Glasgow Math. J. **41** (1999) 197–206.

CYCLIC SUBGROUPS OF IDEAL CLASS GROUPS IN REAL QUADRATIC ORDERS

R. A. MOLLIN

Mathematics Department, University of Calgary, Calgary, Alberta, Canada, T2N 1N4
E-mail: ramollin@math.ucalgary.ca
Website: http://www.math.ucalgary.ca/~ramollin/

(Received 18 June, 1997; revised 8 November, 1997)

Abstract. The primary purpose of this paper is to provide general sufficient conditions for any real quadratic order to have a cyclic subgroup of order $n \in \mathbb{N}$ in its ideal class group. This generalizes results in the literature, including some seminal classical works. This is done with a simpler approach via the interplay between the maximal order and the non-maximal orders, using the underlying infrastructure via the continued fraction algorithm. Numerous examples and a concluding criterion for non-trivial class numbers are also provided. The latter links class number one criteria with new prime-producing quadratic polynomials.

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

Let $D_0 \neq 1$ 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

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

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

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

having underlying fundamental discriminant Δ_0 with associated fundamental radicand D_0.

Let Δ be a discriminant with associated radicand D. Then

$$\omega_\Delta = \begin{cases} (1 + \sqrt{D})/2 & \text{if } \Delta = D \equiv 1 \pmod 4, \\ \sqrt{D} & \text{if } \Delta \equiv 0 \pmod 4, \end{cases}$$

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

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

https://doi.org/10.1017/S0017089599970799 Published online by Cambridge University Press

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

In particular, if we set $\mathcal{O}_\Delta = [1, \omega_\Delta]$, then this is an *order* in K. Also, the index $|\mathcal{O}_{\Delta_0} : \mathcal{O}_\Delta| = f_\Delta$ is the conductor associated with Δ, where $\mathcal{O}_{\Delta_0}$ is the *maximal order* in K, sometimes called the *ring of integers of* K. In other words, the maximal order in K is the order with conductor $f_\Delta = 1$, 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 $\mathcal{O}_\Delta$; (see [**1**, pp. 9–30]).

THEOREM 1.1 (Primitive ideals and norms). *Let Δ be a discriminant, and let $I \neq (0)$ be a $\mathbb{Z}$-submodule of $\mathcal{O}_\Delta$. 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 $\mathcal{O}_\Delta$ if and only if this representation satisfies $c|a$, $c|b$, and $ac|N(b + c\omega_\Delta)$. (For convenience, we call I an $\mathcal{O}_\Delta$-ideal.) If $c = 1$, then we say that a non-zero ideal I is a primitive $\mathcal{O}_\Delta$-ideal. If I is a primitive $\mathcal{O}_\Delta$-ideal, then a is the least positive rational integer in I, denoted $N(I) = a$, called the norm of I.*

An $\mathcal{O}_\Delta$-ideal I is called *reduced* if there does *not* exist any nonzero element $\alpha \in I$ such that both $|\alpha| < N(I)$ and $|\alpha'| < N(I)$, where α' is the algebraic conjugate of α. It is convenient to have an easily verified sufficient condition for reduction; (see [**1**, p. 19]).

THEOREM 1.2. *If $\Delta > 0$ is a discriminant and I is an $\mathcal{O}_\Delta$-ideal with $N(I) < \sqrt{\Delta}/2$, then I is reduced.*

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].) In the sequel, we let $\mathcal{C}_\Delta$ denote the *ideal class group of* the order $\mathcal{O}_\Delta$, and its order h_Δ, the *class number* of $\mathcal{O}_\Delta$. We denote the class of principal ideals in $\mathcal{C}_\Delta$ by $I \sim 1$.

THEOREM 1.3. *Let $\Delta > 0$ be a discriminant with associated radicand $D = t^2 + r$ for $t \in \mathbb{N}$ and $|r| = 1, 4$. If $I \sim 1$ in $\mathcal{C}_\Delta$, with $N(I) < \sqrt{\Delta}/2$, then one of the following holds.*

1. *$N(I) = t/2$, where $r = 1$ and t is even.*
2. *$N(I) = 4$, where $r = 4$ and t is even.*
3. *$N(I) = t - 2$, where $r = -4$ and t is odd.*
4. *$N(I) = 1$.*

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,

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

https://doi.org/10.1017/S0017089599970799 Published online by Cambridge University Press

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]). Also, 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 1.4 (Criterion for invertibility). *Let Δ be a discriminant, and let $I = [N(I), (b + \sqrt{\Delta})/2]$ be a primitive $\mathcal{O}_\Delta$-ideal. Then I is invertible if and only if* $\gcd(N(I), b, c) = 1$, *where* $c = (b^2 - \Delta)/(4N(I))$. *Consequently if* $\gcd(f_\Delta, N(I)) = 1$, *then I is invertible.*

COROLLARY 1.1. *Let $n \in \mathbb{N}$. If $I = [a, (b + \sqrt{\Delta}/2]$ is an invertible $\mathcal{O}_\Delta$-ideal, and* $\gcd(a, b) = 1$, *then* $I^n = [a^n, (b + \sqrt{\Delta})/2]$, *for any $n \in \mathbb{N}$ such that $a^n | N((b + \sqrt{\Delta})/2)$.*

For background, proofs, further details and historical information, see [**1**], and for information on these topics with applications, see [**2**].

2. Results. In this section, we are going to prove results concerning cyclic subgroups of the ideal class groups in real quadratic orders. *Throughout, we maintain the notation Δ_0 to mean the fundamental discriminant, with associated radicand D_0, underlying a given discriminant Δ with associated radicand D. Also, $\mathcal{O}_{\Delta_0}$ will be the underlying maximal order.*

In the vast majority of papers in the literature, the assumption is made that the radicand under investigation is square-free, namely a field radicand as described in the preceding section. Therefore, consideration of radicands of type

$$D = a^2 + r \text{ where } |r| = 1, 4,$$

called *narrow Richaud-Degert types* or simply *narrow R-D types* (see [**1**, p. 77 ff]) is quite restrictive. However, if no assumption is made upon the *square-freeness* of D, then consideration of radicands of this type is no restriction whatsoever. To see this, we observe that if Δ_0 is a fundamental or field discriminant with association radicand D_0, and $\varepsilon_{\Delta_0} = (T + U\sqrt{D_0})/\sigma$ is the fundamental unit of $\mathcal{O}_{\Delta_0}$, then $T^2 - U^2 D_0 = \pm 1, \pm 4$. Thus, $D = U^2 D_0 = T^2 + r$ where $|r| = 1, 4$. Furthermore, by raising the fundamental unit to arbitrary powers, we see that there are infinitely many such radicands D of narrow R-D type. Hence, we may consider arbitrary discriminants Δ of narrow R-D type without loss of generality. Furthermore, we make the following crucial observation.

Suppose that I is a primitive $\mathcal{O}_\Delta$-ideal, of order n in $\mathcal{C}_\Delta$, with norm relatively prime to the conductor, namely $\gcd(N(I), f_\Delta) = 1$, and with

$$\gcd(n, \psi_{\Delta_0}(f_\Delta)/u) = 1. \tag{2.2}$$

Then $n | h_{\Delta_0}$, by Formula 1.1. In particular, this holds for discriminants of R-D type with any *given* underlying field discriminant.

In view of the above, in order to prove that there is a real quadratic field of discriminant Δ_0 with $n | h_{\Delta_0}$ for any given $n \in \mathbb{N}$, it suffices to prove that there is an

associated discriminant Δ of narrow R-D type having an ideal I of order n in $\mathcal{C}_\Delta$, satisfying Equation 2.2, with $\gcd(N(I), \Delta) = 1$. (Note that $\Delta = f_\Delta^2 \Delta_0$. See the discussion at the beginning of the preceding section.) This approach simplifies what has been done classically in such works as that of Yamamoto [**9**], Shanks-Weinberger [**4**], and more recent works such as Washington-Xianke [**6**], and Xianke [**8**]. In the sequel, we use the above method to prove a variety of results that yield classical and recent results with a certain ease missing in the literature thus far.

THEOREM 2.1. *Suppose that Δ is a discriminant with associated radicand $D = t^2 + 1$, $t \in \mathbb{N}$. Assume that there exist $m, n, N \in \mathbb{N}$, with $N, n > 1$, and $t \notin \{2m, 2m - 2\}$ such that*

$$N^n = \begin{cases} 4mt - 4m^2 + 1 & \text{if } D \not\equiv 1 \pmod 4, \\ m(t+1) - m^2 - t/2 & \text{if } D \equiv 1 \pmod 4. \end{cases} \tag{2.3}$$

Moreover, if $\Delta \neq \Delta_0$, assume that $\gcd(N, \Delta) = 1$. Then $\mathcal{C}_\Delta$ has a cyclic subgroup of order n. Furthermore, if Equation 2.2 is satisfied, then $n | h_{\Delta_0}$.

Proof. Let

$$\alpha = \begin{cases} 2m - t + \sqrt{D} & \text{if } D \not\equiv 1 \pmod 4, \\ (2m - t - 1 + \sqrt{D})/2 & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Therefore, $N(\alpha) = -N^n$. Thus, $I = [N, \alpha]$ is a primitive $\mathcal{O}_\Delta$-ideal with norm N, by Theorem 1.1. In order to be able to invoke Corollary 1.1, we need to establish two claims.

Claim 1. $\gcd(\Delta, N) = 1$.

If Δ is *not* fundamental, this is part of the hypothesis, and so we assume that Δ is fundamental. Also, since N is odd when $\Delta \equiv 0 \pmod 4$, then we need only show $\gcd(D, N) = 1$. Suppose that p is a prime such that $p | N$ and $p | D$. Assume first that $\Delta \equiv 0 \pmod 4$. Therefore, by Equation 2.3, we have

$$4mt \equiv 4m^2 - 1 \pmod{p^2}$$

since $n > 1$. Therefore, by squaring: $16m^2t^2 \equiv (4m^2 - 1)^2 \pmod{p^2}$, and by adding $16m^2$ to each side we get

$$16m^2 D = 16m^2 t^2 + 16m^2 \equiv (4m^2 - 1)^2 + 16m^2 \equiv (4m^2 + 1)^2 \pmod{p^2}.$$

Since $p | D$, we have $16m^2 D \equiv 0 \pmod{p^2}$. But p does not divide $4m$ and so $p^2 | D$, contradicting the fact that D is fundamental. Now assume that $\Delta = D \equiv 1 \pmod 4$. Then by considering Equation 2.3 in this case we get

$$2m^2 + t \equiv 2m(t+1) \pmod{p^2}.$$

Squaring yields: $4m^4 + 4m^2 t + t^2 \equiv 4m^2(t+1)^2 \equiv 4m^2 D + 8m^2 t \pmod{p^2}$, and by rewriting, $(2m^2 - t)^2 \equiv 4m^2 D \pmod{p^2}$. Since $p | D$, we have $p^2 | (2m^2 - t)^2$, and so $p^2 | 4m^2 D$. However, p is odd in this case, and $p \nmid m$ since $p \nmid t$, so that $p^2 | D$, again contradicting the fact that D is fundamental. This establishes Claim 1.

https://doi.org/10.1017/S0017089599970799 Published online by Cambridge University Press

Set

$$b = \begin{cases} 4m - 2t & \text{if } D \not\equiv 1 \pmod 4, \\ 2m - t - 1 & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Claim 2. $\gcd(b, N) = 1$.

Since $N(\alpha) = -N^n$, the result follows from Claim 1.

By Claims 1–2, we may invoke Corollary 1.1 to get $I^n = [N^n, \alpha] = (\alpha) = ((b + \sqrt{\Delta})/2)$, so that $I^n \sim 1$. Suppose that $I^j = [N^j, \alpha] \sim 1$ for some $j \in \mathbb{N}$ dividing n. We now show that $j = n$ is the only possibility.

Claim 3. $N^{n/2} < \sqrt{\Delta}/2$.

Suppose that $N^{n/2} > \sqrt{\Delta}/2$. First assume that $D = \Delta \equiv 1 \pmod 4$. Then $N^n = m(t+1) - m^2 - t/2 > \Delta/4 = (t^2+1)/4$, or by rewriting,

$$0 > 4m^2 - 4m(t+1) + 2t + t^2 + 1 = (2m - t - 1)^2,$$

a contradiction. Next, assume that $\Delta \equiv 0 \pmod 4$. Then

$$N^n = 4mt - 4m^2 + 1 > \Delta/4 = D = t^2 + 1,$$

or by rewriting, $0 > t^2 - 4mt + 4m^2 = (t - 2m)^2$, a contradiction that secures Claim 3.

By Claim 3, and Theorem 1.3, either $N^j = 1$, or $N^j = t/2$, where t is even. If $N^j = 1$, this contradicts the assumption that $N > 1$ in the hypothesis. If $N^j = t/2$, then $D \equiv 1 \pmod 4$. Therefore, from Equation 2.3,

$$N^n = m(2N^j + 1) - m^2 - N^j,$$

or by rewriting, $m^2 - (2N^j + 1)m + N^n + N^j = 0$. Thus, by the quadratic formula,

$$m = \frac{2N^j + 1 \pm \sqrt{4N^{2j} - 4N^n + 1}}{2}.$$

This means that $4N^{2j} - 4N^n + 1 \geq 1$ and so $N^{2j} \geq N^n$. Since $j | n$, then $j = n/2$ is forced. Hence, either $m = N^{n/2} = t/2$, or $m = N^{n/2} + 1 = t/2 + 1$. In the former case this is $t = 2m$, and in the latter case this is $t = 2m - 2$, both of which are excluded by the hypothesis. Therefore, $j = n$, and so $\langle I \rangle$ must be a cyclic group of order n in $\mathcal{C}_\Delta$. □

Example 2.1. Let $t = 43$, $N = 5$, and $m = n = 4$. Then $D = 1850 = 2 \cdot 5^2 \cdot 37$, and $N^n = 5^4 = 4mt - 4m^2 + 1 = 4 \cdot 4 \cdot 43 - 4 \cdot 4^2 + 1 = 625$. Thus, $\mathcal{C}_\Delta$ has a cyclic subgroup of order 4. Here $f_\Delta = 5$, $D_0 = 2 \cdot 37 = 74$, and $\Delta_0 = 296$. Theorem 2.1 does not apply to $\mathcal{C}_{\Delta_0}$ since $\gcd(n, \psi_{\Delta_0}(f_{\Delta_0})/u) = \gcd(4, 4) = 4$, where $u = 1$. In fact, from Equation 1.1, $h_\Delta = h_{\Delta_0}\psi_{\Delta_0}(f_\Delta)) = 2 \cdot 4 = 8$.

Example 2.2. If $m = 3$, $n = 6$, $t = 28$, and $N = 2$, then $N^n = 2^6 = 64 = m(t+1) - m^2 - t/2 = 3(28+1) - 3^2 - 14$, and $\Delta = D = 28^2 + 1 = 785 = 5 \cdot 157$. Thus, $\mathcal{C}_\Delta$ has a cyclic subgroup of order 6. In fact, $h_\Delta = 6$.

In order to complete the overall picture, we now prove results for the remaining general discriminants $\Delta = t^2 \pm 4$ and $\Delta = t^2 - 1$. We lose no generality by assuming

https://doi.org/10.1017/S0017089599970799 Published online by Cambridge University Press

that t is odd in the following results, since if t were even we could divide D by 4 and be in the case covered by Theorem 2.1.

THEOREM 2.2. *Let $\Delta = t^2 + 4$ be a discriminant with t an odd natural number. Suppose that there is an $m \in \mathbb{N}$ such that*

$$N^n = mt - m^2 + 1, \tag{2.4}$$

for some integers $N > 1$ and $n > 1$. Also, if $\Delta \neq \Delta_0$, assume that $\gcd(N, \Delta) = 1$. Then $\mathcal{C}_\Delta$ has a cyclic subgroup of order n. Furthermore, if Equation 2.2 is satisfied, then $n | h_{\Delta_0}$. (For the case $m = 1$, see [7].)

Proof. If $\alpha = (2m - t + \sqrt{\Delta})/2$, then $N(\alpha) = -N^n$. By the same reasoning as in the proofs of Claims 1–3 in Theorem 2.1, we show that $I = [N, \alpha]$ is an invertible ideal, and $I^n = [N^n, \alpha]$, with $N^{n/2} < \sqrt{\Delta}/2$ (observing that $N(I) \neq t/2$ since t is odd). Suppose that there is a natural number $j \neq n$ dividing n such that $I^j \sim 1$. Since $N^j \leq N^{n/2} < \sqrt{\Delta}/2$, we have by Theorem 1.3, $N(I^j) = 1$, a contradiction to the hypothesis that $N > 1$. Thus, $j = n$, and the result follows as in the proof of Theorem 2.1. □

EXAMPLE 2.3. If $m = 3316$, $t = 3905$, $n = 9$ and $N = 5$, then

$$\Delta = 15249029 = 3905^2 + 4 = [5^9 + 10995855)/3316]^2 + 4$$

is prime and $\mathcal{C}_\Delta$ has a cyclic subgroup of order 9. In fact, $h_\Delta = 171 = 9 \cdot 9$.

THEOREM 2.3. *Suppose that Δ is a discriminant with associated radicand $D = t^2 - 1$, for some integer $t > 1$. Assume that there is an $m \in \mathbb{N}$ such that*

$$N^n = 4mt - 4m^2 - 1, \tag{2.5}$$

for integers $N > 1$ and $n > 1$. Furthermore, if $\Delta \neq \Delta_0$, assume that $\gcd(N, \Delta) = 1$. Then $\mathcal{C}_\Delta$ has a cyclic subgroup of order n. Moreover, if Equation 2.2 is satisfied, then $n | h_{\Delta_0}$.

Proof. If $\alpha = 2m - t + \sqrt{D}$, then $N(\alpha) = -N^n$. Also, by similar reasoning to that in the proof of Theorem 2.1, $\gcd(N, 2m - t) = 1 = \gcd(\Delta, N)$. (Observe that $\Delta = D$ is not possible since $D \not\equiv 1 \pmod 4$.) Thus, $I = [N, \alpha]$ is a primitive $\mathcal{O}_\Delta$-ideal and $I^n = [N^n, \alpha]$. If $I^j \sim 1$, for some natural number $j \neq n$ dividing n, then since it can be shown using Equation 2.5 that $N^j \leq N^{n/2} < \sqrt{\Delta}/2 = \sqrt{D}$, we get $N^j = 1$ from Theorem 1.3, a contradiction. Hence, $n = j$ and the result follows as in Theorem 2.1. □

EXAMPLE 2.4. If $m = 1$, $N = 3 = n$ and $t = 8$, then $D = 63 = 3^2 \cdot 7 = ((3^3 + 5)/4)^2 - 1 = 8^2 - 1$. Since $h_\Delta = 2$, then there is no subgroup of order 3. Hence, $\gcd(N, \Delta) = 3 > 1$, and we cannot apply Theorem 2.3. However, if we take $m = 1$, $N = 7$, $t = 87$, and $n = 3$, then

$$D = 7568 = 2^4 \cdot 11 \cdot 43 = ((7^3 + 5)/4)^2 - 1 = 87^2 - 1,$$

and $\Delta = 2^6 \cdot 11 \cdot 43$ with $f_\Delta = 2^3$, $h_\Delta = 12$ and $h_{\Delta_0} = 3$, where $\Delta_0 = 11 \cdot 43 = 473 = D_0$. To see this from Formula 1.1,

https://doi.org/10.1017/S0017089599970799 Published online by Cambridge University Press

$$h_\Delta = h_{\Delta_0} f_\Delta \left(1 - \left(\frac{473}{2}\right)\Big/2\right)\Big/u = 3 \cdot 2^3(1 - 1/2) = 12,$$

since $u = 1$ given that $\varepsilon_\Delta = 87 + \sqrt{2^4 \cdot 473} = 87 + 4\sqrt{473} = \varepsilon_{\Delta_0}$. Hence, both $\mathcal{C}_\Delta$ and $\mathcal{C}_{\Delta_0}$ have subgroups of order 3.

In our next result, we lose no generality in assuming that t is odd since division of Δ by 4 would bring us into Theorem 2.3 if Δ were even.

THEOREM 2.4. *Let $\Delta = t^2 - 4$ be a discriminant, where $t > 2$ is an odd integer. Suppose that there are integers m, n, N with $N, n > 1$ such that*

$$N^n = mt - m^2 - 1. \tag{2.6}$$

Also, if $\Delta \neq \Delta_0$, assume that $\gcd(N, \Delta) = 1$. *Then $\mathcal{C}_\Delta$ has a cyclic subgroup of order n. Furthermore, if Equation 2.2 is satisfied, then $n | h_{\Delta_0}$.*

Proof. If $\alpha = (2m - t + \sqrt{\Delta})/2$, then as in the above proofs, $I = [N, \alpha]$ is a primitive $\mathcal{O}_\Delta$-ideal and $I^n = [N^n, \alpha] \sim 1$. By the same reasoning as above, both $\gcd(\Delta, N) = 1$, and $N^{n/2} < \sqrt{\Delta}/2$. If there is a natural number j such that $j \neq n$ and j divides n with $I^j \sim 1$, then by Theorem 1.3, either $N^j = 1$, a contradiction, or $N^j = (t - 2) | \Delta$, a contradiction. □

EXAMPLE 2.5. Let $m = 8$, $N = 7$, $n = 3$ and $t = 51$; then

$$\Delta = 2597 = 51^2 - 4 = 7^2 \cdot 53 = [(7^3 + 65)/8]^2 - 4,$$

and so $\mathcal{C}_\Delta$ has a subgroup of order 3. Here, $h_\Delta = 3$, but $h_{\Delta_0} = 1$, since $\psi_{\Delta_0}(f_{\Delta_0})/u = \psi_{53}(7)/2 = 3$, with $\gcd(N, \Delta) = 7$.

We engage in some remarks about other papers in the literature concerning cyclic subgroups, and how those results also follow from the above techniques. For instance, the Washington-Xianke paper [**6**] looks at general R-D types of radicands, namely those of the form $D = t^2 + r$ where $r | 4t$, which have been widely studied (see [**1**, pp. 77–95]). They consider only square-free D, namely only the field case. Their main result is [**6**, Theorem 2, p. 3], which has eight parts, and these are repeated in [**8**]. We give a generalization and simple proof of one of their cases, and show how the technique used in the proof of Theorem 2.2 can be used to yield any such result. The reader may easily develop generalizations of the balance of the results in [**6**], [**8**] based upon the following template.

THEOREM 2.5. (Washington-Xianke [**6**], Xianke [**8**]). *Suppose that $\Delta = t^2 + 4r$ is a discriminant with $t \in \mathbb{N}$ odd, $r > 0$, $r | t$, $r \neq t$, and*

$$t = N^n + r - 1,$$

for integers $N > 1$ and $n > 1$. Furthermore, if $\Delta \neq \Delta_0$, assume that $\gcd(c, \Delta) = 1$. *Then $\mathcal{C}_\Delta$ has a cyclic subgroup of order n. Also, if Equation 2.2 is satisfied, then $n | h_{\Delta_0}$.*

https://doi.org/10.1017/S0017089599970799 Published online by Cambridge University Press

Proof. If $\alpha = (t + 2 + \sqrt{\Delta})/2$, then $N(\alpha) = N^n$. Hence, by similar techniques to those developed in previous proofs above, $I = [N, \alpha]$ is a primitive invertible $\mathcal{O}_\Delta$-ideal and $I^n = [N^n, \alpha] \sim 1$. If $I^j = [N^j, \alpha] \sim 1$ for any natural number $j|n$ and $j \neq n$, then as above, $N^j \leq N^{n/2} < \sqrt{\Delta}/2$, so that I^j is reduced. Hence, by [**1**, Theorem 2.1.2, p. 44, and Theorem 3.2.1, Case B(b), pp. 78–80], $N^j = r$. However, $r|t = N^n + r - 1$, so that $N = 1$, a contradiction. Thus, $j = n$ and the results follow as in previous proofs. □

EXAMPLE 2.6. If $\Delta = 9^2 + 4 = 85$ with $t = 9$, $N = 3$, $n = 2$, and $r = 1$, then $\mathcal{C}_\Delta$ has a subgroup of order 2 since $t = N^n + r - 1$. In fact, $h_\Delta = 2$.

We also get the main result of [**5**], which is stated with a number of conditions that we can boil down to a simpler version, which we prove based upon the above techniques.

THEOREM 2.6. (Uehara [**5**]). *Let $\Delta = 4D$ be a discriminant with associated radicand $D = t^2 - r$, where $r > 0$, $r|t$, $r \neq t$, and*

$$N^n = 4t + 4r + 1,$$

for some integers $N > 1$ and $n > 1$. Also, if $\Delta \neq \Delta_0$, assume that $\gcd(\Delta, N) = 1$. *Then $\mathcal{C}_\Delta$ has a cyclic subgroup of order n. Additionally, if Equation 2.2. is satisfied, then $n|h_{\Delta_0}$.*

Proof. If $\alpha = 2t + 1 + 2\sqrt{D}$, then $N(\alpha) = N^n$, so that as above, $I = [N, \alpha]$, and $I^n = [N, \alpha] \sim 1$. If there is a natural number $j|n$ such that $I^j = [N^j, \alpha] \sim 1$, then $c^j \leq N^{n/2} < \sqrt{\Delta}/2 = \sqrt{D}$. Thus, by [**1**, Theorem 3.2.1, Case A(d), pp. 78–80], $N^j = r$ or $N^j = 2t - r - 1$, both of which lead easily to contradictions. Hence, $j = n$, and the results follow as above. □

EXAMPLE 2.7. If $\Delta_0 = 3596$, then $D_0 = 899 = 29 \cdot 31$. If $N = 5$, $n = 3$, $t = 30$, and $r = 1$, then $N^n = 4t + 4r + 1$, and so $\mathcal{C}_{\Delta_0}$ has a subgroup of order 3. In fact, C_{Δ_0} is the product of a group of order 3 and one of order 2.

The invocation of Theorem 2.1.2 of [**1**] in the above proofs of Theorems 2.5–2.6 is just another implementation of the continued fraction algorithm, a special case of which we isolated in Theorem 1.3 for narrow R-D types. One of the primary purposes in the writing of this paper is to bring these ideas to the fore, with the implementation of the quite general and new results summarized in Theorems 2.1–2.4, which can also be used indirectly to achieve results such as that in Theorem 2.5 via non-maximal orders of narrow R-D type. This general approach is most often overlooked. Consequently, more difficult techniques with less favourable results are often used. In [**6**], for instance, a special case of [**1**, Theorem 3.2.1] was used, and their results were less precise since they had to exclude finitely many cases. The technique used above is simpler and more accurate. Also, in [**6**], the authors discuss the work of Shanks-Weinberger [**4**] in the exploration of class numbers of maximal orders divisible by powers of 3. They mention that if $\Delta_0 = s^6 + 4$ is square-free, then empirical evidence shows that $9|h_{\Delta_0}$. They go on to say that the multiple of 3 dividing h_{Δ_0} is explainable, but "the extra 3 is unexpected. We do not have a good explanation for this phenomenon." The explanation is given by Theorem 2.2, which

applies whenever $c^9 = xs^3 - x^2 + 1$ has a solution c, $x \in \mathbb{N}$ for given $s \in \mathbb{N}$ (and [**3**, Theorem 4, p. 265] says that there are only finitely many). If there is such a solution, then $\mathcal{C}_\Delta$ has a cyclic subgroup of order 9. Since Theorem 2.2 does not require a maximal order, then there are infinitely many possible such Diophantine equations to try, and via the above results, may account for the high density of such Δ_0 having $9|h_{\Delta_0}$, as discussed via the Cohen-Lenstra heuristics in [**6**].

We conclude with a result that will show the reader how to use the above techniques to develop an algorithm for showing that a class number is bigger than 1. We only prove the result for one of the types of discriminant, but the reader may use this as a template for developing similar results for the other types.

THEOREM 2.7. *Suppose that* $\Delta = t^2 + 4$ *is a discriminant, where* $t \in \mathbb{N}$ *is odd. If there exists an* $m \in \mathbb{N}$ *such that* $mt - m^2 + 1 = N \in \mathbb{N}$ *is composite, and if* $\gcd(f_\Delta, N) = 1$, *then* $h_\Delta > 1$.

Proof. If $\alpha = (2m - t + \sqrt{\Delta})/2$, where $mt - m^2 + 1 = N > 0$ is composite for some $m \in \mathbb{N}$, then $N(\alpha) = -N$. Set $N = c_1 c_2$ with $1 < c_1 \leq c_2$. Since $\gcd(f_\Delta, N) = 1$, then by Theorem 1.4, $I = [c_1, \alpha]$ is a primitive invertible $\mathcal{O}_\Delta$-ideal. We now show that I is not principal. First we prove that $N < \Delta/4$. If $N > \Delta/4$, then $4N = 4mt - 4m^2 + 4 > t^2 + 4$, or by rewriting, we obtain

$$0 > t^2 - 4mt + 4m^2 = (t - 2m)^2,$$

a contradiction. Hence $c_1 \leq N^{1/2} < \sqrt{\Delta}/2$. Therefore, by Theorem 1.3, if $I \sim 1$, then $N(I) = c_1 = 1$, a contradiction. □

A result that is immediate from Theorem 2.7 is related to class number one criteria developed by this author over a decade ago (see [**1**, pp. 138–143, and 158–163]).

COROLLARY 2.1. *If* $\Delta = t^2 + 4$ *is a discriminant with* $h_\Delta = 1$, *then*

$$f(x) = -x^2 + tx + 1$$

is prime, for all natural numbers $x < t$. *Also, if* $m = 1$, *and* t is composite, then $h_\Delta > 1$.

The largest known discriminant $\Delta_0 = t^2 + 4$ with $h_{\Delta_0} = 1$ is $\Delta_0 = 293 = 17^2 + 4$. Notice that $17m - m^2 + 1$ is prime for all $m \in \mathbb{N}$ with $m < 17$. This is related to class number one criteria established for fundamental R-D types by this author; (see [**1**, pp. 158–163]).

ACKNOWLEDGEMENT. The author wishes to thank the referee for comments on the original paper, which led to a better sequence of results, and a cleaner presentation.

REFERENCES

1. R. A. Mollin, *Quadratics* (CRC Press, Boca Raton, New York, London, Tokyo, 1995).
2. R. A. Mollin, *Fundamental number theory with applications* (CRC Press, Boca Raton, New York, London, Tokyo, 1998).

3. L. J. Mordell, *Diophantine equations* (Academic Press, 1969).

4. D. Shanks and P. Weinberger, A quadratic field of prime discriminant requiring three generators for its class group, and related theory, *Acta. Arith*. **21** (1972), 71–87.

5. T. Uehara, Construction of certain real quadratic fields, *Proc. Japan Acad. Ser. A Math. Sci*. **59** (1983), 390–392.

6. L. C. Washington and Zhang Xianke, Cyclic subgroups in class groups of real quadratic fields (International Centre for Theoretical Physics, Trieste, IC/92/393) 1–11.

7. P. Weinberger, Real quadratic fields with class groups divisible by *n*, *J. Number Theory* **5** (1973), 237–241.

8. Zhang Xianke, The determination of subgroups in ideal class groups of real quadratic fields, *Chinese Sci. Bull*. **37** (1992), 890–892.

9. Y. Yamamoto, On unramified Galois extensions of quadratic number fields. *Osaka J. Math*. **7** (1970), 57–76.