Canad. Math. Bull. Vol. 39 (1), 1996 pp. 106–110

A COMPLETELY GENERAL RABINOWITSCH CRITERION FOR COMPLEX QUADRATIC FIELDS

R. A. MOLLIN

ABSTRACT. We provide a criterion for the class group of a complex quadratic field to have exponent at most 2. This is given in terms of the factorization of a generalized Euler-Rabinowitsch polynomial and has consequences for consecutive distinct initial prime-producing quadratic polynomials which we cite as applications.

1. **Introduction.** In [4], we gave necessary and sufficient conditions for the *class group* C_Δ to have *exponent* $e_\Delta \leq 2$ when $\Delta < 0$ is a *discriminant*. The criterion was given in terms of the *Euler-Rabinowitsch polynomial*

$$F_\Delta(x) = x^2 + (\sigma - 1)x + (\sigma - 1 - \Delta)/4$$

where $\sigma = 2$ if $\Delta \equiv 1 \pmod 4$ and $\sigma = 1$ otherwise. This is, in fact, a generalization of the well-known Rabinowitsch class number one criterion for complex quadratic fields. What we provide herein, is an even more general and very useful criterion based upon a generalization of the Euler-Rabinowitsch polynomial as follows.

DEFINITION 1.1. Let q be a positive squarefree divisor of Δ. Put

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

where $\alpha = 1$ if $4q$ divides Δ and $\alpha = 2$ otherwise. We call $F_{\Delta,q}(x)$ the q^{th}*-Euler-Rabinowitsch polynomial*. (Thus, $q = 1$ yields the aforementioned Euler-Rabinowitsch polynomial).

We need therefore, a more general setting than that in [4], so we provide:

DEFINITION 1.2. Let $\Delta < 0$ be a discriminant and let $q \geq 1$ be a squarefree divisor of Δ. Let $F(\Delta, q)$ denote the maximum number of (not necessarily distinct) primes dividing $F_{\Delta,q}(x)$ for any integer $x \in S(q) = \{0, 1, 2, \ldots, \lfloor |\Delta|/(4q) - 1 \rfloor\}$. (Thus, $F(\Delta, 1)$ is the $F(\Delta)$ of [3, Definition 1, p. 178] and $S(1) = I$ of [3, Lemma 3, p. 178].)

In the next section, we will need some ideal theoretic notation. Let $[\gamma, \beta]$ denote the Z-module $\{\gamma x + \beta y : x, y \in Z\}$ and let D be a negative squarefree integer called the *radicand* of the complex quadratic field $Q(\sqrt{D}) = K$. Let $\omega = (\sigma - 1 + \sqrt{D})/\sigma$ called the *principal surd*, then the *discriminant* mentioned above is $\Delta = (\omega - \omega')^2 = 4D/\sigma^2$

Research supported by NSERC, Canada grant # A8484.
Received by the editors July 11, 1994; revised August 22, 1995.
AMS subject classification: 11R09, 11R11, 11R29.
Key words and phrases: prime-producing quadratics, class number, exponent, class group.

https://doi.org/10.4153/CMB-1996-013-1 Published online by Cambridge University Press

where ω' is the *algebraic conjugate* of ω. Thus, $O_\Delta = [1, \omega]$ is the *maximal order* (or *ring of integers* of K). It is well-known that I is an *ideal* of O_Δ if and only if $I = [a, b + c\omega]$ where $a, b, c \in Z$ with $c \mid a$, $c \mid b$ and $ac \mid N(b + c\omega)$ where N is the *norm* from K to Q (*i.e.*, $N(\alpha) = \alpha\alpha'$ for $\alpha \in K$). If $a > 0$ and $c = 1$ then we say that I is *primitive*.

We have provided the essentials for what is needed in the next section. The reader is referred to [3]–[4] for further background and data.

2. **Exponent two and Rabinowitsch.** First we standardize a hypothesis which we will use repeatedly.

HYPOTHESIS 2.1. Let $\Delta = \Delta_0 < 0$ ($\Delta \neq -3, -4$) be a discriminant divisible by exactly $N + 1 (N \geq 0)$ distinct primes $q_i (1 \leq i \leq N + 1)$ with q_{N+1} being the largest, and let $q \geq 1$ be a squarefree divisor of Δ, divisible by exactly $M \geq 0$ of the primes q_i for $i = 1, 2, \ldots, N$.

Now we prove a technical result which is of interest in its own right.

LEMMA 2.1. *Let Δ and q satisfy Hypothesis 2.1. Then*

$$F(\Delta, q) \geq N + 1 - M.$$

PROOF. If $M = 0$, then this is just [4, Corollary 3, p. 180]. We now assume that $M \geq 1$. If $\mathcal{Q} = \Pi_{i=1}^N \mathcal{Q}_i$ is the product of the unique O_Δ-ideals above the primes q_i for $1 \leq i \leq N$, then we may always find a representative of the ideal as $\mathcal{Q} = [Q, b + \omega_\Delta]$ where $0 \leq b < Q = \Pi_{i=1}^N q_i < |\Delta|/4$ and Q divides $N(b + \omega_\Delta)$. Moreover, $\mathcal{Q}$ cannot be principal since it is the product of the generators of the elementary abelian 2-subgroup of C_Δ. Therefore, $N(b + \omega_\Delta)$ is divisible by at least $N + 1$ primes.

CLAIM. $2b + \sigma - 1 = q(2x_0 + \alpha - 1)$ for some non-negative integer $x_0 \leq \big(|\Delta|/(4q) - 1\big)$.

If $\sigma = \alpha$, then q is forced to divide $2b+\alpha-1$, so $2b+\sigma-1 = q(2x_0+\alpha-1)$. If $\alpha \neq \sigma$, then we must have $\alpha = 2$, $\sigma = 1$, and q even. Therefore, q divides $2b = 2b+\sigma-1$ where b is odd, *i.e.*, $2b+\sigma-1 = q(2x_0+\alpha-1)$. Since $0 \leq b < |\Delta|/4$, then $0 \leq x_0 \leq |\Delta|/4q - 1$.

By the Claim, $N(b + \omega_\Delta)/q = \big(q^2(2x_0 + \alpha - 1)^2 - \Delta\big)/4q = F_{\Delta,q}(x_0)$ is divisible by at least $N + 1 - M$ primes.

THEOREM 2.1. *Let Δ and q satisfy Hypothesis 2.1. The following are equivalent:*

(1) $e_\Delta \leq 2$

(2) $F(\Delta, q) = N + 1 - M$ *and* $h_\Delta = 2^{F(\Delta,q)+M-1}$.

PROOF. If (2) holds, then $h_\Delta = 2^N$, so (1) holds by Gauss. If (1) holds, then by Lemma 2.1, $F(\Delta, q) + M - 1 \geq N$. It remains to show that there is no integer x, with $0 \leq x \leq |\Delta|/(4q) - 1$, such that $F_{\Delta,q}(x)$ is divisible by more than $N + 1 - M$ primes. Suppose, to the contrary, that such a value does exist. Let

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

then $qF_{\Delta,q}(x) = F_\Delta(y)$, with $0 \le y \le |\Delta|/4 - 1$, is divisible by more than $N+1$ primes contradicting [4, Theorem 1, p. 179].

The following tables are presented as applications of Theorem 2.1 and are discussed at the end of the paper.

$\|D\|$	q_{N+1}	$F_{\Delta,q}(x)$	B
5	5	$2x^2+2x+3$	2
13	13	$2x^2+2x+7$	6
21	7	$6x^2+6x+5$	3
33	11	$6x^2+6x+7$	6
37	37	$2x^2+2x+19$	18
57	19	$6x^2+6x+11$	9
85	17	$10x^2+10x+11$	8
93	31	$6x^2+6x+17$	15
105	7	$30x^2+30x+11$	3
133	19	$14x^2+14x+13$	9
165	11	$30x^2+30x+13$	5
177	59	$6x^2+6x+31$	29
253	23	$22x^2+22x+17$	11
273	13	$42x^2+42x+17$	6
345	23	$30x^2+30x+19$	11
357	17	$42x^2+42x+19$	8
385	11	$70x^2+70x+23$	5
1365	13	$210x^2+210x+59$	6

TABLE 2.1: $D \equiv 3 \pmod 4$

$\|D\|$	$q_{N+1} = B$	$F_{\Delta,q}(x)$
6	3	$2x^2+3$
10	5	$2x^2+5$
22	11	$2x^2+11$
30	5	$6x^2+5$
42	7	$6x^2+7$
58	29	$2x^2+29$
70	7	$10x^2+7$
78	13	$6x^2+13$
102	17	$6x^2+17$
130	13	$10x^2+13$
190	19	$10x^2+19$
210	7	$30x^2+7$
330	11	$30x^2+11$
462	11	$42x^2+11$

TABLE 2.2. $D \equiv 2 \pmod 4$

$\|D\|$	q_{N+1}	$F_{\Delta,q}(x)$	B
15	5	$3x^2+3x+2$	1
35	7	$5x^2+5x+3$	2
51	17	$3x^2+3x+5$	4
91	13	$7x^2+7x+5$	3
115	23	$5x^2+5x+7$	5
123	41	$3x^2+3x+11$	10
187	17	$11x^2+11x+7$	4
195	13	$15x^2+15x+7$	3
235	47	$5x^2+5x+13$	12
267	89	$3x^2+3x+23$	22
403	31	$13x^2+13x+11$	7
427	61	$7x^2+7x+17$	16
435	29	$15x^2+15x+11$	7
483	23	$21x^2+21x+11$	5
555	37	$15x^2+15x+13$	9
595	17	$35x^2+35x+13$	4
627	19	$33x^2+33x+13$	4
715	13	$55x^2+55x+17$	3
795	53	$15x^2+15x+17$	13
1155	11	$105x^2+105x+29$	2
1435	41	$35x^2+35x+19$	10
1995	19	$105x^2+105x+31$	4
3003	13	$231x^2+231x+61$	3
3315	17	$195x^2+195x+53$	4

TABLE 2.3. $D \equiv 1 \pmod 4)$

An easy application of Theorem 2.1 to prime-producing quadratic polynomials is

COROLLARY 2.1. *If Hypothesis 2.1 is satisfied, $e_\Delta \leq 2$, and $M = N$, then $F_{\Delta,q}(x)$ is prime for all non-negative integers $x \leq \lfloor q_{N+1}/(\sigma\alpha) - 1 \rfloor$.*

Since it is well known that if $\Delta < 0$ and $e_\Delta \leq 2$ with $\Delta \equiv 1 \pmod 8$, then $\Delta = -7$ or -15, we may assume $\Delta \not\equiv 1 \pmod 8$. We note that, by results of Weinberger [7] (see also Louboutin [2]), under the assumption of the generalized Riemann hypothesis (GRH), all $\Delta < 0$ with $e_\Delta = 2$ are known and these are exactly the values in Tables 2.1–2.3. Therefore, under the assumption of the GRH and the hypotheses of Corollary 2.1 we have:

• If $\Delta \equiv 4 \pmod 8$, then the largest string of primes occurs for $F_{\Delta,q}(x) = 6x^2+6x+31$, which is prime for $x = 0, 1, \ldots, 28$, where $D = -177$ and $q = 6$ (see Table 2.1). This example was first noted by C. Coxe (see [6]).

• If $\Delta \equiv 0 \pmod 8$, then the largest string of primes occurs for $F_{\Delta,q}(x) = 2x^2 + 29$, which is prime for $0 \leq x \leq 28$, where $D = -58$ and $q = 2$ (see Table 2.2). This example was cited by Sierpinski in [5], but probably known to Euler.

• If $\Delta \equiv 1 \pmod 4$, then the largest string of primes occurs for $F_{\Delta,q}(x) = 3x^2+3x+23$, which is prime for $0 \leq x \leq 21$, where $D = -267$ and $q = 3$ (see Table 2.3). This example was noticed in 1922 by Levy [1].

The three tables appearing above give all $D < 0$, by congruence modulo 4, together with their non-monic, consecutive, prime-producing quadratics for an initial string of values of x. Furthermore, we list the largest prime q_{N+1} and the number of initial, consecutive, distinct prime values (the column labelled B) generated by the associated quadratic as given by Corollary 2.1.

REFERENCES

1. A. Lévy, Bull. de Math., Elémentaires **19**(1912), 36.
2. S. Louboutin, *Minorationes (sous l'hypothèse de Riemann généralisée) des nombres de classes des corps quadratiques imaginaires*, C. R. Acad. Sci. Paris t., Série 1 **310**(1990), 795–800.
3. R. A. Mollin, *Orders in Quadratic Fields I*, Proc. Japan Acad., Ser. A **69**(1993), 45–48.
4. ———, *Orders in Quadratic Fields III*, Proc. Japan Acad., Ser. A **70**(1994), 176–181.
5. W. Sierpinski, *Elementary Theory of Numbers*, A. Schinzel, ed., Polish Scientific Publishers, Warsaw (1987).
6. B. Van der Pol and P. Speziali, *The primes in k(ζ)*, Indag. Math. **13**(1951), 9–15.
7. P. J. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta. Arith. **22**(1973), 117–124.

Mathematics Department
University of Calgary
Calgary, Alberta
T2N 1N4
e-mail: ramollin@math.ucalgary.ca