

## POLYNOMIALS OF QUADRATIC TYPE PRODUCING STRINGS OF PRIMES

R. A. MOLLIN, B. GODDARD AND S. COUPLAND

**ABSTRACT.** The primary purpose of this paper is to provide necessary and sufficient conditions for certain quadratic polynomials of negative discriminant (which we call Euler-Rabinowitsch type), to produce consecutive prime values for an initial range of input values less than a Minkowski bound. This not only generalizes the classical work of Frobenius, the later developments by Hendy, and the generalizations by others, but also concludes the line of reasoning by providing a complete list of all such prime-producing polynomials, under the assumption of the generalized Riemann hypothesis (GRH). We demonstrate how this prime-production phenomenon is related to the exponent of the class group of the underlying complex quadratic field. Numerous examples, and a remaining conjecture, are also given.

**1. Introduction.** In earlier work (see [3, Theorem 4.1.4, p. 110]), we were able to provide necessary and sufficient conditions for the Euler-Rabinowitsch polynomial  $F_{\Delta,1}(x)$  (defined in Section 2) to generate primes for all nonnegative values of  $x$  less than a Rabinowitsch bound when the discriminant  $\Delta$  is negative. This provided a generalization of the well-known Rabinowitsch criterion for complex quadratic fields, and a class number two criterion of Sasaki. Other class number two criteria in the literature for  $\Delta < 0$  involve the more general  $q$ -th Euler-Rabinowitsch polynomials  $F_{\Delta,q}(x)$  (see Section 2), for input values of  $x$  up to a Minkowski bound. The seminal works are those of Frobenius and Hendy, which were later generalized by others (see [3, Chapter 4, pp. 105–145] for a general overview). In this paper, we conclude this work by providing a complete description of all such  $F_{\Delta,q}(x)$  (under the assumption of the GRH). We also provide necessary and sufficient conditions for the prime-producing capacity of these polynomials in terms of the exponent  $e_{\Delta}$ , of the class group  $C_{\Delta}$ , satisfying  $e_{\Delta} \leq 2$ . We can establish the case where  $\Delta \equiv 0 \pmod{4}$ , and pose a conjecture in the remaining case. Examples are also provided to show that the bounds involved in both our criterion and conjecture are the best possible (in the sense that they cannot be raised or lowered by even a fraction of an integer without invalidating the results). We conclude with substantial evidence for our remaining conjecture.

**2. Notation and preliminaries.** Suppose that  $D < 0$  is a square-free integer. If we set

$$\Delta = 4D/\sigma^2,$$

where  $\sigma = 2$  if  $D \equiv 1 \pmod{4}$  and  $\sigma = 1$  otherwise, then  $\Delta$  is called a (fundamental or field) *discriminant* with (fundamental or field) *radicand*  $D$ . If we denote a  $\mathbb{Z}$ -module

---

Received by the editors March 19, 1996.

AMS subject classification: Primary: 11R11; secondary: 11R09, 11R29.

©Canadian Mathematical Society 1997.

over  $K$  by

$$[\alpha, \beta] = \alpha\mathbb{Z} + \beta\mathbb{Z},$$

with  $\alpha, \beta \in K = \mathbb{Q}(\sqrt{D})$  for a radicand  $D$ , then the *maximal order* or *ring of integers* of  $K$  is given by

$$\mathcal{O}_\Delta = [1, \omega_\Delta],$$

where

$$\omega_\Delta = (\sigma - 1 + \sqrt{D})/\sigma.$$

If  $\alpha \in K$ , we use  $\alpha'$  to denote the *algebraic conjugate* of  $\alpha$ , and  $N(\alpha) = \alpha\alpha'$  to denote the *norm* of  $\alpha$ . An *ideal* of  $\mathcal{O}_\Delta$  (called an  $\mathcal{O}_\Delta$  ideal) can be written as

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

where  $a, b, c \in \mathbb{Z}$ , with  $a, c > 0$ ,  $c|a$ ,  $c|b$ , and  $ac|N(b + c\omega_\Delta)$ . Furthermore, if  $a, b, c \in \mathbb{Z}$  with  $c|b$ ,  $c|a$ , and  $ac|N(b + c\omega_\Delta)$ , then  $I = [a, b + c\omega_\Delta]$  is an ideal of  $\mathcal{O}_\Delta$ . The ideal  $I$  is called *primitive* if it has no rational integer factors other than  $\pm 1$ , and then  $c = 1$ . The *norm of an ideal*  $I = [a, b + \omega_\Delta]$  is defined as  $N(I) = a$ , and the *conjugate ideal* is denoted by  $I' = [a, b + \omega'_\Delta]$ . If  $I = I'$ , then  $I$  is called an *ambiguous ideal* of  $\mathcal{O}_\Delta$ , and if  $I \sim I'$  (where  $\sim$  denotes *equivalence* in the *class group*  $C_\Delta$  of  $\mathcal{O}_\Delta$ ), then  $\{I\}$  is said to be an *ambiguous class* of  $\mathcal{O}_\Delta$  (where  $\{I\}$  denotes the class of  $I$  in  $C_\Delta$ ). The *class number*, or order of  $C_\Delta$ , is denoted by  $h_\Delta$ . The *exponent* of  $C_\Delta$  is the least positive integer  $e_\Delta$  such that  $I^{e_\Delta} \sim 1$  for any  $\{I\} \in C_\Delta$ . In what follows, the symbol  $(*/*)$  will denote the *Kronecker symbol*. Note that throughout the paper we will use the phrase a *split prime* to mean an  $\mathcal{O}_\Delta$ -prime  $P$  above  $p$  such that  $(\Delta/p) = 1$ , in other words,  $(p) = p\mathcal{O}_\Delta = PP'$ , with  $P \neq P'$ . Finally, in terms of notation,  $M_\Delta = \sqrt{-\Delta/3}$  will denote the *Minkowski bound*.

In the next section we will have need of the following to present the aforementioned criterion.

DEFINITION 2.1. Let  $\Delta < 0$  be a discriminant, and let  $q \geq 1$  be a square-free divisor of it. Set  $\alpha = 1$  if  $4q$  divides  $\Delta$  and  $\alpha = 2$  otherwise. We define the *q-th Euler-Rabinowitsch polynomial* to be

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

DEFINITION 2.2. If  $n = \prod_{i=1}^t p_i^{a_i}$  is the canonical prime factorization of  $n \in \mathbb{Z}$ , then set

$$\Omega(n) = \sum_{i=1}^t a_i.$$

With Definition 2.1 in mind, we set:

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

This sets the stage for the statement of a result which follows from earlier work (see [3, Theorem 4.1.5, p. 114]). This is a generalization of the Rabinowitsch criterion for complex quadratic fields (see [3, Theorem 4.1.2, p. 108]).

**THEOREM 2.1.** *Let  $\Delta < -4$  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. If  $q = \prod_{i=1}^N q_i$ , then the following are equivalent:*

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

**3. Prime producing quadratics.** We begin by examining the consequences of the consecutive prime producing capacity of the  $F_{\Delta, q}(x)$ . The following generalizes results of Hendy [2].

**THEOREM 3.1.** *Let  $\Delta < -3$  be a discriminant divisible by exactly  $N + 1$  ( $N \geq 0$ ) distinct primes with  $q_{N+1}$  being the largest. If  $q = \prod_{i=1}^N q_i$  is the product of the remaining prime divisors of  $\Delta$  (with  $q = 1$  if  $N = 0$ ), then (1)  $\Rightarrow$  (2) in what follows:*

- (1)  $F_{\Delta, q}(x)$  is prime for all nonnegative  $x \in \mathbb{Z}$  with  $x < (M_\Delta - \alpha + 1)/\alpha$ .
- (2)  $e_\Delta \leq 2$  and  $M_\Delta < q_{N+1}$ .

**PROOF.** The result will follow from two claims, which we now prove.

**CLAIM 1.** *If  $p < M_\Delta$  is any split prime, then there exists a nonnegative  $x < (M_\Delta - \alpha + 1)/2$  such that  $p$  divides  $F_{\Delta, q}(x)$ .*

If  $p = 2$ , then  $x = 0$  suffices, so we may assume that  $p > 2$ . Since  $(\Delta/p) = 1$ , then there is a  $y \in \mathbb{Z}$  such that  $\Delta \equiv y^2 \pmod{p}$ . Also, since  $p$  does not divide  $\Delta$ , then we may set  $z \equiv yq^{-1} \pmod{p}$ , so  $\Delta \equiv q^2 z^2 \pmod{p}$ . Since we may assume that  $z = 2x + \alpha - 1$ , then  $q^2(2x + \alpha - 1)^2 \equiv \Delta \pmod{p}$ , and we may assume without loss of generality that  $0 \leq 2x + \alpha - 1 < p$  (since we may take the least nonnegative residue modulo  $p$ , and when  $\alpha = 2$ , we may assume that the residue is odd since  $p$  is odd). Hence,  $0 \leq x < (M_\Delta - \alpha + 1)/2$ . This secures Claim 1, since  $4qF_{\Delta, q}(x) = q^2(2x + \alpha - 1)^2 - \Delta$ .

By hypothesis (1) and Claim 1,  $F_{\Delta, q}(x) = p$  for any split prime  $p < M_\Delta$ .

**CLAIM 2.**  *$P \sim Q$  where  $P$  lies over  $p$  and  $Q$  lies over  $q$ .*

To see this, we merely form the ideal  $PQ = [pq, (b + \sqrt{\Delta})/2]$  where  $b = (2x + \alpha - 1)q$ . Therefore, by Claim 1,  $N((b + \sqrt{\Delta})/2) = qF_{\Delta, q}(x) = pq$ . Hence,  $PQ = ((b + \sqrt{\Delta})/2)$ , and so  $P \sim Q$ . This secures Claim 2.

By Claim 2,  $P^2 \sim 1$ , since  $Q$  is ambiguous, so  $e_\Delta \leq 2$  by [3, Theorem 1.3.1, p. 15]. Now we show that  $M_\Delta < q_{N+1}$ . Set  $x = (q_{N+1} - \alpha + 1)/\alpha$  which is in  $\mathbb{Z}$ . Therefore,  $F_{\Delta, q}(x) = q_{N+1}(qq_{N+1} + \alpha/\sigma)/\alpha^2$ , which is composite since the hypothesis rules out  $\Delta = -3$ . Therefore,  $x > \lfloor (M_\Delta - \alpha + 1)/\alpha \rfloor$ , by hypothesis (1). If  $M_\Delta > q_{N+1}$ , then

$$\begin{aligned} x &= (q_{N+1} - \alpha + 1)/\alpha > \lfloor (M_\Delta - \alpha + 1)/\alpha \rfloor > (M_\Delta - \alpha + 1)/\alpha - 1 \\ &> (q_{N+1} - \alpha + 1)/\alpha - 1 = x - 1, \end{aligned}$$

(where  $\lfloor * \rfloor$  denotes the greatest integer function). However, there cannot exist an integer strictly between  $x$  and  $x - 1$ . ■

The converse of Theorem 3.1 fails for  $\Delta \equiv 1 \pmod{4}$ . For example, if  $\Delta = -195$ , then  $\lfloor M_\Delta \rfloor = 8$ , and  $q_{N+1} = 13$ . However,  $F_{\Delta,q}(3) = 11 \cdot 17$ , where  $q = 15$  and  $3 < (M_\Delta - \alpha + 1)/\alpha$ . Nevertheless, the converse of Theorem 3.1 does hold for  $\Delta \equiv 0 \pmod{4}$ .

**THEOREM 3.2.** *If  $\Delta \equiv 0 \pmod{4}$ ,  $\Delta < -4$ , and  $N, q, q_{N+1}$  are as in Theorem 3.1, then the following are equivalent:*

- (1)  $F_{\Delta,q}(x)$  is prime for all integers  $x$  with  $0 \leq x < (M_\Delta - \alpha + 1)/\alpha$ .
- (2)  $e_\Delta \leq 2$  and  $M_\Delta < q_{N+1}$ .

**PROOF.** In view of Theorem 3.1, we need only prove that (2)  $\Rightarrow$  (1). If  $e_\Delta \leq 2$ , then by Theorem 2.1, we have that  $F_{\Delta,q}(x)$  is prime whenever  $0 \leq x \leq \lfloor \Delta \rfloor / (4q) - 1 = q_{N+1} / \alpha - 1$ . If  $\lfloor (M_\Delta - \alpha + 1) / \alpha \rfloor > (q_{N+1} - \alpha + 1) / \alpha - 1$ , then by hypothesis,

$$\begin{aligned} (q_{N+1} - \alpha + 1) / \alpha &> (M_\Delta - \alpha + 1) / \alpha > \lfloor (M_\Delta - \alpha + 1) / \alpha \rfloor \\ &> (q_{N+1} - \alpha + 1) / \alpha - 1, \end{aligned}$$

a contradiction. Hence,  $\lfloor (M_\Delta - \alpha + 1) / \alpha \rfloor \leq (q_{N+1} - \alpha + 1) / \alpha - 1 \leq q_{N+1} / \alpha - 1$ , and so (1) holds. ■

**REMARK 3.1.** We actually know all of the values of  $\Delta < 0$  with  $e_\Delta = 2$ , under the assumption of the GRH, from the work of Weinberger [4]. A complete list, with the prime-producing capacity of  $F_{\Delta,q}(x)$ , may be found in [3, Table 4.1.2, p. 113]. There are fifty-six values in that table, and  $N \leq 4$  for each of them. With the nine well-known values for which  $h_\Delta = e_\Delta = 1$ , namely the case where  $N = 0$  (from Baker, Heegener, Stark), we have a total of sixty-five values of fundamental discriminants  $\Delta < 0$  with  $e_\Delta \leq 2$ .<sup>1</sup> In other words, under the assumption of the GRH, we have a complete list of all fundamental discriminants  $\Delta < 0$  with  $e_\Delta \leq 2$ . We also know, unconditionally, all of the values of  $\Delta < 0$  for which  $h_\Delta = 4$  from the work of Steve Arno (see [3, Chapter 4, pp. 105–128] for background and an overview of the history of the solution of  $h_\Delta \leq 4$  for  $\Delta < 0$ ). In other words, we (unconditionally) know all fundamental discriminants  $\Delta < 0$  with  $N \leq 2$ , having  $e_\Delta \leq 2$ . These values are as follows:

for  $h_\Delta = 1$  (namely  $N = 0$ ), and  $|\Delta| \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$ ,

for  $h_\Delta = 2$  (namely  $N = 1$ ), and  $|D|$  in the following set:

$$\{5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187, 235, 267, 403, 427\},$$

and,

for  $h_\Delta = 4$  (namely  $N = 2$ ), and  $|D|$  in the following set:

$$\begin{aligned} \{21, 30, 33, 42, 57, 70, 78, 85, 93, 102, 130, 133, 177, 190, 195, 253, 435, \\ 483, 555, 595, 627, 715, 795, 1435\}. \end{aligned}$$

---

<sup>1</sup> The interested reader may compare these values with the sixty-five values which are listed by Gauss, in *Disquisitiones Arithmeticae* [1, Section 303], and called *numeri idonei* or *convenient numbers* by Euler, see [3, p. 112–117, and pp. 347–354].

Therefore, the only remaining values with  $e_\Delta \leq 2$  from the original sixty-five, for which we need the GRH, are as follows:

for  $h_\Delta = 8$  (namely  $N = 3$ ), and  $|D|$  in the following set:

$$\{105, 165, 210, 273, 330, 345, 357, 385, 462, 1155, 1995, 3003, 3315\},$$

and

for  $h_\Delta = 16$  (namely  $N = 4$ ), and  $\Delta = -1365$ .

Therefore, we may conclude that, if  $N \leq 2$ , then we know unconditionally the values for which Theorem 3.2 holds. They are as follows:

for  $\Delta \equiv 0 \pmod{8}$ ,  $|D| \in \{6, 10, 22, 58, 78, 102, 190\}$ , and

for  $\Delta \equiv 4 \pmod{8}$ ,  $|D| \in \{5, 13, 21, 33, 37, 57, 85, 93, 133, 177\}$ .

In fact, the only other (known) value for which Theorem 3.2 holds is  $\Delta = -345$ , where  $h_\Delta = 8$ . Therefore, if the class number 8 problem were ever solved for negative fundamental discriminants, we would have an unconditional complete list of values for which Theorem 3.2 holds (and given the current work of Arno and others, this may not be far off indeed). Also, algebraically, the criterion in Theorem 3.2 is as *tight* as possible. To illustrate this, we look at  $D = -130$  for which we have  $[M_\Delta] = 13 = q_{N+1}$ , and it is precisely for this value that (1) of Theorem 3.2 fails, since  $F_{\Delta,q}(x) = 10x^2 + 13$  and  $F_{\Delta,q}(13) = 13 \cdot 131$ . Thus, the bounds in Theorem 3.2 are the most precise possible, in the sense that they are within a fraction of an integer from failing, as with  $D = -130$ . In fact,  $F_{\Delta,q}(q_{N+1})$  is composite when  $\alpha = 1$  (see the proof of Theorem 3.1).

Now we turn to a criterion for  $\Delta \equiv 1 \pmod{4}$ .

**CONJECTURE 3.1.** *If  $\Delta < 0$  is a discriminant with  $N, q$  and  $q_{N+1}$  as in the hypothesis of Theorem 3.1, then the following are equivalent:*

1.  $F_{\Delta,q}(x)$  is prime whenever  $0 \leq x < (M_\Delta - 1)/2$ .
2.  $e_\Delta \leq 2$  and  $M_\Delta < (q_{N+1} + 3)/2$ .

**REMARK 3.2.** Conjecture 3.1 is valid if we assume the GRH (by Remark 3.1). Furthermore, the bounds in Conjecture 3.1 are the most precise possible. To illustrate this allegation, we let  $\Delta = -483$ , where  $q = 21$ ,  $q_{N+1} = 23$ , and

$$F_{\Delta,q}(x) = 21x^2 + 21x + 11.$$

Here,  $13 = (q_{N+1} + 3)/2 > M_\Delta > (q_{N+1} + 2)/2 = 12.5$ , and

$$F_{\Delta,q}(6) = F_{\Delta,q}((q_{N+1} + 1)/4) = 19 \cdot 47.$$

Yet,  $F_{\Delta,q}(x)$  is prime for all nonnegative integers  $x \leq 5 < (M_\Delta - 1)/2 < 6$ . Hence  $\Delta = -483$  is a counterexample to the possibility of lowering the bound in part 2 of Conjecture 3.1 to  $(q_{N+1} + 2)/2$ .

Now consider  $\Delta = -195$  where  $q = 15$ ,  $q_{N+1} = 13$  and

$$F_{\Delta,q}(x) = 15x^2 + 15x + 7.$$

Here,

$$F_{\Delta,q}(3) = F_{\Delta,q}((q_{N+1} - 1)/4) = 11 \cdot 17,$$

where  $3 < (M_{\Delta} - 1)/2$ . Since  $(q_{N+1} + 4)/2 = 8.5 > M_{\Delta}$ , then  $\Delta = -195$  is a counterexample to the possibility of raising the bound in part 2 of Conjecture 3.1 to  $(q_{N+1} + 4)/2$ . Hence, the bound in part 2 cannot be moved even half an integer in either direction. Not often are mathematical bounds this demonstrably tight.

REMARK 3.3. We just miss being able to prove that (1)  $\Rightarrow$  (2) of Conjecture 3.1 holds. We know that  $F_{\Delta,q}(n - 1) = n(nq - q + 1)$ , where  $n = (q + q_{N+1})/4$ . Therefore, if (1) of Conjecture 3.1 holds, then  $(q_{N+1} + q)/4 - 1 \geq (M_{\Delta} - 1)/2$ . In other words,  $(q_{N+1} + q)/2 - 1 \geq M_{\Delta}$ . However, we cannot get closer than this in general. Observe that if  $h_{\Delta} = 2$ , then  $x = n - 1$  is the first value for which  $F_{\Delta,q}(x)$  is composite for the  $\Delta$  listed in Remark 3.1. We note that, in fact, if  $M_{\Delta} < (q_{N+1} + 3)/2$ , then  $h_{\Delta} \leq 4$  from the aforementioned listed values. However, we need the GRH to make this inference. We also observe from the list that if  $M_{\Delta} < (q_{N+1} + 3)/2$  and  $h_{\Delta} \leq 4$ , then  $q = m^2 + r$  where  $|r| \in \{1, 2, 4\}$ . If we could (unconditionally) verify that (1) of Conjecture 3.1 must imply this condition on  $q$ , then we would have a constructive proof that (1)  $\Rightarrow$  (2). For example, if  $q + 1$  is a square, then

$$F_{\Delta,q}((q_{N+1} - 1)/4) = [(q_{N+1} + 1)/4]^2(q + 1) - [(q_{N+1} - 1)/4]^2$$

is a difference of squares, so  $M_{\Delta} \leq (q_{N+1} + 1)/2$ . The values in Remark 3.1 for which  $q + 1$  is a square,  $\Delta \equiv 1 \pmod{4}$ ,  $h_{\Delta} \leq 4$ , and  $M_{\Delta} \leq (q_{N+1} + 1)/2$ , are those  $|\Delta|$  in the following set:

$$\{15, 51, 123, 267, 435, 555, 795\}.$$

In fact, we observe that

$$\begin{aligned} F_{\Delta,q}(n - 1) &= F_{\Delta,q}((q_{N+1} + q)/4 - 1) \\ &= \left[ \frac{(q_{N+1} + q - 4)(q + 1) + 8}{8} \right]^2 - \left[ \frac{(q - 1)(q_{N+1} + q - 4) + 8}{8} \right]^2. \end{aligned}$$

Furthermore, each of the relevant values in Remark 3.1 first makes  $F_{\Delta,q}(x)$  composite for an  $x$  value such that  $F_{\Delta,q}(x)$  is a difference of squares in a unique way depending upon the aforementioned special shape for  $q$ . That this phenomenon even occurs is of interest in its own right, so we tabulate the values below. The column labeled  $x_0$  represents the smallest nonnegative value of  $x$  such that  $F_{\Delta,q}(x_0)$  is composite. The column labeled  $F_{\Delta,q}(x_0)$  lists the value as a difference of squares, and the column labeled  $q$  lists it in its special form  $m^2 + r$  as above. A column for  $F_{\Delta,q}(x)$  is also given. To prove that  $q$  must be of one of these special forms, say  $q = m^2 - 4$ , we must verify that  $q = x_0x_1$  where  $x_0 - x_1 = 4$ , since  $\left(\frac{x_0 + x_1}{2}\right)^2 - \left(\frac{x_0 - x_1}{2}\right)^2 = q$ .

$ \Delta $	$x_0$	$F_{\Delta,q}(x_0)$	$q$	$q_{N+1}$	$F_{\Delta,q}(x)$
15	$1 = (q_{N+1} - 1)/4$	$3^2 - 1^2$	$3 = 2^2 - 1$	5	$3x^2 + 3x + 2$
35	$2 = (q_{N+1} + 1)/4$	$7^2 - 4^2$	$5 = 3^2 - 4$	7	$5x^2 + 5x + 3$
51	$4 = (q_{N+1} - 1)/4$	$9^2 - 4^2$	$3 = 2^2 - 1$	17	$3x^2 + 3x + 5$
91	$4 = (q_{N+1} + 3)/4$	$17^2 - 12^2$	$7 = 3^2 - 2$	13	$7x^2 + 7x + 5$
115	$6 = (q_{N+1} + 1)/4$	$19^2 - 12^2$	$5 = 2^2 + 1$	23	$5x^2 + 5x + 7$
123	$10 = (q_{N+1} - 1)/4$	$21^2 - 10^2$	$3 = 2^2 - 1$	41	$3x^2 + 3x + 11$
187	$6 = (q_{N+1} + 7)/4$	$37^2 - 30^2$	$11 = 3^2 + 2$	17	$11x^2 + 11x + 7$
235	$12 = (q_{N+1} + 1)/4$	$37^2 - 24^2$	$5 = 2^2 + 1$	47	$5x^2 + 5x + 13$
267	$22 = (q_{N+1} - 1)/4$	$45^2 - 22^2$	$3 = 2^2 - 1$	89	$3x^2 + 3x + 23$
403	$10 = (q_{N+1} + 9)/4$	$71^2 - 60^2$	$13 = 3^2 + 4$	31	$13x^2 + 13x + 11$
427	$16 = (q_{N+1} + 3)/4$	$65^2 - 48^2$	$7 = 3^2 - 2$	61	$7x^2 + 7x + 17$
435	$7 = (q_{N+1} - 1)/4$	$30^2 - 7^2$	$15 = 4^2 - 1$	29	$15x^2 + 15x + 11$
483	$6 = (q_{N+1} + 1)/4$	$33^2 - 14^2$	$21 = 5^2 - 4$	23	$21x^2 + 21x + 11$
555	$9 = (q_{N+1} - 1)/4$	$38^2 - 9^2$	$15 = 4^2 - 1$	37	$15x^2 + 15x + 13$
795	$13 = (q_{N+1} - 1)/4$	$54^2 - 13^2$	$15 = 4^2 - 1$	53	$15x^2 + 15x + 17$

What we have achieved is the first necessary *and* sufficient conditions (namely those in Theorem 3.2 and Conjecture 3.1), since the earlier combined efforts of Hendy and others cited above are insufficient to give the criterion.

ACKNOWLEDGMENTS. The first author welcomes the opportunity to recognize the support of this research by NSERC Canada grant # A8484. Also, thanks go to the referee for valuable comments.

#### REFERENCES

1. C. F. Gauss, *Disquisitiones Arithmeticae*, Springer Verlag, English Edition, 1986.
2. M. D. Hendy, *Prime quadratics associated with complex quadratic fields of class number two*, Proc. Amer. Math. Soc. **43**(1974), 253–260.
3. R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, New York, London, Tokyo, 1995.
4. P. 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

WWW home page: <http://www.math.ucalgary.ca/~ramollin/>

Mathematics Department  
East Texas State University  
Commerce, Texas 75428  
U.S.A

Faculty of Medicine  
Department of Surgery  
University of Calgary  
Calgary, Alberta  
T2N 1N4