

## **IDEAL CLASS GROUPS AND GENERALIZED EULER-RABINOWITSCH POLYNOMIALS**

**RICHARD A. MOLLIN and ANITHA SRINIVASAN**

Department of Mathematics and Statistics  
University of Calgary  
Canada  
e-mail: [ramollin@math.ucalgary.ca](mailto:ramollin@math.ucalgary.ca)  
[rsrinivasan.anitha@gmail.com](mailto:rsrinivasan.anitha@gmail.com)

### **Abstract**

In this work, we present a new criterion for class number 1 or 2 that generalizes previous criteria. In particular, we generalize the Euler-Rabinowitsch polynomial introduced by the first author some twenty years ago. This generalization is utilized to obtain known and new results on class numbers. For instance, Rabinowitsch's famous result on class number 1 for complex quadratic fields is obtained as an immediate consequence. Several results are presented that correct and extend results in the literature.

### **1. 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 [5], or for a more advanced approach in [3].

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

---

Received November 8, 2010

2010 Mathematics Subject Classification: Primary 11R11; Secondary 11R29, 11C08, 11D09, 11Y65.

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

© 2011 Pioneer Scientific Publisher

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

where  $\lfloor \alpha \rfloor$  is the floor of  $\alpha$ , namely the greatest integer less than or equal to  $\alpha$ . 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.

**Definition 1.1.** A real number  $\alpha$  is called a *quadratic irrational* if it is an irrational number which is a root of

$$f(x) = ax^2 + bx + c, \quad (1.1)$$

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

**Remark 1.1.** By the quadratic formula, the roots of (1.1) 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

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

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 1.1.** *A real number  $\alpha$  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*

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

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

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

is called the algebraic conjugate of  $\alpha$ . Here both  $\alpha$  and  $\alpha'$  are the roots of

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

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

**Proof.** See [5, Theorem 5.9, p. 222]. □

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

**Definition 1.2.** A quadratic irrational  $\alpha$  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 1.3.** The infinite simple continued fraction of  $\alpha$  is called *periodic* (sometimes called *eventually periodic*) if there exists an integer  $k \geq 0$  and  $l \in \mathbb{N}$  such that  $q_n = q_{n+l}$ , for all integers  $n \geq k$ . We use the notation

$$\alpha = \langle q_0; q_1, \dots, q_{k-1}, \overline{q_k, q_{k+1}, \dots, q_{l+k-1}} \rangle, \tag{1.2}$$

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

**Theorem 1.2.** 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  $Q_0 \mid (D - P_0^2)$ . Recursively define for any  $j \geq 0$ ,

$$\alpha_j = (P_j + \sqrt{D})/Q_j, \tag{1.3}$$

$$P_{j+1} = q_j Q_j - P_j, \tag{1.3}$$

$$q_j = \left\lfloor \frac{P_j + \sqrt{D}}{Q_j} \right\rfloor, \tag{1.4}$$

and

$$D = P_{j+1}^2 + Q_j Q_{j+1}. \quad (1.5)$$

Then

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

Moreover,  $\alpha$  is periodic and when it is reduced it is purely periodic.

**Proof.** See [5, Theorem 5.10, p. 223]. □

Now, we need to define arbitrary real quadratic orders in which we will work. If  $D_0 \in \mathbb{Z}$  is squarefree, then a *fundamental discriminant*  $\Delta_0$  with *fundamental radicand*  $D_0$  is given by

$$\Delta_0 = \begin{cases} D_0, & \text{if } D_0 \equiv 1 \pmod{4}, \\ 4D_0, & \text{if } D_0 \equiv 2, 3 \pmod{4}. \end{cases} \quad (1.6)$$

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

$$\sigma = \begin{cases} 2, & \text{if } \Delta_0 \equiv 1 \pmod{4} \text{ and } f_\Delta \text{ is odd,} \\ 1, & \text{otherwise.} \end{cases} \quad (1.7)$$

Set

$$\omega_\Delta = \begin{cases} (1 + \sqrt{D})/2, & \text{if } \Delta = D \equiv 1 \pmod{4}, \\ \sqrt{D}, & \text{if } \Delta \equiv 0 \pmod{4}, \end{cases} \quad (1.8)$$

called the *principal surd* associated with  $\Delta$  and

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

is called a *quadratic order* in  $\mathbb{Q}(\sqrt{D_0})$  having conductor  $f_\Delta$  and discriminant  $\Delta$  with associated radicand  $D$ . (The reader unfamiliar with the notions of a general discriminant and radicand may consult [3, Section 1.5, pp. 23–24], for instance.)

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

**Theorem 1.3.** *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  $0 \leq b < a$ . Furthermore,  $I$  is an  $\mathcal{O}_\Delta$ -ideal if and only if this representation satisfies  $c|a$ ,  $c|b$ , and  $ac|N(b + c\omega_\Delta)$ . When  $c = 1$ ,  $I$  is called primitive.

**Proof.** See [3, Theorem 1.2.1, p. 9]. □

**Definition 1.4.** To each quadratic irrational  $\alpha = (P + \sqrt{D})/Q$  there corresponds the primitive  $\mathcal{O}_\Delta$ -ideal

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

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

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

**Definition 1.5.** An  $\mathcal{O}_\Delta$ -ideal is said to be *reduced* if it is primitive and does not contain any non-zero element  $\alpha$  such that both  $|\alpha| < N(I)$  and  $|\alpha'| < N(I)$ .

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 1.4.** 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 1.2 in the continued fraction expansion of  $\gamma = \gamma_0 = (P + \sqrt{D})/Q$ . 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 [3, Theorem 2.1.2, p. 44]. □

**Remark 1.2.** The infrastructure given in Theorem 1.4 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  $I$ .

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

$$\{Q_1/\sigma, Q_2/\sigma, \dots, Q_t/\sigma\}$$

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

We will need the following which determines the generators of the ideal class group  $\mathcal{C}_\Delta$  of  $\mathbb{Q}(\sqrt{\Delta})$  having discriminant  $\Delta$ . 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  $N(\mathcal{P})|\Delta$ .

In what follows the Minkowski bound is given by

$$M_\Delta = \begin{cases} \sqrt{-\Delta/3}, & \text{if } \Delta < 0, \\ \sqrt{\Delta/2}, & \text{if } \Delta > 0. \end{cases}$$

**Theorem 1.5.** *If  $\Delta$  is the discriminant of a quadratic field, then every class of  $\mathcal{C}_\Delta$  contains a primitive ideal  $I$  with  $N(I) \leq M_\Delta$ . Furthermore,  $\mathcal{C}_\Delta$  is generated by the non-inert prime  $\mathcal{O}_\Delta$ -ideals  $\mathcal{P}$  with  $N(\mathcal{P}) < M_\Delta$ .*

**Proof.** See [3, Theorem 1.3.1, p. 15]. □

**Remark 1.3.** We will have occasion to invoke the following concept. The conjugate of an  $\mathcal{O}_\Delta$ -ideal  $I = [a, b + \omega_\Delta]$  is the ideal  $I' = [a, b + \omega'_\Delta]$ . If  $I$  is a primitive ideal and  $I = I'$ , then  $I$  is said to be an *ambiguous ideal*. If  $\mathbf{I} = \mathbf{I}'$ , then  $\mathbf{I}$  is called an *ambiguous class of ideals*. The case where  $\mathbf{I}$  is ambiguous without any ideal in the class being ambiguous, called an ambiguous class of ideals without any ambiguous ideals in it, is of considerable interest in Section 2.

**2. Class Number Two and Ambiguous Ideals**

The following corrects and extends results in the literature-see Remark 2.1 below.

**Theorem 2.1.** *Let  $\Delta = m^2 \pm 4$  with  $m$  odd. Then the following are equivalent.*

(a)  $h_\Delta = 2$ .

(b) *One of the following holds:*

(i)  $\Delta = m^2 + 4 = pq$ , where  $p < q$  are primes,  $\ell((1 + \sqrt{\Delta})/2) = 1$ , and all non-inert primes less than  $\sqrt{\Delta}/2$  appear as some  $Q_j$  for  $1 < j < \ell(\alpha)$  in the simple continued fraction expansion of  $\alpha = \sqrt{\Delta}/p$ , corresponding to an ambiguous ideal class. Also, the only values for which this holds, with one GRH-ruled-out exception are  $\Delta \in \{85, 365, 533, 629, 965, 1685, 1853, 2813\}$ .

(ii)  $\Delta = m^2 - 4 = pqr$ ,  $p < q < r$  with  $p, q, r$  primes,  $\ell((1 + \sqrt{\Delta})/2) = 2$ , and all non-inert primes less than  $\sqrt{\Delta}/2$  appear as some  $Q_j$  for  $1 < j < \ell(\alpha)$  in the simple continued fraction expansion of  $\alpha = \sqrt{\Delta}/p$ , corresponding to an ambiguous class of ideals. Also, the only values for which this holds, with one GRH-ruled-out exception are  $\Delta \in \{165, 285, 357, 957, 1085, 2397\}$ .

(iii)  $\Delta = m^2 - 4 = pq = b^2 + 4 \cdot r^2$ , where  $p < q$  are primes,  $\ell((1 + \sqrt{\Delta})/2) = 2$ , and all non-inert primes less than  $\sqrt{\Delta}/2$  appear as some  $Q_j$  for some  $1 < j < \ell(\gamma)$  in the simple continued fraction expansion of  $\gamma = ((b + \sqrt{\Delta})/(2r))$ . Also, therein,  $r$  is prime and the ideal class of  $[r, (b + \sqrt{\Delta})/2]$  is ambiguous without ambiguous ideals in it. Also, the only values for which this holds, with one GRH-ruled-out exception are  $\Delta \in \{221, 1517\}$ .

**Proof.** By [10, Theorem 3.2, p. 99], part (a) implies the values in part (b) (i)-(iii), with one GRH-ruled-out exception, which are then easily checked, in each case to satisfy each of the conditions. Thus, part (a) implies part (b). Assume part (b) holds. Then since each of the parts (i)-(iii) satisfies the property that all of the

non-inert primes less than  $M_\Delta$  appear in either the simple continued fraction expansion of the principal class or in a nonprincipal ambiguous class, then by Theorem 1.5,  $h_\Delta = 2$ . This completes the result.  $\square$

**Remark 2.1.** The most interesting case in Theorem 2.1 is (b)(iii), which corrects, and completes, [6, Theorem 3.12, p. 298], and [3, Theorem 6.2.3, p. 206], where the erroneous parts were left as exercises. In the case of  $\Delta = 221 = 15^2 - 4 = 13 \cdot 17 = 5^2 + 4 \cdot 7^2$ , we have that  $l = [7, (5 + \sqrt{221})/2]$  is in an ambiguous class without any ambiguous ideals and  $\ell(\gamma) = 4$  for  $\gamma = (5 + \sqrt{221})/14$ . This is precisely where the omissions in [3] and [6] occur since only in this case do we get the ambiguous class without ambiguous ideals in which the split primes, less than the Minkowski bound, sit. Unlike the case with (i)-(ii), the split primes 5 and 7 less than  $\sqrt{\Delta}/2$  appear in the simple continued fraction expansion of an ambiguous class of ideals without any ambiguous ideals in it, corresponding to  $\gamma$ , namely  $Q_0/2 = Q_3/2 = 7$  and  $Q_1/2 = Q_2/2 = 5$ . This is what was missed in [3] and [6].

### 3. Generalized Euler-Rabinowitsch Polynomial

In [2], the first author introduced what he dubbed the  $q$ th Euler-Rabinowitsch polynomial in [3]. We now introduce, for the first time, a generalization of this polynomial, which will allow us to provide extensions of results of Rabinowitsch and others.

**Definition 3.1.** Let  $\Delta \equiv 1 \pmod{4}$  be the discriminant of a quadratic field and let  $r$  be a product of non-inert primes or  $r = 1$ . Then  $\Delta \equiv x^2 \pmod{r}$  and we may select an odd value  $x = x_0 > 0$ . Then  $\Delta = x_0^2 + 4rr'$  for some  $r' \in \mathbb{Z}$ . Then

$$F_{x_0, r}(x) = rx^2 + x_0x - r'$$

is called the *generalized Euler-Rabinowitsch (ER) polynomial*.

**Remark 3.1.** If, in Definition 3.1, we set  $r = x_0 = q \mid \Delta = 1 + 4m$ , then we achieve the  $q$ th Euler-Rabinowitsch polynomial:

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

Also, when  $r = x_0 = 1$ , we have the *Rabinowitsch polynomial* which we completely classified in [7].

The following generalizes [3, Lemmas 4.1.2-4.1.4, p. 118] from the  $q$ th Euler-Rabinowitsch polynomial to the generalized Euler-Rabinowitsch polynomial.

**Lemma 3.1.** *Let  $r$  be a non-inert prime in  $\mathbb{Q}(\sqrt{\Delta})$ , where  $\Delta$  is the discriminant of a quadratic field, or  $r = 1$ . Suppose that  $x_0$  is an odd, positive integer such that  $\Delta \equiv x_0^2 \pmod{r}$ . Then for every  $Q$  such that  $\gcd(r, Q) = 1$  with  $Q$  a product of non-inert primes, there exists an integer  $x$  with  $-x_0/(2r) \leq x \leq Q - x_0/(2r)$  such that  $F_{x_0,r}(x) \equiv 0 \pmod{Q}$ .*

**Proof.** We have  $\Delta \equiv y^2 \pmod{2rQ}$  has a solution. As  $y^2 \equiv \Delta \equiv x_0^2 \pmod{r}$ , we have  $y = x_0 + 2rx$  for some  $x \in \mathbb{Z}$  such that

$$0 \leq y = x_0 + 2rx \leq 2Qr$$

which yields

$$-\frac{x_0}{2r} \leq x \leq Q - \frac{x_0}{2r}.$$

Observe that

$$F_{x_0,r}(x) = rx^2 + x_0x - r' = \frac{(2rx + x_0)^2 - \Delta}{4r},$$

so

$$F_{x_0,r}(x) = \frac{y^2 - \Delta}{4r} \equiv 0 \pmod{Q},$$

as required. □

**Remark 3.2.** In Lemma 3.1, note that if  $0 < x_0 \leq r$ , then the range is  $[0, Q - x_0/(2r)]$ . In the case where  $r = x_0$ , we may take  $-Qr \leq y \leq Qr$ . This yields  $-Qr \leq x_0 + 2rx \leq Qr$ , which gives  $-1/2 - Q/2 \leq x \leq Q/2 = 1/2$ .

The following two results are needed in the sequel as important facts.

**Lemma 3.2.** *If  $1 - 4m = \Delta < -4$  is discriminant of a quadratic field and  $x$  is a non-negative integer, then  $F_{1,1}(x) < N(\omega_\Delta)^2$  if and only if  $x \leq \lfloor \lfloor \Delta \rfloor / 4 - 1 \rfloor$ .*

**Proof.** Since  $F_{1,1}((1 - \Delta)/4) = F_{1,1}(m) = m^2 = ((\Delta - 1)/4)^2 = N(\omega_\Delta)^2$ , and  $F_{1,1}(x)$  is an increasing function for  $x \geq 0$ , we have  $F_{1,1}(x) < N(\omega_\Delta)^2$  if and only if  $0 \leq x \leq \lfloor \lfloor \Delta \rfloor / 4 - 1 \rfloor$ .  $\square$

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

**Proof.** See [3, Theorem 1.3.2, p. 16].  $\square$

**Lemma 3.4.** *Let  $\Delta \equiv 1 \pmod{4}$  be the discriminant of a quadratic field and let  $F_{x_0,r}(x)$  be as given in Definition 3.1. If  $a > 0$  is an integer with  $|F_{x_0,r}(x)| = a$ , where  $x$  is a non-negative integer, then there exist  $\mathcal{O}_\Delta$ -ideals  $\mathcal{A}$  and  $\mathcal{R}$  of norms  $a$  and  $r$ , respectively, such that  $\mathcal{R}^{-1} \sim \mathcal{A}$ .*

**Proof.** Form the ideal  $\mathcal{AR} = [ar, (b + \sqrt{\Delta})/2]$ , where  $b = 2rx + x_0$ . Then

$$\left| N\left(\frac{b + \sqrt{\Delta}}{2}\right) \right| = \left| \frac{4r^2x^2 + 4rxx_0 + x_0^2 - x_0^2 - 4rr'}{4} \right| = |F_{x_0,r}(x)| = ar.$$

Therefore,

$$\mathcal{AR} = \left( \frac{b + \sqrt{\Delta}}{2} \right),$$

so  $\mathcal{AR} \sim 1$ . Thus,  $\mathcal{A} \sim \mathcal{R}^{-1}$ .  $\square$

The following, one of our principal results, is a new class number  $h_\Delta \leq 2$  criterion related to the generalized ER-polynomial.

**Theorem 3.1.** *Let  $r$  be a non-inert prime in  $\mathbb{Q}(\sqrt{\Delta})$ , or  $r = 1$ , where  $\Delta = x_0^2 + 4rr'$  is the discriminant of a quadratic field. If  $|F_{x_0,r}(x)|$  is 1 or prime for all integers  $-x_0/(2r) \leq x \leq M_\Delta - x_0/(2r)$ , then  $h_\Delta = 1, 2$ .*

**Proof.** Let  $Q \neq r$  with  $Q < M_\Delta$  be a non-inert prime. Then by Lemma 3.1, there is an integer  $x$  with  $-x_0/(2r) \leq x \leq Q \leq M_\Delta$  such that

$$|F_{x_0,r}(x)| \equiv 0 \pmod{Q}$$

so by hypothesis,  $|F_{x_0,r}(x)| = Q$ . By Lemma 3.4, if  $\mathcal{R}$  is an  $\mathcal{O}_\Delta$ -ideal over  $r$ , then  $Q \sim \mathcal{R}$  or  $Q \sim \mathcal{R}^{-1}$ , as  $\mathcal{R}$  and  $\mathcal{R}^{-1}$  are the only ideals of norm  $r$ . Hence,  $h_\Delta = 1$  if  $\mathcal{R}$  is principal and  $h_\Delta = 2$  otherwise. □

**Remark 3.3.** If  $r = x_0$ , then by Remark 3.2, the interval for  $x$  in Theorem 3.1 may be taken to be  $-1/2 - M_\Delta/2 \leq x \leq M_\Delta/2 - 1/2$ .

The following improves upon results obtained for Richaud-Degert types found in [9] and expounded in [3]. This is the first using the generalized ER-polynomial for class number one criterion.

**Corollary 3.1.** *Let  $\Delta = x_0^2 \pm 4r$  be the discriminant of a quadratic field such that  $r | x_0$  and  $F_{x_0,r} = rx^2 + x_0x \mp 1$ . Then if  $|F_{x_0,r}(x)|$  is 1 or prime for all integers  $x$  with  $-x_0/(2r) \leq x \leq M_\Delta - x_0/(2r)$ , then  $h_\Delta = 1$ . Furthermore, with one GRH-ruled-out exception, the following values are all for which the above cases hold are given as follows.*

$$\{21, 69, 77, 93, 213, 237, 413, 437, 453, 717, 1077, 1133, 1253\}. \tag{3.9}$$

**Proof.** First, we note that by [3, Theorem 3.2.1, p.78],  $\ell((1 + \sqrt{\Delta})/2) = 2$ , in the case  $\Delta = x_0^2 + 4r$ , and  $\ell((1 + \sqrt{\Delta})/2) = 4$ , in the case  $\Delta = x_0^2 - 4r$ . In either case  $Q_{\ell/2} = r$ , so  $r$  is the norm of a principal ideal. Thus, by Theorem 3.1,  $h_\Delta = 1$ . The list of values in (3.9) is verified as all the class number one of ERD-type, with one GRH-ruled-out exception, in [9] – see also the related [7, Conjecture 1, p. 12].

The completeness of the list (3.9) with one GRH-ruled-out exception is a consequence of [9]. □

The next result involves one direction of a still-outstanding conjecture made in [3, Conjecture 4.2.1, p. 140]. This extends and complements Corollary 3.1.

**Corollary 3.2.** *Suppose that  $\Delta = pq$  with primes  $p \equiv q \equiv 3 \pmod{4}$ , and  $p < q$ . Then if  $|px^2 + px + (q-p)/4|$  is 1 or prime for all  $x \in [0, M_\Delta/2 - 1/2]$ , then  $h_\Delta = 1$ .*

**Proof.** Note that  $F_{p,p}(-y) = F_{p,p}(y-1)$ . Let  $-1/2 - M_\Delta/2 < -y < 0$ , so  $0 < y < M_\Delta/2 + 1/2$  and so  $0 \leq y-1 < M_\Delta/2 - 1/2$ . By hypothesis  $F_{p,p}(y-1)$  is 1 or prime which means  $F_{p,p}(-y) = F(y-1)$  is 1 or prime. Hence,  $F_{p,p}(x)$  is 1 or prime for  $x \in [-1/2 - M_\Delta/2, M_\Delta/2 - 1/2]$ . Therefore, by Theorem 3.1 and Remark 3.3, we have  $h_\Delta = 1$  as  $\mathcal{R} = \mathcal{P}$ , the ideal over  $p$ , is principal. Moreover, with one GRH-ruled-out exception, all of the values for which the above holds are given in

$$\{33, 69, 93, 141, 213, 237, 413, 453, 573, 717, 1077, 1133, 1293, 1757\}. \quad (3.10)$$

**Corollary 3.3.** *If  $1 - 4m = \Delta < 0$  is a discriminant, then  $F_{1,1}(x) = x^2 + x + m$  is prime for all non-negative integers  $x \leq \left\lfloor \frac{|\Delta|}{4} - 1 \right\rfloor$  if and only if  $h_\Delta = 1$ . Moreover, the only values for which this holds are*

$$|\Delta| \in \{3, 4, 7, 8, 11, 12, 19, 28, 43, 67, 163\}. \quad (3.11)$$

**Proof.** Suppose that  $h_\Delta = 1$ . If  $F_{1,1}(x) \equiv 0 \pmod{p}$  for a prime  $p$  and  $x \leq \left\lfloor \frac{|\Delta|}{4} - 1 \right\rfloor$ , then by Lemmas 3.2-3.3,  $F_{1,1}(x) = p$ . Conversely, if the condition holds, as in the proof of Corollary 3.2,  $h_\Delta = 1$ . Lastly the values in (3.11) are well known and an overview of the history may be found in [3].  $\square$

**Remark 3.4.** Note that the largest value in Corollary 3.3 is  $|-163| = -\Delta$  for which we get the celebrated Rabinowitsch polynomial from which all the polynomials derived herein arise, namely,

$$F_{1,1}(x) = x^2 + x + 41$$

which is prime for all integers  $x \in [1, 39]$ .

The following is also of interest in terms of how it is proved with the generalized

Euler-Rabinowitsch polynomial in a way that is reminiscent of the  $q$ th Euler-Rabinowitsch polynomial but different in a rather appealing manner. The following was proved in [8] using the Rabinowitsch polynomial and Rabinowitsch intervals.

**Theorem 3.2** (The Mollin-Srinivasan Theorem). *Let  $\Delta = 1 + 4m$  be the discriminant of a real quadratic field. Then the following are equivalent.*

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

$$|F_{p,1}(x)| = |x^2 + px - (\Delta - p^2)/4|$$

is prime for all  $x \in [1, \sqrt{m}]$ .

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  $p = (2[\sqrt{m}] + 1)/3$  is prime and is the only non-inert prime less than  $\sqrt{\Delta}/2$ .

**Proof.** In [8], the equivalence of part 2 with the following was proved:  $1 + 4m = \Delta = pq$  with  $p < q$  primes and  $|F_{1,1}(x)| = |x^2 + x - m|$  is prime for all  $x \in [(p+1)/2, (p-1)/2 + [\sqrt{m}]]$ . By making the translation  $x \mapsto X + (p-1)/2$ , we get the result. □

As noted in [8], the only values, with one GRH-ruled-out exception, for which Theorem 3.2 holds are given by  $\Delta \in \{9, 93, 413, 1133\}$ . The following table illustrates Theorem 3.2 in terms of our new generalized ER-polynomial.

$\Delta$	$F_{p,1}(x)$	$[1, [\sqrt{m}]]$	values of $ F_{p,1}(x) $ for $x \in [1, [\sqrt{m}]]$
69	$x^2 + 3x - 15$	$[1, 4]$	11, 5, 3, 13
93	$x^2 + 3x - 21$	$[1, 4]$	17, 11, 3, 7
413	$x^2 + 7x - 91$	$[1, 10]$	83, 73, 61, 47, 31, 13, 7, 29, 53, 79
1133	$x^2 + 11x - 253$	$[1, 16]$	241, 227, 211, 193, 173, 151, 127, 101,
			73, 43, 11, 23, 59, 97, 137, 179

#### 4. Criteria via Generalized ER-polynomials

The following substantially generalizes [2, Theorem 3.1, p. 357].

**Theorem 4.1.** *Suppose that each of the following holds.*

(i)  $\Delta = x_0^2 + 4rr'$ , for odd  $x_0 > 0$ , is the discriminant of a quadratic field and  $r$  is prime or  $r = 1$ .

(ii)  $\mathcal{R}$  an  $\mathcal{O}_\Delta$ -ideal of norm  $r$  having order 1 or  $q$  in  $\mathcal{C}_\Delta$ , where  $q$  is prime.

(iii)  $\mathcal{S} = \left\{ \text{primes } p < M_\Delta : \left( \frac{\Delta}{p} \right) \neq -1 \right\}$ .

Then the following are equivalent.

(a) If  $\mathcal{J} \in \mathcal{C}_\Delta$ , then  $\mathcal{J}^q \sim 1$ .

(b) For all  $p \in \mathcal{S}$  with  $p \nmid r$ , there exists an  $x$  with  $-x_0/(2r) \leq x \leq \lfloor M_\Delta - x_0/(2r) \rfloor$  such that

$$|F_{x_0, r}(x)| = |rx^2 + x_0x - r'| = p \cdot r_p,$$

where all ideals of norm  $r_p$  have order 1 or  $q$ .

**Proof.** By Theorem 1.5,  $\mathcal{C}_\Delta$  is generated by the non-inert prime  $\mathcal{O}_\Delta$ -ideals  $\mathcal{P}$  with  $N(\mathcal{P}) = p < M_\Delta$ . If (b) holds, then  $|F_{x_0, r}(x)| = p \cdot r_p$ , satisfying the properties therein. Hence, by Lemma 3.4, there exists an  $\mathcal{O}_\Delta$ -ideal  $\mathcal{R}_p$  such that  $\mathcal{P} \sim \mathcal{R}_p^{-1}$ , so that  $\mathcal{P}^q \sim 1$ , and part (a) follows.

Conversely, if (a) holds, then as above all non-inert prime ideals  $\mathcal{P}$  with  $N(\mathcal{P}) = p < M_\Delta$  generate the class group. Also, by Lemma 3.1, there is an integer  $x$  with  $-x_0/(2r) \leq x \leq \lfloor M_\Delta - x_0/(2r) \rfloor$  such that  $p \mid F_{x_0, r}(x)$  so there is an integer  $r_p \in \mathbb{N}$  such that  $|F_{x_0, r}(x)| = p \cdot r_p$ . Thus, by Lemma 3.4, there exists an  $\mathcal{O}_\Delta$ -ideal  $\mathcal{R}_p$  such that  $\mathcal{R}_p \sim \mathcal{P}^{-1}$ , which is of order 1 or  $q$ . As all ideals have order 1 or  $q$ , (b) holds.  $\square$

**Remark 4.1.** Theorem 3.1 is a special case of Theorem 4.1, where  $r_p = 1$  for all  $p$ .

**Example 4.1.** Let  $\Delta = 285 = 15^2 + 4 \cdot 15$  with  $x_0 = 15 = r$  and  $r' = 1$ . Then  $\mathcal{S} = \{3, 5\}$  has no elements  $p$  with  $p \nmid r$ . Thus, part (b) of Theorem 4.1 is vacuously satisfied and  $F_{x_0,r}(x) = 15x^2 + 15x - 1$  with  $F_{x_0,r}(0) = 1 = p \cdot r_p$ , where  $p = r_p = 1$ . Thus,  $\mathcal{C}_\Delta = \{\Omega_3\} = \{\Omega_5\}$  where  $\Omega_3$ , respectively  $\Omega_5$  is the  $\mathcal{O}_\Delta$ -ideal over 3, respectively, 5. Also note that this example is a counterexample to [1, Theorem 3.1, p. 75], where it is asserted that, for instance, if  $\Delta = 1 + 4m$  and  $q \mid \Delta$ , with  $qx^2 + qx + (q^2 - \Delta)/(4q)$  is 1 or prime for all non-negative integers  $x < \lfloor (M_\Delta - 1)/2 \rfloor$ , then  $\mathcal{C}_\Delta = \{\Omega\}$ , where  $\Omega$  lies over  $q$ . Indeed,  $\mathcal{R} \sim 1$ , where  $\mathcal{R}$  has norm 15. In the case of  $\Delta = 285$ , we do have  $F_{x_0,r}(x)$  prime for all  $x \in [0, \lfloor (M_\Delta - 1)/2 \rfloor] = [0, 3]$ .

The following immediate result from Theorem 4.1 is a new criterion in terms of the generalized Euler-Rabinowitsch polynomial, for the class group to be cyclic, with distinguished generator.

**Corollary 4.1.** Let  $F_{x_0,r}(x)$  be given as in Definition 3.1, where  $r$  is prime, and  $\mathcal{S}$  is as given in Theorem 4.1. Then the following are equivalent.

(a) For every  $p \in \mathcal{S}$ , there exists an integer  $x$  with  $-x_0/(2r) \leq x \leq \lfloor M_\Delta - x_0/(2r) \rfloor$  such that  $|F_{x_0,r}(x)| = p \cdot r_p$  with  $r_p$  prime and  $\mathcal{R}_p \sim \mathcal{R}^j$  for some  $j \geq 0$ , where  $\mathcal{R}_p$  is an  $\mathcal{O}_\Delta$ -ideal over  $r_p$ .

(b)  $\mathcal{C}_\Delta = \langle \mathcal{R} \rangle$ .

The following vastly generalizes [4, Theorems 3.2-3.3, pp. 166-167] as a class number one criterion.

**Corollary 4.2.** If  $\Delta = 1 + 4m$  is the discriminant of a quadratic field, then  $h_\Delta = 1$  if and only if for every prime  $p \in \mathcal{S}$ , there exists a non-negative integer  $x < M_\Delta - 1/2$  such that  $|F_{1,1}(x)| = |x^2 + x - m| = pr_p$ , where all ideals of norm  $r_p$  are principal or  $r_p = 1$ .

**Proof.** This follows from Theorem 4.1 with  $r = x_0 = 1$  and  $m = r'$ .  $\square$

**Example 4.2.** Let  $\Delta = 1985$ , for which

$$S = \{2, 5, 7, 11, 13, 17, 19\}.$$

In the simple continued fraction expansion of  $(1 + \sqrt{\Delta})/2$ , we find that  $Q_7/2 = 11$  and  $Q_3/2 = 19$ . Moreover, in the simple continued fraction expansion of  $(5 + \sqrt{\Delta})/14$ , we have  $Q_{11}/2 = 2$ ,  $Q_{13}/2 = 5$ ,  $Q_0/2 = 7$ ,  $Q_{19}/2 = 13$ , and  $Q_{10}/2 = 17$ . Now with  $r = x_0 = 1$  and  $r' = m = 496$ , since  $|F_{1,1}(x)| = 2 \cdot 5 \cdot 7^2$ ,  $|F_{1,1}(4)| = 4 \cdot 7 \cdot 17$ , and  $|F_{1,1}(11)| = 4 \cdot 7 \cdot 13$ , Theorem 4.1 tells us that  $h_\Delta = 2$ .

#### Acknowledgement

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

#### References

- [1] F. Halter-Kock, Prime-producing quadratic polynomials and class numbers of quadratic orders, Computational Number Theory, A. Pethö, M. Pohst, H. C. Williams, and H. Zimmer, eds., de Gruyter, Berlin, 1991, pp.73-82.
- [2] R. A. Mollin, Ambiguous classes in quadratic fields, Math. Comp. 61(203) (1993), 335-360.
- [3] R. A. Mollin, Quadratics, CRC Press, Boca Raton, London, New York, Washington D. C., 1996.
- [4] R. A. Mollin, New prime-producing quadratic polynomials associated with class number one or two, New York J. Math. 8 (2002), 161-168.
- [5] R. A. Mollin, Fundamental Number Theory with Applications, 2nd ed., Chapman and Hall/CRC Press, Taylor and Francis Group, Boca Raton, London, New York, 2008.
- [6] R. A. Mollin, Class number two for real quadratic fields of Richaud-Degert type, Serdica Math. J. 35(3) (2009), 287-300.
- [7] R. A. Mollin, The Rabinowitsch-Mollin-Williams theorem revisited, Int. J. Math. Math. Sci., Art. ID 819068, (2009), 1-14.

## IDEAL CLASS GROUPS AND GENERALIZED EULER-RABINOWITSCH ...17

- [8] R. A. Mollin and A. Srinivasan. Euler-Rabinowitsch polynomials and class number problems revisited. *Functiones et Approximatio* (to appear).
- [9] R. A. Mollin and H. C. Williams. Solution of the class number one problem for real quadratic fields of extended Richaud-Degert type (with one possible exception). *Number Theory*. R. A. Mollin, ed., Walter de Gruyter, Berlin, New York, 1990, pp. 417-425.
- [10] R. A. Mollin and H. C. Williams, On a solution of a class number two problem for a family of real quadratic fields, *Computational Number Theory*, de Gruyter, Berlin, New York, 1991, pp. 95-101.