REVISTA DE LA UNIÓN MATEMÁTICA ARGENTINA
Vol. 65, No. 1, 2023, Pages 187–196
Published online: June 26, 2023
https://doi.org/10.33044/revuma.2571

PRIME-GENERATING QUADRATIC POLYNOMIALS

VÍCTOR JULIO RAMÍREZ VIÑAS

Abstract. Let a, b, c be integers. We provide a necessary condition for the function $|ax^2 + bx + c|$ to generate only primes for consecutive integers. We then apply this criterion to give sufficient conditions for the real quadratic field $\mathcal{K} = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{N}$, to have class number one, in terms of prime-producing quadratic polynomials.

1. Introduction

For centuries there has been a fascination with prime-producing quadratic polynomials. The best-known polynomial that generates (possibly in absolute value) many consecutive primes is $x^2 - x + 41$, due to Euler, which gives distinct primes for the 40 consecutive integers 1 to 40, namely 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, and 1601. Polynomials like this, which generate long strings of primes, are called *prime-generating quadratic polynomials*. Is there any incredible math hidden within these polynomials? In fact, there is a strong relationship between these polynomials and factorization in quadratic fields. At the 1912 International Congress of Mathematicians, Rabinowitsch gave a proof of the following for imaginary quadratic fields: $n^2 + n + q$ is prime for $n = 0, 1, \ldots, q - 2$ iff the imaginary quadratic field $\mathbb{Q}(\sqrt{1 - 4q})$ has class number equal to 1. By the Heegner–Baker–Stark theorem, one now knows that there are exactly nine complex quadratic fields with class number one. They are $\mathbb{Q}(\sqrt{d})$ for $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$. For surveys of these and related results see, for instance, Mollin [4] and Ribenboim [10].

In 1980, applying Rabinowitsch's method, Kutsuna obtained the following for real quadratic fields: If $-n^2 + n + q$ is prime for all positive $n < \sqrt{q} - 1$, then the class number of the field $\mathbb{Q}(\sqrt{1 + 4q})$ must necessarily be one. Subsequently, there have been many investigations of prime-producing polynomials and their connection to the structure of real quadratic fields. For this matter, we suggest reading Mollin's book [3]. In recent years, Byeon, Lee, and Mollin [2, 5] proved an analogue statement to the Rabinowitsch result for real quadratic fields. Let m be a

2020 *Mathematics Subject Classification.* 11N32, 13A05, 11R29.

Key words and phrases. Prime-generating polynomials, unique factorization domain, class number.

positive integer and let $f_m(x)$ be a polynomial of the form $f_m(x) = x^2 + x - m$. We call a polynomial $f_m(x)$ a *Rabinowitsch polynomial* if, for $t = \lfloor \sqrt{m} \rfloor$ and consecutive integers $x = x_0, x_0+1, \ldots, x_0+t-1$, $|f_m(x)|$ is either 1 or a prime for some integer x_0. They proved the following theorem: $f_m(x)$ is a Rabinowitsch polynomial iff $m \in \{1, 2, 3, 4, 5, 7, 9, 13, 17, 19, 23, 25, 43, 49, 73, 103, 109, 169, 283\}$.

Let $d > 1$ be an integer; let $\alpha = \frac{-1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ and $\alpha = \sqrt{d}$ otherwise. It is straightforward to check that $\alpha^2 \in \mathbb{Z} + \mathbb{Z}\alpha$, so that

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha = \{u + v\alpha : u, v \in \mathbb{Z}\}.$$

We give elementary proofs of the following criteria for unique factorization in $\mathbb{Z}[\alpha]$. We remind the reader that if R is a domain then an *irreducible element* in R is a nonzero, nonunit element $q \in R$ that cannot be written as the product of two non-units in R. A nonzero, nonunit element $\pi \in R$ is called a *prime* if $\pi \mid \alpha\beta$, where $\alpha, \beta \in R$, implies that $\pi \mid \alpha$ or $\pi \mid \beta$. The ring R is said to have the *unique factorization property*, or to be a *unique factorization ring* (unique factorization domain, abbreviated UFD), if every nonzero, nonunit, element in R can be expressed as a product of irreducible elements in exactly one way (where two factorizations are counted as the same if one can be obtained from the other by rearranging the order in which the irreducibles appear and multiplying them by units).

The distinction between primes and irreducibles is needed, because in a ring which is not a UFD these notions are not equivalent. Prime elements are always irreducible; the converse holds in a UFD, but not in general.

Theorem 1.1. *Let $d > 1$, $d \equiv 1 \pmod 4$ be an integer. Let a, b, c and x_0 be integers, with $a > 0$. Let Ω be the set of all primes $p \in \mathbb{N}$ satisfying $p \mid a$. Suppose that $b^2 - 4ac = u^2 d$ for some integer $u \geq 1$. Also suppose that, for every $p \in \Omega$, the equation*

$$4p = |x^2 - dy^2|$$

is solvable in integers x, y. If $|an^2 + bn + c|$ is 1 or a prime for every integer n with $x_0 \leq n \leq x_0 + \sqrt{\frac{d}{5}} - 1$, then $\mathbb{Z}[\frac{-1+\sqrt{d}}{2}]$ is a unique factorization domain.

Theorem 1.2. *Let $d \equiv 2, 3 \pmod 4$ be a positive integer. Let a, b, c and x_0 be integers, with $a > 0$. Let Ω be the set of all primes $p \in \mathbb{N}$ satisfying $p \mid a$. Suppose that $b^2 - 4ac = v^2 d$ for some integer $v \geq 1$. Also suppose that, for every $p \in \Omega$, the equation*

$$4p = |x^2 - dy^2|$$

is solvable in integers x, y. If $|an^2 + bn + c|$ is 1 or a prime for every integer n with $x_0 \leq n \leq x_0 + 2\sqrt{\frac{d}{5}} - 1$, then $\mathbb{Z}[\sqrt{d}]$ is a unique factorization domain.

2. Some preliminaries

Lemma 2.1. *Let d be an integer; let $\alpha = \frac{-1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ and $\alpha = \sqrt{d}$ otherwise. Let p, a, b, c and x_0 be integers, with p prime. Suppose that $b^2 - 4ac = u^2 d$*

for some integer $u \geq 1$. If p is not prime in $\mathbb{Z}[\alpha]$ and $p \nmid a$, then there exists $n \in \mathbb{Z}$ such that

$$x_0 \leq n \leq x_0 + p - 1 \qquad \text{and} \qquad an^2 + bn + c \equiv 0 \pmod{p}.$$

Proof. Let $f(x) = x^2 + x + \frac{1-d}{4}$ if $d \equiv 1 \pmod 4$ and $f(x) = x^2 - d$ otherwise. Since α is a root of the polynomial $f(x)$ and p is not prime in $\mathbb{Z}[\alpha]$, by [8, Lemma 2.3] we get that there exists $t \in \mathbb{Z}$ such that

$$t^2 \equiv d \pmod{p}. \tag{2.1}$$

Now, we distinguish these two cases: $p \neq 2$ and $p = 2$. In the first case we get

$$p \nmid 2a; \tag{2.2}$$

from (2.2) we deduce that there exists $w \in \mathbb{Z}$ such that

$$0 \leq w \leq p - 1 \qquad \text{and} \qquad 2aw \equiv ut - (b + 2ax_0) \pmod{p}. \tag{2.3}$$

Let $n = w + x_0$. Then, from (2.3) we obtain

$$x_0 \leq n \leq x_0 + p - 1 \qquad \text{and} \qquad 2an + b \equiv ut \pmod{p}. \tag{2.4}$$

Since $b^2 - 4ac = u^2 d$, from (2.4) and (2.1), we deduce that

$$\begin{aligned} 4a(an^2 + bn + c) &\equiv (2an + b)^2 - (b^2 - 4ac) \\ &\equiv (2an + b)^2 - u^2 d \equiv (ut)^2 - u^2 d \equiv 0 \pmod{p}. \end{aligned} \tag{2.5}$$

Combining (2.2) and (2.5), we get

$$an^2 + bn + c \equiv 0 \pmod{p}.$$

In the second case, when $p = 2$, we get that a is odd. As p is not prime in $\mathbb{Z}[\alpha]$ and $p = 2$, by [8, Lemma 2.3] we deduce that

$$d \not\equiv 5 \pmod 8.$$

Since $b^2 - 4ac = u^2 d$, it follows that bc is even. Therefore $ax_0^2 + bx_0 + c \equiv 0 \pmod 2$ or $a(x_0 + 1)^2 + b(x_0 + 1) + c \equiv 0 \pmod 2$. □

Proposition 2.2. *Let $d \equiv 1 \pmod 4$ be a positive integer. Suppose that $\mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right]$ is not a unique factorization domain. Then, there is a prime p which is irreducible but not prime in $\mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right]$ such that $p \leq \sqrt{\frac{d}{5}}$.*

Proof. Put $\alpha = \frac{-1+\sqrt{d}}{2}$. Suppose that $\mathbb{Z}[\alpha]$ is not a unique factorization domain. Then by [8, Lemma 2.2], there is a prime p which is not prime in $\mathbb{Z}[\alpha]$ such that

$$\omega \in \mathbb{Z}[\alpha] \quad \text{and} \quad p \mid N(\omega) \qquad \text{implies that} \qquad p^2 \leq |N(\omega)|, \tag{2.6}$$

where N stands for the norm map. Since α is a root of the polynomial $x^2 + x + \frac{1-d}{4}$ and p is not prime in $\mathbb{Z}[\alpha]$, by [8, Lemma 2.3] we get that there exists $a \in \mathbb{Z}$ such that

$$0 \leq a \leq (p-1)/2 \qquad \text{and} \qquad a^2 + a + \frac{1-d}{4} \equiv 0 \pmod{p}. \tag{2.7}$$

Let $c = p - 1 - a$. Then, from (2.7) we obtain

$$c^2 + c + \frac{1-d}{4} \equiv 0 \pmod{p},$$
$$p \leq 2c + 1 \leq 2p - 1. \tag{2.8}$$

As

$$N(c - \alpha) = c^2 + c + \frac{1-d}{4},$$

we get that

$$p \mid N(c - \alpha).$$

From (2.6) we deduce that

$$4p^2 \leq 4|N(c - \alpha)| = |(2c + 1)^2 - d|. \tag{2.9}$$

We now show that

$$|(2c + 1)^2 - d| = d - (2c + 1)^2, \tag{2.10}$$

for otherwise $|(2c + 1)^2 - d| = (2c + 1)^2 - d$. From (2.9) and (2.8), we get

$$4p^2 \leq (2c + 1)^2 - d < (2p)^2 - d,$$

which is impossible. So

$$|(2c + 1)^2 - d| = d - (2c + 1)^2.$$

From (2.9), (2.10), and (2.8), we deduce that

$$4p^2 \leq d - (2c + 1)^2 \leq d - p^2,$$

thus giving

$$p \leq \sqrt{\frac{d}{5}}.$$

To show that p is irreducible in $\mathbb{Z}[\alpha]$, first suppose that it is reducible, i.e., $p = xy$ for some non-units x, y in $\mathbb{Z}[\alpha]$; then $p^2 = N(xy) = N(x)N(y)$ with $|N(x)|, |N(y)| > 1$. Thus,

$$p = |N(x)|. \tag{2.11}$$

Combining (2.6) and (2.11) we get $p^2 \leq p$, which is impossible. This contradiction means that if $p = xy$ in $\mathbb{Z}[\alpha]$ then x or y is a unit in $\mathbb{Z}[\alpha]$, i.e., p is irreducible in $\mathbb{Z}[\alpha]$. □

Proposition 2.3. *Let d be a positive integer. Suppose that $\mathbb{Z}[\sqrt{d}]$ is not a unique factorization domain. Then, there is a prime p which is irreducible but not prime in $\mathbb{Z}[\sqrt{d}]$ such that $p \leq 2\sqrt{\frac{d}{5}}$.*

Proof. Put $\alpha = \sqrt{d}$. Suppose that $\mathbb{Z}[\alpha]$ is not a unique factorization domain. Then, by [8, Lemma 2.2], there is a prime number p which is not prime in $\mathbb{Z}[\alpha]$ such that

$$\omega \in \mathbb{Z}[\alpha] \quad \text{and} \quad p \mid N(\omega) \qquad \text{implies that} \qquad p^2 \leq |N(\omega)|. \tag{2.12}$$

Since α is a root of the polynomial $x^2 - d$ and p is not prime in $\mathbb{Z}[\alpha]$, by [8, Lemma 2.3] we get that there exists $a \in \mathbb{Z}$ such that

$$0 \leq a \leq p/2 \qquad \text{and} \qquad a^2 - d \equiv 0 \pmod{p}. \tag{2.13}$$

Let us see that

$$p \leq 2\sqrt{\frac{d}{5}}.$$

Let $b = a - p$. Then, from (2.13) we obtain

$$b^2 - d \equiv 0 \pmod{p} \tag{2.14}$$

and

$$\frac{p}{2} \leq -b \leq p. \tag{2.15}$$

As

$$N(b - \alpha) = b^2 - d,$$

from (2.14) and (2.12) we deduce that

$$p^2 \leq |N(b - \alpha)| = |b^2 - d|. \tag{2.16}$$

Combining (2.16) and (2.15), we get

$$|b^2 - d| = d - b^2. \tag{2.17}$$

From (2.16), (2.17), and (2.15), we deduce that

$$4p^2 \leq 4d - (2b)^2 \leq 4d - p^2,$$

thus giving

$$p \leq 2\sqrt{\frac{d}{5}}.$$

To show that p is irreducible in $\mathbb{Z}[\alpha]$, first suppose that it is reducible, i.e., $p = xy$ for some non-units x, y in $\mathbb{Z}[\alpha]$; then $p^2 = N(xy) = N(x)N(y)$ with $|N(x)|, |N(y)| > 1$. Thus,

$$p = |N(x)|. \tag{2.18}$$

Combining (2.12) and (2.18) we get $p^2 \leq p$, which is impossible. This contradiction means that if $p = xy$ in $\mathbb{Z}[\alpha]$, then either x or y is a unit in $\mathbb{Z}[\alpha]$, i.e., p is irreducible in $\mathbb{Z}[\alpha]$. □

3. Proof of Theorem 1.1

Put $\alpha = \frac{-1+\sqrt{d}}{2}$. Let us see that $\mathbb{Z}[\alpha]$ is a unique factorization domain. Assume otherwise. Then, by Proposition 2.2, there is a prime p which is irreducible but not prime in $\mathbb{Z}[\alpha]$ such that

$$p \leq \sqrt{\frac{d}{5}}. \tag{3.1}$$

We claim that $p \nmid a$. Indeed, suppose that $p \in \Omega$. Then according to our hypothesis there exist integers r and s such that

$$4p = |r^2 - ds^2|. \tag{3.2}$$

Now, let $t = \frac{r-s}{2}$ and let $\beta = t - s\alpha$. Then from (3.2) we get that t is an integer and

$$p = |N(\beta)|,$$

which is impossible because p is irreducible in $\mathbb{Z}[\alpha]$. We thus have that

$$p \nmid a.$$

Since $b^2 - 4ac = u^2 d$ and p is not prime in $\mathbb{Z}[\alpha]$, by Lemma 2.1 we get that there exists $n \in \mathbb{Z}$ such that

$$x_0 \leq n \leq x_0 + p - 1 \tag{3.3}$$

and

$$an^2 + bn + c \equiv 0 \pmod{p}. \tag{3.4}$$

From (3.1) and (3.3), we get

$$x_0 \leq n \leq x_0 + \sqrt{\frac{d}{5}} - 1,$$

and so, according to our hypotheses, $|an^2 + bn + c|$ is 1 or prime. Thus, from (3.4) we get

$$p = |an^2 + bn + c|. \tag{3.5}$$

From (3.5) we deduce that

$$4ap = |(2an + b)^2 - (b^2 - 4ac)| = |(2an + b)^2 - du^2|,$$

hence we get that there exists $\beta \in \mathbb{Z}[\alpha]$ such that

$$ap = |N(\beta)|.$$

As for every $q \in \Omega$ the equation $4q = |x^2 - dy^2|$ is solvable in integers x, y, we get that the equation $q = |N(z)|$ is solvable in $\mathbb{Z}[\alpha]$. Proceeding by induction we deduce, by [9, Theorem 3], that there exists $\gamma \in \mathbb{Z}[\alpha]$ such that

$$p = |N(\gamma)|,$$

which is impossible because p is irreducible in $\mathbb{Z}[\alpha]$. Thus, $\mathbb{Z}[\alpha]$ must be a unique factorization domain. This completes the proof.

4. Proof of Theorem 1.2

Put $\alpha = \sqrt{d}$. Let us see that $\mathbb{Z}[\alpha]$ is a unique factorization domain. Assume otherwise. Then, by Proposition 2.3, there is a prime p which is irreducible but not prime in $\mathbb{Z}[\alpha]$ such that

$$p \leq 2\sqrt{\frac{d}{5}}. \tag{4.1}$$

We claim that $p \nmid a$. Indeed, suppose that $p \in \Omega$. Then according to our hypothesis there exist integers r and s such that

$$4p = |r^2 - ds^2|. \tag{4.2}$$

Now, let $u = \frac{r}{2}$ and $v = \frac{s}{2}$. Then, since $d \equiv 2, 3 \pmod 4$, from (4.2) we get that $u, v \in \mathbb{Z}$ and

$$p = |N(\gamma)|,$$

where $\gamma = u + v\alpha$, which is impossible because p is irreducible in $\mathbb{Z}[\alpha]$. So

$$p \nmid a.$$

Since $b^2 - 4ac = u^2 d$ and p is not prime in $\mathbb{Z}[\alpha]$, by Lemma 2.1 we get that there exists $n \in \mathbb{Z}$ such that

$$x_0 \leq n \leq x_0 + p - 1 \tag{4.3}$$

and

$$an^2 + bn + c \equiv 0 \pmod{p}. \tag{4.4}$$

From (4.1) and (4.3), we get

$$x_0 \leq n \leq x_0 + 2\sqrt{\frac{d}{5}} - 1,$$

and so, according to our hypotheses, $|an^2 + bn + c|$ is 1 or prime. Thus, from (4.4) we get

$$p = |an^2 + bn + c|. \tag{4.5}$$

From (4.5) we deduce that

$$4ap = |(2an + b)^2 - (b^2 - 4ac)| = |(2an + b)^2 - du^2|.$$

Since $d \equiv 2, 3 \pmod 4$ we get that $\beta \in \mathbb{Z}[\alpha]$ and $ap = |N(\beta)|$, where $\beta = \frac{2an+b}{2} + \frac{u}{2}\alpha$. As for every $q \in \Omega$ the equation $q = |x^2 - dy^2| = |N(x + y\alpha)|$ is solvable in integers x, y, proceeding by induction we deduce, by [9, Theorem 3], that there exists $\gamma \in \mathbb{Z}[\alpha]$ such that

$$p = |N(\gamma)|,$$

which is impossible because p is irreducible in $\mathbb{Z}[\alpha]$. Thus, $\mathbb{Z}[\alpha]$ must be a unique factorization domain, which completes the proof.

5. Applications

To show that our conditions are not impossible to use, we present easy proofs of the following seven propositions, which generalize and refine Mollin–Williams' [7, Theorems 3.2, 3.3, and 3.4] and [6, Conjectures 2 and 4]. We remind the reader that the *class number* of a number field is by definition the order of the ideal class group of its ring of integers. Let $\mathcal{K}$ be a number field which is a finite extension field of the rational field $\mathbb{Q}$. If an element α of $\mathbb{C}$ satisfies an algebraic equation $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, where $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$, then α is called an *algebraic integer*. The set of all algebraic integers in $\mathcal{K}$ forms a ring, which is called the *ring of integers* in $\mathcal{K}$. In general, it is not a unique factorization domain. Now let h be the class number of the number field $\mathcal{K}$. It is now well known (see [1, Theorem 12.1.1, p. 300]) that the condition $h = 1$ is equivalent to the unique factorization property on the ring $\mathcal{R}$ of integers in $\mathcal{K}$.

Proposition 5.1. *Let u and x_0 be integers, with u odd. Suppose that $d = 2q$, where q is a prime congruent to 3 (mod 4), and that $|2n^2 - u^2 q|$ is prime or equal to 1 whenever $x_0 \leq n \leq x_0 + 2\sqrt{\frac{d}{5}} - 1$. Then the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$ is equal to one.*

Proof. Clearly $d \equiv 2 \pmod 4$. Also we shall prove that the equation

$$2 = |x^2 - dy^2|$$

is solvable in integers x, y. Since $|2n^2 - u^2 q|$ is 1 or a prime number for every integer n with $x_0 \leq n \leq x_0 + 2\sqrt{\frac{d}{5}} - 1$, by Theorem 1.2 we conclude that the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$ is equal to 1. Now, since q is a prime congruent to 3 (mod 4), according to Walsh [11, Lemma 2.3] we get that the equation

$$1 = |2x^2 - qy^2| \tag{5.1}$$

is solvable in integers x, y. Multiplying both sides of (5.1) by 2 we get

$$2 = 2|2x^2 - qy^2| = |(2x)^2 - dy^2|,$$

and therefore the assertions above follow. □

Proposition 5.2. *Let u and x_0 be integers, with u odd. Suppose that d is a prime congruent to 3 (mod 4), and that $\left|2n^2 + 2n + \frac{1-u^2 d}{2}\right|$ is prime or equal to 1 whenever $x_0 \leq n \leq x_0 + 2\sqrt{\frac{d}{5}} - 1$. Then the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$ is equal to one.*

Proof. By [11, Lemma 2.2] we get that the equation $2 = |x^2 - dy^2|$ is solvable in integers x, y. Thus, by Theorem 1.2, we get that the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$ is equal to one. □

Proposition 5.3. *Let u, x_0 be integers, with u odd. Suppose that $d = pq$, where $p \neq q$ are primes congruent to 3 (mod 4), and that $\left|pn^2 + pn + \frac{p-u^2 q}{4}\right|$ is prime or equal to 1 whenever $x_0 \leq n \leq x_0 + \sqrt{\frac{d}{5}} - 1$. Then the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$ is equal to one.*

Proof. By [11, Lemma 2.4] we get that the equation $p = |x^2 - dy^2|$ is solvable in integers x, y. Thus, by Theorem 1.1, we get that the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$ is equal to 1. □

Lemma 5.4. *Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be algebraic integers. If $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ is a UFD, then the class number of the number field $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is equal to one.*

Proof. Let $\mathcal{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ be the number field and let $\mathcal{R}$ be the ring of integers in $\mathcal{K}$. It is straightforward to check that $\mathbb{Z}[\alpha_1, \ldots, \alpha_n] \subseteq \mathcal{R}$, because $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ are algebraic integers. Now, assume $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ is a UFD; by [1, Theorem 4.2.5, p. 84], we deduce that $\mathbb{Z}[\alpha_1, \ldots, \alpha_n] \supseteq \mathcal{R}$, hence we get that $\mathcal{R} = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$. Consequently, the class number of $\mathcal{K}$ is equal to 1. □

Proposition 5.5. *Let x_0 and d be integers, with $d > 1$, $d \equiv 1 \pmod 4$. Suppose that $d = t^2 \pm p$, where p is an odd prime dividing t. If $\left|pn^2 + pn - \frac{d-p^2}{4p}\right|$ is 1 or prime for every integer n with $x_0 \leq n \leq x_0 + \sqrt{\frac{d}{5}} - 1$, then the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$ is equal to 1.*

Proof. Let $\mathcal{K} = \mathbb{Q}(\sqrt{d})$ be the quadratic field. It is easily checked that $4p = \left|(2t)^2 - d(2)^2\right|$. Thus, by Theorem 1.1, we deduce that $\mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right]$ is a UFD. Therefore, it follows by Lemma 5.4 that the class number of $\mathcal{K}$ is equal to 1. □

Proposition 5.6. *Let x_0 and d be integers, with $d > 1$, $d \equiv 1 \pmod 4$. Suppose that $d = t^2 \pm 4p$, where p is an odd prime dividing t. If $\left|pn^2 + pn - \frac{d-p^2}{4p}\right|$ is 1 or prime for every integer n with $x_0 \leq n \leq x_0 + \sqrt{\frac{d}{5}} - 1$, then the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$ is equal to 1.*

Proof. Let $\mathcal{K} = \mathbb{Q}(\sqrt{d})$ be the quadratic field. It is readily seen that $4p = \left|t^2 - d(1)^2\right|$. Thus, by Theorem 1.1, we deduce that $\mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right]$ is a UFD. Therefore, it follows by Lemma 5.4 that the class number of $\mathcal{K}$ is equal to 1. □

Proposition 5.7. *Let x_0 and d be integers, with $d > 1$, $d \equiv 1 \pmod 4$. If $\left|n^2 + n + \frac{1-d}{4}\right|$ is 1 or prime for every integer n with $x_0 \leq n \leq x_0 + \sqrt{\frac{d}{5}} - 1$, then the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$ is equal to 1.*

Proof. By Theorem 1.1, we deduce that $\mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right]$ is a UFD. Therefore, it follows by Lemma 5.4 that the class number of $\mathbb{Q}(\sqrt{d})$ is equal to 1. □

Remark 5.8. There exist nineteen values of d smaller than 6000 which satisfy the assumption of Proposition 5.7: $(d, x_0) = (5,1)$, $(9,0)$, $(13,1)$, $(17,1)$, $(21,1)$, $(29,1)$, $(37,1)$, $(53,1)$, $(69,2)$, $(77,1)$, $(93,2)$, $(101,1)$, $(173,1)$, $(197,1)$, $(293,1)$, $(413,4)$, $(437,1)$, $(677,1)$, $(1133,6)$.

(a) By the nature of Proposition 5.7, this list may not be exhaustive (since any computer search can only cover finitely many possible values of x_0).

(b) These values of x_0 are not uniquely determined. For example, if we consider the case $d = 677$, and $f(x) = x^2 + x - 169 = x^2 + x + \frac{1-d}{4}$, then $|f(n)|$ is prime for all integers $n \in [x_0, x_0 + 10] = [x_0, x_0 + \lfloor\sqrt{\frac{d}{5}} - 1\rfloor]$, where $x_0 \in \{1, 12, 27\}$.

Proposition 5.9. *Let $d > 1$, $d \equiv 1 \pmod 4$ be an integer. If $\left|n^2 + n + \frac{1-d}{4}\right|$ is 1 or prime for every integer n with $0 \leq n \leq \frac{1}{2}\left(\sqrt{\frac{d}{5}} - 1\right)$, then $\mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right]$ is a unique factorization domain.*

Proof. An easy check shows that

$$(x-1)^2 + (x-1) + \frac{1-d}{4} = (-x)^2 + (-x) + \frac{1-d}{4}$$

and

$$x_0 + \sqrt{\frac{d}{5}} - 1 \leq \frac{1}{2}\left(\sqrt{\frac{d}{5}} - 1\right),$$

with $x_0 = -\left\lfloor \frac{1}{2}\left(\sqrt{\frac{d}{5}} - 1\right)\right\rfloor - 1$. Therefore, the proposition follows from Theorem 1.1 and Lemma 5.4. □

Remark 5.10. There are exactly ten values of d smaller than 6000 which satisfy the assumption of Proposition 5.9:

$$d = 5, 9, 13, 21, 29, 53, 77, 173, 293, 437.$$

Acknowledgments

The author extends his gratitude to the referee for many useful remarks that have led to an improved presentation of the results.

References

[1] Ş. Alaca and K. S. Williams, *Introductory Algebraic Number Theory*, Cambridge Univ. Press, Cambridge, 2004. MR 2031707.

[2] D. Byeon and J. Lee, A complete determination of Rabinowitsch polynomials, *J. Number Theory* **131** (2011), no. 8, 1513–1529. MR 2793892.

[3] R. A. Mollin, *Quadratics*, CRC Press series on discrete mathematics and its applications, CRC Press, Boca Raton, FL, 1996. MR 1383823.

[4] R. A. Mollin, Prime-producing quadratics, *Amer. Math. Monthly* **104** (1997), no. 6, 529–544. MR 1453656.

[5] R. A. Mollin, The Rabinowitsch–Mollin–Williams theorem revisited, *Int. J. Math. Math. Sci.* **2009**, Art. ID 819068, 14 pp. MR 2539701.

[6] R. A. Mollin and H. C. Williams, Prime producing quadratic polynomials and real quadratic fields of class number one, in *Théorie des nombres (Quebec, 1987)*, 654–663, De Gruyter, Berlin, 1989. MR 1024594.

[7] R. A. Mollin and H. C. Williams, Class number one for real quadratic fields, continued fractions and reduced ideals, in *Number Theory and Applications (Banff, 1988)*, 481–496, NATO Adv. Sci. Inst. Ser. C: Math. Phys. Sci., 265, Kluwer, Dordrecht, 1989. MR 1123091.

[8] V. J. Ramírez, A new proof of the unique factorization of $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ for $d = 3, 7, 11, 19, 43, 67, 163$, *Rev. Colombiana Mat.* **50** (2016), no. 2, 139–143. MR 3605643.

[9] V. J. Ramírez, A simple criterion for the class number of a quadratic number field to be one, *Int. J. Number Theory* **15** (2019), no. 9, 1857–1862. MR 4015517.

[10] P. Ribenboim, *The Little Book of Bigger Primes*, second edition, Springer, New York, 2004. MR 2028675.

[11] P. G. Walsh, A note on class number one criteria of Širola for real quadratic fields, *Glas. Mat. Ser. III* **40(60)** (2005), no. 1, 21–27. MR 2195857.

Víctor Julio Ramírez Viñas
Departamento de Matemáticas Puras y Aplicadas, Universidad Simón Bolívar, Venezuela
ramirezv@usb.ve

Received: March 22, 2021
Accepted: January 11, 2022