Revista Colombiana de Matemáticas
Volumen 50(2016)2, páginas 139-143

A new proof of the Unique Factorization of $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ for $d = 3, 7, 11, 19, 43, 67, 163$

Una nueva demostración de la factorización única $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ para $d = 3, 7, 11, 19, 43, 67, 163$

Victor J. Ramirez V.[1]

[1]Universidad Simon Bolivar, Caracas, Venezuela

Abstract. In this paper, we give an elementary proof of the fact that the rings $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ are unique factorization domains for the values $d = 3, 7, 11, 19, 43, 67, 163$. While the result in itself is well known, our proof is new and completely elementary and uses neither the Minkowski convex body theorem, nor the Dedekind and Hasse theorems. Furthermore, it does not use either the theory of algebraic integers, or the theory of Noetherian rings. It only uses basic notions from the theory of commutative rings.

Key words and phrases. Unique factorization domain, prime, irreducible.

2010 Mathematics Subject Classification. 11R29, 13F15.

Resumen. En este artículo, damos una demostración elemental de que los anillos $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ son dominios de factorización única para los valores $d = 3, 7, 11, 19, 43, 67, 163$. Si bien este resultado es conocido, nuestra prueba es nueva y completamente elemental, y no hace uso del teorema del cuerpo convexo de Minkowski, ni del teorema de Dedekind y Hasse. Además, no utiliza la teoría de los enteros algebraicos, ni la teoría de los anillos noetherianos. Sólo utiliza nociones básicas de la teoría de los anillos conmutativos.

Palabras y frases clave. Dominio de factorización única, primo, irreducible.

1. Introduction

The main purpose of this paper is give an elementary proof of the fact that the rings $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ are unique factorization domains, for the values $d = 3, 7, 11, 19, 43, 67, 163$. While the result in itself is well known (See [2] p. 107 and p. 151; [3]; [4] p. 124; [1] p. 62 and p. 315), our proof is new and completely elementary and uses neither the Minkowski convex body theorem (See [2] Chapter VIII), nor the Dedekind and Hasse theorems (See [4] Theorem 9.5, p. 124). Furthermore, it does not use either the theory of algebraic integers, or the theory of Noetherian rings. It only uses basic notions from the theory of commutative rings.

2. Preliminary lemmas

In this paper we shall denote, as usual, the field of complex numbers by $\mathbb{C}$, the ring of rational integers by $\mathbb{Z}$

In all what follows $\alpha \in \mathbb{C}$ is a root of the irreducible polynomial $x^2+tx+q \in \mathbb{Z}[x]$. Its ther root is denoted by $\bar{\alpha}$.

$$N : \mathbb{Z}[\alpha] \longrightarrow \mathbb{Z}, \qquad N(a+b\alpha) = (a+b\alpha)(a+b\bar{\alpha}) = a^2 - tab + qb^2$$

N is the norm map and it is easy to verify that $N(\delta\gamma) = N(\delta)N(\gamma)$ for all $\delta, \gamma \in Z[\alpha]$

Lemma 2.1. *If $\pi \in \mathbb{Z}[\alpha]$ is such that $N(\pi)$ is prime number, then π is prime in $\mathbb{Z}[\alpha]$.*

Proof. Put $p = N(\pi)$. It is then easy to check that

$$\#\left(\frac{\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]}\right) = p^2, \qquad \text{and} \qquad \#\left(\frac{\pi\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]}\right) \neq 1. \tag{1}$$

Since p is prime number and

$$\frac{\mathbb{Z}[\alpha]}{\pi\mathbb{Z}[\alpha]} \cong \frac{(\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha])}{(\pi\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha])},$$

it follows from (1) that $\mathbb{Z}[\alpha]/\pi\mathbb{Z}[\alpha]$ has p elements and is therefore a field. Thus, π is prime in $\mathbb{Z}[\alpha]$. ☑

Lemma 2.2. *If $\mathbb{Z}[\alpha]$ is not an 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*

$$\text{if} \qquad p|N(\omega), \qquad \text{then} \qquad p^2 \leq |N(\omega)|. \tag{2}$$

Proof. Let $\mathcal{S}$ be the set of all elements of $\mathbb{Z}[\alpha]$ which can be written as a product of primes in $\mathbb{Z}[\alpha]$. Let

$$\mathcal{S}' = \mathcal{U}(\mathbb{Z}[\alpha]) \cup \mathcal{S}, \qquad \text{and} \quad \mathcal{W} = \mathbb{Z}[\alpha] \setminus \mathcal{S}'.$$

Since $\mathbb{Z}[\alpha]$ is not an unique factorization domain, it follows that $\mathcal{W}$ is nonempty. Let $\beta \in \mathcal{W}$ be such that

$$|N(\beta)| = \min\{|N(\omega)| : \omega \in \mathcal{W}, \quad \omega \neq 0\}. \tag{3}$$

Note that since $\beta \in \mathcal{W}$ it is not prime in $\mathbb{Z}[\alpha]$. Also, by using the multiplicative property of N and the minimal property of β one can deduce easily that β is irreducible, so by Lemma 2.1 $N(\beta)$ is not a prime number. Thus, there exists a prime number

$$p|N(\beta) \qquad \text{and} \qquad p \leq \sqrt{|N(\beta)|}. \tag{4}$$

Note that p is not prime in $\mathbb{Z}[\alpha]$, because otherwise, since $p|N(\beta)$, we would obtain that p would be an associate of β or $\bar{\beta}$, which is imposible since $\beta \in \mathcal{W}$.

Let us see that the prime p satisfies condition (2). Let $\omega \in \mathbb{Z}[\alpha]$ be such that $p|N(\omega)$. An argument similar to the previous one leads to $\omega \in \mathcal{W}$. Thus, using (3) and (4), we get that

$$p^2 \leq |N(\beta)| \leq |N(\omega)|.$$

☑

Lemma 2.3. *Let p be a prime number. Then p is prime in $\mathbb{Z}[\alpha]$ if and only if $x^2 + tx + q$ is prime in $\mathbb{Z}_p[x]$.*

Proof. This is an immediate consequence of the chain of isomorphisms

$$\begin{aligned}\frac{\mathbb{Z}_p[x]}{(x^2+tx+q)\mathbb{Z}_p[x]} &\cong \frac{(\mathbb{Z}[x]/p\mathbb{Z}[x])}{((x^2+tx+q,p)\mathbb{Z}[x]/p\mathbb{Z}[x])} \cong \frac{\mathbb{Z}[x]}{(x^2+tx+q,p)\,\mathbb{Z}[x]} \\ &\cong \frac{(\mathbb{Z}[x]/p(x^2+tx+q)\mathbb{Z}[x])}{(x^2+tx+q,p)\mathbb{Z}[x]/(x^2+tx+q)\mathbb{Z}[x])} \cong \frac{\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]}.\end{aligned}$$

☑

3. Main Theorems

Theorem 3.1. *Let $d \in \mathbb{N}$ with $d \equiv 1 \pmod 4$. We assume that $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ is not an unique factorization domain. Then, there is a prime number p which is not prime in $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ such that $p \leq \sqrt{d/3}$.*

Proof. We denote $\alpha = \left(1+\sqrt{-d}\right)/2$, is a root of the polynomial $x^2 - x + (1+d)/4$ and $N(a+b\alpha) = a^2 + ab + (1+d)b^2/4$. Since $\mathbb{Z}[\alpha]$ is not an unique factorization domain, by Lemma 2.2, there exists a prime number p such that

$$\omega \in \mathbb{Z}[\alpha] \qquad \text{and} \qquad p|N(\omega) \qquad \text{implies that} \qquad p^2 \leq |N(\omega)|. \tag{5}$$

Since p is not prime in $\mathbb{Z}[\alpha]$, by Lemma 2.3, we get that there exists $b \in \mathbb{Z}$ such that

$$0 \leq b \leq (p+1)/2 \qquad \text{and} \qquad b^2 - b + \frac{1+d}{4} \equiv 0 \pmod{p}, \tag{6}$$

and since

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

we get that $p|N(b-\alpha)$. Combining (5) and (6), we get

$$4p^2 \leq 4N(b-\alpha) = (2b-1)^2 + d \leq p^2 + d,$$

giving $p \leq \sqrt{d/3}$. ☑

Theorem 3.2. *The rings* $\mathbb{Z}\left[\dfrac{1+\sqrt{-d}}{2}\right]$ *with* $d \in 3, 7, 11, 19, 43, 67, 163$ *are Unique Factorization Domains.*

Proof. If $d = 3, 7, 11$, then $\sqrt{d/3} < 2$. By Theorem 3.1, we get that $\mathbb{Z}\left[\dfrac{1+\sqrt{-d}}{2}\right]$ is an Unique Factorization Domain.

If $d = 19, 43, 67$, then $\sqrt{d/3} < 5$. Furthermore, by Lemma 2.3 we get that 2 and 3 are primes in $\mathbb{Z}\left[\dfrac{1+\sqrt{-d}}{2}\right]$. By Theorem 3.1, we get that $\mathbb{Z}\left[\dfrac{1+\sqrt{-d}}{2}\right]$ is an Unique Factorization Domain.

If $d = 163$, then $\sqrt{d/3} < 11$. Furthermore, applying Lemma 2.3, we get that 2, 3, 5, 7 are primes in $\mathbb{Z}\left[\dfrac{1+\sqrt{-d}}{2}\right]$. By Theorem 3.1, we get that $\mathbb{Z}\left[\dfrac{1+\sqrt{-d}}{2}\right]$ is an Unique Factorization Domain. ☑

Acknowledgment. I would like to express my sincere gratitude to Professor Florian Lucas and Professor Pedro Berrizbeitia for reading the manuscript and suggesting various improvements

References

[1] S. Alaca and K. S. Williams, *Introductory algebraic number theory*, Cambridge University Press, 2004.

[2] H. Cohn, *Advanced number theory*, Dover, New York, 1980.

[3] A. Oneto and V. Ramirez, *Dominios principales no euclidianos*, Divul.Mat. **1** (1993), 55–65.

[4] H. Pollard, *The theory of algebraic numbers*, Carus Monograph **9**, MAA, Wiley, New York, 1975.

(Recibido en enero de 2016. Aceptado en marzo de 2016)

Department of Pure and Applied Mathematics
Universidad Simon Bolivar
Caracas, Venezuela
e-mail: ramirezv@usb.ve