Functiones et Approximatio
45.2 (2011), 271–288

EULER-RABINOWITSCH POLYNOMIALS AND CLASS NUMBER PROBLEMS REVISITED

Richard A. Mollin, Anitha Srinivasan

Abstract: We prove a conjecture posed in [11] and continue the process of determining Euler-Rabinowitsch polynomials that produce consecutive primes in a given range of inputs, and the relationship with class numbers of the underlying quadratic field.

Keywords: class numbers; real quadratic fields, prime-producing polynomials, continued fractions.

1. Introduction

In [11], we showed how work of Byeon and Stark in [2]- [3] actually followed from work of the first author some years before the publication of the latter, and corrected, extended and clarified the results of the latter as well. We left a conjecture in [11] that we prove herein and we look at more general Euler-Rabinowitsch polynomials than those considered in [11]. This allows us to get both class number one and two results that extend results in the literature.

2. Preliminaries

We will be using continued fraction expansions herein for which we remind the reader of the following, the details and background of which may be found in [10], or for a more advanced approach in [6].

We denote the infinite simple continued fraction expansion of a given $\alpha \in \mathbb{R}$ by

$$\alpha = \langle q_0; q_1, q_2, \ldots \rangle \qquad \text{where } \; q_j \in \mathbb{N} \text{ for } j \in \mathbb{N} \; \text{ and } \; q_0 = \lfloor \alpha \rfloor,$$

where $\lfloor \alpha \rfloor$ is the floor of α, namely the greatest integer less than or equal to α. It turns out that infinite simple continued fraction expansions are irrational, namely $\alpha \in \mathbb{R} - \mathbb{Q}$. There is a specific type of irrational that we need as follows.

The first author gratefully acknowledges the support of NSERC Canada grant # A8484. Also, we thank the referee for a detailed analysis of the paper that led to a more precise version.

2010 Mathematics Subject Classification: primary: 11R11; secondary: 11R29, 11C08, 11D09, 11Y65

Definition 2.1. *A real number α is called a quadratic irrational if it is an irrational number which is a root of*

$$f(x) = ax^2 + bx + c \tag{2.1}$$

where $a, b, c \in \mathbb{Z}$ and $a \neq 0$.

Remark 2.1. By the quadratic formula, the roots of (2.1) are given by

$$\alpha = \frac{-b + \sqrt{b^2 - 4ac}}{2a},$$

and

$$\alpha' = \frac{-b - \sqrt{b^2 - 4ac}}{2a},$$

so if we take $\Delta = b^2 - 4ac$, $P = -b$, and $Q = 2a$, then

$$\alpha = \frac{P + \sqrt{\Delta}}{Q} \qquad \text{and} \qquad \alpha' = \frac{P - \sqrt{\Delta}}{Q}.$$

Also, $\Delta > 0$ since $\alpha \in \mathbb{R} - \mathbb{Q}$, and $P^2 - \Delta = 4ac$ is divisible by Q. These elementary facts are formalized in what follows.

Theorem 2.1. *A real number α is a quadratic irrational if and only if there exist $P, Q, \Delta \in \mathbb{Z}$ such that $Q \neq 0$, $\Delta \in \mathbb{N}$ is not a perfect square, and*

$$\alpha = \frac{P + \sqrt{\Delta}}{Q}, \qquad (P, Q \in \mathbb{Z}),$$

with $Q | (P^2 - \Delta)$. Also,

$$\alpha' = (P - \sqrt{\Delta})/Q$$

is called the algebraic conjugate of α. Here both α and α' are the roots of

$$f(x) = x^2 - Tr(\alpha)x + N(\alpha),$$

where $Tr(\alpha) = \alpha + \alpha'$ is the trace of α and $N(\alpha) = \alpha \cdot \alpha'$ is the norm of α.

Proof. See [10, Theorem 5.9, p. 222]. ■

We will primarily be concerned with the following type of quadratic irrational.

Definition 2.2. *A quadratic irrational α is called reduced if both $\alpha > 1$ and $-1 < \alpha' < 0$.*

Now we link back to continued fractions, but first need the following notion.

Definition 2.3. *The infinite simple continued fraction of α is called periodic (sometimes called eventually periodic) if there exists an integer $k \geqslant 0$ and $l \in N$ such that $q_n = q_{n+l}$ for all integers $n \geqslant k$. We use the notation*

$$\alpha = \langle q_0; q_1, \cdots q_{k-1}, \overline{q_k, q_{k+1}, \cdots q_{l+k-1}} \rangle, \tag{2.2}$$

as a convenient abbreviation. The smallest such natural number $\ell = \ell(\alpha)$ is called the period length of α, and $q_0, q_1, ..., q_{k-1}$ is called the pre-period of α. If k is the least non-negative integer such that $q_n = q_{n+\ell}$ for all $n \geqslant k$, then $q_k, q_{k+1}, \dots, q_{k+\ell-1}$ is called the fundamental period of α with period length denoted by $\ell(\alpha)$. When $k = 0$ is the least such value, then α is said to be purely periodic, namely $\alpha = \langle \overline{q_0; q_1, \dots, q_{\ell-1}} \rangle$.

Theorem 2.2. *Let $\alpha = (P_0 + \sqrt{D})/Q_0$ be a quadratic irrational, where $D > 0$ is not a perfect square, Q_0 is a nonzero integer, $P_0 \in \mathbb{Z}$, and $Q_0 \big| (D - P_0^2)$. Recursively define for any $j \geqslant 0$,*

$$\alpha_j = (P_j + \sqrt{D})/Q_j,$$

$$P_{j+1} = q_j Q_j - P_j, \tag{2.3}$$

$$q_j = \left\lfloor \frac{P_j + \sqrt{D}}{Q_j} \right\rfloor, \tag{2.4}$$

and

$$D = P_{j+1}^2 + Q_j Q_{j+1}. \tag{2.5}$$

Then

$$\alpha = \langle q_0; q_1, q_2, \dots \rangle.$$

Moreover, α is periodic and when it is reduced it is purely periodic.

Proof. See [10, Theorem 510, p. 223]. ■

We will need the following facts – see [6, §2.1, pp. 41–63] for complete details. If $\ell(\alpha) = \ell$ is even, then

$$P_{\ell/2} = P_{\ell/2+1}, \tag{2.6}$$

$$Q_{\ell/2+1} = Q_{\ell/2-1}, \tag{2.7}$$

and if ℓ is odd, then

$$P_{(\ell+3)/2} = P_{(\ell-1)/2}, \tag{2.8}$$

$$Q_{(\ell+1)/2} = Q_{(\ell-1)/2}. \tag{2.9}$$

Moreover, for any reduced quadratic irrational α with $0 \leqslant j < \ell$, we have

$$0 < Q_j < 2\sqrt{D}, \tag{2.10}$$

and

$$0 < P_j < \sqrt{D}. \tag{2.11}$$

Now we need to define arbitrary real quadratic orders in which we will work. If $D_0 > 1$ is a squarefree integer, then a fundamental discriminant Δ_0 with fundamental radicand D_0 is given by

$$\Delta_0 = \begin{cases} D_0 & \text{if } D_0 \equiv 1 \pmod 4, \\ 4D_0 & \text{if } D_0 \equiv 2, 3 \pmod 4. \end{cases} \tag{2.12}$$

Now suppose that $\Delta = f_\Delta^2 \Delta_0 = 4D/\sigma^2$ for a given positive integer f_Δ, called the conductor for Δ with associated radicand D with σ defined by

$$\sigma = \begin{cases} 2 & \text{if } \Delta_0 \equiv 1 \pmod 4 \text{ and } f_\Delta \text{ is odd}, \\ 1 & \text{otherwise}. \end{cases} \tag{2.13}$$

Set

$$\omega_\Delta = \begin{cases} (1+\sqrt{D})/2 & \text{if } \Delta = D \equiv 1 \pmod 4, \\ \sqrt{D} & \text{if } \Delta \equiv 0 \pmod 4, \end{cases} \tag{2.14}$$

called the principal surd associated with Δ and

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

is called a real quadratic order in $\mathbb{Q}(\sqrt{D_0})$ having conductor f_Δ and discriminant Δ with associated radicand D. (The reader unfamiliar with the notions of a general discriminant and radicand may consult [6, Section 1.5, pp. 23–24], for instance.)

We need information—see [6, pp. 54–59] for Equations (2.15)–(2.18) below—on the continued fraction expansion of

$$\omega_\Delta = \langle q_0; \overline{q_1, q_2, \ldots, q_{\ell-1}, 2q_0 - \sigma + 1}\,\rangle,$$

where $\ell = \ell(\omega_\Delta)$, $q_0 = \lfloor \omega_\Delta \rfloor$, and $q_1 q_2 \ldots q_{\ell-1}$ is a palindrome, namely for $1 \leqslant j \leqslant \ell$,

$$q_j = q_{\ell-j}. \tag{2.15}$$

The jth convergent for ω_Δ for any non-negative integer j is given by

$$\frac{A_j}{B_j} = \langle q_0; q_1, q_2, \ldots, q_j \rangle,$$

where

$$A_j = q_j A_{j-1} + A_{j-2},$$
$$B_j = q_j B_{j-1} + B_{j-2},$$

with $A_{-2} = 0$, $A_{-1} = 1$, $B_{-2} = 1$, and $B_{-1} = 0$. Also,

$$A_{\ell-1}^2 - B_{\ell-1}^2 D = (-1)^\ell. \tag{2.16}$$

The complete quotients for ω_Δ are given by $(P_j + \sqrt{D})/Q_j$ where $P_0 = \sigma - 1$, $Q_0 = \sigma$, and for $j \in \mathbb{N}$ as defined in Theorem 2.2, from which we also get

$$\sigma \big| Q_j \qquad \text{for all } j \geqslant 0, \tag{2.17}$$

and

$$Q_j = \sigma \text{ for any } 0 \leqslant j \leqslant \ell \qquad \text{if and only if} \qquad j \in \{0, \ell\}. \tag{2.18}$$

We now establish the link between quadratic irrationals and ideals. We begin with the following.

Theorem 2.3. *Let I be a nonzero $\mathbb{Z}$-submodule of $\mathcal{O}_\Delta$. Then I has a representation in the form*

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

where $a, c \in \mathbb{N}$ and $0 \leqslant b < a$. Furthermore, I is an $\mathcal{O}_\Delta$- ideal if and only if this representation satisfies $c\big|a$, $c\big|b$, and $ac\big|N(b + c\omega_\Delta)$. When $c = 1$, I is called primitive.

Proof. See [6, Theorem 1.2.1, p. 9] or [7, Theorem 3.5.1, p. 173]. ∎

Definition 2.4. *To each quadratic irrational $\alpha = (P + \sqrt{D})/Q$ there corresponds the primitive $\mathcal{O}_\Delta$-ideal*

$$I = \left[|Q|/\sigma, (P + \sqrt{D})/\sigma\right].$$

We denote this ideal by $[\alpha] = I$ and write $l(I)$ for $l(\alpha)$.

The next result sets the stage for our primary discussion.

Note that the notion of reduction for quadratic irrationals translates to ideals, namely we have the following.

Definition 2.5. *An $\mathcal{O}_\Delta$-ideal is said to be reduced if it is primitive and does not contain any non-zero element α such that both $|\alpha| < N(I)$ and $|\alpha'| < N(I)$.*

Theorem 2.4. *$I = [a, (b + \sqrt{\Delta})/2]$ is reduced if and only if there is a $\beta \in I$ such that $I = [N(I), \beta]$ with $\beta > N(I)$ and $-N(I) < \beta' < 0$.*

Proof. See [6, Lemma 1.4.1, p. 19] or [7, Theorem 5.5.1, p. 258]. ∎

Corollary 2.1. *If $\Delta > 0$ is a discriminant and $[a, b + \omega_\Delta]$ is a primitive ideal with $a < \sqrt{\Delta}/2$, then I is reduced.*

Proof. See [6, Corollary 1.4.3, p. 19]. ∎

Now, we let $\mathcal{C}_\Delta$ be the ideal-class group of $\mathcal{O}_\Delta$ and $h_\Delta = |\mathcal{C}_\Delta|$ the ideal class number. If I, J are $\mathcal{O}_\Delta$-ideals, then equivalence of classes in $\mathcal{C}_\Delta$ is denoted by $I \sim J$ and the class of I is denoted by $\mathbf{I}$. The following is crucial to the interplay between ideals and continued fractions, known as the infrastructure theorem for real quadratic fields or the continued fraction algorithm.

Theorem 2.5. *Let $\Delta = 4D/\sigma^2$ be a discriminant with associated radicand D, and let $I = I_1 = [Q/\sigma, (P + \sqrt{D})/\sigma]$ be a primitive $\mathcal{O}_\Delta$-ideal. Set $P_0 = P$, $Q_0 = Q$, and for $j \in \mathbb{N}$, let $I_j = [Q_{j-1}/\sigma, (P_{j-1} + \sqrt{D})/\sigma]$ as given in Theorem 2.2 in the continued fraction expansion of $\gamma = \gamma_0 = (P + \sqrt{D})/Q$. Then $I_1 \sim I_j$ for all $j \geqslant 1$. Moreover, there exists a least value $m \in \mathbb{N}$ such that I_{m+i} is reduced for all $i \geqslant 0$.*

Proof. See [6, Theorem 2.1.2, p. 44]. ■

Remark 2.2. The infrastructure given in Theorem 2.5 demonstrates that if we begin with any primitive $\mathcal{O}_\Delta$-ideal I, then after applying the continued fraction algorithm to $\alpha = \alpha_0$, we must ultimately reach a reduced ideal $I_m \sim I$ for some $m \geqslant 1$. Furthermore, once we have produced this ideal I_m, we enter into a periodic cycle of reduced ideals, and this periodic cycle contains all the reduced ideals equivalent to I.

If $I = [Q/\sigma, (P+\sqrt{D})/\sigma]$ is a reduced $\mathcal{O}_\Delta$-ideal, then the set

$$\{Q_1/\sigma, Q_2/\sigma, \dots, Q_\ell/\sigma\}$$

represents the norms of all the reduced ideals equivalent to I (via the continued fraction expansion of $\alpha = (P+\sqrt{D})/Q$).

Note that by Corollary 2.1, whenever there is an ideal of norm less than $\sqrt{\Delta}/2$, then there is a reduced ideal with norm less than $\sqrt{\Delta}/2$. Thus, Corollary 2.2 below applies to all such ideals and we will make extensive use of it in the balance of the paper.

Corollary 2.2. *A reduced ideal $I = [Q/\sigma, (P+\sqrt{D})/\sigma]$ of $\mathcal{O}_\Delta$ is principal if and only if $Q = Q_j$ for some positive integer $j \leqslant \ell(\omega_\Delta)$ in the continued fraction expansion of ω_Δ.*

Proof. See [5]. ■

We will utilize the following in the next section.

Theorem 2.6. *Suppose that $\Delta = 4D/\sigma^2$ is a discriminant. Then the following hold.*

1. *If Q_j/σ is a squarefree divisor of $2D$ for some $j \in \mathbb{N}$ with $j < \ell$, then $j = \ell/2$.*
2. *If ℓ is even, then $Q_{\ell/2}/\sigma \big| 2D$, where $Q_{\ell/2}/\sigma$ is not necessarily squarefree.*

Proof. See [6, Theorem 6.1.4, p. 193]. ■

We will need the following which determines the generators of the ideal class group $\mathcal{C}_\Delta$ of $\mathbb{Q}(\sqrt{\Delta})$ having discriminant Δ. Recall that a non-inert prime ideal $\mathcal{P}$ is one whose norm $N(\mathcal{P})$ satisfies the Legendre symbol inequality $(\Delta/N(\mathcal{P})) \neq -1$, while a split prime ideal is one with $(\Delta/N(\mathcal{P})) = 1$, and a ramified prime ideal is one with $N(\mathcal{P})\big|\Delta$.

Theorem 2.7. *If Δ is the discriminant of a real quadratic field, then every class of $\mathcal{C}_\Delta$ contains a primitive ideal I with $N(I) \leqslant \sqrt{\Delta}/2$. Furthermore, $\mathcal{C}_\Delta$ is generated by the non-inert prime $\mathcal{O}_\Delta$-ideals $\mathcal{P}$ with $N(\mathcal{P}) < \sqrt{\Delta}/2$.*

Proof. See [6, Theorem 1.3.1, p. 15]. ■

3. Euler-Rabinowitsch Polynomials

Definition 3.1. *Let $\Delta = 4D/\sigma^2$ be an arbitrary discriminant with associated radicand D and $q \in \mathbb{N}$ a square-free divisor of Δ. Let $\alpha_\Delta = 1$ if $4q \big| \Delta$ and $\alpha_\Delta = 2$ otherwise. Then*

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

is called the Euler-Rabinowitsch polynomial*, which was introduced by the first author in [6, Chapter 4] to discuss prime-producing quadratic polynomials. The special case of $F_{\Delta,1}(x)$ was rediscovered in [2] and called a* Rabinowitsch polynomial*. The following four lemmas, involving the Euler-Rabinowitsch polynomial, will be needed in the sequel. In all of the lemmas, we assume that Δ is a discriminant with associated conductor f_Δ and q is a positive square free divisor of Δ such that* $\gcd(q, f_\Delta) = 1$.

Lemma 3.1. *If p is prime then the following are equivalent.*

(a) *$F_{\Delta,q}(x) \equiv 0 \pmod{p}$ for some non-negative integer x.*
(b) *The Legendre symbol $(\Delta/p) \neq -1$ and p does not divide q.*

Proof. See [6, Lemma 4.1.2, p. 118]. ■

Lemma 3.2. *If B is any positive real number and $p < B$ is any non-inert prime in $\mathbb{Q}(\sqrt{D})$, with $p \nmid q$, then there exists an integer $x \geqslant 0$ with $x < (B - \alpha_\Delta + 1)/2$ such that $p \big| F_{\Delta,q}(x)$.*

Proof. See [6, Lemma 4.1.3, p. 118]. ■

Lemma 3.3. *If the radicand D associated with Δ satisfies $D \equiv 3 \pmod{4}$ and $D \neq 2p^2 + 1$ for any prime p, then the following are equivalent.*

(a) *$|F_{\Delta,2}(x)|$ is 1 or prime for all non-negative integers $x \leqslant \sqrt{D-1}/2$.*
(b) *The Legendre symbol $(D/p) = -1$ for all odd primes $p < \sqrt{D-2}/2$.*

Proof. See [6, Theorem 5.4.9, p. 183]. ■

In the next result, the ideal over q is unique since q is divisible only by ramified primes.

Lemma 3.4. *If $a > 0$ is an integer with $|F_{\Delta,q}(x)| = a$ for some non-negative integer x, then $\mathcal{Q} \sim \mathcal{A}$, where $\mathcal{A}$ is an $\mathcal{O}_\Delta$-ideal with norm a and $\mathcal{Q}$ is the unique $\mathcal{O}_\Delta$-ideal over q.*

Proof. See [6, Lemma 4.1.4, p. 118]. ■

Corollary 3.1. *If $q = 1$ in Lemma 3.4, then whenever $|F_{\Delta,q}(x)| = a$ for some non-negative integer x, then $\mathcal{A} \sim 1$.*

Proof. This is immediate from Lemma 3.4. ■

We begin by showing how all Rabinowitsch polynomials for $q = 2$ may be determined. The following generalize results obtained in [6, Theorems 4.2.5, p. 134], where an assumption was made that we show below is not necessary. Furthermore, the results below are more specific.

Theorem 3.1. *Suppose that $\Delta = 4(4m+3) = 4D$, for $D > 3$, where D is not prime. Then the following are equivalent.*

1. $|F_{\Delta,2}(x)| = |2x^2 + 2x - 2m - 1|$ *is prime for all integers* $x \in [0, (\sqrt{D}-1)/2]$.
2. $D = p^2 + 2p = (p+1)^2 - 1$ *where p and $p+2$ are primes,* $h_\Delta = 2$, *and* $\ell(\sqrt{D}) = 2$.
3. $D \in \{15, 35, 143\}$.

Proof. Assume that 1 holds. Clearly, D is not a square since $D \equiv 3 \pmod 4$. Moreover, we now show that D is square-free. If $D = r^2 D_0$ where $D_0 > 1$ is square-free, then it follows that

$$\left|F_{\Delta,2}\left(\frac{r-1}{2}\right)\right| = r^2 \left|\frac{1-D_0}{2}\right|,$$

so since $(r-1)/2 < (\sqrt{D}-1)/2$, then by hypothesis $r = 1$, so D has no non-trivial square factor.

Observe that by (2.16), $\ell = \ell(\sqrt{D})$ must be even since $D \equiv 3 \pmod 4$, so if ℓ were odd, then -1 would be a square modulo D which is impossible. Suppose that $D = ps$ where p is a prime such that $2 < p < s$, then

$$|F_{\Delta,2}((p-1)/2)| = p\left(\frac{s-p}{2}\right).$$

Therefore, since $0 < (p-1)/2 \leqslant (\sqrt{D}-1)/2$, then $s = p+2$, but the period length of $\sqrt{D}$ for $D = p^2 + 2p$ is well known to be $\ell(\sqrt{D}) = 2$—see [6, Theorem 3.2.1, p.78]. By tabulating the values for $p + \sqrt{D}$, corresponding to the reduced ideal $[1, p+\sqrt{D}]$, from Theorem 2.5, we get:

i	0	1	2
P_i	p	p	p
Q_i	1	$2p$	1
q_i	$2p$	1	$2p$

and tabulating for $(p+\sqrt{D})/2$, corresponding to the reduced ideal $[2, p+\sqrt{D}]$, we get:

i	0	1	2
P_i	p	p	p
Q_i	2	p	2
q_i	p	2	p

The first table corresponds to the principal cycle and the second to a non-principal cycle for the non-principal reduced ideal $\mathcal{Q} = [2, p + \sqrt{D}]$ above the ramified prime 2, hence of order 2 in $\mathcal{C}_\Delta$. If there is a non-inert prime $r < p = \lfloor \sqrt{D} \rfloor$ with $r \neq 2$ then, by Lemmas 3.2 and 3.4, $\mathcal{A} \sim \mathcal{Q} = [2, p + \sqrt{D}]$, the ideal over 2, and where $\mathcal{A}$ is an $\mathcal{O}_\Delta$-ideal of norm r. Hence, there are no more non-principal ideals, so we have shown that $h_\Delta = 2$ via Theorem 2.7. Now if $p+2$ is not prime, then via Remark 2.2, there is a divisor of $p+2$ that has to appear as a Q_j in one of the above two cycles, but the only Q_js are $1, 2, p, 2p$, so this is not possible and $p+2$ must be prime. We have shown that 1 implies 2.

Furthermore, by [4], the only values, unconditionally, are given in the list in 3 under the assumption in 2, so 2 implies 3. Also, 3 implies 1 is an easy check. ■

Theorem 3.2. *Suppose that $\Delta = 4(4m+3) = 4D$ where $4m+3$ is prime. Then the following are equivalent.*

(a) $|F_{\Delta,2}(x)| = |2x^2 + 2x - 2m - 1|$ *is 1 or prime for all* $x \in [0, (\sqrt{D} - 1)/2]$.

(b) *One of the following holds:*

(i) $D = \lfloor \sqrt{D} \rfloor^2 + 2, l(\sqrt{D}) = 2, h_\Delta = 1$, *and there are no split primes* $p < \sqrt{D}$. *Moreover, the only values, with one possible exception, for which this holds are*

$$D \in \{3, 11, 83, 227\}. \tag{3.1}$$

(ii) $D = (\lfloor \sqrt{D} \rfloor + 1)^2 - 2, l(\sqrt{D}) = 4, h_\Delta = 1$, *and* $p = 2\lfloor \sqrt{D} \rfloor - 1$ *is the only split prime less than* $\sqrt{\Delta}$. *Moreover, the only values, with one possible exception, for which this holds are*

$$D \in \{7, 23, 47, 167\}. \tag{3.2}$$

Proof. Assume that part (a) holds. We have that $\ell(\sqrt{D})$ must be even by the same reasoning as in the proof of Theorem 3.1. Since $Q_{\ell/2} | 2D$ by Theorem 2.6, then for any odd prime $r | Q_{\ell/2}$, $r | D$. However, D is prime so $D = r$, a contradiction since $Q_{\ell/2} < 2\sqrt{D}$ by (2.10) and Theorem 2.6. This forces $Q_{\ell/2} = 2$. We first show that $h_\Delta = 1$. Suppose that there is a split prime $q < \sqrt{D}$. Then by Lemma 3.2, there exists a non-negative integer $x < (\sqrt{D} - 1)/2$ such that $q \big| F_{\Delta,2}(x)$. By hypothesis (a), this forces $|F_{\Delta,2}(x)| = q$. Thus, by Lemma 3.4, $\mathcal{Q} \sim \mathcal{P}$ where $\mathcal{Q}$ is the $\mathcal{O}_\Delta$-prime over q and $\mathcal{P}$ is an $\mathcal{O}_\Delta$-prime over 2. However, since $Q_{\ell/2} = 2$, then by Corollaries 2.1–2.2, $\mathcal{P} \sim 1$. Hence, $h_\Delta = 1$, by Corollaries 2.1–2.2, Remark 2.2, and Theorem 2.7.

Now by (2.5),

$$D = P_1^2 + Q_1. \tag{3.3}$$

(Note that, in the following, we may invoke Lemma 3.3 since if $D = 2p^2 + 1$ for any prime p, then $2m + 1 = p^2$, so $|F_{\Delta,2}(0)| = p^2$, contradicting (a).)

Let p be a prime dividing Q_1. By Lemma 3.3, there cannot be any odd split primes less than $\sqrt{D}/2$, so p must be larger than $\sqrt{D}/2$, given that any prime dividing Q_j for any j must be non-inert by (2.5). However, by Lemma 3.2, if $p > 2$, then $p|F_{\Delta,2}(x)$ for some $x < (\sqrt{D} - 1)/2$. Thus, by hypothesis,

$$|F_{\Delta,2}(x)| = \frac{D - (2x+1)^2}{2} = Q_1 = p,$$

so,

$$D = (2x+1)^2 + 2p. \tag{3.4}$$

However

$$D = P_1^2 + Q_1 = P_1^2 + p, \tag{3.5}$$

by (2.5). Equating (3.4) and (3.5), we get,

$$p = P_1^2 - (2x+1)^2 = (P_1 - 2x - 1)(P_1 + 2x + 1).$$

Thus, $P_1 = 2x + 2 = \lfloor \sqrt{D} \rfloor$ and $p = 4x + 3$, from which we get $D = (2x+3)^2 - 2$. Now we demonstrate that $\ell = 4$ by simply tabulating the values from Theorem 2.2:

i	0	1	2	3	4
P_i	0	$2x+2$	$2x+1$	$2x+1$	$2x+2$
Q_i	1	$4x+3$	2	$4x+3$	1
q_i	$2x+2$	1	$2x+1$	1	$4x+4$

Now, by Corollary 2.2, a prime $r < \sqrt{\Delta}$ is principal and reduced if and only if $r = Q_j$ for some positive $j < \ell(\sqrt{D})$. Thus, the only possibility is that $p = 2\lfloor\sqrt{D}\rfloor - 1 = 4x + 3$, so it is the only split prime less than $\sqrt{\Delta}$. This is (b)(ii).

Now assume that $p = 2$. Then by (3.3), $P_1 = 2x_1 + 1$ for some $x_1 \geqslant 0$. We have,

$$|F_{\Delta,2}(x_1)| = |2x_1^2 + 2x_1 - 2m - 1| = \left|\frac{P_1^2 - D}{2}\right| = \frac{Q_1}{2},$$

so by the hypothesis in (a), $Q_1 \in \{2, 2q\}$ for a prime $q > 2$. However, $Q_1 \neq 2q$, since we have shown in the above that when an odd prime divides Q_1, then Q_1 is prime. Therefore, $Q_1 = 2$, so, by Theorem 2.6, $\ell = 2$, and

$$D = P_1^2 + Q_1 Q_0 = \lfloor\sqrt{D}\rfloor^2 + 2.$$

Since $h_\Delta = 1$, then by Corollaries 2.1–2.2, if there were a split prime $q < \sqrt{D}$, we would have $Q_j = q$ for some positive integer $j < \ell$. However, this is impossible as $\ell = 2 = Q_1 = Q_{\ell/2}$. This is (b)(i).

Moreover, from [12] the only values satisfying b(ii), with one GRH-ruled-out exception, are given in the list (3.2) and those satisfying b(i) are those in the list (3.1).

Lastly to show that (b) implies (a), we invoke Lemma 3.3 since there are no split prime less than $\sqrt{D}/2$, observing that $D \neq 2p^2 + 1$ for any prime p since $\ell(\sqrt{2p^2+1}) = 1$ by [6, Theorem 3.2.1, p. 78]. ■

The following is proved in an entirely analgous fashion to the above so we state the result without proof.

Theorem 3.3. *Suppose that* $\Delta = 4D \equiv 0 \pmod 8$ *for* D *a non-negative integer. Then the following are equivalent.*

1. $|F_{\Delta,2}(x)| = |2x^2 - D/2|$ *is prime for all* $x \in [0, (\sqrt{D}-1)/2]$.
2. *One of the following holds.*
   (a) $D = p^2 + 1 = 2q$, *where* $p = 1$ *or* p *is prime and* $q \equiv 1 \pmod 4$ *is prime. Moreover,* $\ell(\sqrt{D}) = 1, h_\Delta = 2$, *and* p *is the only split prime less than* $\sqrt{D}$. *The only values, with one possible exception, for which this holds are*
   $$D \in \{2, 10, 26, 122, 362\}. \tag{3.6}$$
   (b) $D = (\lfloor\sqrt{D}\rfloor)^2 + 2 = 2q$, *where* $q \equiv 3 \pmod 4$ *is prime,* $l(\sqrt{D}) = 2$, $h_\Delta = 1$, *and there are no split primes less than* $\sqrt{D}$. *The only values, with one possible exception, for which this holds are*
   $$D \in \{6, 38\}. \tag{3.7}$$
   (c) $D = [\frac{p+3}{2}]^2 - 2 = 2q$ *where* $q = 2[(p+3)/2]^2 - 1$ *is prime,* $p > \sqrt{D}$ *is prime,* $h_\Delta = 1$, *and* $\ell(\sqrt{D}) = 4$. *Also, there are no split primes less than* $\sqrt{D}$ *and the only values, with one possible exception, for which this holds are*
   $$D \in \{14, 62, 398\}. \tag{3.8}$$

If we extend q in $F_{\Delta,q}(x)$ to values bigger than 2, we can achieve all the values of Extended Richaud-Degert (ERD) type with class group of exponent 2, rather than just of order 2 as above, as observed in [6]. (Recall that an ERD type is one of the form $D = a^2 + r$ where $r \big| 4a$.) Herein, we have displayed the techniques that extract the specific information about the values of Δ using the continued fraction approach. In the next section, we switch gears for the proof of a conjecture left in [11]. Since we coined the latter therein, we deemed it appropriate to title the next section with attribution to that fact.

4. The Mollin-Srinivasan Conjecture

Let $\Delta = 1 + 4m$ and $t = \lfloor\sqrt{m}\rfloor$. If $|F_{\Delta,1}(x)|$ is prime or equal to 1 for $x \in I = [x_0, x_0 + t - 1]$, for some integer x_0 and $t \in \mathbb{N}$, we call I a Rabinowitsch interval. Also $F_{\Delta,1}(x)$ is called a Rabinowitsch polynomial.

We will need the following

Lemma 4.1. *Suppose that* $\Delta = 4m+1$, *and* $F_{\Delta,1}(x)$ *is a Rabinowitsch polynomial with Rabinowitsch interval* $I = [x_0, x_0+t-1]$ *where* $t = \lfloor\sqrt{m}\rfloor$. *Then if* $t \geqslant a > 1$ *is an integer such that* $|F_{\Delta,1}(x)| \equiv 0 \pmod a$ *for some non-negative integer* x, *then* a *is prime and there is an integer* $y \in I$ *such that* $x \equiv y \pmod a$, *and* $|F_{\Delta,1}(y)| = a$.

Proof. As $a \leqslant t$ we can find an integer $y \in I$ such that $x \equiv y \pmod a$. Then $F_{\Delta,1}(y) \equiv F_{\Delta,1}(x) \equiv 0 \pmod a$, so $|F_{\Delta,1}(y)| = a$ and a is prime since I is a Rabinowitsch interval. ■

Also, in [3] the following theorem is proved.

Theorem 4.1. *There are finitely many Rabinowitsch polynomials. Also if $F_{\Delta,1}(x)$ is a Rabinowitsch polynomial, then $\Delta = 9$ or $\Delta = 1 + 4t^2$ where t is either prime or 1, or $\Delta = n^2 \pm 4$ or $\Delta = 9p^2 \pm 4p$, where p is an odd prime.*

In [3], their list of "all possible Rabinowitsch polynomials with one-possible exception" was incomplete, which the following, proved in [11, Theorem 3.3], corrected. Also, all Rabinowitsch polynomials with $[1, t]$ as a Rabinowitsch interval were given unconditionally.

Theorem 4.2 (Rabinowitsch-Mollin-Williams Updated). *If $\Delta = 4m + 1$, $m \neq 2$, then the following are equivalent.*

1. *$|F_{\Delta,1}(x)| = |x^2 + x - m|$ is 1 or prime for all $x \in [1, t]$.*
2. *$h_\Delta = 1$ and Δ is one of the following forms.*
   (a) *$n^2 - 4$ for some $n \in \mathbb{N}$.*
   (b) *$p^2 + 4$ for a prime $p > 2$.*
   (c) *$4p^2 + 1$ where either $p = 1$ or p is prime.*
3. *$\Delta \in \{5, 13, 17, 21, 29, 37, 53, 77, 101, 173, 197, 293, 437, 677\}$.*

Now under the GRH we have the list of all Rabinowisch intervals for a given Δ because we have a list, with one GRH-ruled-out exception, of all the values of Δ from which this may be deduced upon inspection. On examination of this list it is seen that in each case either $[1, t]$ or $[\frac{t+2}{3}, \frac{4t-1}{3}]$ is a Rabinowitsh interval. Here in Theorem 4.2 we present an equivalence for the remaining Rabinowitsch polynomials that have $[\frac{t+2}{3}, \frac{4t-1}{3}]$ as a Rabinowitsch interval. This completes the classification of Rabinowitsch polynomials in terms of their Rabinowitsch intervals and also solves the following conjecture posed in [11].

Conjecture 4.1. *If $1 + 4m = \Delta = pq$ with $p < q$ primes and $|F_{\Delta,1}(x)| = |x^2 + x - m|$ is prime for all $x \in [(p + 1)/2, (p - 1)/2 + \lfloor\sqrt{m}\rfloor]$, then*

$$h_\Delta = 1 \qquad \text{and} \qquad \Delta = 9p^2 \pm 4p. \tag{4.1}$$

Moreover, the only values for which (4.1) holds are

$$\Delta \in \{69, 93, 413, 1133\}. \tag{4.2}$$

Theorem 4.3. *If $\Delta = 1 + 4m$, then the following are equivalent.*

1. *$\Delta = pq$ with $p < q$ primes and*

$$|F_{\Delta,1}(x)| = |x^2 + x - m| \qquad \text{is prime for all } x \in I = \left[\frac{p+1}{2}, \sqrt{m} + \frac{p-1}{2}\right]. \tag{4.3}$$

2. (a) $h_\Delta = 1$.
   (b) $\ell(\alpha) = \ell \in \{2, 4\}$ *where* $\alpha = (1 + \sqrt{\Delta})/2$.
   (c) $\Delta = 9p^2 \pm 4p$, *where* $t = \lfloor \sqrt{m} \rfloor$, *and* $p = (2t + 1)/3$ *is prime and is the only non-inert prime less than* $\sqrt{\Delta}/2$.

Proof. Assume statement 1 holds. Then $F_{\Delta,1}(x)$ is a Rabinowitsch polynomial with Rabinowitsch interval I. Therefore, by Lemmas 3.2 and 4.1, for every split prime $p < \sqrt{\Delta}/2$, there is an integer $x \in [(p+1)/2, (p-1)/2 + \sqrt{m}]$ such that $|F_{\Delta,1}(x)| = p$. By Corollary 3.1 and Theorem 2.7, we must have that $h_\Delta = 1$, which is statement 2(a). It is well known that $h_\Delta = 1$ cannot happen for $p \equiv q \equiv 1 \pmod 4$ – see [8, Theorem 3.70, p. 162], for instance. Hence, $p \equiv q \equiv 3 \pmod 4$. It follows from (2.16) that if ℓ is odd, then

$$-1 \equiv A_{\ell-1}^2 \pmod \Delta,$$

which is impossible for Δ divisible by a prime congruent to 3 modulo 4. We have shown that ℓ is even.

If m is even, then $\Delta \equiv 1 \pmod 8$, and

$$\left| F_{\Delta,1}\left(\frac{p+1}{2}\right) \right| = \left| \frac{(p+2)^2 - pq}{4} \right| \equiv 0 \pmod 2,$$

so $(p+2)^2 - pq = \pm 8$. Thus, either $p(p+4-q) = p^2 + 4p - pq = 4$ or $p(p+4-q) = -12$. In the first instance, $p = 2$ is forced, which is impossible since Δ is odd. In the second case $p = 3$ and $q = 11$ is forced. However $F_{\Delta,1}((p+3)/2) = F_{\Delta,1}(3) = 4$, which is a contradiction since $(p+3)/2 = \lfloor \sqrt{m} \rfloor + (p-1)/2 = 3 \in I$, with $m = 8$. We have shown that m is odd.

By Theorem 2.6, $Q_{\ell/2} | 4\Delta = 4pq$. Thus, given the facts:

$$Q_{\ell/2} < 2q \qquad \text{by (2.10)},$$

$$Q_j \text{ is even for all } j \geqslant 0, \qquad \text{given that } \sigma = 2 \text{ in (2.17)},$$

and

$$Q_{\ell/2} \equiv 2 \pmod 4 \qquad \text{by (2.5) since } \Delta \not\equiv 1 \pmod 8,$$

then $Q_{\ell/2} = 2p$ is forced. By (2.5), since Δ is odd, we may set $P_{\ell/2} = 2x_{\ell/2} + 1$, then by (2.5) again,

$$|F_{\Delta,1}(x_{\ell/2})| = \left| \frac{(2x_{\ell/2} + 1)^2 - \Delta}{4} \right| = \frac{Q_{\ell/2} Q_{\ell/2-1}}{4}. \tag{4.4}$$

By Theorem 2.6, $2p = Q_{\ell/2} | 2P_{\ell/2}$, so $P_{\ell/2} = px$ for some $x \in \mathbb{N}$. If $x > 1$, then $\lfloor \sqrt{m} \rfloor + (p-1)/2 \geqslant x_{\ell/2} \geqslant (p+1)/2$ so $x_{\ell/2} \in I$, which forces $Q_{\ell/2-1} = 2$ by hypothesis, namely $\ell = 2$ by (2.18). We have

$$(P_{\ell/2} - 1)/2 = x_{\ell/2} = (px - 1)/2. \tag{4.5}$$

Now since $P_{\ell/2} = px < \sqrt{\Delta}$ and $x > 1$ with $P_{\ell/2}$ odd, then by (2.11),

$$3p \leqslant P_{l/2} < \sqrt{\Delta} < 2\sqrt{m+1},$$

which implies $p < \sqrt{m}$. Therefore $(3p-1)/2 \in I = [(p+1)/2, \sqrt{m} + (p-1)/2]$. Suppose $(5p-1)/2 \in I$. Then

$$\left|F_{\Delta,1}\left(\frac{3p-1}{2}\right)\right| = p = \left|F_{\Delta,1}\left(\frac{5p-1}{2}\right)\right|.$$

From the left-hand equality, we get

$$9p^2 + 4p = \Delta, \tag{4.6}$$

and from the right-hand equality we get,

$$25p^2 + 4p = \Delta. \tag{4.7}$$

Equating (4.6)–(4.7) yields an impossibility. We have shown that $x = 3$ and hence

$$p = (2x_{\ell/2} + 1)/3 \tag{4.8}$$

from (4.5). From (2.5),

$$\Delta = P_{\ell/2}^2 + Q_{\ell/2}Q_{\ell/2-1} = (2x_{\ell/2} + 1)^2 + 4p = 9p^2 + 4p.$$

Now we show that $x_{\ell/2} = t$, which will give us statement 2(c) with the plus sign via (4.8). We have

$$\frac{3p+1}{2} = \sqrt{\frac{(3p+1)^2}{4}} > \sqrt{\frac{\Delta - 1}{4}} > \sqrt{\frac{(3p-1)^2}{4}} = \frac{3p-1}{2},$$

so since $t = \lfloor\sqrt{m}\rfloor = \lfloor\sqrt{(\Delta-1)/4}\rfloor$, then the only possibility is that $t = (3p-1)/2 = x_{\ell/2}$.

Now assume that $x = 1$. If $\ell = 2$, then by (2.5), $\Delta = p^2 + 4p$ and hence

$$\left|F_{\Delta,1}\left(\frac{p+1}{2}\right)\right| = 1,$$

which contradicts the hypothesis. Now we are left with the case that $\ell > 2$ and $x = 1$. We now proceed to show that $\ell = 4$. We first establish some salient features that will lead to period length four.

Claim 4.1. $q_{\ell/2-1} = 1$.

From (4.4), $|F_{\Delta,1}(x_{\ell/2})| = pQ$ where $Q = Q_{\ell/2-1}/2$.

We first show that $p \leqslant \sqrt{m}$ by way of contradiction. Suppose that $p > \sqrt{m}$. Then it follows that $Q < \sqrt{m}$. Thus, if $Q \neq 1$, by Lemma 4.1, there is a $y = x_{\ell/2} + zQ = (p-1)/2 + zQ \in I$, with $z \in \mathbb{N}$, since $x_{\ell/2} = (P_{\ell/2} - 1)/2$. Therefore,

$$|F_{\Delta,1}(y)| = \left|\frac{\Delta - (2y+1)^2}{4}\right| = \left|\frac{\Delta - (p+2zQ)^2}{4}\right| = Q(z^2Q + pz - p).$$

By assumption $|F_{\Delta,1}(y)|$ is prime and since $Q > 1$, the only possibility is that $z^2Q+pz-p = 1$. Thus, $z^2Q+pz = p+1$ which, for $z > 1$, means that $p+1 > p+Q$, a contradiction, so $z = 1$ which forces $|F_{\Delta,1}(y)| = Q^2$, a contradiction. We have shown that $Q = 1$. Hence, $\ell = 2$, which is a contradiction to the assumption above. Hence, $p \leqslant \sqrt{m}$.

By (2.6), $p = P_{\ell/2} = P_{\ell/2+1}$, by (2.15), $q_{\ell/2-1} = q_{\ell/2+1}$, and by (2.7), $Q_{\ell/2-1} = Q_{\ell/2+1}$. Thus,

$$q_{\ell/2-1} = q_{\ell/2+1} = \left\lfloor \frac{P_{l/2+1} + \sqrt{\Delta}}{Q_{l/2+1}} \right\rfloor = \left\lfloor \frac{p + \sqrt{4m+1}}{Q_{l/2+1}} \right\rfloor . \tag{4.9}$$

However, by (2.5),

$$\begin{aligned}\Delta = 4m+1 = P_{\ell/2}^2 + Q_{\ell/2}Q_{\ell/2-1} &= p^2 + 2pQ_{\ell/2-1} \\ = p^2 + 2pQ_{\ell/2+1} &\leqslant m + 2\sqrt{m}Q_{\ell/2+1},\end{aligned}$$

then

$$Q_{\ell/2+1} \geqslant \frac{3m+1}{2\sqrt{m}}. \tag{4.10}$$

Thus if, $q_{\ell/2-1} \geqslant 2$, then from (4.9),

$$p + \sqrt{4m+1} \geqslant 2Q_{\ell/2+1}.$$

Hence, from (4.10),

$$\sqrt{m} + \sqrt{4m+1} \geqslant p + \sqrt{4m+1} \geqslant 2Q_{\ell/2+1} \geqslant \frac{3m+1}{\sqrt{m}},$$

and by squaring the left- and right-hand inequalities we get,

$$5m + 1 + 2\sqrt{4m^2+m} \geqslant 9m + 6 + 1/m > 9m + 6,$$

which implies

$$\sqrt{4m^2+m} > 2m + 5/2 > 2m + 2,$$

so squaring again yields the contradiction,

$$4m^2 + m > 4m^2 + 8m + 4,$$

which secures Claim 4.1.

Claim 4.2. *$p = (r+s)/2$, where $r = Q_{\ell/2-1}/2$ and $s = Q_{\ell/2-2}/2$.*

By (2.5), $\Delta = P_{\ell/2-1}^2 + Q_{\ell/2-1}Q_{\ell/2-2}$ and by Claim 4.1 and (2.3), $p = P_{\ell/2} = Q_{\ell/2-1} - P_{\ell/2-1}$. Thus,

$$\Delta = (Q_{\ell/2-1} - p)^2 + 4rs = (2r-p)^2 + 4rs = p^2 - 4pr + 4r^2 + 4rs. \tag{4.11}$$

Also, by (2.5),

$$\Delta = P_{\ell/2}^2 + Q_{\ell/2}Q_{\ell/2-1} = p^2 + 2pQ_{\ell/2-1} = p^2 + 4pr, \tag{4.12}$$

then via (4.11)–(4.12), we get $p = (r+s)/2$, which is Claim 4.2.

Claim 4.3. $P_{\ell/2-1}^2 = (3r-s)^2/4$.

By (2.5) and (2.6), $\Delta = P_{\ell/2+1}^2 + 2pQ_{\ell/2+1} = p^2 + 2pQ_{\ell/2+1} = p^2 + 4pr$. Therefore, by Claim 4.2,

$$P_{\ell/2-1}^2 = \Delta - Q_{\ell/2-1}Q_{\ell/2-2} = p^2 + 4pr - 4rs = \left(\frac{3r-s}{2}\right)^2,$$

which secures Claim 4.3.

Now we are ready to establish period length four, namely $s = 1$ by (2.18). We have, from Claims 4.1–4.3,

$$\begin{aligned} \Delta = P_{\ell/2-1}^2 + Q_{\ell/2-1}Q_{\ell/2-2} &= \left(\frac{3r-s}{2}\right)^2 + 4rs \\ &= \frac{9r^2+10rs+s^2}{4} = 9p^2 - 4ps. \end{aligned} \tag{4.13}$$

However from (4.13),

$$F_{\Delta,1}\left(\frac{3p-1}{2}\right) = \left(\frac{3p-1}{2}\right)^2 + \left(\frac{3p-1}{2}\right) + \frac{1-\Delta}{4} = ps.$$

Now, since $p < \sqrt{m}$, then $(3p-1)/2 < (p-1)/2 + \sqrt{m}$, so $(3p-1)/2 \in I$. We have shown that $s = 1$, namely $\ell = 4$.

We have shown that $\Delta = 9p^2 - 4p$ with $p = (r+1)/2$ and $\ell = 4$. Now we show that $p = (2t+1)/3$ which amounts to showing that $r = (4t-1)/3$ by Claim 4.2. We have,

$$\sqrt{m} + \frac{1}{2} < \frac{\sqrt{4m+1}+1}{2} < \sqrt{m} + 1.$$

However,

$$q_0 = \left\lfloor \frac{P_0 + \sqrt{4m+1}}{2} \right\rfloor = \left\lfloor \frac{1+\sqrt{4m+1}}{2} \right\rfloor,$$

so $q_0 = \lfloor \sqrt{m} \rfloor = t$.

Therefore, by (2.3), $P_1 = 2q_0 - 1$, so by Claim 4.3 and (2.3),

$$P_1 = 2q_0 - 1 = 2t - 1 = P_{\ell/2-1} = \frac{3r-1}{2},$$

from which we get $r = (4t-1)/3$, which is statement 2(c) with the minus sign. To conclude the proof that statement 1 implies statement 2, we know, by Corollaries 2.1–2.2, that there cannot exist any primes other than p that are non-inert and less than $\sqrt{\Delta}/2$ since otherwise they would have to appear as a $Q_j/2$ in the simple continued fraction expansion of α. To see why this holds explicitly, consider the following. We have shown that $\ell \in \{2, 4\}$. If $\ell = 2$, then by [6, Theorem 3.2.1, p. 78], $Q_1 = 2p = Q_{\ell/2}$. Similarly, if $\ell = 4$, then $Q_2 = Q_{\ell/2} = 2p$ and $Q_1 = Q_3 = 4p - 2 > \sqrt{\Delta}/2$. Since $Q_0 = Q_2 = 2$ in either case, we are done with this part of the proof.

Next assume statement 2 holds. Suppose that a prime $q\big||F_{\Delta,1}(x)|$ for some $x \in I$. If $q < \sqrt{\Delta}/2$, then since $h_\Delta = 1$, by Corollaries 2.1–2.2, $Q_j/2 = q$ for some j. But as argued above for the discriminants of the form $\Delta = 9p^2 \pm 4p$, the only possibility for $Q_j/2$ to be a prime less than $\sqrt{\Delta}/2$ is $q = p$. Also, since

$$|F_{\Delta,1}(x)| = \left|\frac{(2x+1)^2 - \Delta}{4}\right| \equiv 0 \,(\mathrm{mod}\ p),$$

then $2x+1 \equiv 0\,(\mathrm{mod}\ p)$, namely $x = (kp-1)/2$ for some odd integer k. Therefore,

$$\frac{p+1}{2} < x = \frac{kp-1}{2} < \sqrt{m} + \frac{p-1}{2} < \frac{3p+1+p-1}{2} = 2p,$$

given that $4m+1 = 9p^2 \pm 4p$. Hence, $k = 3$ and

$$\left|F_{\Delta,1}\left(\frac{3p-1}{2}\right)\right| = p,$$

so now we may assume there is a prime $q\big||F_{\Delta,1}(x)|$ where $x \in I$ and $q > \sqrt{\Delta}/2$. If there exists another prime $r\big||F_{\Delta,1}(x)|$, then it too must be larger than $\sqrt{\Delta}/2$ since by the above argument, the only other possibility is that $r = p$ and $|F_{\Delta,1}(x)| = p$. Also, since $p = (2\lfloor\sqrt{m}\rfloor + 1)/3$ and $x \leqslant \lfloor\sqrt{m}\rfloor + (p-1)/3$, then $(2x+1)^2 \leqslant (8\lfloor\sqrt{m}\rfloor + 1)/3)^2 < 8m+1$, so

$$|F_{\Delta,1}(x)| = |((2x+1)^2 - \Delta)/4| < (8m+1-4m-1)/4 = m.$$

Hence,

$$m > |F_{\Delta,1}(x)| \geqslant rq > \Delta/4 = m + \frac{1}{4},$$

a contradiction. We have shown that $|F_{\Delta,1}(x)|$ is prime for all $x \in I$ if $|F_{\Delta,1}(x)| > 1$. If $|F_{\Delta,1}(x)| = 1$, then $\Delta = (2x+1)^2 \pm 4$. However, if $\Delta = (2x+1)^2+4$, then $\ell = 1$ by [6, Theorem 3.2.1, p. 78], contradicting that $\ell \in \{2, 4\}$. Thus, $\Delta = (2x+1)^2 - 4$, for which $\ell = 2$ and $Q_1 = 4x-2$. Yet by hypothesis (c), employing [6, Theorem 3.2.1, p. 78], $\Delta = 9p^2 + 4p$ with $\ell = 2$ and $Q_1 = 2p$. Hence, $p = 2x-1$, from which we get

$$4x^2 + 4x - 3 = \Delta = 9(2x-1)^2 + 4(2x-1) = 36x^2 - 28x + 5,$$

for which the only solution is $x = 1/2$, a contradiction. The fact that $9p \pm 4$ is prime follows from the hypothesis that $h_\Delta = 1$ via the well-known fact from Gauss—[8, Theorem 3.70, p. 162]—as used at the outset of the proof. Thus, statement 1 follows. ■

Corollary 4.1. *With one GRH-ruled-out exception Theorem 4.3 holds only for the values*

$$\Delta \in \{69, 93, 413, 1133\}. \tag{4.14}$$

Proof. The list in (4.14) follows with one GRH-rules-out exception by using a result of Tatuzawa–see [6, Theorem 5.4.1, p. 174] – that gives a lower bound for the

L-function appearing in the analytic class number formula – see [6, (5.4.1), p. 173], and this bound holds with one possible exceptional value. This exceptional value disappears under the assumption of the GRH – see [6, Chapter 5] for details. ■

Remark 4.1. Note that if $|F_{\Delta,1}(x)|$ is allowed to equal 1 in Theorem 4.2, then $\Delta = p^2 + 4p$ with $p = 2t + 1$ and that unconditionally, via [1], these are exactly the composite values that appear in part 2(a) of Theorem 4.2, namely $\Delta \in \{21, 77, 437\}$.

References

[1] D. Byeon, M. Kim and J. Lee, *Mollin's conjecture*, Acta Arith. **126** (2007), 99–114.

[2] D. Byeon and H. M. Stark, *On the finiteness of certain Rabinowitsch polynomials*, J. Number Theory **94** (2002), 219–221.

[3] D. Byeon and H. M. Stark, *On the finiteness of certain Rabinowitsch polynomials II*, J. Number Theory **99** (2003), 177–180.

[4] J. Lee, *The complete determination of narrow Richerd-Degert type which is not 5 modulo 8 with class number 2*, J. Number Theory **129** (2009), 604–620.

[5] S. Louboutin, R. A. Mollin and H. C. Williams, *Class numbers of real quadratic fields, continued fractions, reduced ideals, prime-producing quadratic polynomials and quadratic residue covers,* Canad. J. Math. **44** (1992), 824–842.

[6] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, New York, London, Tokyo, 1996.

[7] R. A. Mollin, *Fundamental Number Theory with Applications*, First Edition, CRC Press, Boca Raton, London, New York, Washington, D.C., 1998.

[8] R. A. Mollin, *Algebraic Number Theory,* Chapman&Hall/CRC, 1999.

[9] R. A. Mollin, *Continued fractions and class number two*, Internat. J. Math. & Math. Sci. (2001), 565–571.

[10] R. A. Mollin, *Fundamental Number Theory with Applications* , Second Edition, Chapman and Hall/CRC, Taylor and Francis Group, Boca Raton, London, New York, Washington, D.C., 2008.

[11] R. A. Mollin, *The Rabinowitsch-Mollin-Williams Theorem Revisited*, International J. Math. and Math. Sci., 2009, Article ID 819068, 14 pages, doi:10.1155/2009/819068.

[12] R. A. Mollin and H. C. Williams, *Prime producing quadratic polynomials and real quadratic fields of class number one*, Theorie des Nombres (Quebec, 1987), de Gruyter, Berlin (1989), 654–663.

Addresses: Richard A. Mollin: Department of Mathematics and Statistics, University of Calgary, Canada;
Anitha Srinivasan: Department of Mathematics, Siddhartha college of arts, science and commerce, Mumbai 23, India.

E-mail: ramollin@math.ucalgary.ca, rsrinivasan.anitha@gmail.com

Received: 4 October 2010; **revised:** 2 December 2010