Hindawi Publishing Corporation
International Journal of Mathematics and Mathematical Sciences
Volume 2009, Article ID 819068, 14 pages
doi:10.1155/2009/819068

Research Article

The Rabinowitsch-Mollin-Williams Theorem Revisited

R. A. Mollin

Department of Mathematics and Statistics, University of Calgary, Calgary, AB, Canada T2N 1N4

Correspondence should be addressed to R. A. Mollin, ramollin@math.ucalgary.ca

Received 24 April 2009; Revised 24 June 2009; Accepted 20 August 2009

Recommended by Aloys Krieg

We completely classify all polynomials of type $(x^2+x-(\Delta-1))/4$ which are prime or 1 for a range of consecutive integers $x \geq 0$, called *Rabinowitsch polynomials*, where $\Delta \equiv 1(\text{mod}4)$ with $\Delta > 1$ square-free. This corrects, extends, and completes the results by Byeon and Stark (2002, 2003) via the use of an updated version of what Andrew Granville has dubbed the Rabinowitsch-Mollin-Williams Theorem—by Granville and Mollin (2000) and Mollin (1996). Furthermore, we verify conjectures of this author and pose more based on the new data.

1. Introduction

The renowned Rabinowitsch result for complex quadratic fields proved in 1913, published in [1], says that if $\Delta = 1 - 4m$ is square-free, then the class number, h_Δ, of the complex quadratic field $\mathbb{Q}(\sqrt{\Delta})$ is 1 exactly when $x^2 + x + m$ is prime for all integers $x \in [0, m-3]$. The Rabinowitsch-Mollin-Williams Theorem is the real quadratic field analogue of the Rabinowitsch result, introduced in 1988, published in [2] by this author and Williams. In [2] and in subsequent renderings of the result, we considered all values of Δ. However, the case where $\Delta \not\equiv 1(\text{mod}\,4)$ is essentially trivial, and the values (unconditionally) known for these Rabinowitsch polynomials are $\Delta \in \{2, 3, 6, 7, 11\}$—see [3]. Therefore, we consider only the interesting case, namely, $\Delta \equiv 1(\text{mod}\,4)$.

Theorem 1.1 (Rabinowitsch-Mollin-Williams). *If $\Delta = 1 + 4m$, where $m \in \mathbb{N}$, then the following are equivalent.*

(a) *$f_m(x) = x^2 + x - m$ is 1 or prime for all integers $x \in [1, \sqrt{m}]$.*

(b) *$h_\Delta = 1$ and $\Delta = s^2 + r$, where $r \in \{1, \pm 4\}$.*

Proof. See [2], as well as [4, 5] and Theorem 3.14 below for an update. □

A version of Theorem 1.1 was rediscovered by Byeon and Stark [6] in 2002. Then in 2003 [7], they claimed to have classified all of the Rabinowitsch polynomials. However, their list is incomplete. In this paper, we provide the complete and unconditional solution of finding all Rabinowitsch polynomials of *narrow Richaud-Degert type*, namely, those for which $\Delta = s^2 + r$ where $r \in \{\pm 1, \pm 4\}$, adding three values missed in [7]. The balance of the Rabinowitsch polynomials turn out to be of *wide Richaud-Degert type*, namely for those of the form $\Delta = s^2 + r$, where $r \mid 4s$. In this case, we cite the well-known methodology for showing that the balance of the list is complete "with one possible GRH-ruled-out exception" and add two values missed in [7]. (Here GRH means the generalized Riemann hypothesis.) Lastly, we show how four conjectures posed by this author in 1988 in [8] are affirmatively settled via the above and complement another conjecture by this author affirmatively verified by Byeon et al. in [9].

2. Preliminaries

We will be discussing 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 [4].

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

$$\alpha = \langle q_0; q_1, q_2, \ldots \rangle \quad \text{where } q_j \in \mathbb{N} \text{ for } j \in \mathbb{N},\ q_0 = \lfloor \alpha \rfloor, \tag{2.1}$$

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. There is a specific type of irrational that we need as follows.

Definition 2.1 (quadratic irrationals). A real number α is called a *quadratic irrational* if it is an irrational number which is the root of $f(x) = ax^2 + bx + c$, where $a, b, c \in \mathbb{Z}$ and $a \neq 0$.

Remark 2.2. 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

$$\alpha = \frac{P + \sqrt{\Delta}}{Q}, \quad (P, Q \in \mathbb{Z}). \tag{2.2}$$

Moreover, if α is a quadratic irrational, then $Q \mid (P^2 - \Delta)$. Also,

$$\alpha' = \frac{\left(P - \sqrt{\Delta}\right)}{Q} \tag{2.3}$$

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

$$f(x) = x^2 - \mathrm{Tr}(\alpha)x + N(\alpha), \tag{2.4}$$

where $\mathrm{Tr}(\alpha) = \alpha + \alpha'$ is the *trace* of α, and $N(\alpha) = \alpha \cdot \alpha'$ is the *norm* of α—see [10, Theorem 5.9, page 222].

Now, given a quadratic irrational $\alpha = (P + \sqrt{\Delta})/Q$, set $P = P_0$, $Q = Q_0$, and for $j \geq 0$ define

$$P_{j+1} = q_j Q_j - P_j, \tag{2.5}$$

$$\Delta = P_{j+1}^2 + Q_j Q_{j+1}, \tag{2.6}$$

$$\alpha_j = \frac{P_j + \sqrt{\Delta}}{Q_j}, \tag{2.7}$$

$$q_j = \lfloor \alpha_j \rfloor. \tag{2.8}$$

Since we are primarily concerned with the case $\Delta \equiv 1 (\mathrm{mod}\, 4)$, *we assume this for the balance of the discussion*.

We need to link quadratic irrationals associated with discriminant Δ to $\mathcal{O}_\Delta$-ideals, namely, ideals in

$$\mathcal{O}_\Delta = \mathbb{Z}\left[\frac{1+\sqrt{\Delta}}{2}\right] = \mathbb{Z} \oplus \left(\frac{1+\sqrt{\Delta}}{2}\right)\mathbb{Z}, \tag{2.9}$$

the *ring of integers* or *maximal order* in $\mathbb{Q}(\sqrt{\Delta})$—see [11, Theorem 1.77, page 41]. We begin with the following.

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

$$I = \left[a, b' + \frac{c\left(1+\sqrt{\Delta}\right)}{2}\right], \tag{2.10}$$

where $a, c \in \mathbb{N}$, and $0 \leq b' < a$. Furthermore, I is an $\mathcal{O}_\Delta$-ideal if and only if this representation satisfies $c \mid a$, $c \mid b'$, and $ac \mid N((b' + c(1+\sqrt{\Delta})/2))$.

Proof. See [4, Theorem 1.2.1, page 9] or [12, Theorem 3.5.1, page 173]. □

Remark 2.4. If $c = 1$, then $I = [a, (b + \sqrt{\Delta})/2]$ is called a *primitive* $\mathcal{O}_\Delta$-ideal, where $b = 2b' + 1$ in Theorem 2.3, when $b^2 \equiv \Delta (\mathrm{mod}\, 4a)$. Furthermore, there is a one-to-one correspondence between the *primitive* $\mathcal{O}_\Delta$-ideals and quadratic irrationals of the form

$$\alpha = \frac{P' + \left(1+\sqrt{\Delta}\right)/2}{Q'} = \frac{2P' + 1 + \sqrt{\Delta}}{2Q'} = \frac{P + \sqrt{\Delta}}{Q}, \tag{2.11}$$

where $P = 2P' + 1$, $Q = 2Q'$, and $P^2 \equiv \Delta (\mathrm{mod}\, Q)$. To see this, let $I = [a, (b + \sqrt{\Delta})/2]$ be a primitive $\mathcal{O}_\Delta$-ideal, and set $\alpha = (b + \sqrt{\Delta})/(2a)$, which is a quadratic irrational, since $b^2 \equiv \Delta (\mathrm{mod}\, 4a)$ by Theorem 2.3. By setting $P = b$ and $Q = 2a$, then $\alpha = (P + \sqrt{\Delta})/Q$ and $I = [Q, /2, (P + \sqrt{\Delta})/2]$. Thus, to each primitive $\mathcal{O}_\Delta$-ideal there exists a quadratic irrational of the form (2.11).

Conversely, suppose that we have a quadratic irrational of the form (2.11). Then set $a = |Q|/2$ and $b = P$. Then $I = [a, (b + \sqrt{\Delta})/2]$ is a primitive $\mathcal{O}_\Delta$-ideal by Theorem 2.3, so to each quadratic irrational of type (2.11), there corresponds a primitive $\mathcal{O}_\Delta$-ideal.

Example 2.5. It is possible to have a quadratic irrational of type (2.11) corresponding to a *non*primitive $\mathcal{O}_\Delta$-deal. However, this does not alter the fact that there is a one-to-one correspondence between them and the primitive $\mathcal{O}_\Delta$-deals, as demonstrated in Remark 2.4. For instance, the principal ideal $I = (4) = [4, 1+\sqrt{5}]$ is *not* primitive in $\mathcal{O}_\Delta = \mathcal{O}_5 = \mathbb{Z}[(1+\sqrt{5})/2]$ since $c = 2$. Yet the quadratic irrational $\alpha = (1 + \sqrt{5})/4$ is of type (2.11). But α corresponds to the primitive ideal $[2, (1 + \sqrt{5})/2]$ via the methodology in Remark 2.4. However, it is worthy of note that if we allow *nonmaximal* orders, then this permits the solution of an interesting Diophantine problem as follows. If $\Delta \equiv 5 (\mathrm{mod}\, 8)$ and we conisder the nonmaximal order $\mathbb{Z}[\sqrt{\Delta}]$, then the Diophantine equation $|x^2 - \Delta y^2| = 4$ with $\gcd(x, y) = 1$ is solvable if and only if $I = [4, 1 + \sqrt{\Delta}]$ is a principal ideal in $\mathbb{Z}[\sqrt{\Delta}]$—see [4, Exercise 2.1.16, page 61] and [4, Section 1.5, pages 23–30] for background details on nonmaximal orders.

Also, to see why we must specialize to quadratic irrationals of type (2.11), we have $2 + \sqrt{5}$, which is a quadratic irrational by Definition 2.1, but is not of type (2.11). Moreover, it corresponds to the ideal $[1, 2 + \sqrt{5}]$, which is not primitive, and it does not correspond to any primitive ideal as does α above.

Remark 2.4 and Example 2.5 motivate the following.

Definition 2.6 (ideals and quadratic irrationals). To each quadratic irrational $\alpha = (P + \sqrt{\Delta})/Q$, with P odd, Q even, (and $\Delta \equiv 1 (\mathrm{mod}\, 4)$), there corresponds the primitive $\mathcal{O}_\Delta$-ideal

$$I = \left[\frac{|Q|}{2}, \frac{\left(P + \sqrt{\Delta}\right)}{2} \right]. \tag{2.12}$$

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

The infinite simple continued fraction of α given by $\langle q_0; q_1, q_2, \ldots \rangle$ is called *periodic* (sometimes called *eventually periodic*), if there exists an integer $k \geq 0$ and $\ell \in \mathbb{N}$ such that $q_n = q_{n+\ell}$ for all integers $n \geq k$. We use the notation

$$\alpha = \langle q_0; q_1, \ldots, q_{k-1}, \overline{q_k, q_{k+1}, \ldots, q_{\ell+k-1}} \rangle, \tag{2.13}$$

as a convenient abbreviation. The smallest such natural number $\ell = \ell(\alpha)$ is called the *period length of* α, and $q_0, q_1, \ldots, q_{k-1}$ is called the *preperiod* of α. If k is the *least* nonnegative integer such that $q_n = q_{n+\ell}$ for all $n \geq k$, then $q_k, q_{k+1}, \ldots, q_{k+\ell-1}$ is called the *fundamental period* of α. In particular, we consider the so-called *principal surd of* $\mathcal{O}_\Delta$, $\alpha = (1 + \sqrt{\Delta})/2$ for which it is known that

$$\frac{1 + \sqrt{\Delta}}{2} = \left\langle q_0; \overline{q_1, \ldots, q_{\ell-1}, 2q_0 - 1} \right\rangle. \tag{2.14}$$

We will need the following facts concerning period length.

If $\ell(\alpha) = \ell$ is even, then

$$P_{\ell/2} = P_{\ell/2+1}, \tag{2.15}$$

and if ℓ is odd, then

$$Q_{(\ell+1)/2} = Q_{(\ell-1)/2}. \tag{2.16}$$

Furthermore, since we are assuming $\Delta \equiv 1 (\mathrm{mod}\ 4)$, then for $1 \leq j \leq \ell(\alpha)$,

$$Q_j = Q_0 = 2 \quad \text{iff } j = \ell(\alpha), \tag{2.17}$$

$$Q_j \text{ is even} \quad P_j \text{ is odd} \quad \text{for all such } j. \tag{2.18}$$

Now we link pure periodicity with an important concept that will lead to the intimate link with ideals.

Definition 2.7 (reduced quadratic irrationals). Let $\alpha = (P + \sqrt{\Delta})/Q$ be a quadratic irrational. If $\alpha > 1$ and $-1 < \alpha' < 0$, then α is called *reduced*.

The next result sets the stage for our primary discussion.

Theorem 2.8 (pure periodicity equals reduction). *Let $\alpha = \langle q_0; q_1, \ldots \rangle$ be an infinite simple continued fraction, with $\ell(\alpha) = \ell \in \mathbb{N}$. Then α is reduced if and only if α is purely periodic, which means $k = 0$ in* (2.13)*, namely,*

$$\alpha = \langle \overline{q_0; q_1, \ldots, q_{\ell-1}} \rangle. \tag{2.19}$$

Proof. See [10, Theorem 5.12, page 228]. □

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

Definition 2.9 (reduced ideals). An $\mathcal{O}_\Delta$-ideal is said to be *reduced* if it is primitive and does not contain any nonzero element α such that both $|\alpha| < N(I)$ and $|\alpha'| < N(I)$.

To see how this is tied to Definition 2.7, we need the following.

Theorem 2.10 (reduced ideals and quadratic irrationals). *$I = [a, (b + \sqrt{\Delta})/2]$ 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 [4, Lemma 1.4.1, page 19] or [12, Theorem 5.5.1, page 258]. □

Corollary 2.11. *If $I = [a, (b + \sqrt{\Delta})/2]$ is a primitive $\mathcal{O}_\Delta$-ideal, with $\gamma = (b + \sqrt{\Delta})/a > 1$ and $-1 < (b - \sqrt{\Delta})/2 < 0$, then I is reduced.*

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*. (This holds for arbitrary Δ, not just $\Delta \equiv 1 (\mathrm{mod}\ 4)$.)

Theorem 2.12 (the continued fraction algorithm). *Let $I = I_1 = [Q_0/2, (P_0 + \sqrt{\Delta} + 1)/2]$ be an $\mathcal{O}_\Delta$-ideal corresponding to the quadratic irrational $\alpha = \alpha_0 = (P_0 + \sqrt{\Delta})/2$, and let P_j, Q_j be as given in* (2.5)–(2.7). *If $I_j = [Q_{j-1}/2, (P_{j-1} + \sqrt{\Delta})/2]$, then $I_1 \sim I_j$ for all $j \geq 1$. Moreover, there exists a least value $m \in \mathbb{N}$ such that I_{m+i} is reduced for all $i \geq 0$.*

Proof. See [4, Theorem 2.1.2, page 44]. □

Corollary 2.13. *A reduced $\mathcal{O}_\Delta$-ideal, $I = [Q/2, (P + \sqrt{\Delta}/2]$ for $\Delta \equiv 1 (\mathrm{mod}\ 4)$ is principal if and only if $Q = Q_j$ for some positive integer $j \leq \ell((1+\sqrt{\Delta})/2)$ in the simple continued fraction expansion of $(1 + \sqrt{\Delta})/2$.*

Proof. See [13]. □

Remark 2.14. The infrastructure given in Theorem 2.12 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 $m \geq 1$. 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.

By Remark 2.14, once we have achieved a reduced ideal I_m via the continued fraction algorithm, then the cycle becomes periodic. Thus, it makes sense to have a name for this period length. This is given in what follows, motivated by Definition 2.6 and the continued fraction algorithm.

Definition 2.15 (cycles and periods of reduced ideals). If $I = I_1 = [Q/2, (P + \sqrt{\Delta})/2]$ is a reduced $\mathcal{O}_\Delta$-ideal and ℓ is the least positive integer such that $I_1 = I_{\ell+1} = [Q_\ell/2, (P_\ell + \sqrt{\Delta})/2]$, then $\alpha_j = (P_j + \sqrt{\Delta})/Q_j$ for $j \geq 0$ all have the same period length $\ell(\alpha_j) = \ell(\alpha_0) = \ell(\alpha)$ via

$$[\alpha_j] = I_{j+1} = \left[\frac{Q_j}{2}, \frac{\left(P_j + \sqrt{\Delta}\right)}{2}\right]. \tag{2.20}$$

We denote this common value by $\ell = \ell(\mathcal{C})$ where $\mathcal{C}$ is the equivalence class of I in $\mathcal{C}_\Delta$, and call this value the *period length of the cycle of reduced ideals equivalent to I*. If we wish to keep track of the specific ideal, then we write $\ell(I)$ for ℓ.

Remark 2.16. If $I = [Q/2, (P + \sqrt{\Delta})/2]$ is a reduced $\mathcal{O}_\Delta$-ideal, then the set

$$\left\{\frac{Q_1}{2}, \frac{Q_2}{2}, \ldots, \frac{Q_\ell}{2}\right\} \tag{2.21}$$

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

3. Prime-Producing Polynomials

We begin by stating a very palatable result by Biro that we will employ in our classification.

Lemma 3.1 (Chowla's conjecture verified). *If $\Delta = 4p^2 + 1$ is square-free with some integer $p > 1861$, then $h_\Delta > 1$.*

Proof. See [14, Corollary, page 179]. □

Corollary 3.2. *The only values for which $h_\Delta = 1$ with $\Delta = 4p^2 + 1$ square-free are given by $p \in \{1, 2, 3, 5, 7, 13\}$.*

In what follows, $\Delta = 4m + 1$ for $m \in \mathbb{N}$, and $q \in \mathbb{N}$ is a square-free divisor of Δ, with

$$F_{\Delta,q}(x) = qx^2 + qx - m. \tag{3.1}$$

$F_{\Delta,q}(x)$ is called the *Euler-Rabinowitsch polynomial*, which was introduced by this author in [4, Chapter 4], to discuss prime-producing quadratic polynomials and is a generalization of $f_m(x) = F_{\Delta,1}(x)$ used in [6, 7], where he dubbed it the *Rabinowitsch polynomial*. We now show how all Rabinowitsch polynomials may be determined.

Theorem 3.3. *If $|f_m(x)| = |F_{\Delta,1}(x)|$ is prime for all $x \in [1, \sqrt{m}]$, then $\Delta = 4p^2 + 1$ for some prime p and $h_\Delta = 1$. Also, the only values for which the above holds are*

$$\Delta \in \{17, 37, 101, 197, 677\}. \tag{3.2}$$

Proof. First we show that Δ cannot be a perfect square. If $\Delta = r^2$, then

$$F_{\Delta,1}\left(\frac{r-1}{2}\right) = \left(\frac{r-1}{2}\right)^2 + \frac{r-1}{2} - \frac{r^2-1}{4} = 0, \tag{3.3}$$

contradicting the hypothesis since $(r-1)/2 < \sqrt{m}$.

Now we prove that Δ must be square-free. If $\Delta = r^2\Delta_0$, then $\Delta_0 \neq 1$ since Δ is not a perfect square. Hence, $\Delta_0 \geq 5$. Also, if $r > \sqrt{m}$, then

$$r^2 > m = \frac{r^2\Delta_0 - 1}{4} \geq \frac{5r^2 - 1}{4} > r^2, \tag{3.4}$$

a contradiction, so $r \leq \sqrt{m}$. Therefore, since

$$F_{\Delta,1}\left(\frac{r-1}{2}\right) = r^2\left(\frac{1-\Delta_0}{4}\right), \tag{3.5}$$

this contradicts the hypothesis if $r > 1$. Hence, $r = 1$, and Δ is square-free and so may be used for simple continued fraction expansions in the maximal order $\mathcal{O}_\Delta = \mathbb{Z}[(1 + \sqrt{\Delta})/2]$.

If m is even, then

$$|F_{\Delta,1}(2)| = \left|2\left(3 - \frac{m}{2}\right)\right| \tag{3.6}$$

is composite unless $m = 4$, namely, unless $\Delta = 17$, observing that $m \neq 2, 6$ since $4 \cdot 2 + 1 = 3^2$ and $4 \cdot 6 = 1 = 5^2$. Thus, we may assume that m is odd.

In the continued fraction expansion of $\alpha = (1 + \sqrt{\Delta})/2$, $\Delta = P_j^2 + Q_j Q_{j-1}$ for all natural numbers $j \leq \ell(\alpha)$ by (2.6). We now show that $\ell(\alpha) = 3$.

Suppose that $\ell(\alpha) > 3$. By (2.18), for each $j = 1, 2, \ldots, \ell(\alpha)$, we may set

$$x_j = \frac{P_j - 1}{2}. \tag{3.7}$$

Since $1 \leq P_j < \sqrt{\Delta}$ by (2.6), then $0 \leq x_j \leq (\sqrt{\Delta} - 1)/2$. If $Q_j = 2$ for any $j = 1, 2, 3$, then by (2.17), $\ell(\alpha) \leq 3$, a contradiction. Thus, $Q_j \neq 2$ for $j \in \{1, 2, 3\}$. However, if $x_j \neq 0$, then $|F_{\Delta,1}(x_j)|$ is prime by hypothesis since $x_j \leq \lfloor \sqrt{m} \rfloor$ for $j = 1, 2, 3$. We have, by (2.6), that

$$\left|F_{\Delta,1}(x_j)\right| = \left|x_j^2 + x_j - m\right| = \left|\frac{P_j^2 - \Delta}{4}\right| = \frac{Q_j Q_{j-1}}{4}. \tag{3.8}$$

Therefore, $Q_j Q_{j-1} = 4p$ where p is prime if $x_j \neq 0$. Now suppose that $j = 2$. Since Q_j is even for all $j \in \mathbb{N}$ by (2.18), then $Q_1 = 2p$ and $Q_2 = 2$, a contradiction as above. We have shown that $x_2 = 0$. If $j = 3$, then by the same argument $Q_3 = 2$, a contradiction. We have shown that $x_3 = 0$. Hence, by (2.5),

$$P_3 = 1 = q_2 Q_2 - P_2 = q_2 Q_2 - 1, \tag{3.9}$$

which implies that $2 = q_2 Q_2$ forcing $Q_2 = 2$, a contradiction. We have shown that $\ell(\alpha) \leq 3$.

If $\ell(\alpha) = 1$, then $Q_0 = Q_1 = 2$, and $\Delta = P_1^2 + 4$ with

$$|F_{\Delta,1}(x_1)| = \frac{Q_1 Q_0}{4} = 1, \tag{3.10}$$

contradicting the hypothesis unless $x_1 = 0$ which means $\Delta = 5$. However, $F_{5,1}(1) = 1$, where $1 \in [1, \sqrt{m}] = \{1\}$, contradicting the hypothesis. Hence, $\ell(\alpha) > 1$.

If $\ell(\alpha) = 2$, then by (3.8), $Q_1 = 2p$ for a prime p, $Q_2 = 2$, and $P_2 = P_1$ by (2.15). Hence, by (2.5)

$$P_1 = P_2 = q_1 2p - P_1, \tag{3.11}$$

which implies that $P_1 = q_1 p$. Now we show that $q_1 = 1$.

Assume to the contrary that $q_1 \geq 3$, since P_1 is odd by (2.18). Then by (2.6), $\Delta = P_1^2 + 4p$. Therefore $p < \sqrt{\Delta} - 2$. If we let $x = (p-1)/2 \leq \sqrt{m}$, then

$$|F_{\Delta,1}(x)| = \left| \frac{p^2 - \Delta}{4} \right| = p \left| \frac{p - \Delta/p}{4} \right| = p, \tag{3.12}$$

by hypothesis, which forces $p - \Delta/p = -4$, namely, $\Delta = p^2 + 4p$, and $q_1 = 1$. Therefore, $m = (p^2 + 4p - 1)/4$, so $(p+1)/2 < \sqrt{m} < (p+2)/2$, which implies that $\lfloor \sqrt{m} \rfloor = (p+1)/2$. Therefore,

$$F_{\Delta,1}\left(\frac{p+1}{2}\right) = \left(\frac{p+1}{2}\right)^2 + \frac{p+1}{2} - \left(\frac{p^2 + 4p - 1}{4}\right) = 1, \tag{3.13}$$

contradicting the hypothesis which says $F_{\Delta,1}(x)$ is prime for all $x \in [1, \sqrt{m}]$. We have shown that $\ell(\alpha) = 3$. Thus, $Q_2 \neq 2$, so by (3.8), for $j = 2$, we get $x_2 = 0$, which means $P_2 = 1$. For $j = 1$, (3.8) tells us that $Q_1 = 2p$ where p is prime since $Q_0 = 2$. By (2.16), $Q_2 = Q_1$ since $\ell(\alpha) = 3$, so by (2.6)

$$\Delta = 4m + 1 = P_2^2 + Q_2 Q_1 = 1 + 4p^2, \tag{3.14}$$

as we sought to show. Now we show that $h_\Delta = 1$ for these values.

By Theorem 2.12, if $\mathbf{I}$ is an ideal class in $\mathcal{C}_\Delta$, then $\mathbf{I}$ contains a reduced ideal $I = [Q/2, (P + \sqrt{\Delta})/2]$. Using a similar argument to the above on $\beta = (P + \sqrt{\Delta})/Q$ as we did for $\alpha = (1 + \sqrt{\Delta})/2$, we achieve that I is in a cycle of period length 3, namely $\ell(\beta) = \ell(I) = 3$. Now in the simple continued fraction expansion of β, let $Q = Q_0$ and $P = P_0$. Then, as in the case for α, (where we use the same symbols Q_j without risk of confusion since we are done with α), $Q_2 = Q_1$, $P_2 = 1$, and by (3.8) applied to βs values of Q_j, we must have that $Q_1 Q_0 = 4q$ for some prime q. If $Q_0 = 2$, then by Corollary 2.13, $I \sim 1$. If $Q_0 > 2$, then since Q_1 is even by (2.18), we must have either $q = 2 = Q_1$ and $Q_0 = 4$, or $Q_0 = 2q$ and $Q_1 = 2$. In either case, by Corollary 2.13 again, $I \sim 1$. Hence, $h_\Delta = 1$.

By Lemma 3.1, the only values for which the result holds are in the list (3.2). □

The following is the affirmative solution of four conjectures by this author posed in 1988 in [8, Conjectures 1–4, page 20]—see also [15, page 311]. Note that the equivalence of the conjectures follows from [2].

Corollary 3.4. *For a prime $p = 4m + 1 = 4q^2 + 1$, where q is prime, $|f_{q^2}(x)| = |x^2 + x - q^2|$ is prime for $x \in [1, q]$ if and only if $q \leq 13$.*

Corollary 3.5. *Suppose that $p = 4q^2 + 1$ is prime, where q is prime. Then all odd primes $r < q$ are inert in $\mathbb{Q}(\sqrt{p})$ if and only if $q \leq 13$.*

Corollary 3.6. *Suppose that $p = 4q^2 + 1$ is prime, where q is prime. Then $f_{q^2}(x) \not\equiv 0 (\mathrm{mod}\, r)$ for all positive integers x and primes r satisfying $x < r < q$ if and only if $q \leq 13$.*

Corollary 3.7. *Suppose that $p = 4q^2 + 1$ is prime, where q is prime and $F = \mathbb{Q}(\sqrt{p})$ with Dedekind-zeta function ζ_F. Then $2\zeta_F(-1) = q(2q^2 + 7)/45$ if and only if $q \leq 13$.*

Example 3.8. A nice illustration of Corollary 3.7 is for $q = 3$, with $p = 37$, where

$$\zeta_F(-1) = \frac{q(2q^2+7)}{90} = \frac{5}{6}. \tag{3.15}$$

Now we look at a slight variation that captures more of the results in [6, 7], as well as some missed by them. We will be using the following other beautiful result by Biro.

Lemma 3.9 (Yokoi's conjecture verified). *If $\Delta = p^2+4$ is square-free for some odd integer $p > 1861$, then $h_\Delta > 1$.*

Proof. See [16]. □

Corollary 3.10. *If $h_\Delta = 1$ for $\Delta = p^2 + 4$ square-free, then $p \in \{1, 3, 5, 7, 13, 17\}$.*

As well, we will be employing the following equally pleasant result by Byeon, Kim, and Lee, who used methods similar to those of Biro.

Lemma 3.11 (Mollin's conjecture verified). *If $\Delta = n^2 - 4$ is square-free, then $h_\Delta > 1$ for $n > 21$.*

Proof. See [9]. □

Corollary 3.12. *If $h_\Delta = 1$ for $\Delta = n^2 - 4$ square-free, then $n \in \{3, 5, 9, 21\}$.*

Theorem 3.13. *If $|f_m(x)| = |F_{\Delta,1}(x)|$ is 1 or prime for all $x \in [0, \sqrt{m} - 1]$, where $\Delta = 4m + 1$, then for $\Delta \neq 9$, either*

$$\Delta = n^2 - 4 \quad \text{for some } n \in \mathbb{N},\ h_\Delta = 1, \tag{3.16}$$

or

$$\Delta = p^2 + 4 \quad \text{for a prime } p > 2,\ h_\Delta = 1. \tag{3.17}$$

Also, the only values for which (3.16) *holds are*

$$\Delta \in \{5, 21, 77, 437\}, \tag{3.18}$$

and the only values for which (3.17) *holds are*

$$\Delta \in \{13, 29, 53, 173, 293\}. \tag{3.19}$$

Proof. If $\Delta = r^2$, then by hypothesis $|F_{\Delta,1}(0)| = (r^2-1)/4 = p$, where p is prime. Thus, $(r-1)(r+1) = 4p$, from which we deduce that the only possibility is $p = 2 = m$ and $r = 3$, namely, $\Delta = 9$, contradicting the hypothesis. Thus, Δ is not a square. Moreover, by the same argument as in the proof of Theorem 3.3, Δ is square-free. Hence, we may apply continued fraction theory as above.

If m is even, then $F_{\Delta,1}(0) = -m$, contradicting the hypothesis unless $m = 2$, for which $\Delta = 9$. Hence we may assume that m is odd and since $m = 1$ gives $\Delta = 5$ which satisfies the hypothesis, we assume that $m > 1$ is odd.

Let $\alpha = (1 + \sqrt{\Delta})/2$, so in the continued fraction expansion of α, $\Delta = P_j^2 + Q_j Q_{j-1}$ for $1 \le j \le \ell(\alpha)$ by (2.6). If x_j is given by (3.7), then by (3.8), we see that since $x_j \in [0, \sqrt{m} - 1]$, then by hypothesis

$$\left|F_{\Delta,1}(x_j)\right| = \frac{Q_j Q_{j-1}}{4} \tag{3.20}$$

is prime for $j = 1, 2, \ldots, \ell(\alpha)$. In particular, $Q_1 = 2p$ for a prime p, and $Q_1 Q_2 = 4q$ for a prime q. However, since Q_j is even for all j by (2.18), then $Q_2 = 2$, and $Q_1 = 2q$ is the only possibility. Thus, $\ell(\alpha) = 2$, so $p = q$ and $Q_1 = Q_2$. By the same argument as in the proof of Theorem 3.3, $\Delta = p^2 + 4p = (p + 2)^2 - 4$.

By virtually the same argument as used in the proof of Theorem 3.3, we get $h_\Delta = 1$. However, by Corollary 3.12, the values of Δ are those in the list (3.18).

Lastly, we may assume that $\ell(\alpha) = 1$, namely, $\Delta = P_1^2 + 4$. Again, by the same argument as used in the proof of Theorem 3.3, we get that $P_1 = p$, a prime, and $h_\Delta = 1$. Thus, by Corollary 3.10, the values are those in the list (3.19). □

Putting Theorems 3.3 and 3.13 together, we get an (unconditional) update on the Rabinowitsch-Mollin-Williams Theorem as follows. This is a complete determination of all narrow Richaud-Degert types with class number 1, for which there exist exactly 14 Rabinowitsch polynomials, based upon the recent solution of the Chowla, Mollin, and Yokoi conjectures in Lemmas 3.1–3.11. Note as well that in both [7, 17] it is proved there are only finitely many Rabinowitsch polynomials f_m.

We list the 14 values (of narrow Richaud-Degert types) *unconditionally* in Theorem 3.14, whereas the remaining list of four wide Richaud-Degert types is complete with one possible exception, whose existence would be a counterexample to the GRH. We list the 18 Rabinowitsch polynomials below, excluding the degenerate case of $\Delta = 9$ which is included in the 14 values in [7].

Note, as well, that although the original Theorem 1.1 only considers the values of $x \in [1, \sqrt{m}]$, and Theorem 3.13 considers $x \in [0, \sqrt{m} - 1]$, the value of the Rabinowitsch polynomials therein also has $|f_m(\lfloor\sqrt{m}\rfloor)|$ being 1 or prime as well. The restriction in Theorem 3.13 for the range of x values was made to be in synch with the setup in [6, 7] in order to correct and complete their results. Hence, the following is indeed an update and an unconditional rendering of the original.

Theorem 3.14 (Rabinowitsch-Mollin-Williams updated). *If* $\Delta = 4m + 1$, $m \neq 2$, *then the followings are equivalent.*

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

(b) $h_\Delta = 1$ *and* Δ *is one of the following forms:*

  (i) $n^2 - 4$ *for some* $n \in \mathbb{N}$,
  (ii) $p^2 + 4$ *for a prime* $p > 2$,
  (iii) $4p^2 + 1$ *for a prime* p.

(c) $\Delta \in \{5, 13, 17, 21, 29, 37, 53, 77, 101, 173, 197, 293, 437, 677\}$.

Remark 3.15. This remark is provided for the sake of completeness and explaining details in extending the results in [7]. Therein the authors missed all of the values 21, 77, and 437. The value 21 is of their type (iii) with, in their notation, $x_0 = 0$, $n = -1$, $t = 2$, and $m = 5$, so the corresponding Rabinowitsch polynomial is

$$f_5(x) = x^2 + x - 5 \quad \text{which is prime for } x \in [0,1] = [x_0, x_0 + t - 1]. \tag{3.21}$$

The value 77 is of type (iii) with $x_0 = 0$, $n = -1$, $t = 4$, and $m = 19$, with Rabinowitsch polynomial

$$f_{19}(x) = x^2 + x - 19 \quad \text{being prime for } x \in [0,3] = [x_0, x_0 + t - 1]. \tag{3.22}$$

Indeed, $f_{19}(x)$ is prime or 1 for all $x \in [0,9]$ or three times the length. Lastly, 437 is of type (iii) with $x_0 = 0$, $n = -1$, $t = 10$, and $m = 109$, with

$$f_{109}(x) = x^2 + x - 109 \quad \text{which is 1 or prime for } x \in [0,9] = [x_0, x_0 + t - 1]. \tag{3.23}$$

Again, here $f_{109}(x)$ is 1 or prime for triple the length, namely, for $x \in [0,27]$. These 14 values are exactly the values listed in [4, Table 4.2.3, page 139], after the statement of the Rabinowitsch-Mollin-Williams Theorem therein. Also in the following we capture the remaining values from [7] and others they missed.

The following deals with wide Richaud-Degert types and captures the balance of the values using the Euler-Rabinowitsch polynomial $F_{\Delta,p}(x)$ for a prime p dividing Δ. Recall that $h_\Delta = 1$ for a composite Δ can occur only if $\Delta = pq$, where $p \equiv q \equiv 3 \pmod 4$, are primes.

In [4, Conjecture 4.2.1, page 140], we provided the following conjecture for wide Richaud-Degert types that remains open.

Conjecture 1. *If $\Delta = pq \equiv 5 \pmod 8$, where $p \equiv q \equiv 3 \pmod 4$, are primes with $p < q$, then the following are equivalent.*

(a) $|F_{\Delta,p}(x)|$ *is* 1 *or prime for all* $x \in [0, (\sqrt{\Delta} - 2)/4]$.

(b) $\Delta = p^2 s^2 \pm 4p$ *of* $\Delta = 4p^2 s^2 - p$ *for some* $s \in \mathbb{N}$ *and* $h_\Delta = 1$.

Remark 3.16. We have a list of values for Conjecture 1, which as above, we know is valid with one possible GRH-ruled-out exception. It is

$$\Delta \in \{33, 69, 93, 141, 213, 237, 413, 453, 573, 717, 1077, 1133, 1253, 1293, 1757\}. \tag{3.24}$$

The use of $F_{\Delta,p}(x)$ is much less demanding than the use of $f_m(x)$, and the lone two values found in [7] attest to this. However, they missed two other values for $f_m(x)$ that we now provide and we are able to pose a new conjecture on the basis of it, which does not appear in literature thus far.

Table 1

Δ	m	$[x_0, y_0]$	Values of $\lvert f_m(x)\rvert$ for $x \in [x_0, y_0]$
5	1	[0,1]	1,1
13	3	[0,1]	3,1
17	4	[1,2]	2,2
21	5	[0,2]	5,3,1
29	7	[0,2]	7,5,1
37	9	[1,3]	7,3,3
53	13	[0,3]	13,11,7,1
69	17	[2,5]	17,5,3,13
77	19	[0,4]	19,17,13,7,1
93	23	[2,5]	17,11,3,7
101	25	[1,5]	23,19,13,5,5
173	43	[0,6]	43,41,37,31,23,13,1
197	49	[1,7]	47,43,37,29,19,7,7
293	73	[0,8]	73,71,67,61,53,43,31,17,1
413	103	[4,13]	83,73,61,47,31,13,7,29,53,79
437	109	[0,10]	109,107,103,97,89,79,67,53,37,19,1
677	169	[1,13]	167,163,157,149,139,127,113,97,79,59,37,13,13
1133	283	[6,21]	241,227,211,193,173,151,127,101,73,43,11, 23,59,97,137,179

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

$$\Delta = 9p^2 \pm 4p \quad \text{for an odd prime } p,\ h_\Delta = 1. \tag{3.25}$$

Moreover, the only values for which (3.25) *holds are*

$$\Delta \in \{69, 93, 413, 1133\}. \tag{3.26}$$

By the above discussion, we know that the list (see Table 1) in (3.26) is complete with one possible GRH-ruled-out exception. The wide Richaud-Degert values missed in [7] are $\Delta = 69$ and $\Delta = 93$. We now have a complete list of the 18 Rabinowisch polynomials with one possible exception on the wide Richaud-Degert types, where we exclude $\Delta = 9$ for reasons given above. If we included the latter then the corrected list in [7] grows from 14 to 19 values.

Remark 3.17. After the writing of this paper Anitha Srinivasan informed me that, in an unpublished manuscript, she has proved Conjecture 2. Thus, we will address this and other matters in later joint work.

Acknowledgments

The author gratefully acknowledges the support of NSERC Canada Grant no. A8484. Moreover, thanks go to the referee for suggestions that led to the clarification, increased readability, and streamlining of the presentation.

References

[1] G. Rabinowitsch, "Eindeutigkeit der zerlegung in primzahlfaktoren in quadratischen Zahlkörpern," *Journal für die Reine und Angewandte Mathematik*, vol. 142, pp. 153–164, 1913.

[2] R. A. Mollin and H. C. Williams, "On prime valued polynomials and class numbers of real quadratic fields," *Nagoya Mathematical Journal*, vol. 112, pp. 143–151, 1988.

[3] R. A. Mollin and H. C. Williams, "Prime producing quadratic polynomials and real quadratic fields of class number one," in *Théorie des Nombres (Quebec, PQ, 1987)*, pp. 654–663, de Gruyter, Berlin, Germany, 1989.

[4] R. A. Mollin, *Quadratics*, CRC Press Series on Discrete Mathematics and Its Applications, CRC Press, Boca Raton, Fla, USA, 1996.

[5] R. A. Mollin, "An elementary proof of the Rabinowitsch-Mollin-Williams criterion for real quadratic fields," *Journal of Mathematical Sciences*, vol. 7, no. 1, pp. 17–27, 1996.

[6] D. Byeon and H. M. Stark, "On the finiteness of certain Rabinowitsch polynomials," *Journal of Number Theory*, vol. 94, no. 1, pp. 219–221, 2002.

[7] D. Byeon and H. M. Stark, "On the finiteness of certain Rabinowitsch polynomials. II," *Journal of Number Theory*, vol. 99, no. 1, pp. 177–180, 2003.

[8] R. A. Mollin, "Necessary and sufficient conditions for the class number of a real quadratic field to be one, and a conjecture of S. Chowla," *Proceedings of the American Mathematical Society*, vol. 102, no. 1, pp. 17–21, 1988.

[9] D. Byeon, M. Kim, and J. Lee, "Mollin's conjecture," *Acta Arithmetica*, vol. 126, no. 2, pp. 99–114, 2007.

[10] R. A. Mollin, *Fundamental Number Theory with Applications*, Discrete Mathematics and Its Applications, Chapman & Hall/CRC, Taylor and Francis, Boca Raton, Fla, USA, 2nd edition, 2008.

[11] R. A. Mollin, *Algebraic Number Theory*, Discrete Mathematics and Its Applications, Chapman & Hall/CRC, Taylor and Francis, Boca Raton, Fla, USA, 1999.

[12] R. A. Mollin, *Fundamental Number Theory with Applications*, Chapman & Hall/CRC, Taylor and Francis, Boca Raton, Fla, USA, 1st edition, 1998.

[13] 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," *Canadian Journal of Mathematics*, vol. 44, no. 4, pp. 824–842, 1992.

[14] A. Biró, "Chowla's conjecture," *Acta Arithmetica*, vol. 107, no. 2, pp. 179–194, 2003.

[15] P. Ribenboim, *The Book of Prime Number Records*, Springer, New York, NY, USA, 1988.

[16] A. Biró, "Yokoi's conjecture," *Acta Arithmetica*, vol. 106, no. 1, pp. 85–104, 2003.

[17] J.-C. Schlage-Puchta, "Finiteness of a class of Rabinowitsch polynomials," *Archivum Mathematicum*, vol. 40, no. 3, pp. 259–261, 2004.