Canad. Math. Bull. Vol. **41** (3), 1998 pp. 328–334

CLASS NUMBER ONE AND PRIME-PRODUCING QUADRATIC POLYNOMIALS REVISITED

R. A. MOLLIN

ABSTRACT. Over a decade ago, this author produced class number one criteria for real quadratic fields in terms of prime-producing quadratic polynomials. The purpose of this article is to revisit the problem from a new perspective with new criteria. We look at the more general situation involving arbitrary real quadratic orders rather than the more restrictive field case, and use the interplay between the various orders to provide not only more general results, but also simpler proofs.

1. **Notation and Preliminaries.** We will be considering arbitrary real quadratic orders, so we first introduce the notions of arbitrary discriminants and radicands.

Let $D_0 > 1$ be a square-free integer, and set

$$\Delta_0 = \begin{cases} D_0 & \text{if } D_0 \equiv 1 \pmod 4, \\ 4D_0 & \text{otherwise.} \end{cases}$$

Then Δ_0 is called a *fundamental discriminant* with associated *fundamental radicand* D_0. Let $f_\Delta \in \mathbb{N}$, and set $\Delta = f_\Delta^2 \Delta_0$. Then

$$\Delta = \begin{cases} D & \text{if } D_0 \equiv 1 \pmod 4) \text{ and } f_\Delta \text{ is odd,} \\ 4D & \text{if otherwise.} \end{cases}$$

is a *discriminant* with *conductor* f_Δ, and associated *radicand*

$$D = \begin{cases} f_\Delta^2 D_0 & \text{if } D_0 \not\equiv 1 \pmod 4 \text{ or } f_\Delta \text{ is odd,} \\ (f_\Delta/2)^2 D_0 & \text{otherwise,} \end{cases}$$

having underlying fundamental discriminant Δ_0 with associated fundamental radicand D_0.

If $\Delta > 0$ is a discriminant with associated radicand D, then

$$\omega_\Delta = \begin{cases} (1 + \sqrt{D})/2 & \text{if } D_0 \equiv 1 \pmod 4 \text{ and } f_\Delta \text{ is odd,} \\ \sqrt{D} & \text{otherwise,} \end{cases}$$

is called the *principal surd* associated with Δ. This will provide our canonical basis element for quadratic orders. First we need notation for a $\mathbb{Z}$-module:

$$[\alpha, \beta] = \{\alpha x + \beta y : x, y \in \mathbb{Z}\},$$

where $\alpha, \beta \in \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{D_0})$, the real quadratic field of discriminant Δ_0 and radicand D_0. For this reason, fundamental discriminants are often called *field discriminants*.

Received by the editors March 19, 1997.
AMS subject classification: Primary: 11R11; secondary: 11R09, 11R29.

https://doi.org/10.4153/CMB-1998-045-6 Published online by Cambridge University Press

In particular, if we set

$$O_\Delta = [1, \omega_\Delta],$$

then this is an order in K. Also, the index $|O_{\Delta_0} : O_\Delta| = f_\Delta$ is the conductor associated with Δ, where O_{Δ_0} is the *maximal order* in K, sometimes called the *ring of integers of* K. In other words, the maximal order is the order with conductor $f_\Delta = 1$ in K, having square-free radicand D_0 and fundamental discriminant Δ_0.

We also need to be able to distinguish those $\mathbb{Z}$-modules that are ideals in O_Δ (see [1, pp. 9–30]).

PROPOSITION 1.1 (IDEAL CRITERION). *Let Δ be a discriminant, and let $I \neq (0)$ be a $\mathbb{Z}$-submodule of O_Δ. Then I has a representation of the form*

$$I = [a, b + c\omega_\Delta],$$

where $a, c \in \mathbb{N}$ and $b \in \mathbb{Z}$ with $0 \leq b < a$. Furthermore, I is an ideal of O_Δ if and only if this representation satisfies $c \mid a$, $c \mid b$, and $ac \mid N(b + c\omega_\Delta)$. (For convenience, we call I an O_Δ-ideal.) If $c = 1$, then I is called primitive, *and I has a canonical representation as*

$$I = \left[a, (b + \sqrt{\Delta})/2\right],$$

with $-a \leq b < a$.

If $I = [a, b + \omega_\Delta]$ is a primitive O_Δ-ideal, then a is the least positive rational integer in I, denoted $N(I) = a$ called the *norm of I*.

An O_Δ-ideal I is called *reduced* if there does *not* exist any element $\alpha \in I$ such that both $|\alpha| < N(I)$ and $|\alpha'| < N(I)$, where α' denotes the *algebraic conjugate* of $\alpha \in O_\Delta$, namely if $\alpha = (x + y\sqrt{\Delta})/2$, then $\alpha' = (x - y\sqrt{\Delta})/2$. It is convenient to have an easily verified sufficient condition for reduction (see [1, p. 19]).

THEOREM 1.1. *If $\Delta > 0$ is a discriminant and I is an O_Δ-ideal with $N(I) < \sqrt{\Delta}/2$, then I is reduced. Conversely, if I is reduced, then $N(I) < \sqrt{\Delta}$.*

An ideal I is called *principal* in O_Δ if there exists an element $\alpha \in O_\Delta$ such that $I = (\alpha) = \{\alpha\beta : \beta \in O_\Delta\}$, where α is called the *generator* of I. Now we may define an equivalence relation among O_Δ-ideals. If I and J are non-zero O_Δ-ideals, then we say that I and J are *equivalent*, denoted $I \sim J$, if there exist $\alpha, \beta \in O_\Delta$ such that $(\alpha)I = (\beta)J$.

The notion of a primitive ideal has an analogue for $\alpha \in O_\Delta$, which is called *primitive* if it has no rational integer factors other than ± 1, namely if $\alpha = n\beta$ where $n \in \mathbb{Z}$ and $\beta \in O_\Delta$, then $|n| = 1$. It is easily verified that (α) is a primitive, principal O_Δ-ideal if and only if α is a primitive element in O_Δ. Also, $N[(\alpha)] = |N[\alpha]|$, namely the norm of a principal ideal is the absolute value of the norm of a generator.

The following special case of the Continued Fraction Algorithm will prove to be a highly useful tool in the next section (see [1, Exercise 1.5.9, p. 29, Theorem 2.1.2, p. 44, and Theorem 3.2.1, pp. 78–80]).

https://doi.org/10.4153/CMB-1998-045-6 Published online by Cambridge University Press

THEOREM 1.2. *Let $\Delta = t^2 \pm 4$ for $t \in \mathbb{N}$ be a discriminant. If I is a principal $\mathcal{O}_\Delta$-ideal with $N(I) < \sqrt{\Delta}/2$, then one of the following holds.*

1. *$N(I) = 4$, where $\Delta = t^2 + 4$ and t is even.*
2. *$N(I) = t - 2$, where $\Delta = t^2 - 4$ and t is odd.*
3. *$N(I) = 1$.*

Since we are not necessarily dealing with the maximal order, then we need the following notions. A *fractional ideal* is a non-zero, finitely generated, $\mathcal{O}_\Delta$-submodule of K (which includes all non-zero ideals of $\mathcal{O}_\Delta$, called *integral* ideals to distinguish them from more general fractional ideals). Thus, fractional $\mathcal{O}_\Delta$-ideals are of the form $(\alpha)I$, where $\alpha \in K$ is non-zero and I is an integral $\mathcal{O}_\Delta$-ideal. A fractional $\mathcal{O}_\Delta$-ideal I is called *invertible* if there is another fractional ideal I^{-1} such that $II^{-1} = \mathcal{O}_\Delta$. When such an I^{-1} exists we may take it to be $I^{-1} = \{\beta \in K : \beta I \subseteq \mathcal{O}_\Delta\}$. Thus, invertible ideals are those I for which $\mathcal{O}_\Delta = \{\beta \in K : \beta I \subseteq I\}$.

If $I(\Delta)$ denotes the set of invertible fractional ideals in an order $\mathcal{O}_\Delta$, then $I(\Delta)$ is a group under multiplication of ideals. The principal $\mathcal{O}_\Delta$-ideals form a subgroup $P(\Delta)$ of $I(\Delta)$ and $C_\Delta = I(\Delta)/P(\Delta)$ is a finite abelian group called the *ideal class group of* $\mathcal{O}_\Delta$. Its order is h_Δ, the *class number* of $\mathcal{O}_\Delta$. A formula for the class number of an order is given by

$$h_\Delta = h_{\Delta_0}\psi_{\Delta_0}(f_\Delta)/u, \tag{1.1}$$

where f_Δ is the conductor associated with Δ,

$$\psi_{\Delta_0}(f_\Delta) = f_\Delta \prod_{p \mid f_\Delta} \left(1 - \frac{(\Delta_0/p)}{p}\right),$$

with $(*/*)$ being the Kronecker symbol, and with the product ranging over all distinct prime factors of f_Δ. Finally, u is the *unit index* of $\mathcal{O}_\Delta$ in $\mathcal{O}_{\Delta_0}$, namely

$$\varepsilon_\Delta = \varepsilon_{\Delta_0}^u,$$

where ε_Δ is the fundamental unit of $\mathcal{O}_\Delta$ and ε_{Δ_0} is the fundamental unit of the maximal order $\mathcal{O}_{\Delta_0}$ having class number h_{Δ_0} (see [1, pp. 23–30]).

It will be useful in the next section to have a criterion for the invertibility of integral ideals in canonical form (see [1, Proposition 1.5.1, p. 25]).

THEOREM 1.3. *Let Δ be a discriminant, and let $I = [a, (b + \sqrt{\Delta})/2]$ be a primitive $\mathcal{O}_\Delta$-ideal. Then I is invertible if and only if $\gcd(a, b, c) = 1$, where $c = (b^2 - \Delta)/(4a)$. Consequently, if $\gcd(f_\Delta, a) = 1$, then I is invertible. Moreover, every class of C_Δ has an integral, reduced ideal I, with $\gcd\bigl(f_\Delta, N(I)\bigr) = 1$.*

The last statement of Theorem 1.1 says more than that every class has an invertible ideal, which is obvious given the definition of C_Δ. However, not all invertible ideals have norm prime to the conductor. For instance, see [1, Example 1.5.2, p. 24].

https://doi.org/10.4153/CMB-1998-045-6 Published online by Cambridge University Press

We conclude this section with an example that illustrates the necessity to insist upon invertible ideals when dealing with class number one questions in arbitrary quadratic orders. It is possible to have $h_\Delta = 1$, yet have the existence of a primitive non-invertible ideal $I \not\sim 1$, since the notion of equivalence of ideals defined above is quite general and does not require a class group structure.

EXAMPLE 1.1. Let $\Delta = 80 = 4D$, with $f_\Delta = 4$. Then $\Delta_0 = 5 = D_0$. Since $\varepsilon_\Delta = 9+\sqrt{80} = \varepsilon_{\Delta_0}^6 = \omega_{\Delta_0}^6 = \left((1+\sqrt{5})/2\right)^6$, then by formula (1.1),

$$h_\Delta = h_{\Delta_0} \cdot f_\Delta \left(1 - \left(\frac{\Delta_0}{2}\right) \Big/ 2\right) \Big/ u = 1 \cdot 4 \cdot (1+1/2)/6 = 1,$$

since $(\frac{\Delta_0}{2}) = -1$, given that $\Delta_0 = 5$, and $u = 6$. However, $I = [2, \sqrt{20}]$ is a primitive, reduced $\mathcal{O}_\Delta$-ideal by Proposition 1.1, and Theorem 1.1. Also, $I \not\sim 1$. To see this, we note that for I to be principal, there would have to exist a primitive element $\alpha = (x + y\sqrt{D}) \in \mathcal{O}_\Delta = [1, \sqrt{20}]$ such that $I = (\alpha)$, so $N(\alpha) = x^2 - 20y^2 = \pm 2$, which is impossible. By Theorem 1.3, I is not invertible.

For proofs of the above results and further background detail, see [1].

2. **Results.** In this section, we establish criteria for class number one in terms of prime-producing quadratic polynomials in real quadratic orders. In the literature, restriction to field discriminants is usually considered. Therefore, consideration of discriminants of type $\Delta = a^2 \pm 4$, an example of *narrow Richaud-Degert types*, or simply *R-D types* (see [1, p. 77 ff]) is quite restrictive. However, if no assumption is made upon the *square-freeness* of the associated radicand D, then consideration of discriminants of this type is no restriction whatsoever. To see this, we observe that if Δ_0 is a fundamental or field discriminant, and $\varepsilon_{\Delta_0} = (T + U\sqrt{\Delta_0})/2$ is the fundamental unit of $\mathcal{O}_{\Delta_0}$, then $T^2 - U^2\Delta_0 = \pm 4$. Thus, $\Delta = U^2\Delta_0 = T^2 \pm 4$. Furthermore, by raising the fundamental unit to arbitrary powers, we see that there are infinitely many such discriminants Δ of narrow R-D type, with any given field discriminant Δ_0. Hence, we may consider arbitrary discriminants Δ of narrow R-D type without loss of generality.

THEOREM 2.1. *Let* $\Delta = t^2 + 4$, $t \in \mathbb{N}$. *Set*

$$f(x) = -x^2 + xt + 1,$$

and assume that $\gcd\left(f_\Delta, f(x)\right) = 1$ *for all natural numbers* $x < t$. *Then* $h_\Delta = 1$ *if and only if* $f(x)$ *is prime for all natural numbers* $x < t$.

PROOF. If $h_\Delta > 1$, then there exists a non-principal, invertible, reduced ideal I with $\gcd\left(N(I), f_\Delta\right) = 1$ by Theorem 1.3. Also, by Proposition 1.1, I has a representation

$$I = \left[a, (b+\sqrt{\Delta})/2\right], \quad \text{with } -a \le b < a.$$

https://doi.org/10.4153/CMB-1998-045-6 Published online by Cambridge University Press

Since I is reduced, then $a < \sqrt{\Delta}$ by Theorem 1.1, so $b < t$. Set $b = t - 2x$ for some $0 < x < t$. Since $I \not\sim 1$, there exists an integer $c > 1$ such that $N\big((b + \sqrt{\Delta})/2\big) = -ac$. (Otherwise, $I = \big((b + \sqrt{\Delta})/2\big) \sim 1$.) Therefore,

$$ac = (\Delta - b^2)/4 = \big(t^2 + 4 - (t - 2x)^2\big)/4 = -x^2 + tx + 1.$$

We have shown by contrapositive that if $f(x)$ is prime for all natural numbers $x < t$, then $h_\Delta = 1$.

Conversely, suppose that $f(x)$ is composite for some natural number $x < t$, say $c = c_1c_2 = f(x)$ with $1 < c_1 \leq c_2$. Set $\alpha = (2x - t + \sqrt{\Delta})/2$. Then α is primitive and $N(\alpha) = -c$. Thus, $I = [c_1, \alpha]$ is a primitive O_Δ-ideal with $N(I) = c_1$, by Proposition 1.1. By hypothesis, $\gcd\big(N(I), f_\Delta\big) = 1$, so by Theorem 1.3, I is invertible. We now show that $c_1 < \sqrt{\Delta}/2$. It suffices to show that $4c < \Delta$. If $4c > \Delta$, then $-4x^2+4xt+4 > t^2+4$. Thus, $0 > t^2 - 4xt + 4x^2 = (t - 2x)^2$, a contradiction. Hence, by Theorem 1.1, I is reduced. If $I \sim 1$, then by Theorem 1.2, $c_1 = 1$, a contradiction. We have shown by contrapositive that if $h_\Delta = 1$, then $f(x)$ is prime for all $x \in \mathbb{N}$ with $x < t$. This secures the result. ∎

EXAMPLE 2.1. If $\Delta = 17^2 + 4 = 293$, then $f(x) = -x^2 + 17x + 1$ is prime for $x = 1, 2, \ldots, 16$, so $h_\Delta = 1$ by Theorem 2.1.

REMARK 2.1. In 1986, Yokoi conjectured that if $\Delta_0 = t^2 + 4$ is a fundamental discriminant, then $h_{\Delta_0} > 1$ for any $t > 17$ (see [1, Conjecture 5.4.2, p. 176]).

The notion introduced in the proof of Theorem 2.1 allows us to determine when a class number is bigger than one. In fact, properly posed, it can tell us when C_Δ has a cyclic subgroup of given order.

COROLLARY 2.1. *Suppose that $\Delta = t^2 + 4$ is a discriminant for odd $t \in \mathbb{N}$. If there exists an $x \in \mathbb{N}$ such that $-x^2 + xt + 1 = c^n$ for some natural numbers $c > 1$ and $n > 1$, with* $\gcd(\Delta, c) = 1$, *then C_Δ has a cyclic subgroup of order n (see [2] for the case $x = 1$).*

PROOF. Set $\alpha = (2x - t + \sqrt{\Delta})/2$. Then $N(\alpha) = -c^n$. By Theorem 1.3, $I = [c, \alpha]$ is an invertible O_Δ-ideal, and by [1, Multiplication Formulae, pp. 10–11], $I^n = [c^n, \alpha]$, so $I^n \sim 1$. By the same reasoning as in the proof of Theorem 2.1, $c^{n/2} < \sqrt{\Delta}/2$. Suppose that $I^j = [c^j, \alpha] \sim 1$ for some $j \mid n$. Since $c^j \leq c^{n/2} < \sqrt{\Delta}/2$, then by Theorem 1.1, I^j is reduced. Therefore, by Theorem 1.2, $c^j = 1$, a contradiction. Thus, $j = n$ and so C_Δ has a cyclic subgroup of order n. ∎

EXAMPLE 2.2. If $x = 2356$, $t = 3185$, $n = 9$ and $c = 5$, then

$$D = \Delta = 3185^2 + 4 = 10144229 = 29 \cdot 349801.$$

Notice that

$$c^n = 5^9 = -2356^2 + 3185 \cdot 2356 + 1 = -x^2 + xt + 1.$$

Hence, C_Δ has a cyclic subgroup of order 9. In fact, $h_\Delta = 126 = 9 \cdot 14$.

https://doi.org/10.4153/CMB-1998-045-6 Published online by Cambridge University Press

EXAMPLE 2.3. If $x = 1514$, $c = 3$, $n = 9$, and $t = 1527$, then $\Delta = D = 2331733 = 1527^2 + 4$, is prime and C_Δ has a cyclic subgroup of order 9. In fact, $h_\Delta = 81$. Here we have $c^n = 3^9 = -1514^2 + 1514 \cdot 1527 + 1 = -x^2 + xt + 1$.

THEOREM 2.2. *Let $\Delta = t^2 - 4$ for an integer $t > 3$. Set*

$$f(x) = -x^2 + xt - 1,$$

and assume that $\gcd\big(f_\Delta, f(x)\big) = 1$ for all natural numbers $x < t$. Then $h_\Delta = 1$ if and only if $f(x)$ is prime for all natural numbers $x < t$.

PROOF. This proof is exactly the same as the proof for Theorem 2.1, with the one exception that in the proof of the converse, it is possible that $c_1 = t - 2 > 1$ via Theorem 1.2 when t is odd. However, this cannot occur since $c_1 < \sqrt{\Delta}/2$, so $c_1 \leq (t-1)/2$, and $t > 3$. ■

EXAMPLE 2.4. Let $\Delta = 21^2 - 4 = 437$. Since $f(x) = -x^2 + 21x - 1$ is prime for $x = 1, 2, \ldots, 20$, then $h_\Delta = 1$.

REMARK 2.2. In 1987, this author conjectured that if $\Delta_0 = t^2 - 4$ is a fundamental discriminant with $t > 21$, then $h_{\Delta_0} > 1$ (see [1, Conjecture 5.4.3, p. 176]).

In the same fashion as in Corollary 2.1, we get the following.

COROLLARY 2.2. *If $\Delta = t^2 - 4$ with $t > 3$ an odd integer, and if there exists an $x \in \mathbb{N}$ such that $-x^2 + xt - 1 = c^n$ for some natural numbers $c > 1$ and $n > 1$, with $\gcd(\Delta, c) = 1$, then C_Δ has a cyclic subgroup of order n.*

EXAMPLE 2.5. If $\Delta = 25^2 - 4 = 3^3 \cdot 23 = 621$, then $5^3 = -7^2 + 25 \cdot 7 - 1$, so by Corollary 2.2, C_Δ has a cyclic subgroup of order 3. Here, $f_\Delta = 3$, $c = 5$, $n = 3$, and $\Delta_0 = 3 \cdot 23 = 69$. By formula (1.1), $h_\Delta = h_{\Delta_0} \cdot 3\big(1 - (\frac{69}{3})/3\big)/u = 3$, since $h_{69} = 1 = h_{\Delta_0}$, and $u = 1$ given that

$$\varepsilon_\Delta = (25 + \sqrt{\Delta})/2 = (25 + 3\sqrt{\Delta_0})/2 = (25 + 3\sqrt{69})/2 = \varepsilon_{\Delta_0}.$$

General R-D types are those discriminants $\Delta = t^2 + r$ where $r \mid 4t$, and these have been widely studied (see [1, p. 77 ff]). With reference to Remarks 2.1–2.2, in 1989, this author and H. C. Williams posed three other conjectures, which made up the balance of the R-D types, along with S. Chowla's conjecture (see [1, Conjectures 5.4.4–5.4.6, p. 176]). This author and H. C. Williams have come the closest to proving these conjectures by establishing a list of all R-D type fundamental discriminants with class number one, with one possible exception remaining, whose existence would be a counterexample to the Generalized Riemann hypothesis (see [1, Theorem 5.4.3, p. 176] for the complete list). We conclude with a comparison of the above results with those proved by this author a decade ago (see [1, pp. 158–186]).

We cite only the result for discriminants of the form $t^2 + 4$ since the others are similar (see [1, Exercise 5.2.3, p. 163]). This result says that if $\Delta_0 = t^2 + 4$ is a fundamental

https://doi.org/10.4153/CMB-1998-045-6 Published online by Cambridge University Press

discriminant, then $h_{\Delta_0} = 1$ if and only if $|g(x)|$ is 1 or prime for all natural numbers $x < (t+1)/2$, where $g(x) = x^2 + x + (1 - \Delta)/4$. Notice that if we take the polynomial $f(x) = -x^2 + xt + 1$ and perform the translation $x \longmapsto (t-1)/2 - x$, then we get $-x^2 - x + (\Delta - 1)/4$. Multiplying by -1 yields $g(x)$, and the bounds on x match once the translations are taken into account. Hence, the original versions, which were proved in a more difficult fashion, are now seen to be translations to a more general setting with proofs easily set down from the perspective of ideals in quadratic orders.

ACKNOWLEDGMENTS. The author gratefully acknowledges the support of NSERC Canada grant # A8484.

REFERENCES

1. R. A. Mollin, *Quadratics*. CRC Press, Boca Raton, New York, London, Tokyo, 1995.
2. P. Weinberger, *Real quadratic fields with class groups divisible by n*. J. Number Theory **5**(1973), 237–241.

Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta
T2N 1N4
email: ramollin@math.ucalgary.ca
Website: http://www.math.ucalgary.ca/˜ramollin/

https://doi.org/10.4153/CMB-1998-045-6 Published online by Cambridge University Press