Scientia Et Technica
ISSN: 0122-1701
scientia@utp.edu.co
Universidad Tecnológica de Pereira
Colombia

Ávila, Jesús; Correa-Amaya, Juan Sebastian; Cupitra-Vergara, Emma
Números complejos sobre anillos
Scientia Et Technica, vol. 23, núm. 4, 2018, Septiembre-, pp. 581-585
Universidad Tecnológica de Pereira
Colombia

# Números complejos sobre anillos

## Complex numbers on rings

Jesús Ávila[1], Juan Sebastian Correa-Amaya[2], Emma Cupitra-Vergara[1]
*Departamento de matemáticas y estadística, Universidad del Tolima, Ibagué, Colombia*
*Maestría en Matemáticas, Universidade Federal do Juiz de Fora, Brasil*
javila@ut.edu.co
jscorrea@ut.edu.co
ecupitra@ut.edu.co

***Resumen*— El propósito de este artículo es presentar la construcción de los números complejos usando el conjunto $\mathbb{R}\times\mathbb{R}$ con algunas operaciones especiales y también mostrar la representación de este conjunto usando matrices especiales de $2\times 2$ y la correspondiente versión algebraica $\mathbb{R}[x]/\langle x^2+1\rangle$. También se estudiaron las tres construcciones previas pero para el caso $\mathbb{Z}_p\times\mathbb{Z}_p$, $p$ primo y determinamos cuales de ellas permanecen válidas o en su defecto, determinan bajo qué condiciones esto es verdadero.**

***Palabras clave*— Anillo conmutativo, número primo, Teorema de Fermat, isomorfismo de anillos.**

**A*bstract*— The purpose of this paper is to present the construction of the complex numbers by using the set $\mathbb{R}\times\mathbb{R}$ with some special operations and also to show the representation of this set by using special matrices of $2\times 2$ and the corresponding algebraic version $\mathbb{R}[x]/\langle x^2+1\rangle$. it was also studied the three previous constructions but for the case $\mathbb{Z}_p\times\mathbb{Z}_p$, $p$ prime and determine whether they remain valid or in its defect, determine under which conditions this is true.**

***Key Word* — Commutative ring, prime number, Fermat's Theorem, isomorphism of rings.**

## I. INTRODUCCIÓN

Los números complejos surgen naturalmente al buscar todas las raíces de una ecuación algebraica. Su aparición fue debida a G. Cardano en el siglo XVI, quien los utiliza para hallar raíces de ciertas ecuaciones, a las que denomina como "raíces sofisticadas" [1]. Sin embargo Cardano no vislumbra la importancia de dicho conjunto para las matemáticas posteriores. Hacia el año 1572, el matemático italiano R. Bombelli introduce formalmente las reglas de operación con números imaginarios y complejos [1]. Y es el gran genio de Gauss quien en el siglo XVIII logra dar una descripción formal y coherente de los números complejos, al mismo tiempo que los interpreta como parejas de puntos del plano, tal como se presentan en los textos modernos de variable compleja [2].

Actualmente, la primera noción de número complejo que se presenta a un estudiante, consiste en definir el conjunto $\mathbb{C}=\{a+bi: a,b\in\mathbb{R}, i^2=-1\}$, donde la suma se hace componente a componente y el producto se define como $(a+bi)(c+di)=(ac-bd)+(ad+bc)i$, para todo $a+bi, c+di\in\mathbb{C}$. Con esto se prueba que el conjunto $\mathbb{C}$ tiene estructura de cuerpo. En cursos más avanzados de álgebra los complejos se ven como el anillo cociente $\mathbb{R}[x]/_{<x^2+1>}$ o también como el conjunto de matrices cuadradas $M(R)=\left\{\begin{pmatrix} a & b\\ -b & a\end{pmatrix}: a,b\in\mathbb{R}\right\}$, con las operaciones usuales [3,4].

Y en un primer curso de variable compleja los complejos se construyen de manera más formal tomando el conjunto $\mathbb{R}\times\mathbb{R}$, donde la suma se hace componente a componente y el producto se define como $(a,b)(c,d)=(ac-bd,ad+bc)$, para todo $(a,b),(c,d)\in\mathbb{R}\times\mathbb{R}$ [5]. El conjunto $\mathbb{R}\times\mathbb{R}$ con las operaciones anteriormente descritas será denotado como $\mathbb{R}\otimes\mathbb{R}$.

Estos tres conjuntos tienen estructura de cuerpo y todos ellos son isomorfos, es decir, son tres representaciones "distintas" de los números complejos $\mathbb{C}$ (ver Figura 1).

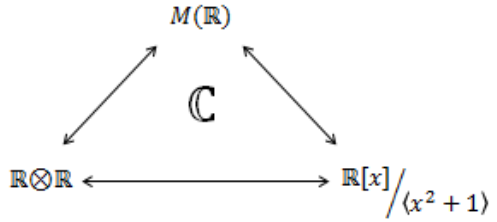


Figura 1. Las tres representaciones isomorfas de $\mathbb{C}$.

Al observar las tres construcciones anteriores se nota que todas ellas tienen como conjunto base a los números reales $\mathbb{R}$. De esta forma resulta natural hacerse los siguientes interrogantes, los cuales definen los problemas que se estudiarán en el presente trabajo.

Fecha de Recepción: 28 de febrero de 2018
Fecha de Aceptación: 20 de diciembre de 2018

¿Las tres construcciones anteriores se pueden hacer considerando como conjunto base, cualquier anillo conmutativo con unidad $A$?

¿Qué sucede si en las construcciones anteriores se cambia el cuerpo $\mathbb{R}$ por un cuerpo finito $\mathbb{Z}_p$, $p$ primo?

¿El conjunto $\mathbb{Z}_p \times \mathbb{Z}_p$ , $p$ primo, es cuerpo con las operaciones arriba mencionadas? En caso afirmativo, ¿Se mantienen también las otras representaciones? En caso negativo, ¿Para cuáles primos $p$, el conjunto $\mathbb{Z}_p \times \mathbb{Z}_p$ resulta ser un cuerpo?

## II. LA COMPLEJIFICACIÓN DE UN ANILLO

En esta sección se toma un anillo conmutativo con unidad $A$ y se definen conjuntos y operaciones análogas a las mencionadas arriba. Se prueba que dichos conjuntos son anillos conmutativos con unidad, los cuales son isomorfos. Y finalmente se muestra que dichos conjuntos corresponden a lo que podría llamarse "**números complejos sobre el anillo $A$**" o "**complejificación del anillo $A$**" [6].

Sea $A$ un anillo conmutativo con unidad 1 y tomemos el conjunto $A \times A$, donde la suma se hace componente a componente y el producto se define como $(a,b)(c,d) = (ac - bd, ad + bc)$, para todo $(a,b),(c,d) \in A \times A$.

**Afirmación 2.1.** Si $A$ es un anillo conmutativo con unidad 1, entonces el conjunto $A \times A$ es un anillo conmutativo con unidad.

**Demostración.** Ya que la suma de parejas es componente a componente se observa fácilmente que $(A \times A, +)$ es un grupo abeliano. Claramente el producto es conmutativo, pues $A$ es conmutativo. Ahora para $(a,b),(c,d),(e,f) \in A \times A$ se tiene que $(a,b)\big((c,d)(e,f)\big) = (ace - adf - bcf - bde, acf + ade + bce - bdf) = ((a,b)(c,d))(e,f)$ y además $(a,b)\big((c,d) + (e,f)\big) = (ac + ae - bd - bf, ad + af + bc + be) = (a,b)(c,d) + (a,b)(e,f)$. Finalmente se observa que la otra propiedad distributiva es consecuencia de esta última igualdad y de la conmutatividad, y que la pareja $(1,0)$ es el neutro para el producto. Así concluimos que el conjunto $A \times A$ con las operaciones indicadas, es un anillo conmutativo con unidad. ■

Recordemos que si $A$ es un anillo conmutativo con unidad 1, entonces el conjunto de matrices de tamaño $2 \times 2$ con entradas en $A$, denotado $M_2(A)$, es un anillo con unidad $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ no conmutativo [3,4]. Dentro de $M_2(A)$ consideramos el conjunto $M(A) = \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in A\right\}$ con las operaciones usuales de matrices. Obtenemos entonces el siguiente resultado.

**Afirmación 2.2.** Si $A$ es un anillo conmutativo con unidad 1, entonces el conjunto $M(A)$ es un anillo conmutativo con unidad.

**Demostración.** Es claro que $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M(A)$. Ahora para $E = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $F = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in M(A)$ se tiene que

$$E - F = \begin{pmatrix} a-c & b-d \\ -(b-d) & a-c \end{pmatrix} \in M(A),$$

$$EF = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix} \in M(A).$$

Es decir, $M(A)$ es un subanillo de $M_2(A)$. Y como $EF = FE$ concluimos que $M(A)$ es un anillo conmutativo con unidad. ■

**Observación 2.3.** Aunque podría pensarse que los anillos $A \times A$ y $M(A)$ construidos anteriormente son distintos, puede verse fácilmente que ellos son algebraicamente iguales, es decir, son isomorfos. En efecto, basta considerar la función $\theta: A \times A \to M(A)$ definida por $\theta\big((a,b)\big) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, para todo $(a,b) \in A \times A$.

Para terminar esta sección veamos la relación que existe entre los anillos introducidos anteriormente y lo que conocemos como números complejos.

Comenzamos determinando la relación existente entre los anillos $A$ y $A \times A$. Puede probarse, fácilmente, que la función $\emptyset : A \to A \times A$ definida por $\emptyset(a) = (a,0)$ para todo $a \in A$ es un homomorfismo inyectivo. Esto significa que el anillo $A \times A$ contiene un subanillo isomorfo al anillo $A$ o también podemos decir que cualquier elemento $a \in A$ puede identificarse con la pareja $(a,0) \in A \times A$ y viceversa. Ahora si $(a,b) \in A \times A$, entonces $(a,b) = (a,0) + (b,0)(0,1)$. Y usando la identificación mencionada y teniendo en cuenta que $(0,1)^2 = (-1,0)$, entonces podemos concluir que $(a,b) = a + bi$ donde $a, b \in A$ e $i = (0,1)$ es tal que $i^2 = -1$. Y por esto es que el anillo $A \times A$ se conoce como la "**Complejificación del anillo $A$**" [6]. Note que esta construcción generaliza la construcción presentada en la introducción, es decir, si $A = \mathbb{R}$, entonces se obtienen los clásicos números complejos $\mathbb{C}$. También si $A = \mathbb{Z}$, se obtiene el anillo de enteros gaussianos $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ [4, 7, 8]. Si $A = \mathbb{Z}_n$, entonces se obtienen los enteros Gaussianos módulo $n$, $\mathbb{Z}_n[i] = \{a + bi : a, b \in \mathbb{Z}_n\}$ [3, 9]. El anillo de enteros gaussianos $\mathbb{Z}[i]$ es de gran importancia en matemáticas, no solo porque es un subanillo de los complejos. Sino también porque sus características algebraicas lo hacen el conjunto indicado para resolver variados problemas de teoría de números [4, 10].

El anillo $A \times A$ con las operaciones anteriormente descritas será denotado indistintamente como $A \otimes A$ o $A[i]$.

La construcción realizada en esta sección, sugiere una pregunta inmediata: si $A$ es cuerpo, entonces $A \otimes A$ es un cuerpo? Ya sabemos que la respuesta es afirmativa si $A$ es el cuerpo de números reales $\mathbb{R}$. Pero, sucederá lo mismo cuando $A$ es un

cuerpo finito? En particular, qué sucede cuando $A = \mathbb{Z}_p$, $p$ primo? La respuesta a estos interrogantes son el objetivo de la Sección 3.

## III. NÚMEROS COMPLEJOS SOBRE $Z_p$, $p$ PRIMO

En la sección anterior se generalizaron algunas de las construcciones de los números complejos a un anillo conmutativo con unidad $A$. En esta sección se estudia el caso en que $A = \mathbb{Z}_p$, $p$ primo y se determinan los valores $p$ para los cuales se obtienen las tres construcciones análogas y los tres isomorfismos análogos, obtenidos para el caso de los números reales $\mathbb{R}$.

El primer interrogante que resulta es: ¿$\mathbb{Z}_p \otimes \mathbb{Z}_p$ es un cuerpo para cualquier primo $p$? Para esto tomemos los dos casos particulares en que $p = 2$ y $p = 3$ y observemos las tablas de multiplicar en cada caso (Tabla 1 y Tabla 2).

| | (1,0) | (0,1) | (1,1) |
|---|---|---|---|
| (1,0) | (1,0) | (0,1) | (1,1) |
| (0,1) | (0,1) | (1,0) | (1,1) |
| (1,1) | (1,1) | (1,1) | (0,0) |

Tabla 1. Tabla de multiplicar en $\mathbb{Z}_2 \otimes \mathbb{Z}_2$.

| | (0.1) | (0,2) | (1,0) | (1,1) | (1,2) | (2,0) | (2,1) | (2,2) |
|---|---|---|---|---|---|---|---|---|
| (0,1) | (2,0) | (1,0) | (0,1) | (2,1) | (1,1) | (0,2) | (2,2) | (1,2) |
| (0,2) | (1,0) | (2,0) | (0,2) | (1,2) | (2,1) | (0,1) | (1,1) | (2,1) |
| (1,0) | (0,1) | (0,2) | (1,0) | (1,1) | (1,2) | (2,0) | (2,1) | (2,2) |
| (1,1) | (2,1) | (1,2) | (1,1) | (0,2) | (2,0) | (2,2) | (1,0) | (0,1) |
| (1,2) | (1,1) | (2,2) | (1,2) | (2,0) | (0,1) | (2,1) | (0,2) | (1,0) |
| (2,0) | (0,2) | (0,1) | (2,0) | (2,2) | (2,1) | (1,0) | (1,2) | (1,1) |
| (2,1) | (2,2) | (1,1) | (2,1) | (1,0) | (0,2) | (1,2) | (0,1) | (2,0) |
| (2,2) | (1,2) | (2,1) | (2,2) | (0,1) | (1,0) | (1,1) | (2,0) | (0,2) |

Tabla 2. Tabla de multiplicar en $\mathbb{Z}_3 \otimes \mathbb{Z}_3$.

En la Tabla 1 se observa que la pareja $(1,1)$ no tiene inverso multiplicativo, es decir, $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ no es un cuerpo. En la Tabla 2 se observa que todos los elementos no nulos son invertibles, es decir, $\mathbb{Z}_3 \otimes \mathbb{Z}_3$ sí es un cuerpo. Esto nos permite concluir que el anillo $\mathbb{Z}_p \otimes \mathbb{Z}_p$, $p$ primo, no es un cuerpo en general. Nos preguntamos entonces para cuales primos $p$ se tiene que el anillo $\mathbb{Z}_p \otimes \mathbb{Z}_p$ es un cuerpo.

Realizando las tablas de multiplicar para otros valores del primo $p$, obtenemos que $\mathbb{Z}_7 \otimes \mathbb{Z}_7$ y $\mathbb{Z}_{11} \otimes \mathbb{Z}_{11}$ sí son cuerpos, mientras que $\mathbb{Z}_5 \otimes \mathbb{Z}_5$ y $\mathbb{Z}_{13} \otimes \mathbb{Z}_{13}$ no son cuerpos.

Ahora bien, los primos 2, 5 y 13 son suma de dos cuadrados, mientras que los primos 3, 7 y 13 no lo son. Esto nos indica cual debe ser el camino para solucionar este problema como se observa en el siguiente resultado.

**Afirmación 3.1.** Sea $p$ un primo. Si $\mathbb{Z}_p \otimes \mathbb{Z}_p$ es un cuerpo, entonces $p$ no es suma de dos cuadrados.

**Demostración.** Supongamos que $p$ es suma de dos cuadrados. Entonces, $p = c^2 + d^2$ con $c, d \in \mathbb{Z}$ y $1 \leq c, d < p$. Luego la pareja $(\overline{c}, \overline{d}) \neq (\overline{0}, \overline{0})$ y como $\mathbb{Z}_p \otimes \mathbb{Z}_p$ es un cuerpo, entonces la pareja $(\overline{c}, \overline{d})$ es invertible. Luego existe $(\overline{a}, \overline{b}) \in \mathbb{Z}_p \otimes \mathbb{Z}_p$ tal que

$$(\overline{c}, \overline{d})(\overline{a}, \overline{b}) = (\overline{1}, \overline{0}) \quad (1)$$

$$(\overline{c}\,\overline{a} - \overline{d}\,\overline{b}, \overline{c}\,\overline{b} + \overline{d}\,\overline{a}) = (\overline{1}, \overline{0}) \quad (2)$$

$$\overline{c}\,\overline{a} - \overline{d}\,\overline{b} = \overline{1} \quad (3)$$

$$\overline{c}\,\overline{b} + \overline{d}\,\overline{a} = \overline{0} \quad (4)$$

Ahora multiplicando la ecuación (3) por $\overline{c}$, la (4) por $\overline{d}$ y sumando se obtiene

$$\overline{c}^2\,\overline{a} + \overline{d}^2\,\overline{a} = \overline{c} \quad (5)$$

$$\overline{a}(\overline{c^2 + d^2}) = \overline{c} \quad (6)$$

$$\overline{a}\,\overline{0} = \overline{c} \quad (7)$$

Y de la ecuación (7) se obtiene que $\overline{c} = \overline{0}$. De manera análoga se obtiene que $\overline{d} = \overline{0}$, es decir, $(\overline{c}, \overline{d}) = (\overline{0}, \overline{0})$ lo cual es contradictorio. Se concluye entonces que $p$ no es suma de dos cuadrados. ■

Antes de probar el recíproco de la Afirmación 3.1, debemos tener en cuenta algunos resultados sobre el anillo de enteros gaussianos $\mathbb{Z}[i]$.

Sea $D$ un anillo. Un elemento no invertible $a \in D \backslash \{0\}$ se llama irreducible (en $D$) si para todo $b, c \in D$ tales que $a = bc$, se tiene que $b$ o $c$ es invertible en $D$.

Siguiendo [4] tenemos que los elementos invertibles en $\mathbb{Z}[i]$ están caracterizados como aquellos $a + bi \in \mathbb{Z}[i]$ tales que $N(a + bi) = 1$. La función $N: \mathbb{Z}[i] \to \mathbb{N}$ (función norma) está definida como $N(a + bi) = a^2 + b^2$ para todo $a + bi \in \mathbb{Z}[i]$. Y además un cálculo directo muestra que si $\alpha, \beta \in \mathbb{Z}[i]$ entonces $N(\alpha\beta) = N(\alpha)N(\beta)$.

Tenemos entonces que el anillo $\mathbb{Z}[i]$ es un dominio de factorización única. Es decir, todo elemento no nulo y no invertible de $\mathbb{Z}[i]$ se representa de manera única como producto de elementos irreducibles de $\mathbb{Z}[i]$. Y esto implica que todo elemento irreducible $\mathrm{t} \in \mathbb{Z}[i]$ satisface que si para cualesquiera $a, b \in \mathbb{Z}[i]$, $\mathrm{t} \mid ab$ entonces $\mathrm{t} \mid a$ o $\mathrm{t} \mid b$.

El siguiente teorema que incluimos es un resultado clásico de teoría de números. Su demostración puede encontrarse en [5], [11] o [12].

**Teorema 3.2**. (Pequeño Teorema de Fermat) Sea $p$ un número primo. Entonces $\overline{x}^{p-1} = \overline{1}$ para todo $\overline{x} \in \mathbb{Z}_p \backslash \{\overline{0}\}$.

El siguiente teorema recoge varios resultados importantes de teoría de números. Incluimos la demostración completa ya que es de gran importancia para este trabajo.

**Teorema 3.3**. (Fermat) Sea $p$ un número primo. Las siguientes afirmaciones son equivalentes:

1. $p = 2$ o $p \equiv 1 \bmod 4$.
2. Existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -1 \bmod p$.
3. $p$ no es irreducible en $\mathbb{Z}[i]$.
4. $p$ es suma de dos cuadrados.

**Demostración.** $1 \Rightarrow 2$. Si $p = 2$ basta tomar $a = 1$. Sea $p = 4n + 1$ para algún $n \in \mathbb{N}$. El Teorema 3.2 implica que $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ son las raíces del polinomio $x^{p-1} - \overline{1} \in \mathbb{Z}_p[x]$. Luego

$$x^{p-1} - \overline{1} = (x - \overline{1})(x - \overline{2}) \ldots (x - \overline{p-1})$$

Y como $p - 1 = 4n$ se tiene que

$$x^{p-1} - \overline{1} = x^{4n} - \overline{1} = (x^{2n} - \overline{1})(x^{2n} + \overline{1}).$$

Es decir,

$$(x^{2n} - \overline{1})(x^{2n} + \overline{1}) = (x - \overline{1})(x - \overline{2}) \ldots (x - \overline{p-1}).$$

Como $\mathbb{Z}_p[x]$ es un dominio de factorización única se concluye que $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ son todas las raíces del polinomio $(x^{2n} - \overline{1})(x^{2n} + \overline{1})$. Luego existe $b \in \{1,2, \ldots, p-1\}$ tal que $\overline{b}^{2n} + \overline{1} = \overline{0}$. Así tomando $a = b^n$ se tiene que $\overline{a}^2 = -\overline{1}$. Es decir, $a^2 \equiv -1 \bmod p$.

$2 \Rightarrow 3$. Supongamos que existe $a \in \mathbb{Z}$ tal que $a^2 + 1 = kp$ para algún $k \in \mathbb{Z}$ y que $p$ es irreducible en $\mathbb{Z}[i]$. Entonces, $(a + i)(a - i) = kp$ y tenemos que $p \mid (a + i)(a - i)$. Luego $p \mid a + i$ o $p \mid a - i$. En el primer caso se tiene que $a + i = pe + pfi$ para algunos $e, f \in \mathbb{Z}$. Luego $1 = pf$ lo cual es contradictorio. El otro caso también conduce a una contradicción. Por tanto, $p$ no es irreducible en $\mathbb{Z}[i]$.

$3 \Rightarrow 4$. Por hipótesis existen $a + bi, c + di \in \mathbb{Z}[i]$ tales que $p = (a + bi)(c + di)$ y $N(a + bi) = a^2 + b^2 \neq 1$, $N(c + di) = c^2 + d^2 \neq 1$. Tomando normas a ambos lados de la igualdad resulta $p^2 = (a^2 + b^2)(c^2 + d^2)$. Y esto implica que $p = a^2 + b^2$.

$4 \Rightarrow 1$. Hay sólo tres posibilidades para el primo $p$: $p = 2$, $p$ es de la forma $4k + 1$ o $p$ es de la forma $4k + 3$. Veamos que ningún entero de la forma $4k + 3$ es suma de dos cuadrados. Si $a$ es un entero cualquiera, entonces $\overline{a} = \overline{0}, \overline{1}, \overline{2}$ o $\overline{3}$ (mod 4). Así $\overline{a}^2 = \overline{0}$ o $\overline{1}$ (mod 4). Por tanto si $a, b \in \mathbb{Z}$ las únicas posibilidades para $\overline{a}^2 + \overline{b}^2$ son $\overline{0}, \overline{1}$ o $\overline{2}$ (mod 4). Y como cualquier entero de la forma $4k + 3$ es igual $\overline{3}$ (mod 4), concluimos que cualquier entero de esta forma no es suma de dos cuadrados. ■

Una de las consecuencias del Teorema 3.3 es que todo número primo $p$ de la forma $4k + 3$ es irreducible en $\mathbb{Z}[i]$, o equivalentemente, si $p$ es un primo que no es suma de dos cuadrados, entonces $p$ es irreducible en $\mathbb{Z}\{i]$.

**Afirmación 3.4.** Sea $p$ un primo que no es suma de dos cuadrados. Si para algún $k \in \mathbb{Z}$, $kp = a^2 + b^2$, para algunos $a, b \in \mathbb{Z}$, entonces $a$ y $b$ son múltiplos de $p$.

**Demostración.** Supongamos que $kp = a^2 + b^2$ con $a, b \in \mathbb{Z}$. Entonces, $kp = (a + bi)(a - bi)$ y entonces $p \mid a + bi$ o $p \mid a - bi$ por el Teorema 3.3. En el primer caso $a + bi = pe + pfi$ para algunos $e, f \in \mathbb{Z}$. Así, $a = pe$ y $b = pf$, es decir, $a$ y $b$ son múltiplos de $p$. En el segundo caso un razonamiento análogo muestra también que $a$ y $b$ son múltiplos de $p$. Por tanto, en cualquier caso $a$ y $b$ son múltiplos de $p$. ■

Ahora sí podemos probar el recíproco de la Afirmación 3.1.

**Afirmación 3.5.** Sea $p$ un primo. Si $p$ no es suma de dos cuadrados, entonces $\mathbb{Z}_p \otimes \mathbb{Z}_p$ es un cuerpo.

**Demostración.** Sea $(\overline{c}, \overline{d}) \in \mathbb{Z}_p \times \mathbb{Z}_p$ con $(\overline{c}, \overline{d}) \neq (\overline{0}, \overline{0})$. Entonces $\overline{c} \neq \overline{0}$ o $\overline{d} \neq \overline{0}$, es decir, $c$ no es múltiplo de $p$ o $d$ no es múltiplo de $p$. Así por la Afirmación 3.4, $c^2 + d^2 \neq kp$ para todo $k \in \mathbb{Z}$, lo cual implica que $\overline{c^2 + d^2} \neq \overline{0}$ en $\mathbb{Z}_p$. Como $\mathbb{Z}_p$ es un cuerpo, entonces existe el inverso de $\overline{c^2 + d^2}$, es decir, $\left(\overline{c^2 + d^2}\right)^{-1} \in \mathbb{Z}_p$. Por tanto el elemento dado por $\left(\overline{c}\left(\overline{c^2 + d^2}\right)^{-1}, -\overline{d}\left(\overline{c^2 + d^2}\right)^{-1}\right) \in \mathbb{Z}_p \otimes \mathbb{Z}_p$ y es fácil ver que este elemento es el inverso de la pareja $(\overline{c}, \overline{d})$. Luego se concluye que $\mathbb{Z}_p \times \mathbb{Z}_p$ es un cuerpo. ■

Uniendo la Afirmación 3.1 y la Afirmación 3.5 el problema propuesto queda completamente determinado en la siguiente forma "*Sea $p$ un primo. El anillo $\mathbb{Z}_p \otimes \mathbb{Z}_p$ es un cuerpo, si y solo si, $p$ no es suma de dos cuadrados*". O usando el Teorema 3.3, nuestro resultado también puede ser enunciado como "*Sea $p$ un primo. El anillo $\mathbb{Z}_p \otimes \mathbb{Z}_p$ es un cuerpo, si y solo si, $p$ es de la forma $4k + 3$*".

Por la Observación 2.3 tenemos que para un primo $p$ cualquiera, los anillos $\mathbb{Z}_p \otimes \mathbb{Z}_p$ y $M(\mathbb{Z}_p)$ son isomorfos. Así

para el caso en que el primo $p$ es de la forma $4k+3$, tenemos que $\mathbb{Z}_p \otimes \mathbb{Z}_p$ y $M(\mathbb{Z}_p)$ son cuerpos isomorfos.

Recordemos que queremos obtener el análogo de los complejos para el caso finito $\mathbb{Z}_p$, $p$ primo. Resta ver entonces un cociente adecuado de $\mathbb{Z}_p[x]$. Nuevamente el Teorema 3.3 nos dice que "El *primo* $p$ *es de la forma* $4k+1$ *o es* 2, *si y solo si, existe* $a \in \mathbb{Z}$ *tal que* $a^2 \equiv -1$ *(mod* $p$*)*". O equivalentemente, "*El primo* $p$ *es de la forma* $4k+3$*, si y solo si,* $\overline{a}^2 + \overline{1} \neq \overline{0}$ *(mod* $p$*), para todo* $a \in \mathbb{Z}$".

Así tenemos que si $p$ es un primo de la forma $4k+3$, entonces el polinomio $x^2 + \overline{1} \in \mathbb{Z}_p[x]$ no tiene raíces en $\mathbb{Z}_p$. Como dicho polinomio es de grado menor o igual que 3, concluimos entonces que es irreducible sobre $\mathbb{Z}_p$. De este modo el anillo cociente $\mathbb{Z}_p[x]/\langle x^2+\overline{1}\rangle$ es un cuerpo, el cual está dado por

$$\mathbb{Z}_p[x]/\langle x^2+\overline{1}\rangle = \{\overline{a} + \overline{b}x + \langle x^2+\overline{1}\rangle : \overline{a}, \overline{b} \in \mathbb{Z}_p\}$$

Con esto encontramos entonces el siguiente isomorfismo.

**Afirmación 3.5**. Sea $p$ un primo de la forma $4k+3$. Los cuerpos $\mathbb{Z}_p \otimes \mathbb{Z}_p$ y $\mathbb{Z}_p[x]/\langle x^2+\overline{1}\rangle$ son isomorfos.

**Demostración**. Basta definir la función $\varphi: \mathbb{Z}_p \otimes \mathbb{Z}_p \to \mathbb{Z}_p[x]/\langle x^2+\overline{1}\rangle$, como $\varphi\left((\overline{a}, \overline{b})\right) = \overline{a} + \overline{b}x + \langle x^2+\overline{1}\rangle$ para todo $(\overline{a}, \overline{b}) \in \mathbb{Z}_p \otimes \mathbb{Z}_p$. ■

Obtenemos entonces el siguiente diagrama de cuerpos isomorfos (Figura 2), análogo al obtenido para los números reales (Figura 1).

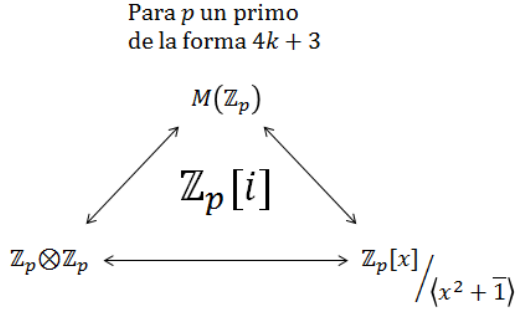


Figura 2. Representaciones isomorfas del cuerpo $\mathbb{Z}_p[i]$.

## IV. CONCLUSIONES

Los resultados obtenidos en este trabajo pueden resumirse en las siguientes líneas.

- Se presentaron las tres versiones conocidas de los números complejos como el producto cartesiano $\mathbb{R} \otimes \mathbb{R}$ con algunas operaciones especiales, como el conjunto de matrices $M(\mathbb{R})$ con las operaciones usuales y como el cociente $\mathbb{R}[x]/\langle x^2+1\rangle$. Y se mostró porqué los números complejos pueden escribirse como $\mathbb{C} = \{a + bi : a, b \in \mathbb{R},\ i^2 = -1\}$.

- A partir de un anillo conmutativo con unidad $A$, se hicieron las construcciones análogas $A \otimes A$ y $M(A)$ y se mostró que las dos corresponden a anillos conmutativos con unidad, los cuales son isomorfos. Además se mostró que ellas representan el conjunto de números complejos sobre el anillo $A$, los cuales se denotaron como $A[i] = \{a + bi : a, b \in A,\ i^2 = -1\}$.

- Se observó que el anillo $\mathbb{Z}_p[i]$, $p$ primo, no es un cuerpo en general. Y se demostró con todo detalle que $\mathbb{Z}_p[i]$ es un cuerpo, si y solo si, $p$ es un primo de la forma $4k+3$ o equivalentemente el primo $p$ no es suma de dos cuadrados (Afirmación 3.1 y Afirmación 3.5).

- Se demostró que para cualquier primo $p$ de la forma $4k+3$, el cuerpo $\mathbb{Z}_p[i]$ tiene las mismas tres representaciones isomorfas, obtenidas para los números complejos $\mathbb{C}$ (ver Figura 2).

## REFERENCIAS


[1]. K. Ríbnikov, *Historia de las Matemáticas*, Moscú: Editorial Mir, 1987.

[2]. J. R. Newman, *Sigma: El mundo de las Matemáticas*, Barcelona: Ediciones Grijalbo S.A., 1985.

[3]. D. S. Dummit and R. M. Foote, *Abstract Algebra*, New Delhi: Wiley India Pvt. Ltd., 2016.

[4]. A. Garcia and Y. Lequain, *Elementos de Álgebra*, Rio de Janerio: IMPA, 2013.

[5]. J. B. Conway, *Functions of One Complex Variable*, New York: Springer-Verlag, 1995.

[6]. K. H. Spindler, *Abstract Algebra and Applications, Vol. II Rings and Fields*, New York: Marcel Dekker Inc., 1994.

[7]. J. B. Fraleigh, *A First Course in Abstract Algebra*, New York: Addison-Wesley, 1982.

[8]. A. Gonçalves, *Introdução à Álgebra*, Rio de Janeiro: IMPA, 2006.

[9]. A. A. Allam, M. J. Dunne, J. R. Jack, J. C. Lynd and H. W. Ellingsen Jr., "Classification of the or the group of units in the Gaussian integers modulo N", *Pi Mu Epsilon Journal*, Vol. 12, No. 9, pp., 513-519, 2008.

[10]. J. Stillwell, *Elements of Number Theory*, New York: Springer-Verlag, 2003.

[11]. R. Jiménez, E. Gordillo y G. Rubiano, *Teoría de Números para Principiantes*, Bogotá: Unibiblos, 1999.

[12]. I. Vinogradov, *Fundamentos de la Teoría de los Números*, Moscú: Editorial Mir, 1977.