ON THE STUDY OF THE POLYNOMIAL FUNCTION $px^2 + bx + c$ EXPRESSING PRIME NUMBERS

VÍCTOR JULIO RAMÍREZ VIÑAS

Communicated by Alexandru Zaharescu

Let d be a positive integer, $m = \frac{d-1}{4}$ if $d \equiv 1 \pmod 4$ and $m = d$ otherwise. Let p, b, c and x_0 be integers, where p is a prime. Suppose that $b^2 - 4pc = t^2 d$, for some integer $t \geq 1$, and there exist integers x and y such that $p = |x^2 - dy^2|$. We prove that if $|pn^2 + bn + c|$ is prime or 1 for all integer n with $x_0 \leq n \leq x_0 + \sqrt{\frac{m}{2}} - 1$, then the class number of the field $\mathbb{Q}(\sqrt{d})$ must necessarily be one.

AMS 2010 Subject Classification: 11N32, 11R29, 13A05.

Key words: Unique factorization domain, primes, prime producing polynomial.

1. INTRODUCTION

It has been known for a long time that there exists a close connection between prime producing polynomials and the class number one problem for quadratic fields. Lehmer [2] observed in 1936 that if $x^2 + x + q$ is prime for $x = 0, 1, ..., q-2$, then the class number of the field $\mathbb{Q}(\sqrt{1-4q})$ must necessarily be one. In 1980 Kutsuna [1] proved 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. After this, many authors have studied analogous criteria. For this matter, we refer to the book of Mollin [3].

The aim of this paper is to prove the following theorems:

Theorem 1. *Let $d = 1 + 4m$ be a positive integer. Let p, b, c and x_0 be integers, where p is a prime. Suppose that $\sqrt{\frac{d}{5}}$ is not prime, and that $b^2 - 4pc = u^2 d$, for some integer $u \geq 1$. Suppose that there exist integers r_1, s_1, r_2, s_2 such that*

$$p = |r_1^2 - ds_1^2|, \qquad \delta = |r_2^2 - ds_2^2|,$$

where $\delta = 1$ if m is odd and $\delta = 2$ otherwise. If $|pn^2 + bn + c|$ is prime or 1 for all integers n with $x_0 \leq n \leq x_0 + \sqrt{\frac{|m-2|}{2}} - 1$, then $\mathbb{Z}[\frac{-1+\sqrt{d}}{2}]$ is a unique factorization domain.

THEOREM 2. *Let d be a positive integer, with $d \neq 5$. Let p, b, c and x_0 be integers, where p is a prime. Suppose that $b^2 - 4pc = v^2 d$, for some integer $v \geq 1$. Suppose that there exist integers r_1, s_1, r_2, s_2 such that*

$$p = |r_1^2 - ds_1^2|, \qquad 2 = |r_2^2 - ds_2^2|.$$

If $|pn^2 + bn + c|$ is prime or 1 for all integers n with $x_0 \leq n \leq x_0 + \sqrt{\frac{d}{2}} - 1$, then $\mathbb{Z}[\sqrt{d}]$ is a unique factorization domain.

2. PRELIMINARIES

LEMMA 1. *Let α be a quadratic integer, let q and n be positive integers, where q is a prime number. Suppose that there are $\delta, \beta \in \mathbb{Z}[\alpha]$ such that $q = |N(\delta)|$ and $qn = |N(\beta)|$, where N stands for the norm map. Then, there exists $\gamma \in \mathbb{Z}[\alpha]$ such that $n = |N(\gamma)|$.*

Proof. By [4, Lemma 2.1] we have that δ is a prime in $\mathbb{Z}[\alpha]$. As $\beta\bar{\beta} = N(\beta)$ we have $\delta \mid \beta\bar{\beta}$, and so, as δ is prime, we deduce that $\delta \mid \beta$ or $\delta \mid \bar{\beta}$. Let

$$\gamma = \begin{cases} \beta/\delta, & \text{if } \delta \mid \beta \\ \bar{\beta}/\delta, & \text{if } \delta \mid \bar{\beta}. \end{cases} \tag{1}$$

From (1), we deduce that

$$|N(\gamma)| = \frac{|N(\beta)|}{|N(\delta)|} = n.$$

□

LEMMA 2. *Let $d = 1 + 4m$ be a positive integer that is not a perfect square, $\alpha = \frac{-1+\sqrt{d}}{2}$. Let n be a positive integer. If there exist integers r and s such that $4n = |r^2 - ds^2|$, then there exists $\gamma \in \mathbb{Z}[\alpha]$ such that $n = |N(\gamma)|$.*

Proof. It is easy to verify that $\gamma \in \mathbb{Z}[\alpha]$ and $n = |N(\gamma)|$, where

$$\gamma = (r - s)/2 + s\alpha.$$

□

LEMMA 3. *Let d be a positive integer, with $d \neq 5$. Suppose that $\mathbb{Z}[\sqrt{d}]$ is not a unique factorization domain. Then, there is a prime q which is irreducible but not prime in $\mathbb{Z}[\sqrt{d}]$ such that $q \leq \sqrt{\frac{d}{2}}$.*

Proof. Put $\alpha=\sqrt{d}$. Suppose that $\mathbb{Z}[\alpha]$ is not a unique factorization domain. Then, by [4, Lemma 2.2], there is a prime number q which is not prime in $\mathbb{Z}[\alpha]$ such that

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

Since α is a root of the polynomial x^2-d and q is not prime in $\mathbb{Z}[\alpha]$, by [4, Lemma 2.3], we get that there exists $a\in\mathbb{Z}$ such that

$$0\le a\le q/2 \qquad \text{and} \qquad a^2-d\equiv 0 \pmod q. \tag{3}$$

Let us see that

$$q\le\sqrt{\frac{d}{2}}. \tag{4}$$

Let $b=a-q$. Then, from (3) we obtain

$$b^2-d\equiv 0 \pmod q, \tag{5}$$

and

$$\frac{q}{2}\le -b\le q. \tag{6}$$

As

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

from (5) and (2) we deduce that

$$q^2\le |N(b-\alpha)|=|b^2-d|. \tag{7}$$

Combining (7) and (6), we get

$$|b^2-d|=d-b^2. \tag{8}$$

From (7), (8) and (6), we deduce that

$$4q^2\le 4d-(2b)^2\le 4d-q^2,$$

thus giving

$$5q^2\le 4d. \tag{9}$$

Let $c=a+q$. Then, from (3) we obtain

$$c^2-d\equiv 0 \pmod q, \tag{10}$$

and

$$q\le c\le \frac{3q}{2}. \tag{11}$$

As

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

from (10) and (2) we deduce that

$$q^2 \leq |N(c-\alpha)| = |c^2 - d|. \tag{12}$$

We now show that

$$|c^2 - d| = d - c^2. \tag{13}$$

For otherwise $|c^2 - d| = c^2 - d$. From (12), (9) and (11), we get

$$4q^2 \leq (2c)^2 - 4d \leq 9q^2 - 5q^2 = 4q^2.$$

This forces that $4d = 5q^2$, which is impossible because $d \neq 5$. So

$$|c^2 - d| = d - c^2.$$

Combining (12), (13) and (11), we get

$$q^2 \leq d - c^2 \leq d - q^2,$$

giving

$$q \leq \sqrt{\frac{d}{2}}.$$

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

$$q = |N(x)|. \tag{14}$$

Combining (2) and (14) we get $q^2 \leq q$, which is impossible. This contradiction means that if $q = xy$ in $\mathbb{Z}[\alpha]$ then x or y is a unit in $\mathbb{Z}[\alpha]$, *i.e.* q is irreducible in $\mathbb{Z}[\alpha]$. $\square$

PROPOSITION 1. *Let $d = 1+4m$ be a positive integer. Suppose that $\sqrt{\frac{d}{5}}$ is not a prime number, and that $\mathbb{Z}[\frac{-1+\sqrt{d}}{2}]$ is not a unique factorization domain. Then, there is a prime q which is irreducible but not prime in $\mathbb{Z}[\frac{-1+\sqrt{d}}{2}]$ such that $q \leq \sqrt{\frac{|m-2|}{2}}$.*

Proof. Put $\alpha = \frac{-1+\sqrt{1+4m}}{2}$. Suppose that $\mathbb{Z}[\alpha]$ is not a unique factorization domain. Then, by [4, Lemma 2.2], there is a prime number q which is not prime in $\mathbb{Z}[\alpha]$ such that

$$\omega \in \mathbb{Z}[\alpha] \quad \text{and} \quad q \mid N(\omega) \qquad \text{implies that} \qquad q^2 \leq |N(\omega)|. \tag{15}$$

Let us see that

$$q \leq \sqrt{\frac{|m-2|}{2}}. \tag{16}$$

Since α is a root of the polynomial x^2+x-m and q is not prime in $\mathbb{Z}[\alpha]$, by [4, Lemma 2.3], we get that there exists $a \in \mathbb{Z}$ such that

$$0 \leq a \leq (q-1)/2 \qquad \text{and} \qquad a^2+a-m \equiv 0 \pmod{q}. \tag{17}$$

Let $b=a-q$. Then, from (17) we obtain

$$b^2+b-m \equiv 0 \pmod{q}, \tag{18}$$

and

$$\frac{q+1}{2} \leq -b \leq q. \tag{19}$$

As

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

from (18) and (15) we deduce that

$$4q^2 \leq 4|N(b-\alpha)| = |(2b+1)^2-4m-1|. \tag{20}$$

Combining (20) and (19), we get

$$|(2b+1)^2-4m-1| = 4m+1-(2b+1)^2. \tag{21}$$

From (20), (21) and (19), we deduce that

$$4q^2 \leq 4m+1-(2b+1)^2 \leq 4m+1-q^2,$$

thus giving

$$5q^2 \leq 1+4m. \tag{22}$$

Let $c=a+q$. Then, from (17) we obtain

$$c^2+c-m \equiv 0 \pmod{q}, \tag{23}$$

and

$$q \leq c \leq \frac{3q-1}{2}. \tag{24}$$

As

$$N(c-\alpha)=c^2+c-m,$$

from (23) and (15) we deduce that

$$4q^2 \leq 4|N(c-\alpha)| = |(2c+1)^2-4m-1|. \tag{25}$$

We now show that

$$|(2c+1)^2-4m-1| = 4m+1-(2c+1)^2. \tag{26}$$

For otherwise $|(2c+1)^2-4m-1| = (2c+1)^2-4m-1$. From (25), (22) and (24), we get

$$4q^2 \leq (2c+1)^2-(1+4m) \leq 9q^2-5q^2 = 4q^2.$$

This forces that $d = 5q^2$, which is impossible because $\sqrt{\frac{d}{5}}$ is not a prime number. So

$$|(2c+1)^2 - 4m - 1| = 4m + 1 - (2c+1)^2.$$

Combining (25), (26) and (24), we get

$$4q^2 \leq 4m + 1 - (2c+1)^2 \leq 4m + 1 - (2q+1)^2,$$

giving

$$q \leq \sqrt{\frac{|m-2|}{2}}.$$

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

$$q = |N(x)|. \tag{27}$$

Combining (15) and (27) we get $q^2 \leq q$, which is impossible. This contradiction means that if $q = xy$ in $\mathbb{Z}[\alpha]$ then x or y is a unit in $\mathbb{Z}[\alpha]$, i.e. q is irreducible in $\mathbb{Z}[\alpha]$. □

3. PROOF OF THEOREM 1

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

$$q \leq \sqrt{\frac{|m-2|}{2}}. \tag{28}$$

Since α is a root of the polynomial $x^2 + x - m$ and q is not prime in $\mathbb{Z}[\alpha]$, by [4, Lemma 2.3], we get that there exists $t \in \mathbb{Z}$ such that

$$t^2 + t - m \equiv 0 \pmod{q}. \tag{29}$$

As q is irreducible in $\mathbb{Z}[\alpha]$ and

$$p = |r_1^2 - ds_1^2| = |N(r_1 + s_1\sqrt{d})|,$$

we get that $q \neq p$. As

$$\delta = |r_2^2 - ds_2^2| = |N(r_2 + s_2\sqrt{d})|,$$

and $\delta = 2$ if m is even, from (29) we get that $q \neq 2$. Thus

$$q \nmid 2p, \tag{30}$$

and so we deduce that there exists $n \in \mathbb{Z}$ such that

$$x_0 \leq n \leq x_0 + q - 1 \qquad \text{and} \qquad 2pn + b \equiv u(2t+1) \pmod{q}. \tag{31}$$

As $b^2-4pc=u^2d$ from (30), (29) and (31), we deduce that

$$pn^2+bn+c\equiv 0 \pmod q. \tag{32}$$

From (28) and (31), we get

$$x_0\le n\le x_0+\sqrt{\frac{|m-2|}{2}}-1,$$

and so, according to our hypotheses $|pn^2+bn+c|$ is 1 or prime. Thus, from (32) we get

$$q=|pn^2+bn+c|. \tag{33}$$

From (33) we deduce that

$$4pq=|(2pn+b)^2-(b^2-4pc)|=|(2pn+b)^2-du^2|$$

and so, by Lemma 2 there exists $\beta\in\mathbb{Z}[\alpha]$ such that

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

As $p=|N(r_1+s_1\sqrt{d})|$, by Lemma 1, we deduce that there exists $\gamma\in\mathbb{Z}[\alpha]$ such that

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

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

4. PROOF OF THEOREM 2

Put $\alpha=\sqrt{d}$. Suppose that $\mathbb{Z}[\alpha]$ is not a unique factorization domain. Then, by Lemma 3, there is a prime q which is irreducible but not prime in $\mathbb{Z}[\alpha]$ such that

$$q\le\sqrt{\frac{d}{2}}. \tag{34}$$

Since α is a root of the polynomial x^2-d and q is not prime in $\mathbb{Z}[\alpha]$, by [4, Lemma 2.3], we get that there exists $t\in\mathbb{Z}$ such that

$$t^2-d\equiv 0 \pmod q. \tag{35}$$

As q is irreducible in $\mathbb{Z}[\alpha]$ and

$$p=|r_1^2-ds_1^2|=|N(r_1+s_1\alpha)|,\qquad 2=|r_2^2-ds_2^2|=|N(r_2+s_2\alpha)|, \tag{36}$$

we deduce that

$$q\nmid 2p, \tag{37}$$

and so we get that there exists $n \in \mathbb{Z}$ such that

$$x_0 \leq n \leq x_0 + q - 1 \qquad \text{and} \qquad 2pn + b \equiv vt \pmod{q}. \tag{38}$$

As $b^2 - 4pc = v^2 d$ from (37), (35) and (38), we deduce that

$$pn^2 + bn + c \equiv 0 \pmod{q}. \tag{39}$$

From (34) and (38), we get

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

and so, according to our hypotheses $|pn^2 + bn + c|$ is 1 or prime. Thus, from (39) we get

$$q = |pn^2 + bn + c|. \tag{40}$$

From (40) we deduce that

$$4pq = |(2pn + b)^2 - (b^2 - 4pc)| = |(2pn + b)^2 - dv^2|,$$

and from (36), and Lemma 1, we deduce that there exists $\gamma \in \mathbb{Z}[\alpha]$ such that

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

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

5. APPLICATIONS

THEOREM 3. *Let $d = 1 + 4m$ be a positive integer. Let u and x_0 be integers, where u is odd. Suppose that $d = pq \equiv 5 \pmod{8}$, where $p \neq q$ are primes congruent to $3 \pmod{4}$, and that $|pn^2 + pn + \frac{p - u^2 q}{4}|$ is prime or equal to 1 whenever $x_0 \leq n \leq x_0 + \sqrt{\frac{|m-2|}{2}} - 1$. Then $\mathbb{Z}[\frac{-1+\sqrt{d}}{2}]$ is a unique factorization domain.*

Proof. By [5, Lemma 2.4] we get that the equation

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

is solvable in integers x, y. Thus, by Theorem 1, we get that $\mathbb{Z}[\frac{-1+\sqrt{d}}{2}]$ is a unique factorization domain. $\square$

THEOREM 4. *Let u and x_0 be integers, where u is odd. Suppose that $d = 2q$ where q is a prime congruent to $3 \pmod{4}$, and that $|2n^2 - u^2 q|$ is prime or equal to 1 whenever $x_0 \leq n \leq x_0 + \sqrt{\frac{d}{2}} - 1$. Then $\mathbb{Z}[\sqrt{d}]$ is a unique factorization domain.*

Proof. By [5, Lemma 2.3] we get that the equation

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

is solvable in integers x, y. Thus, by Theorem 2, we get that $\mathbb{Z}[\sqrt{d}]$ is a unique factorization domain. $\square$

THEOREM 5. *Let u, x_0 be integers, where u is odd. Suppose that d is a prime congruent to $3 \pmod 4$, and that $|2n^2+2n+\frac{1-u^2d}{2}|$ is prime or equal to 1 whenever $x_0 \le n \le x_0+\sqrt{\frac{d}{2}}-1$. Then $\mathbb{Z}[\sqrt{d}]$ is a unique factorization domain.*

Proof. By [5, Lemma 2.2] we get that the equation

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

is solvable in integers x, y. Thus, by Theorem 2, we get that $\mathbb{Z}[\sqrt{d}]$ is a unique factorization domain. $\square$

Acknowledgments. The author wishes to thank the referees for so carefully checking the manuscript.

REFERENCES

[1] M. Kutsuna, *On a criterion for the class number of a quadratic number field to be one.* Nagoya Math. J. **79** (1980), 123–129.

[2] D. H. Lehmer, *On the function x^2+x+A* Sphinx **6** (1936), 212–214.

[3] R. A. Mollin, *Quadratics.* CRC Press, Boca Raton, 1996.

[4] 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. (2) **50** (2016), 139–143.

[5] P. G. Walsh, *A note on class number one criteria of Sirola for real quadratic fields.* Glasnik Matematicki **40 (60)** (2005), 21–27.

Received February 12, 2018

Universidad Simón Bolívar
Departamento de Matemáticas Puras y Aplicadas
ramirezv@usb.ve