

# Proof of the Mollin-Srinivasan Conjecture and Other Class Number problems\*

R.A. Mollin<sup>†</sup> and A. Srinivasan<sup>‡</sup>

## Abstract

We prove the Mollin-Srinivasan conjecture posed in [10] 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.

## 1 Introduction

In [10], 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 [10] that we prove herein and we look at more general Euler-Rabinowitsch polynomials than those considered in [10]. This allows us to get both class number one and two results that extend results in the literature.

## 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 [6].

---

\*Mathematics Subject Classification 2000: Primary: 11R11 ; Secondary: 11R29; 11C08; 11D09; 11Y65. Key words and phrases: Class numbers; real quadratic fields; prime-producing polynomials; continued fractions.

<sup>†</sup>Department of Mathematics and Statistics, University of Calgary – email address: [ramollin@math.ucalgary.ca](mailto:ramollin@math.ucalgary.ca) – URL: <http://www.math.ucalgary.ca/~ramollin/>

<sup>‡</sup>Department of Mathematics, Siddhartha college, (affiliated to Mumbai University), India – email address: [rsrinivasan.anitha@gmail.com](mailto:rsrinivasan.anitha@gmail.com)

We will be concerned, in the next section, with the simple continued fraction expansions of  $\sqrt{D}$ , where  $D$  is an integer that is not a perfect square. We denote this expansion by,

$$\sqrt{D} = \langle q_0; \overline{q_1, q_2, \dots, q_{\ell-1}, 2q_0} \rangle,$$

where  $\ell = \ell(\sqrt{D})$  is the period length,  $q_0 = \lfloor \sqrt{D} \rfloor$  (the *floor* of  $\sqrt{D}$ ), and  $q_1 q_2, \dots, q_{\ell-1}$  is a palindrome, namely for  $1 \leq j \leq \ell - 1$

$$q_j = q_{\ell-j}. \quad (2.1)$$

The  $j$ th *convergent* of  $\sqrt{D}$  for  $j \geq 0$  is given by,

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

where

$$A_j = q_j A_{j-1} + A_{j-2}, \quad (2.2)$$

$$B_j = q_j B_{j-1} + B_{j-2}, \quad (2.3)$$

with  $A_{-2} = 0$ ,  $A_{-1} = 1$ ,  $B_{-2} = 1$ ,  $B_{-1} = 0$ . The *complete quotients* are given by,  $(P_j + \sqrt{D})/Q_j$ , where  $P_0 = 0$ ,  $Q_0 = 1$ , and for  $j \geq 1$ ,

$$P_{j+1} = q_j Q_j - P_j, \quad (2.4)$$

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

and

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

We will also need the following facts (which can be found in most introductory texts in number theory, such as [9]. Also, see [6] for a more advanced exposition).

$$A_j B_{j-1} - A_{j-1} B_j = (-1)^{j-1}. \quad (2.6)$$

Also,

$$A_{j-1}^2 - B_{j-1}^2 D = (-1)^j Q_j. \quad (2.7)$$

In particular,

$$A_{\ell-1}^2 - B_{\ell-1}^2 D = (-1)^\ell. \quad (2.8)$$

There are also symmetry properties that we will need. For instance, if  $0 \leq j < \ell$ , then

$$Q_{\ell-j} = Q_j. \quad (2.9)$$

Also, for any  $0 \leq j < \ell$ ,

$$P_{j+1} = P_{\ell/2-j}. \quad (2.10)$$

In particular, if  $\ell$  is even, then by Equation (2.4),

$$Q_{\ell/2} \mid 2P_{\ell/2}, \quad (2.11)$$

where  $Q_{\ell/2}$  is called the *central norm*, (via Equation (2.7)), where

$$Q_{\ell/2} \mid 2D. \quad (2.12)$$

In fact the following is important for our work in the next section.

**Lemma 2.1** *If  $D > 1$  is not a perfect square, then  $Q_j \mid 2D$  for  $0 < j < \ell(\sqrt{D})$  in the simple continued fraction expansion of  $\sqrt{D}$  if and only if  $j = \ell/2$ .*

*Proof.* See [6, Theorem 6.1.4, p. 193]. □

In general, the values  $Q_j$  are called the *principal norms*, since they are the norms of the principal reduced ideals in the order  $\mathbb{Z}[\sqrt{D}]$ , due to the association between the simple continued fraction expansion of  $\sqrt{D}$  and the infrastructure of the underlying real quadratic order that we now develop. Typically in what follows,  $\Delta = 4D$  as will be case in the next section. For the general scenario, see [6, Section 1.5, pp. 23–30].

**Definition 2.1** *Let  $\alpha = (P + \sqrt{\Delta})/Q$  be a quadratic irrational. If  $\alpha > 1$  and  $-1 < \alpha' < 0$ , then  $\alpha$  is called reduced.*

The next result sets the stage for our primary discussion.

**Theorem 2.1** *Let  $\alpha = \langle q_0; q_1, \dots \rangle$  be an infinite simple continued fraction, with  $\ell(\alpha) = \ell \in \mathbb{N}$ . Then  $\alpha$  is purely periodic if and only if  $\alpha$  is reduced.*

*Proof.* See [9, Theorem 5.12, p. 228].  $\square$

Now we link continued fractions with ideals in the ring of integers of  $\mathbb{Q}(\sqrt{\Delta})$ . Since we will be concerned primarily with the case where  $\Delta \not\equiv 1 \pmod{4}$ , then we specialize to that case now. The ring of integers of  $\mathbb{Q}(\sqrt{\Delta})$ , in this case, is

$$\mathcal{O}_\Delta = \mathbb{Z} \left[ \sqrt{\Delta} \right].$$

An ideal in  $\mathcal{O}_\Delta$  is denoted by

$$I = \left[ a, \frac{b + \sqrt{\Delta}}{2} \right],$$

where  $b^2 \equiv \Delta \pmod{4a}$ . The value  $a$  is called the *norm of  $I$*  and is denoted by  $N(I) = a$ . Hence, we see that, to each quadratic irrational,  $\alpha = (P + \sqrt{\Delta})/Q$ , there corresponds an  $\mathcal{O}_\Delta$ -ideal,  $I = [Q/2, (P + \sqrt{\Delta})/2]$ . We denote this ideal by  $[\alpha] = I$  and write  $\ell(I)$  for  $\ell(\alpha)$ .

Note that the notion of reduction for quadratic irrationals translates to ideals, namely  $I = [a, (b + \sqrt{\Delta})/2]$  is *reduced* if and only if there is a  $\beta \in I$  such that  $I = [N(I), \beta]$  with  $\beta > N(I)$  and  $-N(I) < \beta' < 0$ .

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.

**Theorem 2.2** *Let  $I = I_1 = [Q_0/2, (P_0 + \sqrt{\Delta})/2]$  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 above. 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 [6, Theorem 2.1.2, p. 44].  $\square$

**Corollary 2.1** *A reduced ideal  $I = [Q/2, (P + \sqrt{\Delta})/2]$  of  $\mathcal{O}_\Delta$  is principal if and only if  $Q = Q_j$  for some positive integer  $j \leq \ell(\alpha)$  in the continued fraction expansion of  $\alpha$ .*

*Proof.* See [5].  $\square$

### 3 Prime-Producing Euler-Rabinowitsch Polynomials

Let  $\Delta > 1$  be a positive integer and  $q \in \mathbb{N}$  a square-free divisor of  $\Delta$ , and set

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

if  $4q$  does not divide  $\Delta$ , and

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

if  $4q \mid \Delta$ .  $F_{\Delta,q}(x)$  is called the *Euler-Rabinowitsch polynomial*, which was introduced by this 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*. We now show how all Rabinowitsch polynomials for  $q = 2$  may be determined. The following generalize results obtained in [6, Theorems 4.2.5], where an assumption was made that we show below is not necessary. Furthermore, the result below is more specific.

**Theorem 3.1** *Suppose that  $\Delta = 4(4m + 3) = 4D$  for  $m$  a nonnegative integer. If*

$$|F_{\Delta,2}(x)| = |2x^2 + 2x - 2m - 1|$$

*is prime for all  $x \in [0, \sqrt{m}]$ , then  $D$  is square-free, and one of the following holds.*

- (i)  $D = \lfloor \sqrt{D} \rfloor^2 + 2$  is prime,  $\ell(\sqrt{D}) = 2$ ,  $h_\Delta = 1$ , and there are no split primes  $p < \sqrt{D}$ .
- (ii)  $D = (\lfloor \sqrt{D} \rfloor + 1)^2 - 2$  is prime,  $\ell(\sqrt{D}) = 4$ ,  $h_\Delta = 1$ , and  $p = 2\lfloor \sqrt{D} \rfloor - 1$  is the only split prime less than  $\sqrt{\Delta}$ .
- (iii)  $D = p^2 + 2p = (2p + 1)^2 - 1$  where  $p$  and  $p + 2$  are primes,  $h_\Delta = 2$ , and  $\ell(\sqrt{D}) = 2$ .

*Also, the only values, with one possible exception, for which the (i) holds are*

$$\Delta \in \{3, 11, 83, 227\}, \quad (3.13)$$

*the only values, with one possible exception, for which the (ii) holds are*

$$\Delta \in \{7, 23, 47, 167\}, \quad (3.14)$$

and the only values, unconditionally, for which (iii) holds are

$$\Delta \in \{15, 35, 143\}. \quad (3.15)$$

*Proof.* Clearly,  $D$  is not a square since  $D \equiv 3 \pmod{4}$ . Thus,  $\sqrt{D}$  may be used for continued fraction expansions. 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  $(r-1)/2 < (\sqrt{D}-1)/2 < \sqrt{m}$ , then by hypothesis  $r = 1$ , so  $D$  has no non-trivial square factor.

Observe that by (2.8),  $\ell = \ell(\sqrt{D})$  must be even. 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  $0 < (p-1)/2 \leq \sqrt{m}$ , then  $s = p+2$ , but the period length of  $D = p^2 + 2p$  are well known to be  $\ell = 2$  and  $Q_{\ell/2} = 2p$ —see [6, Theorem 3.2.1, p.78]. In this case, since  $(p+1)/2 < \sqrt{m}$  and

$$|F_{\Delta, 2}((p+1)/2)| = p+2,$$

so by hypothesis,  $p+2$  must be prime. Moreover, the hypothesis implies that  $h_{\Delta} = 2$  by [8, Theorem 3.3, p. 569], since any non-inert prime  $q < p = \lfloor D \rfloor$  with  $q \neq 2, p$  must have a principal  $\mathcal{O}_{\Delta}$ -ideal above it by [6, Lemma 4.1.4, p. 118]. (Recall that  $\mathcal{C}_{\Delta}$  is generated by the non-inert primes with norm less than  $\sqrt{\Delta}/2$ —see [6, Theorem 1.31., p. 15]. Also, observe that the  $\mathcal{O}_{\Delta}$ -prime over 2 is not principal in our case by Corollary 2.1, given that  $Q_0 = Q_2 = 1$  and  $Q_1 = 2p$ .) Furthermore, by [4], the only values, *unconditionally*, are given in the list (3.15). This is (iii).

Hence, we may assume that  $D$  is prime. Since  $Q_{\ell/2} \mid 2D$  by (2.12), then for any odd prime  $r \mid Q_{\ell/2}$ ,  $r \mid P_{\ell/2}$  by (2.11), so  $r \mid D$ . However,  $D$  is prime so  $D = r$ , a contradiction since  $Q_{\ell/2} < 2\sqrt{D}$  by (2.5) and (2.12). This forces  $Q_{\ell/2} = 2$ .

**Case 3.1** Suppose that  $P_1 = 2x_1$  for some  $x_1 \geq 1$ .

By (2.5),

$$D = P_1^2 + Q_1.$$

Therefore,  $Q_1 > 1$  is odd. By [6, Theorem 5.4.9, p. 183] there cannot be any split primes less than  $\sqrt{D}/2$ , so any prime  $p$  dividing  $Q_1$  must be larger than  $\sqrt{D}/2$ , given that any prime dividing  $Q_j$  for any  $j$  must be split by (2.5). However, by [6, Lemma 4.1.2, p. 118],  $p \mid F_{\Delta,2}(x)$  for some  $x < (\sqrt{D} - 1)/2 < \sqrt{m}$ . Thus, by hypothesis,

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

so

$$D = (2x + 1)^2 + 2p. \quad (3.16)$$

However,

$$D = P_1^2 + Q_1 = P_1^2 + p, \quad (3.17)$$

by (2.5). Equating (3.16)–(3.17), 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  $D = (2x + 3)^2 - 2$ . However, by [6, Theorem 3.2.1, p.78],  $\ell = 4$ . Thus,  $p = 2\lfloor \sqrt{D} \rfloor - 1$  is the only split prime less than  $\sqrt{\Delta}$ . Moreover, from [11] the only values, with one GRH-ruled-out exception, are given in the list (3.19). This is (ii).

**Case 3.2** *Suppose that  $P_1 = 2x_1 + 1$  for some  $x_1 \geq 0$ .*

Then

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

so  $Q_1 \in \{2, 2p\}$  for a prime  $p > 2$ . Since  $\ell$  is even,  $Q_1 > 1$ . Thus, by Lemma 2.1,  $\ell = 2, 4$  are the only possibilities, with either  $Q_1 = Q_{\ell/2} = 2$  or  $Q_2 = Q_{\ell/2} = 2$ . If  $\ell = 2$ , then

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

and there are no split primes less than  $\sqrt{D}$ . Again, by [11], the only values, with one GRH-ruled-out exception, are given in the list (3.18). This is (i)

We are left with  $\ell = 4$  for which  $Q_2 = 2$ ,  $Q_1 = p = Q_3$ , and  $Q_0 = Q_4 = 1$ . Since  $D = P_1^2 + Q_1 = P_1^2 + p$ , which puts us back into Case 3.1, with which we have already dealt.  $\square$

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

**Theorem 3.2** *Suppose that  $\Delta = 4D \equiv 0 \pmod{8}$  for  $m$  a nonnegative integer. If*

$$|F_{\Delta,2}(x)| = |2x^2 - D|$$

*is prime for all  $x \in [0, \sqrt{D-1}/2]$ , then  $D$  is square-free, and one of the following holds.*

- (i)  $D = p^2 + 1 = 2q$ , 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  $\sqrt{D}$ .
- (ii)  $D = (\lfloor \sqrt{D} \rfloor)^2 + 2 = 2q$ , where  $q \equiv 3 \pmod{4}$  is prime,  $\ell(\sqrt{D}) = 2$ ,  $h_{\Delta} = 1$ , and there are no split primes less than  $\sqrt{D}$ .
- (iii)  $D = \left[\frac{p+3}{2}\right]^2 - 2 = 2q$  where  $q = 2[(p+3)/2]^2 - 1$  is prime,  $p > \sqrt{D}$  is prime,  $h_{\Delta} = 1$ , and  $\ell(\sqrt{D}) = 4$ , and there are no split primes less than  $\sqrt{D}$ .

*Also, the only values, with one possible exception, for which the (i) holds are*

$$\Delta \in \{2, 10, 26, 122, 362\}, \quad (3.18)$$

*the only values, with one possible exception, for which the (ii) holds are*

$$\Delta \in \{6, 38\}, \quad (3.19)$$

*and the only values, with one possible exception, for which (iii) holds are*

$$\Delta \in \{14, 62, 398\}. \quad (3.20)$$

If we extend  $q$  in  $F_{\Delta,q}(X)$  to values bigger than 2, we can achieve all the values of Extended Richaud-Degert type with class group of exponent 2 as observed in [6]. Herein, we have displayed the techniques that extract the specific information about the values of  $\Delta$  using the continued fraction approach. In the next section, we switch gears for the proof of a conjecture left in [10].

## 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  $x \in I = [x_o, x_o + t]$ , we call  $I$  a Rabinowitsch interval. Also  $F_{\Delta,1}(x)$  is called a Rabinowitsch polynomial. 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], several values on their list of “all possible Rabinowitsch polynomials with one-possible exception” were missed and the following, proved in [10, Theorem 3.3], corrected and all Rabinowitsch polynomials with  $[1, t]$  as a Rabinowitsch interval are 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  $\Delta$  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 Rabinowitsch intervals for a given  $\Delta$ . 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 Rabinowitsch interval. Here in Theorem 4.3 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 [10].

**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*

$$h_{\Delta} = 1 \text{ and } \Delta = 9p^2 \pm 4p. \quad (4.21)$$

Moreover, the only values for which (4.21) holds are

$$\Delta \in \{69, 93, 413, 1133\}. \quad (4.22)$$

We prove our results via properties of continued fractions involving  $F_{\Delta,1}(x)$ . we use the continued fraction expansion of  $(1 + \sqrt{D})/2$  which is similar to the development given in Section 2 for  $\sqrt{D}$ —see [6].

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

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

$$|F_{\Delta,1}(x)| = |x^2 + x - m| \text{ is prime for all } x \in I = \left[ \frac{p+1}{2}, \sqrt{m} + \frac{p-1}{2} \right]. \quad (4.23)$$

2.  $h_{\Delta} = 1$  and  $\Delta = 9p^2 \pm 4p$  where  $p = \frac{2t+1}{3}$  is prime.

3. With one GRH-ruled-out exception 2 holds for the values

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

*Proof.* Assume statement 1 holds. Then  $I$  is a Rabinowitsch interval. Also, by [6, Lemma 4.1.2, p. 118], for every split prime  $a < \sqrt{\Delta}/2$ , there is an integer  $x \in [(p+1)/2, (p-1)/2 + \sqrt{m}]$  such that  $|F_{\Delta,1}(x)| \equiv 0 \pmod{a}$ . Since  $I$  is Rabinowitsch, then,  $|F_{\Delta,1}(x)| = a = Q_j$  in the simple continued fraction expansion of  $(1 + \sqrt{D})/2$ , so  $h_{\Delta} = 1$  by Corollary 2.1. It is well known that  $h_{\Delta} = 1$  cannot happen if  $p \equiv q \equiv 1 \pmod{4}$ —see [6, Theorem 1.3.3, p. 16] for instance. Hence,  $p$  and  $q$  are primes with  $p \equiv q \equiv 3 \pmod{4}$ . Thus, by (2.8),  $\ell(\alpha)$  is even where  $\alpha = (1 + \sqrt{\Delta})/2$ .

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  $(p+2)^2 - pq = 2$ , namely  $\Delta = p^2 + 4p \equiv 1 + 4p \equiv 1 \pmod{8}$ , which is impossible since  $p > 2$ . Thus,  $m$  is odd.

By (2.12),  $Q_{\ell/2} \mid 2\Delta$  so  $Q_{\ell/2} = 2p$  is forced. Let  $P_{\ell/2} = 2x_{\ell/2} + 1$ , then

$$|F_{\Delta,1}(x_{\ell/2})| = \left| \frac{(2x_{\ell/2} + 1)^2 - \Delta}{4} \right| = \frac{Q_{\ell/2}Q_{\ell/2-1}}{4}, \quad (4.24)$$

by (2.5). Therefore, since  $Q_{\ell/2} \mid 2P_{\ell/2}$  by (2.11), then  $P_{\ell/2} = px$ . If  $x > 1$ , then  $\lfloor \sqrt{m} \rfloor + (p-1)/2 \geq x_{\ell/2} \geq (p+1)/2$  so  $x_{\ell/2} \in I$ , which forces  $Q_{\ell/2-1} = 2$  by hypothesis, namely  $\ell = 2$ . We have  $x_{\ell/2} = (kp-1)/2$  for some integer  $k$ .

Now since  $P_{\ell/2} = px < \sqrt{\Delta}$  and  $x > 1$  with  $P_{\ell/2}$  odd, then by (2.5),

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

so

$$p < \sqrt{m}.$$

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

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

which is not possible. Hence  $x = 3$  and

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

and  $p = (2t+1)/3$ . This is statement 2 with the plus sign.

Now assume that  $x = 1$ . Now we cannot conclude that  $Q_{\ell/2-1} = 2$  from (4.24). However, if  $\ell = 2$ , then  $\Delta = p^2 + 4p$  and hence  $|F_{\Delta,1}(\frac{p+1}{2})| = 1$ , which is a contradiction. Now assume 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**  $q_{\ell/2-1} = 1$ .

Suppose that  $p > \sqrt{m}$ . Since there exists a  $y \in I$  such that  $y \equiv x_{\ell/2} \pmod{p}$ , then  $y = x_{\ell/2} + zp$  for some  $z \in \mathbb{N}$ . Thus, if  $q = Q_{\ell/2-1}/2$ , then

$$|F_{\Delta,1}(y)| = p = p(z^2p + zp - q),$$

so  $z^2p + zp - q = 1$ . Therefore,  $p \mid (q+1)$ . So there exists a  $w \in \mathbb{N}$  such that  $q+1 = wp \geq 2\sqrt{m}$ , and

$$4m+1 = \Delta = p^2 + 4pq > m + 4\sqrt{m}(2\sqrt{m}-1) = 9m - 4\sqrt{m},$$

which is impossible. Hence  $p < \sqrt{m}$ .

By (2.10),  $p = P_{\ell/2} = P_{\ell/2+1}$ , by (2.1),  $q_{\ell/2-1} = q_{\ell/2+1}$ , and by (2.9),  $Q_{\ell/2-1} = Q_{\ell/2+1}$ . Thus,

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

However, since

$$\Delta = 4m + 1 = p^2 + 2pQ_{\ell/2-1} = p^2 + 2pQ_{\ell/2+1} \leq m + 2\sqrt{m}Q_{\ell/2+1},$$

then

$$Q_{\ell/2+1} \geq \frac{3m+1}{2\sqrt{m}}.$$

Thus if,  $q_{\ell/2-1} \geq 2$ , then

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

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

$$\sqrt{4m^2 + m} \geq 2m + 2,$$

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  $s = Q_{\ell/2-2}/2$

Since  $\Delta = P_{\ell/2-1}^2 + Q_{\ell/2-1}Q_{\ell/2-2}$  and  $p = P_{\ell/2} = Q_{\ell/2-1} - P_{\ell/2-1}$  by Claim 4.1 and (2.4), then

$$\Delta = (Q_{\ell/2-1} - p)^2 + 4rs = (2r - p)^2 + 4rs = p^2 - 4pr + 4r^2 + 4rs. \quad (4.25)$$

Also, since

$$\Delta = p^2 + 2pQ_{\ell/2-1} = p^2 + 4pr, \quad (4.26)$$

then via (4.25)–(4.26), we get  $p = (r + s)/2$ , which is Claim 4.2.

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

Since  $\Delta = P_{\ell/2+1}^2 + 2pQ_{\ell/2+1} = p^2 + 2pQ_{\ell/2+1} = p^2 + 4pr$ , then

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

which secures Claim 4.3.

Now we are ready to establish period length four, namely  $s = 1$ . We have

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

However,

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

and since  $(3p-1)/2 \in I$ , then  $s = 1$ .

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  $r = (4t-1)/3$ . Since

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

it follows that

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

Therefore, since  $P_1 = 2q_0 - 1$ , then

$$\frac{3r-1}{2} = P_1 = 2t - 1,$$

from which we get  $r = (4t-1)/3$ , which is statement 2 with the minus sign.

Next assume statement 2 holds. Let  $x \in [\frac{p+1}{2}, \sqrt{m} + \frac{p-1}{2}]$ . If  $|F_{\Delta,1}(x)| = 1$ , then we have  $\Delta = (2x+1)^2 \pm 4$  which is not possible as  $\Delta = 9p^2 \pm 4p$ . If  $|F_{\Delta,1}(x)|$  is not prime or 1 then it has a prime divisor  $a$  less than  $\sqrt{|F_{\Delta,1}(x)|} \leq t$  (if  $0 < F_{\Delta,1}(x) = x(x+1) - m$  then  $F_{\Delta,1}(x) \leq (2p-1)2p - t^2 \leq t^2$  and if  $0 < -F_{\Delta,1}(x) = m - x^2 - x$  then  $|F_{\Delta,1}(x)| < m < t^2$ ). As  $h_{\Delta} = 1$ , from the continued fraction expansion of  $(1 + \sqrt{\Delta})/2$ , we have  $a = p$ .

Now  $|F_{\Delta,1}(x)| = \left| \frac{(2x+1)^2 - \Delta}{4} \right| \equiv 0 \pmod{p}$ , hence  $2x+1 \equiv 0 \pmod{p}$ , that is  $x = (kp-1)/2$  for some integer  $k$ . Hence  $x = \frac{3p-1}{2}$ . Also  $|F_{\Delta,1}(x)| = \left| \frac{9p^2 - \Delta}{4} \right| = p$  which is prime. Thus  $|F_{\Delta,1}(x)|$  is prime for all  $x \in [\frac{p+1}{2}, \sqrt{m} + \frac{p-1}{2}]$ . This is statement 1. Statement 3 follows from the techniques described in [6].  $\square$

**Remark 4.1** *If  $D = 9p^2 - 4p$ , then  $\ell = 4$  and  $Q_2 = 2p$ , and  $Q_1 = Q_3 = 4p - 2$ . Also, if  $D = 9p^2 + 4p$ , then  $\ell = 2$ , and  $Q_1 = 2p$ , so the class number  $h_{\Delta} = 1$  becomes explicitly clearer. Also, note that the hypothesis assuming (4.23) does not restrict us from finding new values since if  $|F_{\Delta,1}(x)|$  is allowed to equal 1, then by the proof of Theorem 4.3,  $\Delta = p^2 + 4p$  with  $p = 2t + 1$  and that unconditionally, via [1], these are exactly the composite values that appear in part (a) of Theorem 4.2, namely  $\Delta \in \{21, 77, 437\}$ .*

**Acknowledgements:** The first author gratefully acknowledges the support of NSERC Canada grant # A8484.

## 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] Lee, Jungyun, *The complete determination of narrow Richerd-Degert type which is not 5 modulo 8 with class number 2*, J. Number Theory. **129**(2009), no. 3, 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, *When the central norm equals 2 in the simple continued fraction expansion of a quadratic surd*, C.R. Math. Rep. Acad. Canada **26** (2004), 51–54.
- [8] R.A. Mollin, *Continued fractions and class number two*, Internat. J. Math. & Math. Sci. (2001), 565-571.
- [9] R.A. Mollin, **Fundamental Number Theory with Applications, Second Edition**, Chapman and Hall/CRC, Taylor and Francis Group, (2008).
- [10] R.A. Mollin, *The Rabinowitsch-Mollin-Williams Theorem Revisited*, to appear.
- [11] 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.
- [12] R.A. Mollin and H.C. Williams, *On a solution of a class number two problem for a family of real quadratic fields*, in **Computational Number Theory**, de Gruyter, Berlin (1991), 95–101.