CLASS NUMBER ONE CRITERIA FOR QUADRATIC FIELDS

VÍCTOR JULIO RAMÍREZ VIÑAS

Communicated by Alexandru Zaharescu

In this study we obtain a criterion for the class number of the quadratic number fields to be one. We also apply this criterion to give an elementary proof of the fact that rings $\mathbb{Z}[\frac{-1+\sqrt{-d}}{2}]$ are unique factorization domains for $d = 3, 7, 11, 19, 43, 67, 163$. We also prove that the rings $\mathbb{Z}[\frac{-1+\sqrt{D}}{2}]$ are unique factorization domains for $D = 5, 13, 21, 29, 53, 77$.

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. For this matter, we suggest reading the book of Mollin [3].

The aim of this paper is to prove the following:

THEOREM. *Let q be an integer. If $|x^2 + x + q|$ is 1 or prime for $x = 0, 1, ..., \lfloor\sqrt{|q|/3}\rfloor$, then $\mathbb{Z}[\frac{-1+\sqrt{1-4q}}{2}]$ is a unique factorization domain.*

We also apply this criterion to give an elementary proof of the fact that rings $\mathbb{Z}[\frac{-1+\sqrt{-d}}{2}]$ are unique factorization domains for $d = 3, 7, 11, 19, 43, 67, 163$. We also prove that the rings $\mathbb{Z}[\frac{-1+\sqrt{D}}{2}]$ are unique factorization domains for $D = 5, 13, 21, 29, 53, 77$.

2. PRELIMINARIES

We shall denote, as usual, the field of complex numbers by $\mathbb{C}$, the ring of rational integers by $\mathbb{Z}$. In what follows $\alpha \in \mathbb{C}$ is a root of the irreducible polynomial $x^2 + x + q \in \mathbb{Z}[x]$.

Lemma 1. *Let p be a prime. Then p is prime in $\mathbb{Z}[\alpha]$ if and only if x^2+x+q is irreducible in $\mathbb{Z}_p[x]$.*

Proof. See [4, Lemma 2.3, page 141]. □

Lemma 2. *If $\mathbb{Z}[\alpha]$ is not a unique factorization domain, then there is a prime number p which is not prime in $\mathbb{Z}[\alpha]$ such that whenever $\omega \in \mathbb{Z}[\alpha]$ is such that*

$$(1) \qquad p \mid N(\omega), \qquad \textit{then} \qquad p^2 \le |N(\omega)|,$$

where N stands for the norm map.

Proof. See [4, Lemma 2.2, page 140]. □

3. MAIN THEOREM

Theorem 1. *If $|x^2+x+q|$ is 1 or prime for $x=0,1,...,\lfloor\sqrt{|q|/3}\rfloor$, then $\mathbb{Z}[\alpha]$ is a unique factorization domain.*

Proof. Suppose that $\mathbb{Z}[\alpha]$ is not a unique factorization domain. Then by Lemma 2, there is a prime number p which is not prime in $\mathbb{Z}[\alpha]$ such that

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

Since p is not prime in $\mathbb{Z}[\alpha]$, by Lemma 1, we get that there exists $a \in \mathbb{Z}$ such that

$$(3) \qquad 0 \le a \le (p-1)/2 \qquad \text{and} \qquad a^2+a+q \equiv 0 \pmod{p},$$

and since

$$N(a-\alpha) = a^2+a+q,$$

we get that $p \mid N(a-\alpha)$. Combining (2) and (3), we get

$$4p^2 \le 4|N(a-\alpha)| = |(2a+1)^2+4q-1| \le (2a+1)^2+4|q|+1 \le p^2+4|q|+1,$$

giving

$$(4) \qquad 3p^2 \le 4|q|+1.$$

From (3) and (4), we get that $a \le \sqrt{\frac{|q|}{3}}$, so by our assumption $|a^2+a+q|$ is prime. Thus,

$$(5) \qquad p = |a^2+a+q|.$$

Combining (2) and (5) we get $p^2 \le p$, which is impossible. Thus, $\mathbb{Z}[\alpha]$ must be a unique factorization domain. □

4. APPLICATIONS OF THEOREM 1

As an immediate corollary we also get

THEOREM 2 (Lehmer [2]). *If x^2+x+q is prime for $x=0,1,...,q-2$, then $\mathbb{Z}[\alpha]$ is a unique factorization domain.*

THEOREM 3 (Kutsuna [1]). *If $-x^2+x+q$ is prime for every integer x with $1 \le x \le \sqrt{q}-1$, then $\mathbb{Z}[\alpha]$ is a unique factorization domain.*

Proof. It is easy to verify that

$$-x^2+x+q=-(x-1)^2-(x-1)+q.$$

Thus, by Theorem 1, we get that $\mathbb{Z}[\alpha]$ is a unique factorization domain. □

THEOREM 4. *Let $d \in \{3,7,11,19,43,67,163\}$. Then the ring $\mathbb{Z}[\frac{-1+\sqrt{-d}}{2}]$ is a unique factorization domain.*

Proof. Put $f(x)=|x^2+x+q|$, $\delta=\sqrt{|q|/3}$ and $\alpha=\frac{-1+\sqrt{1-4q}}{2}$.

If $q=1,2$, then $\delta<1$ and $f(0)$ is 1 or prime. By Theorem 1, we get that $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$ and $\mathbb{Z}\left[\frac{-1+\sqrt{-7}}{2}\right]$ are unique factorization domains.

If $q=3,5,11$, then $\delta<2$. Furthermore, we get that $f(0)$ and $f(1)$ are prime numbers. By Theorem 1, we get that $\mathbb{Z}\left[\frac{-1+\sqrt{-11}}{2}\right]$, $\mathbb{Z}\left[\frac{-1+\sqrt{-19}}{2}\right]$ and $\mathbb{Z}\left[\frac{-1+\sqrt{-43}}{2}\right]$ are unique factorization domains.

If $q=17$, then $\delta<3$. Furthermore, we get that $f(0)$, $f(1)$ and $f(2)$ are prime numbers. By Theorem 1, we get that $\mathbb{Z}\left[\frac{-1+\sqrt{-67}}{2}\right]$ is a unique factorization domain.

If $q=41$, then $\delta<4$. Furthermore, we get that $f(0)$, $f(1)$, $f(2)$ and $f(3)$ are prime numbers. By Theorem 1, we get that $\mathbb{Z}\left[\frac{-1+\sqrt{-163}}{2}\right]$ is a unique factorization domain. □

It is now well-known (see [5]) that there exactly nine complex quadratic fields with class number one. They are $\mathbb{Q}(\sqrt{-d})$ for $d \in \{1,2,3,7,11,19,43,67,163\}$. Combining this with theorem 1 we get the remarkable:

THEOREM 5. *Let q be a positive integer, let $f_q(x)=x^2+x+q$. Then, the following assertions are equivalent:*

1. $q=1,2,3,5,11,17,41$.
2. *$f_q(x)$ is 1 or prime for $x=0,1,...,\lfloor\sqrt{q/3}\rfloor$.*

3. $\mathbb{Z}[\frac{-1+\sqrt{1-4q}}{2}]$ *is a unique factorization domain.*

Proof. The implication 1) $\Rightarrow$ 2) has been already verified in the proof of Theorem 4. The implication 2) $\Rightarrow$ 3) is an immediate consequence of Theorem 1. The proof of 3)$\Rightarrow$ 1) follows from the complete determination of all imaginary quadratic fields with class number 1. $\square$

THEOREM 6. *Let* $d \in \{5, 13, 21, 29, 53, 77\}$. *Then the ring* $\mathbb{Z}[\frac{-1+\sqrt{d}}{2}]$ *is a unique factorization domain.*

Proof. Put $f(x) = |x^2 + x + q|$, $\delta = \sqrt{|q|/3}$ and $\alpha = \frac{-1+\sqrt{1-4q}}{2}$.

If $q = -1, -3, -5, -7$, then $\delta < 2$. Furthermore, we get that $f(0)$ and $f(1)$ are 1 or prime numbers. By Theorem 1, we get that $\mathbb{Z}\left[\frac{-1+\sqrt{5}}{2}\right]$, $\mathbb{Z}\left[\frac{-1+\sqrt{13}}{2}\right]$, $\mathbb{Z}\left[\frac{-1+\sqrt{21}}{2}\right]$ and $\mathbb{Z}\left[\frac{-1+\sqrt{29}}{2}\right]$ are unique factorization domains.

If $q = -13, -19$, then $\delta < 3$. Furthermore, we get that $f(0)$, $f(1)$ and $f(2)$ are prime numbers. By Theorem 1, we get that $\mathbb{Z}\left[\frac{-1+\sqrt{53}}{2}\right]$ and $\mathbb{Z}\left[\frac{-1+\sqrt{77}}{2}\right]$ are unique factorization domains. $\square$

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] H. M. Stark. A complete determination of the complex quadratic fields of class number one, *Michigan Math. J.* **14** (1967), 1–27

Received July 14, 2017

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