ACTA ARITHMETICA
LXXIV.1 (1996)

Quadratic polynomials producing consecutive, distinct primes and class groups of complex quadratic fields

by

R. A. Mollin (Calgary, Alberta)

1. Introduction. For centuries there has been a fascination with prime-producing quadratic polynomials. We will describe the relationship between such polynomials and class groups of complex quadratic fields with exponent 1 or 2. In Section 2, we set up the notation and preliminaries including a consequence of a result which we proved in [15], namely Theorem 2.3. We illustrate how all the consecutive prime-producing polynomials of Euler–Rabinowitsch type (Definition 2.2) are known under the generalized Riemann hypothesis (GRH). This was inspired by the seminal work of Frobenius [7].

In Section 3, we provide a necessary and sufficient condition for the class group to have exponent 1 or 2 in terms of the split primes less than a Minkowski bound (see Theorem 3.1). This provides some revealing consequences (see Corollary 3.1).

The last three results (one for each discriminant congruent to 5, 4 or 0 modulo 8) together with examples give a complete description of the elementary abelian 2-subgroups of the class groups of a complex quadratic field by explicitly listing the elements of the group; and this is done directly from the representatives of the discriminant as a difference of two squares. This has significant consequences when the exponent of the class group is 2.

Numerous examples, descriptions, sufficient conditions and delineation of consequences are included to show the richness of the theory, as well as to make the path for the reader an easily trod one.

2. Notation and preliminaries. Let $D < 0$ be a square-free integer, and $\Delta = 4D/\sigma^2$ where $\sigma = 2$ if $D \equiv 1 \pmod 4) and \sigma = 1$ otherwise, then Δ is called a *discriminant* with *radicand* D. Let $[\alpha, \beta] = \alpha\mathbb{Z}+\beta\mathbb{Z}$ with $\alpha, \beta \in K$

1991 *Mathematics Subject Classification*: 11R09, 11R11, 11R29.

$= \mathbb{Q}(\sqrt{D})$ for a radicand D, then the *maximal order* of K is $\mathcal{O}_\Delta = [1, w_\Delta]$, where $w_\Delta = (\sigma - 1 + \sqrt{D})/\sigma$. If $\alpha \in K$ we use α' to denote the *algebraic conjugate* of α, $N(\alpha) = \alpha\alpha'$ to denote the *norm* of α, and $\mathrm{Tr}(\alpha) = \alpha + \alpha'$ to denote the *trace* of α.

An ideal of $\mathcal{O}_\Delta$ can be written as $I = [a, b + cw_\Delta]$ where $a, b, c \in \mathbb{Z}$ with $a, c > 0$, $c \mid a$, $c \mid b$, and $ac \mid N(b + cw_\Delta)$. Furthermore, if $a, b, c \in \mathbb{Z}$ with $c \mid b$, $c \mid a$ and $ac \mid N(b + cw_\Delta)$, then $I = [a, b + cw_\Delta]$ is an ideal of $\mathcal{O}_\Delta$. The ideal I is called *primitive* if it has no rational integer factors other than ± 1, and in this case $c = 1$. The *norm* of an ideal $I = [a, b + w_\Delta]$ is defined as $a = N(I)$, and the *conjugate ideal* is denoted by $I' = [a, b + w'_\Delta]$. If $I = I'$, then I is called an *ambiguous ideal* of $\mathcal{O}_\Delta$, and if $I \sim I'$ (where $\sim$ denotes equivalence of ideals in the *class group* C_Δ of $\mathcal{O}_\Delta$), then I is said to be in an *ambiguous class* of $\mathcal{O}_\Delta$. The *class number*, or order of C_Δ, is denoted by h_Δ. An ideal of $\mathcal{O}_\Delta$ is said to be *reduced* if I is primitive and there does not exist a non-zero $\beta \in I$ such that $|\beta| < N(I)$, where $|\beta|^2 = \beta\beta' = N(\beta)$.

The following useful fact is well known (for example see [4]). In what follows, the symbol $(*/*)$ will denote the Kronecker symbol.

Theorem 2.1. *If $\Delta < 0$ is a discriminant, then*

(1) *Every class of C_Δ contains a primitive ideal I with $N(I) < M_\Delta = \sqrt{-\Delta/3}$ (M_Δ is called a Minkowski bound).*

(2) *The class group C_Δ is generated by the non-inert prime ideals $\mathcal{P}$ with $N(\mathcal{P}) < M_\Delta$ (where non-inert means that $(\Delta/p) \neq -1$).*

Note that throughout the paper we will use the phrase "a split prime p" to mean a prime $\mathcal{P}$ in $\mathcal{O}_\Delta$ above p such that $(\Delta/p) = 1$, i.e. $(p) = \mathcal{P}\mathcal{P}'$, $\mathcal{P} \neq \mathcal{P}'$.

All of the results of this section can be found in this author's book [13], including a proof of the following result, for which no other *ideal-theoretic* proof exists in the literature.

Theorem 2.2. *If $\Delta < 0$ is a discriminant, then*

(1) *If I is a primitive ideal of $\mathcal{O}_\Delta$, then there exists some $\beta \in I$ with $I = [N(I), \beta]$ and $|\mathrm{Tr}(\beta)| \leq N(I)$. Furthermore, $|\mathrm{Tr}(\beta)|$ is unique (i.e. if $I = [N(I), \beta] = [N(I), \beta_0]$ and $|\mathrm{Tr}(\beta)| \leq N(I)$, $|\mathrm{Tr}(\beta_0)| \leq N(I)$, then $|\mathrm{Tr}(\beta)| = |\mathrm{Tr}(\beta_0)|$).*

(2) *If I is a primitive ideal of $\mathcal{O}_\Delta$ and $I = [N(I), \beta]$ with $|\mathrm{Tr}(\beta)| \leq N(I)$, then I is a reduced ideal if and only if $|\beta| \geq N(I)$.*

(3) *If I is a reduced ideal of $\mathcal{O}_\Delta$, then $N(I) < \sqrt{|\Delta|/3}$.*

(4) *If I is a primitive ideal of $\mathcal{O}_\Delta$ and $N(I) < \sqrt{|\Delta|/4}$, then I is a reduced ideal.*

(5) *There are at most two reduced ideals in any given equivalence class of ideals, i.e. if I and J are reduced ideals of $\mathcal{O}_\Delta$ such that $I = [N(I), \beta] \sim$*

$J = [N(J), \beta_0]$ *with* $|\mathrm{Tr}(\beta)| \le N(I)$ *and* $|\mathrm{Tr}(\beta_0)| \le N(J)$, *then* $N(I) = N(J)$ *and* $|\mathrm{Tr}(\beta)| = |\mathrm{Tr}(\beta_0)|$.

(6) *If* $I = [N(I), \beta]$ *is a reduced ideal of* $\mathcal{O}_\Delta$ *with* $|\mathrm{Tr}(\beta)| \le N(I)$, *and if* I *is in an ambiguous class of* $\mathcal{O}_\Delta$, *then either* $N(I)$ *or* $2N(I) + |\mathrm{Tr}(\beta)|$ *is a divisor of* Δ.

(7) *Every ambiguous class of* C_Δ *contains an ambiguous ideal.*

We remind the reader of

Definition 2.1. The *exponent* e_Δ of C_Δ is the least positive integer such that $I^{e_\Delta} \sim 1$ for every ideal I representing a class of C_Δ.

Definition 2.2. Let $\Delta < 0$ be a discriminant and let $q \ge 1$ be a squarefree divisor of Δ. Set $\alpha = 1$ if $4q$ divides Δ and $\alpha = 2$ otherwise. We call

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

the *q-th Euler–Rabinowitsch polynomial.*

We may consider the following a generalization of the Ono invariant (see [15]).

Definition 2.3. Let Δ and q be as in Definition 2.2, and let $\Omega(n) = \sum_{i=1}^{m} e_i$ where $n = \prod_{i=1}^{m} p_i^{e_i}$ is the canonical prime factorization of positive $n \in \mathbb{Z}$. Set

$$F(\Delta, q) = \max\{\Omega(F_{\Delta,q}(x)) : 0 \le x \le \lfloor |\Delta|/(4q) - 1 \rfloor\}.$$

The following is a straightforward consequence of [15, Theorem 1, p. 179].

Theorem 2.3. *Let* $\Delta < 0$ $(\Delta \ne -3, -4)$ *be a discriminant divisible by exactly* $N + 1$ $(N \ge 0)$ *distinct primes* q_i $(1 \le i \le N + 1)$, *with* q_{N+1} *being the largest. If* $q = \prod_{i=1}^{N} q_i$, *then the following are equivalent*:

(1) $e_\Delta \le 2$.

(2) $F(\Delta, q) = 1$ *and* $h_\Delta = 2^N$.

Before illustrating Theorem 2.3 with several applications, we make an assumption, as a notational device, which we will cite in order to avoid repetition. After the applications, we will explain the role of the GRH in all of this.

Assumption 2.1. Let $\Delta < 0$ be a discriminant $(\Delta \ne -3, -4)$ divisible by exactly $N + 1$ $(N \ge 0)$ distinct primes with q_{N+1} the largest and set $q = \prod_{i=1}^{N} q_i$, the product of the remaining prime divisors of Δ (with $q = 1$ if $N = 0$).

Application 2.1. If $\Delta \equiv 4 \pmod 8$ satisfies Assumption 2.1, then

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

is prime for all non-negative integers $x < q_{N+1}/2 - 1$ whenever $e_\Delta \le 2$. Under the assumption of GRH, the largest string of primes occurs when $D = -177$ and $q = 6$, where

$$F_{\Delta,6}(x) = 6x^2 + 6x + 31$$

is prime for $x = 0, 1, \dots, 28$. This example was observed by Van der Pol and Speziali (via Coxe) [24] and motivated this result.

Application 2.2. If $\Delta \equiv 0 \pmod 8$ satisfies Assumption 2.1, then if $e_\Delta \le 2$,

$$F_{\Delta,q}(x) = qx^2 + q_{N+1}$$

is prime whenever $0 \le x \le q_{N+1} - 1$. Under the assumption of GRH, the largest such string is given by $D = -58$ and $q = 2$, where

$$F_{\Delta,2}(x) = 2x^2 + 29$$

is prime for $0 \le x \le 28$. This example was cited by Sierpiński in [21] (probably known to Euler) and motivated this result.

Application 2.3. If $\Delta \equiv 1 \pmod 4$ satisfies Assumption 2.1, then whenever $e_\Delta \le 2$,

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

is prime for all non-negative integers $x < \lfloor q_{N+1}/4 - 1 \rfloor$. Under the assumption of GRH, the largest string occurs when $D = -267$ and $q = 3$, where

$$F_{\Delta,3}(x) = 3x^2 + 3x + 23$$

is prime whenever $0 \le x \le 21$. A version of this example was noticed by Lévy [11] in 1914, and motivated our result.

From the work of Weinberger [25], all $\Delta < 0$ with $e_\Delta = 2$ are known under the GRH assumption. There are 56 values of Δ with $\Delta = -3315$ being the largest. Hence, each of these values together with their respective q values provide all possible consecutive, distinct, prime-producing $F_{\Delta,q}(x)$. The optimal ones for each congruence class modulo 4 are provided in Applications 2.1–2.3, which have been ubiquitous in the literature without an explanation as to why they occur. The reason is $e_\Delta = 2$. (See [13] for a complete list of the $F_{\Delta,q}(x)$.)

Recall that, if $\Delta \equiv 1 \pmod 8$, then $e_\Delta = 2$ implies that $\Delta = -7$ or -15. To see this in a one-line proof: Since $(2) = \mathcal{P}\mathcal{P}'$ with $\mathcal{P} \ne \mathcal{P}'$ and $\mathcal{P}^2 \sim 1$, then there exists an $\alpha \in \mathcal{O}_\Delta$, $\alpha \notin \mathbb{Z}$, with $N(\alpha) = 4$, i.e. $16 = x^2 - \Delta y^2$ for some $x, y \in \mathbb{Z}$, $y \ne 0$; so $|\Delta| \le 15$. Also, recall that if $h_\Delta \le 4$ and $e_\Delta = 2$, then we do not need the GRH, i.e. all of such $\Delta < 0$ values are known. This is a result of the $h_\Delta \le 2$ solution of Baker [2]–[3], Stark [22]–[23], and the $h_\Delta = 4$ solution of Arno [1].

This concludes the discussion of the non-monic prime-producing quadratic polynomials. The most celebrated of the monic prime-producing polynomials is Euler's polynomial $f(x) = x^2 - x + 41$ discovered in 1772 (see [6]). This polynomial is prime for $x = 1, 2, \ldots, 40$. Similarly, Legendre [9] observed that the polynomial $g(x) = x^2 + x + 41$ is prime for all integers $x = 0, 1, \ldots, 39$. However, $g(x)$ has come to be known as the Euler polynomial (e.g. see [19, p. 24], [10], and [4, p. 155]). In any case, the prime-producing capacity of these polynomials has less to do with their specific form than it does with their discriminant $\Delta = -163$. This is explained by Rabinowitsch's criterion [17]–[18] (which Theorem 2.3 generalizes), together with the Baker [2], Heegner [8], and Stark [22] solution of the class number one problem of Gauss for $\Delta < 0$. It follows from this that $f_\Delta(x) = x^2 + x + A$ cannot be consecutively prime for $x = 0, 1, 2, \ldots, A - 2$ when $A > 41$. The reason, of course, is that $A = (1 - \Delta)/4$ and $\Delta = -163$ is the last complex quadratic field with $h_\Delta = 1$. Hence, Euler's polynomial tops the list of the consecutive, distinct prime-producing monic polynomials of negative discriminant. If one allows *repetitions*, then we can get larger strings of consecutive primes in an initial range of x values. For example, we can transform $x^2 + x + 41$ via $x \to x - 40$ into $x^2 - 79x + 1601$, discovered by Escott [5] in 1899. The latter polynomial is prime for the 80 values $x = 0, 1, 2, \ldots, 79$ with each prime repeated twice.

We conclude by noting that if $\Delta > 0$ then quadratic prime-producers have been found which supplant Euler's polynomial. Among them are $h(x) = 47x^2 - 2247x + 21647$ and $k(x) = 36x^2 - 810x + 2753$. The former is called the Fung polynomial which is prime for $x = 0, 1, \ldots, 42$, and the latter is called the Ruby polynomial which is prime for $x = 0, 1, \ldots, 44$ (see [13]).

3. Quadratic prime-producers and class groups. The following technical lemmata will be required in what follows. (For the definition of M_Δ see Theorem 2.1, and for that of α and $F_{\Delta,q}(x)$ see Definition 2.2.)

LEMMA 3.1. *Let $\Delta < 0$ be a discriminant and let $q \geq 1$ be a square-free divisor of it. If $p < M_\Delta$ is any non-inert prime which does not divide q, then there exists a non-negative integer $x < (M_\Delta - \alpha + 1)/2$ such that p divides $F_{\Delta,q}(x)$.*

Proof. If $p = 2$, then q is odd. If $\alpha = 1$ and $D \equiv 3 \pmod 4$, then $F_{\Delta,q}(1)$ is even. If $D \equiv 0 \pmod 2$, then $F_{\Delta,q}(0)$ is even. If $\alpha = 2$, then $\sigma = 2$, so $\Delta \equiv 1 \pmod 8$. Thus, $F_{\Delta,q}(0)$ is even. We may now assume that $p > 2$. By [14, Lemma 2.1, p. 46], there is an integer $x \geq 0$ such that p divides $F_{\Delta,q}(x)$. Thus, $q^2(2x + \alpha - 1)^2 \equiv \Delta \pmod p$. Therefore, we may assume without loss of generality that $0 \leq 2x + \alpha - 1 < p$ (since we may take the least non-negative residue modulo p, and when $\alpha = 2$ we may assume that the residue is odd since p is odd). Hence, $0 \le x < (M_\Delta - \alpha + 1)/2$. ■

Lemma 3.2. *Let $\Delta < 0$ be a discriminant with $q \ge 1$ a square-free divisor of $|\Delta|$. If $a > 0$ is an integer with $F_{\Delta,q}(x) = a$, where x is any non-negative integer, then $\mathcal{Q} \sim \mathcal{A}$, an $\mathcal{O}_\Delta$-ideal above a.*

Proof. Form the ideal $\mathcal{A}\mathcal{Q} = [aq, (b+\sqrt{\Delta})/2]$, where $b = (2x + \alpha - 1)q$. Then $N\big((b+\sqrt{\Delta})/2\big) = qF_{\Delta,q}(x) = aq$. Therefore, $\mathcal{A}\mathcal{Q} = \big((b+\sqrt{\Delta})/2\big)$, i.e. $\mathcal{Q} \sim \mathcal{A}$. ■

The reader will recognize that Lemma 3.2 basically says that representation of integers is tantamount to equivalence of ideals.

Remark 3.1. It is worth pointing out that Lemma 3.2 tells us that when $q = 1$, then $\mathcal{A} \sim 1$. What this means is that the factorization of the Euler–Rabinowitsch polynomial $F_{\Delta,1}(x) = F_\Delta(x)$ up to the Rabinowitsch bound $(|\Delta|/4 - 1)$ as given by Theorem 2.3, yields the equivalence classes in C_Δ. For instance, we have

Example 3.1. Let $\Delta = -3315$. Then $F_\Delta(x) = x^2 + x + 829$ and $h_\Delta = 8$, and the Rabinowitsch bound is $\lfloor |\Delta|/4 - 1 \rfloor = 827$. The only split primes $p < M_\Delta$ are 29 and 31 (see Table 3.1 below), and since $F_\Delta(19) = 3 \cdot 13 \cdot 31$, then $\mathcal{Q}_3\mathcal{Q}_{13} \sim \mathcal{Q}_{31}$, where $\mathcal{Q}_q$ lies over q in $\mathcal{O}_\Delta$. Also since $F_\Delta(25) = 3\cdot 17\cdot 29$, then $\mathcal{Q}_3\mathcal{Q}_{17} \sim \mathcal{Q}_{29}$. In fact, Theorem 3.1 below says a great deal about $e_\Delta \le 2$ and the number of split primes $p < M_\Delta$.

Lemma 3.3. *If $\Delta < 0$ is a discriminant and $I = [a, b+\omega_\Delta]$ is a primitive ideal of $\mathcal{O}_\Delta$ with $N(b + \omega_\Delta) < N(\omega_\Delta)^2$, then I is a principal ideal if and only if $a = 1$ or $a = N(b + \omega_\Delta)$.*

Proof. See [20] (and [15] for a generalization which also appears in [13]). ■

Remark 3.2. No such criterion exists if $\Delta > 0$. In fact, it often happens that when $\Delta > 0$ we have $[a, b + \omega_\Delta] \sim 1$, yet $N(w_\Delta)^2 > N(b + \omega_\Delta) > a > 1$. For instance, if $\Delta = 4 \cdot 19$, then $\mathcal{P} = [2, -1 + \sqrt{19}] \sim 1$. In fact, $\mathcal{P} = (13 + 3\sqrt{19})$ but there is no representation of $\mathcal{P}$ in the form $[2, b + \omega_\Delta]$ with $N(b + \omega_\Delta) = 2$.

Now we provide a necessary and sufficient condition for $e_\Delta \le 2$.

Theorem 3.1. *If $\Delta < 0$ is a discriminant, then the following are equivalent:*

(1) *$e_\Delta \le 2$.*

(2) *For every split prime $p < M_\Delta$ there exists a proper square-free divisor $q > p$ of $|\Delta|$ such that $\Delta = q^2 - 4pq$.*

Proof. If (2) holds, then (1) follows from Theorem 2.1 and Lemma 3.2, since $F_{\Delta,q}(0) = p$ when $\Delta \not\equiv 0 \pmod 8$, which we may assume, since such a split prime p does not exist otherwise.

Conversely, if (1) holds and $p < M_\Delta$ is any split prime, then there exists an $\mathcal{O}_\Delta$-ideal $I = [p, \beta]$, where $\beta = (b + \sqrt{\Delta})/2$ for some $b \in \mathbb{Z}$ with $|b| < p$, since we may choose any appropriate b with $\Delta \equiv b^2 \pmod p$. By Theorem 2.2(7), there exists an ambiguous ideal $J \sim I$ with $q = N(J) < \sqrt{|\Delta|}$, and $J = [q, (\varepsilon q + \sqrt{\Delta})/2]$, where $\varepsilon = 1$ if Δ/q is square-free, and $\varepsilon = 0$ otherwise. Since $IJ \sim 1$, we have $IJ = (\gamma)$ for some $\gamma \in J$ (since ideals which "divide" are those which "contain", i.e. $J \mid (\gamma)$ implies $\gamma \in J$). Therefore, there exist $x, y \in \mathbb{Z}$ such that $2\gamma = qx + y\sqrt{\Delta}$. By taking norms and dividing by q we have

$$4p = qx^2 - y^2\Delta/q < 4\sqrt{|\Delta|/3}.$$

If either $x = 0$, or $y = 0$, then $p \mid |\Delta|$, a contradiction. Since $q < \sqrt{-\Delta}$ we have $y^2 \le 1$ so $|y| = 1$. If $|x| \ge 2$, then

$$4q + |\Delta|/q < 4p < 4\sqrt{|\Delta|/3},$$

so

$$8|\Delta| < 16q^2 + 8|\Delta| + \Delta^2/q^2 < 16|\Delta|/3,$$

a contradiction. Thus $|x| = 1$, and $\Delta = q^2 - 4pq$, as required. Since $p = (q_1 + q)/4$ where $\Delta = -qq_1$, it follows that $q_1^2 - 4pq_1 = \Delta = q^2 - 4pq$. Therefore, we may assume that $q > p$ since one of q or q_1 must be. ■

Observe that, in the above proof, we did not make any assertion regarding the "reduction" of I, since we did not need it. However, we pose

CONJECTURE 3.1. *If $e_\Delta \le 2$ and $p < M_\Delta$ is a split prime, then the $\mathcal{O}_\Delta$-ideal $I = [p, (b + \sqrt{\Delta})/2]$ is reduced for some $|b| < p$.*

COROLLARY 3.1. *If $\Delta < 0$ and $e_\Delta \le 2$ for a discriminant Δ, then*

(1) *If $\Delta \equiv 4, 5 \pmod 8$, then any reduced ideal $\mathcal{P}$ above a split prime $p < M_\Delta$ must be of the form $\mathcal{P} = [p, (q - 2p + \sqrt{\Delta})/2]$, where $\mathcal{P} \sim \mathcal{Q}$, the unique ideal above q $(> p)$ dividing $|\Delta|$, together with its conjugate $\mathcal{P}' = [p, (q' - 2p + \sqrt{\Delta})/2]$, where $q' = |\Delta|/q$.*

(2) *If $\Delta \equiv 0 \pmod 8$, then there are no split primes $p < M_\Delta$.*

(3) *If $\Delta \equiv 1 \pmod 8$, then $\Delta = -7$ or -15.*

(4) *If $h_\Delta = 1$, then there are no split primes $p < M_\Delta$.*

Proof. All of (1)–(3) are essentially contained in the proof of Theorem 3.1. If $h_\Delta = 1$, then Theorem 2.2(5) tells us that the trivial ideal (1) is the only reduced ideal in the class. ■

We have not been successful in proving the following conjecture which holds under the assumption of the GRH.

Conjecture 3.2. *If $\Delta < 0$ is a discriminant with $\Delta \equiv 5 \pmod 8$ and $e_\Delta \le 2$, then there are at most* 2 *split primes $p < M_\Delta$, and if $\Delta \equiv 4 \pmod 8$, then there is at most one such prime.*

However, we can give the following unconditional proof for a certain case.

Theorem 3.2. *If $\Delta < 0$ is a discriminant satisfying Assumption* 2.1 *with $\Delta \not\equiv 0 \pmod 8$ and $F_{\Delta,q}(x)$ is prime whenever $0 \le x < (M_\Delta - 1)/2$, then there is at most one split prime $p < M_\Delta$.*

Proof. If $F_{\Delta,q}(1) < M_\Delta$, then $2q+(q^2-\Delta)/(4q) = (9q+q_{N+1})/4 < M_\Delta$, if $\Delta \equiv 1 \pmod 4$. Thus, $243q^2 + 38qq_{N+1} + 3q_{N+1}^2 < 0$, a contradiction. Therefore, by Lemma 3.1, the only possible split prime $p < M_\Delta$ is $p = (q + \alpha q_{N+1}/\sigma)/4$. The case $\Delta \equiv 4 \pmod 8$ is similar. ∎

Remark 3.3. The GRH tells us that the only possible remaining values (not covered by Theorem 3.2) are $-\Delta \in \{195, 595, 627, 715, 1155, 1995, 3003, 3315\}$, where the first four values have $h_\Delta = 4$ and the last four values have $h_\Delta = 8$. The first four values have at most one split prime $p < M_\Delta$ (namely 7 for -195, 13 for -595, -627, and none for -715). The last four values have at most two split primes $p < M_\Delta$ (17 and 19 for -1155, 23 for -1995, and 29, 31 for both -3003 and -3315).

To illustrate Theorems 3.1–3.2 and Conjecture 3.2, we provide the list (Table 3.1) for which a split prime $p < M_\Delta$ exists together with a value of q such that $\Delta = q^2 - 4pq$ (and its associate q' where $qq' = \prod_{i=1}^{N+1} q_i$, with the q_i's being all the distinct primes dividing Δ). The table is split into 2 parts, one for $\Delta \equiv 4 \pmod 8$ and one for $\Delta \equiv 5 \pmod 8$.

Table 3.1

$\Delta \equiv 4 \pmod 8$

$-D$	p	q	q'
21	5	14	6
105	11	30	14
133	13	38	14
165	13	30	22
273	17	42	26
345	19	46	30
357	19	42	34
1365	37	78	70

$\Delta \equiv 5 \pmod 8$

$-\Delta$	p	q	q'
35	3	7	5
91	5	13	7
187	7	17	11
195	7	15	13
403	11	31	13
435	11	29	15
483	11	23	21
555	13	37	15
595	13	35	17
627	13	33	19
1155	17	35	33
1155	19	55	21
1995	23	57	35
3003	29	77	39
3003	31	91	33
3315	29	65	51
3315	31	85	39

Remark 3.4. In [14] we made a conjecture which came close to Theorem 3.1. However, we showed in [15] that the conjecture is false. But, that conjecture was overly ambitious in that we need not have considered it necessary to include ramified primes. Theorem 3.1 then proves the lesser conjecture, namely $e_\Delta \le 2$ if and only if, for each split $p < M_\Delta$, there exists a square-free divisor q of Δ with $F_{\Delta,q}(x) = p$ for some $x \ge 0$. In fact, we have done far more. We have shown that we may always choose $x = 0$!

Now we show how the structure of the elementary abelian 2-subgroup of C_Δ for $\Delta < 0$ is completely determined by the representation of Δ as a difference of two squares. This has some consequences when $e_\Delta = 2$, which we illustrate after the result.

Theorem 3.3. *If* $\Delta \equiv 5 \pmod 8$ *is a discriminant satisfying Assumption* 2.1, *then* Δ *is a difference of squares in exactly* 2^N *distinct ways*, *namely*

$$\Delta = a_i^2 - 4b_i^2$$

with $b_i \le N(\omega_\Delta)$, $a_i = (q_{N+1}q^{(i)} \mp q_1^{(i)})/2$ *and* $b_i = (q_{N+1}q^{(i)} \pm q_1^{(i)})/4$, *where* $q = q^{(i)}q_1^{(i)}$ *runs thorough all* 2^{N-1} *distinct factorizations for* $q^{(i)} \ge 1$. *Furthermore*, *the primitive ideals* $[b_i, (a_i + \sqrt{\Delta})/2]$ *comprise the elementary abelian* 2-*subgroup* $C_{\Delta,2}$ *of* C_Δ. *Also*, *for each* $i \le 2^{N-1}$,

$$\Delta = (q_{N+1}q^{(i)})^2 \mp 4b_iq_{N+1}q^{(i)}$$

(*where* $\mp$ *corresponds to* $\pm$ *in the definition of* b_i *above*).

Proof. q_{N+1}, being prime, has exactly one representation as a difference of two squares, namely

$$q_{N+1} = [(q_{N+1}+1)/2]^2 - [(q_{N+1}-1)/2]^2.$$

Moreover, q has exactly 2^{N-1} distinct such representations, namely

$$q = [(q^{(i)} + q_1^{(i)})/2]^2 - [(q^{(i)} - q_1^{(i)})/2]^2$$

for each of the 2^{N-1} distinct factorizations $q = q^{(i)}q_1^{(i)}$ for $i = 1, 2, \ldots, 2^{N-1}$, with $q^{(i)} \ge 1$. Furthermore, each such representation for q yields 2 distinct such representations for Δ as follows (where $x = (q_{N+1}-1)/2$, $y = (q_{N+1}+1)/2$, $u = (q^{(i)} + q_1^{(i)})/2$ and $v = (q^{(i)} - q_1^{(i)})/2$):

$$\Delta = (x^2 - y^2)(u^2 - v^2) = (xu \pm yv)^2 - (yu \pm xv)^2.$$

Moreover, since $\Delta \equiv 5 \pmod 8$, it follows that $yu \pm xv$ is divisible by 4 and $yu + xv = (q_{N+1}q^{(i)} + q_1^{(i)})/2$ has its largest possible value at $q^{(i)} = q$ and $q_1^{(i)} = 1$, i.e. $(yu + xv)/2 = (1 - \Delta)/4 = N(\omega_\Delta)$. Thus, for

$$b_i = ((q_{N+1}q^{(i)})^2 - \Delta)/(4q_{N+1}q^{(i)})$$

and

$$b_i^{(1)} = ((q_{N+1}q^{(i)})^2 - \Delta)/(4q_{N+1}q_1^{(i)}),$$

$\mathcal{B}_i \sim \mathcal{Q}_{N+1}\mathcal{Q}^{(i)}$ and $\mathcal{B}_i^{(1)} \sim \mathcal{Q}_{N+1}\mathcal{Q}_1^{(i)}$, where $\mathcal{B}_i$, $\mathcal{B}_i^{(1)}$, $\mathcal{Q}_{N+1}$, $\mathcal{Q}_1^{(i)}$ and $\mathcal{Q}^{(i)}$ are $\mathcal{O}_\Delta$-primes above b_i, $b_i^{(1)}$, q_{N+1}, $q_1^{(i)}$ and $q^{(i)}$ respectively, by Lemma 3.2. If $\mathcal{B}_i \sim \mathcal{B}_j$ or $\mathcal{B}_i \sim \mathcal{B}_j^{(1)}$ for any $i \neq j$ (say $\mathcal{B}_i \sim \mathcal{B}_j$ for convenience) then $\mathcal{Q}^{(i)}\mathcal{Q}^{(j)} \sim 1$. However, after possibly removing square factors of ideals from $\mathcal{Q}^{(i)}\mathcal{Q}^{(j)}$ (since squares are necessarily principal) we are left with a non-trivial principal $\mathcal{O}_\Delta$-prime whose norm divides q. This is a contradiction since the value q is the product of those ramified primes whose $\mathcal{O}_\Delta$-primes generate $C_{\Delta,2}$. Hence the $[b_i, (a+\sqrt{\Delta})/2]$ comprise $C_{\Delta,2}$. The last statement of the theorem is an easy check. ■

We illustrate Theorem 3.3 with the following example.

Example 3.2. Let $\Delta = -3315$. Then $h_\Delta = 8$ ($N = 3$), $q_{N+1} = 17 = q^2 - 8^2$ and $q = 195 = 14^2 - 1^2 = 22^2 - 17^2 = 34^2 - 31^2 = 98^2 - 97^2$. Hence

$$\begin{aligned}
\Delta &= (8^2 - 9^2)(14^2 - 1^2)\\
&= (8\cdot 14 + 9\cdot 1)^2 - (9\cdot 14 + 8\cdot 1)^2\\
&= 121^2 - 4\cdot 67^2 \qquad (3.1)\\
&= (8\cdot 14 - 9\cdot 1)^2 - (9\cdot 14 - 8\cdot 1)^2\\
&= 103^2 - 4\cdot 59^2 \qquad (3.2)\\
&= (8^2 - 9^2)(22^2 - 17^2)\\
&= (8\cdot 22 + 9\cdot 17)^2 - (9\cdot 22 + 8\cdot 17)^2\\
&= 329^2 - 4\cdot 167^2 \qquad (3.3)\\
&= (8\cdot 22 - 9\cdot 17)^2 - (9\cdot 22 - 8\cdot 17)^2\\
&= 23^2 - 4\cdot 31^2 \qquad (3.4)\\
&= (8^2 - 9^2)(34^2 - 31^2)\\
&= (8\cdot 34 + 9\cdot 31)^2 - (9\cdot 34 + 8\cdot 31)^2\\
&= 551^2 - 4\cdot 277^2 \qquad (3.5)\\
&= (8\cdot 34 - 9\cdot 31)^2 - (9\cdot 34 - 8\cdot 31)^2\\
&= 7^2 - 4\cdot 29^2 \qquad (3.6)\\
&= (8^2 - 9^2)(98^2 - 97^2)\\
&= (8\cdot 98 + 9\cdot 97)^2 - (9\cdot 98 + 8\cdot 97)^2\\
&= 1657^2 - 4\cdot 829^2 \qquad (3.7)\\
&= (8\cdot 98 - 9\cdot 97)^2 - (9\cdot 98 - 8\cdot 97)^2\\
&= 89^2 - 4\cdot 53^2. \qquad (3.8)
\end{aligned}$$

We note that each of the $8 = 2^N$ distinct representatives (3.1)–(3.8), of Δ as a difference of squares yield the class group C_Δ via the primitive ideals $I_1 = [67, (11^2 + \sqrt{\Delta})/2]$, $I_2 = [59, (103 + \sqrt{\Delta})/2]$, $I_3 = [167, (329 + \sqrt{\Delta})/2]$, $I_4 = [31, (23 + \sqrt{\Delta})/2]$, $I_5 = [277, (551 + \sqrt{\Delta})/2]$, $I_6 = [29, (7 + \sqrt{\Delta})/2]$, $I_7 = [829, (1657 + \sqrt{\Delta})/2]$ and $I_8 = [53, (89 + \sqrt{\Delta})/2]$. These ideals are not necessarily reduced but the two representing the split primes $p < M_\Delta$, namely I_4 and I_6 are reduced. Furthermore, via the last statement of Theorem 3.3 we have

$$\Delta = (q_{N+1}q^{(i)})^2 - 4b_i q_{N+1} q^{(i)} = (17\cdot 5)^2 - 4\cdot 31\cdot 17\cdot 5 = (17\cdot 3)^2 - 4\cdot 29\cdot 17\cdot 3,$$

as predicted by Theorem 3.1. Moreover, it can be shown via the factorization of the Euler–Rabinowitsch polynomial as given in Theorem 2.3 that $I_1 \sim \mathcal{Q}_{13}$, $I_2 \sim \mathcal{Q}_3\mathcal{Q}_5$, $I_3 \sim \mathcal{Q}_5$, $I_4 \sim \mathcal{Q}_3\mathcal{Q}_{13}$, $I_5 \sim \mathcal{Q}_3$, $I_6 \sim \mathcal{Q}_3\mathcal{Q}_{17}$, $I_7 \sim 1$, and $I_8 \sim \mathcal{Q}_{17}$. Thus $C_\Delta = \langle\{I_1\}\rangle \times \langle\{I_3\}\rangle \times \langle\{I_5\}\rangle$, where $\{I\}$ denotes the class of I in C_Δ.

Thus Theorem 3.3 provides a description of the class group C_Δ via differences of squares when $e_\Delta = 2$. Note that by Theorem 3.1, if $e_\Delta = 2$, then necessarily all $p < M_\Delta$ which are split primes must appear as some b_i in Theorem 3.3.

Remark 3.5. If we let $q^{(i)} = q/q_i$ and $q_1^{(i)} = q_i$ in Theorem 3.3 for $i = 1, \ldots, N$, then we conclude that N differences of squares $(xu + yv)^2 - (yu + xv)^2$ (for x, y, u and v as given in the proof of Theorem 3.3) give rise to N generators of $C_{\Delta,2}$. Thus, we have

Corollary 3.2. *If $\Delta \equiv 5 \pmod 8$ is a discriminant satisfying Assumption 2.1, then $C_{\Delta,2}$ is generated by the classes containing $[b_i, (a_i + \sqrt{\Delta})/2]$ for $i = 1, \ldots, N$, where*

$$b_i = (q_i^2 - \Delta)/(4q_i) \quad \textit{and} \quad a_i = -(q_i^2 + \Delta)/(2q_i).$$

We also have similar results for $\Delta \equiv 0 \pmod 4$ which we state without proof since the verification is similar to that of Theorem 3.3.

Theorem 3.4. *If $\Delta \equiv 4 \pmod 8$, $\Delta < 0$ is a discriminant divisible by exactly $N + 1$ distinct primes with $q_1 = 2 < q_2 < \ldots < q_{N+1}$ then $C_{\Delta,2}$ is generated by the classes containing the ideals $[b_i, a_i + \sqrt{D}]$, where*

$$b_i = (q_i^2 - D)/(2q_i) \quad \textit{and} \quad a_i = -(q_i^2 + D)/(2q_i)$$

for $i = 2, \ldots, N$, and

$$b_1 = (1 - D)/2, \qquad a_1 = -(1 + D)/2.$$

Note that the ideals in Theorem 3.4 arise from D as a difference of 2 squares in much the same way as Theorem 3.3. For instance, we have

Example 3.3. Let $\Delta = -4\cdot 1365 = -4\cdot 3\cdot 5\cdot 7\cdot 13$, where $105 = q = 3\cdot 5\cdot 7 = q_2q_3q_4$ and $q_5 = q_{N+1} = 13$. Also, $q = 19^2 - 16^2 = 11^2 - 4^2 =$

$53^2 - 52^2 = 13^2 - 8^2$ and $q_{N+1} = 7^2 - 6^2$. Hence,

$$\begin{aligned} D &= (6^2 - 7^2)(19^2 - 16^2) = 226^2 - 229^2 \\ &= (6^2 - 7^2)(11^2 - 4^2) = 94^2 - 101^2 \\ &= (6^2 - 7^2)(53^2 - 52^2) = 682^2 - 683^2 \\ &= (6^2 - 7^2)(13^2 - 8^2) = 134^2 - 139^2 \end{aligned}$$

and these four representations give rise to the generators of C_Δ, namely $I_1 = [229, 226 + \sqrt{D}]$, $I_2 = [101, 94 + \sqrt{D}]$, $I_3 = [683, 682 + \sqrt{D}]$, $I_4 = [139, 134 + \sqrt{D}]$. Also, we observe (from the factorization of the Euler–Rabinowitsch polynomial as given in Theorem 2.3) that $I_1 \sim \mathcal{Q}_2\mathcal{Q}_3$, $I_2 \sim \mathcal{Q}_2\mathcal{Q}_7$, $I_3 \sim \mathcal{Q}_2$, and $I_4 \sim \mathcal{Q}_2\mathcal{Q}_5$, where $\mathcal{Q}_q$ is the unique $\mathcal{O}_\Delta$-ideal above q.

We now present a result for $\Delta \equiv 0 \pmod 8$ which we do not prove since it is again similar to that of the proof of Theorem 3.3.

Theorem 3.5. *If $\Delta \equiv 0 \pmod 8$ with $\Delta < 0$ is a discriminant divisible by exactly $N + 1$ distinct primes q_i, then $C_{\Delta,2}$ is generated by the classes of the ideals $I_i = [b_i, a_i + \sqrt{\Delta}]$ for $i = 1, \ldots, N$, where*

$$b_i = 2\overline{q}/q_i + q_i \quad \text{and} \quad a_i = -q_i$$

with $\overline{q}$ being the product of the N distinct odd primes $q_2, q_3, \ldots, q_{N+1}$.

Theorem 3.5 is illustrated by the following which shows how the ideals arise from Δ as a difference of squares.

Example 3.4. Let $\Delta = 1848 = 8 \cdot 3 \cdot 7 \cdot 11$. Here $8 = 3^2 - 1$ and $231 = 3 \cdot 7 \cdot 11 = 40^2 - 37^2 = 20^2 - 13^2 = 16^2 - 5^2$. Thus

$$\begin{aligned} \Delta &= (1^2 - 3^2)(40^2 - 37^2) = 151^2 - 157^2 \\ &= (1^2 - 3^2)(20^2 - 13^2) = 59^2 - 73^2 \\ &= (1^2 - 3^2)(16^2 - 5^2) = 31^2 - 53^2. \end{aligned}$$

If we set $q_2 = 3$, $q_3 = 7$, $q_4 = 11$ and $\overline{q} = 231$, then $b_1 = 157$, $b_2 = 73$, and $b_3 = 53$. Thus the generators are $I_1 = [157, -3+\sqrt{D}] = [157, 154+\sqrt{D}]$, $I_2 = [73, -7+\sqrt{D}] = [73, 66+\sqrt{D}]$, and $I_3 = [53, -11+\sqrt{D}] = [53, 42+\sqrt{D}]$. We observe that, unlike the cases in Examples 3.2–3.3, D cannot be represented as a difference of two squares since $D \equiv 2 \pmod 4$.

What we have essentially done in Theorems 3.2–3.4 is construct the group $C_{\Delta,2}$.

This concludes our discussion of prime-producing quadratic polynomials of negative discriminant.

When $\Delta > 0$ we looked at such restrictions on the number of primes $p < M_\Delta$, and obtained complete classifications for certain Δ when $e_\Delta \le 2$ in previous work. We will deal with prime-producing quadratics for $\Delta > 0$ in later work (see [12], and [16] for a precursor).

Acknowledgements. The author's research is supported by NSERC Canada grant #A8484. The author also thanks the referee for many valuable comments which helped to shorten and refine the paper.

References

[1] S. Arno, *The imaginary quadratic fields of class number* 4, Acta. Arith. 60 (1992), 321–334.

[2] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika 13 (1966), 204–216.

[3] —, *Imaginary quadratic fields with class number two*, Ann. of Math. 94 (1971), 139–152.

[4] H. Cohn, *A Second Course in Number Theory*, Wiley, 1962.

[5] E. B. Escott, *Réponses 1133 "Formule d'Euler* x^2+x+41 *et formules analogues"*, L'intermédiaire des Math. 6 (1899), 10–11.

[6] L. Euler, *Extrait d'une lettre de M. Euler le père à M. Bernoulli concernant le mémoire imprimé parmi ceux de 1771*, p. 381, Nouveaux mémoirs de l'Académie des Sciences de Berlin 1772, (1774) Histoire, 35–36; Opera Omnia, I_3, Commentationes Arithmeticae, II, Teubner, Lipsiae et Berolini, 1917, 335–337.

[7] F. G. Frobenius, *Über quadratische Formen die viele Primzahlen darstellen*, Sitzungsber. Kgl. Preuss. Akad. Wiss. Berlin 1912, 966–980.

[8] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. 56 (1952), 227–253.

[9] A. M. Legendre, *Théorie des nombres*, Libraire Scientifique A. Hermann, Paris, 1798, 69–76; 2nd ed., 1808, 61–67; 3rd ed., 1830, 72–80.

[10] D. H. Lehmer, *On the function* $x^2 + x + A$, Sphinx 6 (1936), 212–214.

[11] A. Lévy, *Sur les nombres premiers dérivés de trinomes du second degré*, Sphinx-Oedipe 9 (1914), 6–7.

[12] S. Louboutin, R. A. Mollin and H. C. Williams, *Class groups of exponent two in real quadratic fields*, in: Advances in Number Theory, F. Q. Gouvéa and N. Yui (eds.) in consultation with A. Granville, R. Gupta, E. Kani, H. Kisilevsky, R. A. Mollin, and C. Stewart, Clarendon Press, Oxford, 1993, 499–513.

[13] R. A. Mollin, *Quadratics*, C.R.C. Press, Florida, 1995; to appear.

[14] —, *Orders in quadratic fields I*, Proc. Japan Acad. Ser. A 69 (1993), 45–48.

[15] —, *Orders in quadratic fields III*, ibid. 70 (1994), 176–181.

[16] R. A. Mollin and H. C. Williams, *Prime-producing quadratic polynomials and real quadratic fields of class number one*, in: Number Theory, J. M. De Koninck and C. Levesque (eds.), de Gruyter, Berlin, 1989, 654–663.

[17] G. Rabinowitsch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*, in: Proc. Fifth Internat. Congress Math., Cambridge, I, 1913, 418–421.

[18] —, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*, J. Reine Angew. Math. 142 (1913), 153–164.

[19] P. Ribenboim, *Euler's famous prime generating polynomial and class numbers of imaginary quadratic fields*, Enseign. Math. 34 (1988), 23–42.

[20] R. Sasaki, *On a lower bound for the class numbers of an imaginary quadratic field*, Proc. Japan Acad. Ser. A 62 (1986), 37–39.

[21] W. Sierpiński, *Elementary Theory of Numbers*, Polish Scientific Publ., Warszawa, 1964.

[22] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. 14 (1967), 1–27.

[23] —, *A transcendence theorem for class number problems*, Ann. of Math. 94 (1971), 153–173.

[24] B. Van der Pol and P. Speziali, *The primes in $k(\zeta)$*, Indag. Math. 13 (1951), 9–15.

[25] P. J. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta Arith. 22 (1973), 117–124.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALGARY
CALGARY, ALBERTA
T2N 1N4, CANADA
E-mail: RAMOLLIN@MATH.UCALGARY.CA

Received on 11.5.1994
and in revised form on 16.6.1995 (2612)