x \leq A_\Delta$.

Remark 3.5. It is interesting to note that the only ERD types d, with class number 1, that do *not* appear in Table 3.1 are $d = 17$, 37, 47, 83, 101, 167, 197, 227 and 677. Moreover, the only *non*-ERD types which *are* in Table 3.1 are 341 and 917. Also, the values which have class number bigger than 1 are 10, 15, 26, 30, 35, 42, 66, 78, 85, 102, 110, 122, 138, 165, 182, 222, 230, 258, 285, 318, 357, 362, 365, 402, 645, 678, 957, 965, 1085, 1245, 1685, 1965, 2085, 2373, 2397 and 4245, *all* of which have class number 2.

We note that if $F_{\Delta,q}(x)$ is 1 or prime for all integers x with $0 \leq x \leq A_\Delta$, we cannot even guarantee that $h_\Delta \leq 2$. Given Remark 3.4 and Conjecture 3.1 above, we must turn to negative discriminants.

Example 3.6. Let $\Delta = -520 = -2^3 \cdot 5 \cdot 13$ and set $q = 10$, whence $\lfloor M_\Delta \rfloor = 13$, and so $A_\Delta = 6$. Also, $F_{\Delta,q}(x) = 10x^2 + 13 = 13$, 23, 53, 103, 173, 263 and 373 for $x = 0$, 1, 2, 3, 4, 5 and 6, respectively. However, $h_\Delta = 4$. In fact, then $C_\Delta \neq \{1, \mathscr{Q}_{10}\}$. If in Theorem 3.1 we take $q_1 = 5$ and $q_2 = 13$, then $F_{\Delta,65}(0) = 2$, which is the only noninert prime less than M_Δ (other than 5 and 13), so the hypothesis of Theorem 3.1 is satisfied and we have that $C_\Delta = \langle \mathscr{Q}_5 \rangle \times \langle \mathscr{Q}_{13} \rangle$. We observe that both $F_{\Delta,5}(0)$ and $F_{\Delta,13}(0)$ are composite. This illustrates that the generation of C_Δ by ambiguous ideals dividing q, in general, has less to do with the prime-producing capacity of $F_{\Delta,q}(x)$ for an initial string of x values, as asserted in [1], than it does with its local capacity to "hit" certain primes.

We have made significant progress with negative discriminants and quadratic polynomials, which will be published at a later date.

Acknowledgment

The author's research is supported by NSERC Canada grant #A8484. Moreover, the author welcomes the opportunity to thank Mike Jacobson, a student of Hugh Williams, for doing the computations which led to Table 3.1.

Bibliography

1. F. Halter-Koch, *Prime-producing quadratic polynomials and class numbers of quadratic orders*, Computational Number Theory (A. Pethö, M. Pohst, H. C. Williams, and H. Zimmer, eds.), de Gruyter, Berlin, 1991, pp. 73–82.
2. 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 residue covers*, Canad. J. Math. **44** (1992), 1–19.
3. R. A. Mollin and H. C. Williams, *Prime producing quadratic polynomials and real quadratic fields of class number one*, Number Theory (J. M. De Koninck and C. Levesque, eds.), de Gruyter, Berlin, 1989, pp 654–663.
4. ——, *On prime valued polynomials and class numbers of real quadratic fields*, Nagoya Math. J. **112** (1988), 143–151.
5. ——, *Solution of the class number one problem for real quadratic fields of extended Richaud-Degert type (with one possible exception)*, Number Theory (R. A. Mollin, ed.), de Gruyter, Berlin, 1990, pp. 417–425.

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