

12. Orders in Quadratic Fields. I

By R. A. MOLLIN

Mathematics Department, University of Calgary, Canada

(Communicated by Shokichi IYANAGA, M. J. A., March 12, 1993)

Abstract: The primary purpose herein is to provide sufficient conditions for a quadratic order to have its class group generated by ambiguous ideals, and we conjecture that the conditions are in fact necessary. These conditions are given in terms of certain prime-producing quadratic polynomials.

Key words and phrases: Real quadratic order; class Group; quadratic polynomial.

§1. Notation and preliminaries. Let $[\alpha, \beta]$ denote the \mathbf{Z} -module $\{\alpha x + \beta y : x, y, \in \mathbf{Z}\}$ and fix $D_0 \in \mathbf{Z}$ as a (positive or negative) square-free integer. Set $\sigma = 2$ if $D_0 \equiv 1 \pmod{4}$ and $\sigma = 1$ otherwise. Define $\omega_0 = (\sigma - 1 + \sqrt{D_0})/\sigma$, $\Delta_0 = (\omega_0 - \bar{\omega}_0)^2 = 4D_0/\sigma^2$, where $\bar{\omega}_0$ is the algebraic conjugate of ω_0 , and let $\omega_\Delta = f\omega_0 + h$ where $f, h \in \mathbf{Z}$. If we set $\mathcal{O}_\Delta = [1, f\omega_0] = [1, \omega_\Delta]$ and $\Delta = (\omega_\Delta - \bar{\omega}_\Delta)^2 = f^2\Delta_0$ then \mathcal{O}_Δ is an order in $Q(\sqrt{\Delta}) = Q(\sqrt{D_0})$ having conductor f , and fundamental discriminant Δ_0 . Moreover D_0 is the radicand; i.e., the square-free kernel of the discriminant Δ . It is well-known (e.g. see [1]) that I is a non-zero ideal in \mathcal{O}_Δ if and only if $I = [a, b + c\omega_\Delta]$ where $a, b, c, \in \mathbf{Z}$ with $c \mid b$, $c \mid a$, and $ac \mid N(b + c\omega_\Delta)$, where N is the norm from $Q(\sqrt{\Delta})$ to Q ; i.e., $N(\alpha) = \alpha\bar{\alpha}$. I is called *primitive* if $c = 1$, and $a > 0$. In this case a is the smallest positive integer in I and $a = N(I) = (\mathcal{O}_\Delta : I)$. A primitive ideal I can be written as $I = [a, b + \omega_\Delta]$ with $0 \leq b \leq a$. An ideal I in \mathcal{O}_Δ is called *regular* if $\mathcal{O}_0 = \{\alpha \in Q(\sqrt{\Delta}) : \alpha I \subseteq \mathcal{O}_0\}$. All regular ideals are *invertible*. Note that an ideal I is invertible if there is an element $\gamma \in I$ such that $\gcd(f, N(\gamma)) = 1$, (e.g. see [1, Theorem 7, p.122]). Thus if $\gcd(f, N(I)) = 1$ then I is invertible. We denote *equivalence of ideals* by $I \sim J$ (by which we mean that there are non-zero elements α_1 and α_2 of \mathcal{O}_Δ with $\alpha_1 I = \alpha_2 J$), and we denote the group of equivalence classes by C_Δ (and note that $C_\Delta \cong \text{Pic } \mathcal{O}_\Delta$). Let h_Δ be the order of C_Δ ; i.e., the *class number* of \mathcal{O}_Δ . We denote the *exponent* of C_Δ by e_Δ ; i.e., the smallest positive integer e_Δ such that $I^{e_\Delta} \sim 1$ for all I in C_Δ . Also *principal* ideals generated by a single element α are denoted by (α) . We denote finally

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

The following is well-known, (e.g. see [1, Theorem 11, p.141]).

Theorem 1.1. Every class in C_Δ contains a regular, primitive ideal I with $N(I) < M_\Delta$.

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

Theorem 1.2. C_Δ is generated by the primitive regular prime ideals \mathcal{P} with $N(\mathcal{P}) < M_\Delta$.

Proof. By Theorem 1.1 there is an ideal I in each class of C_Δ with $N(I) < M_\Delta$. Each such ideal is divisible by a primitive, regular prime ideal \mathcal{P} , and $N(\mathcal{P}) \leq N(I) < M_\Delta$. The result now follows.

We recall finally that, an *Extended Richaud-Degert type* radicand (or simply ERD-type) is one of the form $l^2 + r$ where $4l \equiv 0 \pmod{r}$.

§2. Ambiguous ideals and quadratic polynomials. All of the above notation is in force throughout. First we need the following.

Definition 2.1. Let q be a positive square-free divisor of Δ_0 with $\gcd(q, f) = 1$, 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.

To obtain the main result we first need a technical result which generalizes [3, Lemma 3.1, p.830].

Lemma 2.1. Let $q \geq 1$ be a square-free divisor of Δ_0 with $\gcd(q, f) = 1$. 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 is an odd prime then there exists an integer x such that $\Delta \equiv q^2(2x + \alpha - 1)^2 \pmod{p}$; i.e., $F_{\Delta, q}(x) = qx^2 + qx(\alpha - 1) + \frac{1}{4q}((\alpha - 1)q^2 - \Delta) \equiv 0 \pmod{p}$. If $p = 3$ then either $x = 0$ or $x = 1$ suffices.

Conversely, if $F_{\Delta, q}(x) \equiv 0 \pmod{p}$ then $\Delta \equiv [q(2x + \alpha - 1)]^2 \pmod{p}$; whence $(\Delta/p) \neq -1$. Also if p divides q then $p = 2$ is forced and it is easy to see that this leads to a contradiction.

Now we provide a proof of the main result.

Theorem 2.1. Let $q_i \geq 1$ for $1 \leq i \leq n$ be pairwise relatively prime, square-free divisors of Δ_0 with $\gcd(f, q_i) = 1$ for all such i . For each prime $p < M_\Delta$ with $(\Delta/p) \neq -1$ and $p \neq q_i$ for any positive $i \leq n$, assume that the following both hold.

(1) There is a $q = \prod_{i \in \mathcal{S}} q_i$ for some $\mathcal{S} \subseteq \{1, 2, \dots, n\}$ such that $|F_{\Delta, q}(x)| = pr$ for some integer $x \geq 0$, and some $r \geq 1$, where r is not divisible by any unramified primes

and,

(2) If $r > 1$ then there exists a $t = \prod_{i \in \bar{\mathcal{S}}} q_i$ with $\bar{\mathcal{S}} \subseteq \{1, 2, \dots, n\}$ such that $|F_{\Delta, t}(x)| = r$ for some integer $x \geq 0$. Then $C_\Delta = \{1, \mathcal{Q}_1, \dots, \mathcal{Q}_n\}$, where \mathcal{Q}_i is the unique \mathcal{O}_Δ -ideal over q_i .

Proof. By Theorem 1.2, C_Δ is generated by the primitive, regular 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 (1), there is a $q = \prod_{i \in \mathcal{S}} q_i$ for some $\mathcal{S} \subseteq \{1, 2, \dots, n\}$ such that $|F_{\Delta, q}(x)| = pr$ for some integer x (with the observation that, by

Lemma 2.1, p does not divide q . Therefore $\frac{1}{4}(q(2x + \alpha - 1)^2 - \Delta/q) = pr$. Thus, $\frac{1}{4}[(q(2x + \alpha - 1))^2 - \Delta] = pqr$. Now, set

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

Let \mathcal{Q}, \mathcal{R} and \mathcal{T} be \mathcal{O}_Δ -ideals over q, r and t respectively. Hence $\mathcal{P}\mathcal{Q}\mathcal{R} = [pq, b + \omega_\Delta]$ is a primitive, regular ideal with $N(b + \omega_\Delta) = pqr$; i. e., $\mathcal{P}\mathcal{Q}\mathcal{R} \sim 1$ since, in fact, $\mathcal{P}\mathcal{Q}\mathcal{R} = (b + \omega_\Delta)$. Similarly, from hypothesis (2) we get that $\mathcal{T}\mathcal{R} \sim 1$. Thus, $\mathcal{P} \sim \mathcal{T}\mathcal{Q}$ and the result follows.

Now we illustrate the above with an example.

Example 2.1. Let $\Delta = 4 \cdot 25935 = 4 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19$, then $[M_\Delta] = 144$, $h_\Delta = 16$ and $A_\Delta = \lfloor (M_\Delta - 1)/2 \rfloor = 71$. Let $q_1 = 3, q_2 = 5, q_3 = 7$ and $q_4 = 13$. We may verify that other than these q_i 's the non-inert primes $p < M_\Delta$ are in the set $\mathcal{S} = \{2, 19, 29, 31, 41, 43, 67, 71, 79, 89, 97, 101, 103, 107, 109, 139\}$. We verify this for example by looking at a print out of the divisors $p < M_\Delta$ of $F_{\Delta,1}(x)$ for $0 \leq x \leq A_\Delta$ using Lemma 2.1. Moreover, from a listings of all $|F_{\Delta,q}(x)|$ for all divisors q of $3 \cdot 5 \cdot 7 \cdot 13$ and $0 \leq x \leq A_\Delta$ we glean from Theorem 2.1 that

q	x	$F_{\Delta,q}(x)$	$p \in \mathcal{S}$
7	23	2	2
1365	0	19	19
114	1	29	29
266	0	31	31
39	4	41	41
30	5	43	43
5	32	67	67
210	0	71	71
91	2	79	79
190	0	89	89
182	0	97	97
26	6	101	101
3	54	103	103
95	190	107	107
21	8	109	109
65	2	139	139

Therefore,

$$C_\Delta = \{1, \mathcal{Q}_2, \mathcal{Q}_3, \mathcal{Q}_5, \mathcal{Q}_7, \mathcal{Q}_{13}\}, \text{ but } \mathcal{Q}_2 \sim \mathcal{Q}_7 \text{ so,}$$

$$C_\Delta = \langle \mathcal{Q}_3 \rangle \times \langle \mathcal{Q}_5 \rangle \times \langle \mathcal{Q}_7 \rangle \times \langle \mathcal{Q}_{13} \rangle, \text{ since } h_\Delta = 16.$$

Remark 2.1. We observe that, in Example 2.1, Δ is the penultimate $\Delta \equiv 0 \pmod{4}$ of ERD-type having C_Δ of exponent 2 (see[4]). By results of [4], if there is an ERD-type of exponent 2 with $h_\Delta \geq 32$ then it would be a counterexample to the Riemann hypothesis.

Another example is

Example 2.2. Let $\Delta = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 = 1,021,020$ where $h_\Delta = 32$ then by a similar kind of analysis as that given in Example 2.1 we get from Theorem 2.1 that and

$$C_\Delta = \langle \mathcal{Q}_3 \rangle \times \langle \mathcal{Q}_5 \rangle \times \langle \mathcal{Q}_7 \rangle \times \langle \mathcal{Q}_{11} \rangle \times \langle \mathcal{Q}_{13} \rangle.$$

Example 2.3. Let $\Delta = -4 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ then $h_\Delta = 16$ and, as above

$$C_\Delta = \langle \mathcal{Q}_3 \rangle \times \langle \mathcal{Q}_5 \rangle \times \langle \mathcal{Q}_7 \rangle \times \langle \mathcal{Q}_{13} \rangle.$$

We have sufficient data to leave the reader with

Conjecture. The conditions in Theorem 2.1 are necessary *and* sufficient. In fact we are convinced that $r = 1$ must occur as in Example 2.1.

Acknowledgements. The author's research is supported by NSERC Canada grant #A8484.

References

- [1] H. Cohn: A Second Course in Number Theory. Wiley, New York (1962).
- [2] S. Louboutin: Continued fractions and real quadratic fields. J. Number Theory, **30**, 167-176 (1988).
- [3] 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. Can. J. Math., **44**, 824-842 (1992).
- [4] —: Class groups of exponent two in real quadratic fields (to appear: Proceedings of the third Canadian Number Theory Association Conference 1991, Oxford University Press).