PROPIEDAD DE LA DIAGONAL EN ANILLOS CONMUTATIVOS

ANGIE SANDALIE ENRIQUEZ JARAMILLO

FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
2018

PROPIEDAD DE LA DIAGONAL EN ANILLOS CONMUTATIVOS

ANGIE SANDALIE ENRIQUEZ JARAMILLO

Trabajo presentado como requisito parcial para optar al título de Licenciada en Matemáticas

Asesor
John Hermes Castillo Gómez
Doctor en Matemáticas

FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA
UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
2018

Nota de Responsabilidad

Todas las ideas y conclusiones aportadas en el siguiente trabajo son responsabilidad exclusiva del autor.

Artículo 1^{ro} del Acuerdo No. 324 de octubre 11 de 1996 emanado por el Honorable Consejo Directivo de la Universidad de Nariño.

Nota de Aceptación

John Hermes Castillo Gómez
Presidente de Tesis

Wilson Fernando Mutis
Jurado

Viviana Carolina Guerrero
Jurado

San Juan de Pasto, 22 de Febrero de 2018

Este trabajo está dedicado a mi familia por haberme brindado su apoyo incondicional durante todo este tiempo.

Agradecimientos

La vida se encuentra llena de retos y sueños, uno de ellos es la Universidad. Tras verme dentro de ella, me he dado cuenta que mas allá de ser un reto o un sueño, es una base no solo para mi entendimiento y comprensión de las matemáticas, sino para lo que concierne en la vida misma, el ser persona y en mi futuro.

Le agradezco infinitamente a Dios por darme la sabiduría para acabar esta etapa, a mi familia en especial a mi padre y madre, a quienes les debo como persona y quienes con su comprensión y apoyo incondicional me han permitido hacer muchos sueños realidad. Finalmente a mi asesor Dr. Jhon Castillo por la orientación, el seguimiento y la supervisión continua de este trabajo, pero sobre todo por la dedicación, la motivación y apoyo a lo largo de este tiempo.

Angie Sandalie Enriquez Jaramillo

Universidad de Nariño
Febrero 2018.

Resumen

Algunos números satisfacen ciertas propiedades que los hace especiales. En este trabajo se estudia una propiedad especial que tienen los divisores de 24, los divisores de 12 y los divisores de 4 o de 6. La primera se aprecia cuando se realiza la tabla multiplicativa de Cayley para los anillos $\mathbb{Z}_n$, en la cual los 1's aparecen únicamente en la diagonal principal, si n es un divisor de 24. Esta surgió en una clase de teoría de números, en la cual el estudiante del Profesor Chebolu llamado Elliott Mahler formuló la siguiente pregunta: ¿Para qué valores de n, los 1's están unicamente en la diagonal principal y nunca fuera de ella? En la actualidad este patrón se denomina La propiedad de la diagonal y en este trabajo se realiza el estudio detallado de esta propiedad en los anillos $\mathbb{Z}_n$, en los anillos de polinomios $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$ y su extensión a la propiedad cúbica de la diagonal para los anillos $\mathbb{Z}_n$. Finalmente, se plantean algunas cuestiones abiertas para la investigación las cuales están relacionadas con la propiedad de la diagonal en otros anillos.

Abstract

Some numbers satisfy certain properties that make them special. In this work we study one special property of the divisors of 24, the divisors of 12 and the divisors of 4 or 6. The first is seen when the multiplication Cayle's table is made for the rings $\mathbb{Z}_n$, for which the 1's appear only in the main diagonal, if n is a divisor of 24. The above arose in a number theory class of the Professor Chebolu's a student named Elliott Mahler asked the following question: "I see that 1's in these multiplication tables appear only on the diagonal. Is that always true?" Nowadays, this pattern is known as the diagonal property. In this work we give a detailed study of this property for the rings $\mathbb{Z}_n$, the rings of polynomials $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$ and its extension called the diagonal cubic property for the rings $\mathbb{Z}_n$. Finally, we state some research open questions related to the study of the diagonal property in other rings.

Índice general

Introducción

El estudio de la propiedad de la diagonal es muy reciente debido a que surge del estudio del Profesor Sunil K. Chebolu de la Universidad Estatal de Ilinois en el año 2012, quien en su artículo titulado "What is special about the divisors of 24?", ver [4]; menciona que por medio de la observación de una tabla multiplicativa de Cayley su estudiante Elliott Mahler se formula la siguiente pregunta: ¿para qué valores de n, los 1's están unicamente en la diagonal principal y nunca fuera de ella? Esto ha despertado el interés de varios investigadores como: Chebolu, Genzlinger, Lockridge, entre otros, ver [4, 6, 10]. En estas investigaciones se utilizaron diferentes herramientas de la teoría de números, grupos y anillos.

Este trabajo se enfoca específicamente en recopilar y organizar algunos resultados que obtuvieron diferentes investigadores en el estudio de la propiedad de la diagonal en los anillos $\mathbb{Z}_n$, anillos de polinomios $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$ y su extensión a la propiedad de la diagonal cúbica para los anillos $\mathbb{Z}_n$.

De esta manera este trabajo se ha organizado en cuatro capítulos que se han denominado de la siguiente manera: Preliminares, Propiedad de la diagonal para anillos $\mathbb{Z}_n$, Propiedad de la diagonal para anillos $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$ y finalmente un capítulo denominado Propiedad cúbica de la diagonal para anillos $\mathbb{Z}_n$.

En el primer capítulo se muestra algunas definiciones y teoremas que serán de utilidad para el desarrollo y comprensión de los temas que se abordan en los capítulos posteriores, en el segundo se da respuesta al interrogante: ¿Para cuales valores de n los 1's están en la diagonal principal y nunca fuera de ella? que es precisamente la propiedad de la diagonal, además se presentan cinco demostraciones diferentes que dan respuesta a este interrogante, cada una de ellas basada desde diferentes teoremas muy importantes de la teoría de números. En el tercer capítulo se estudia la propiedad de la diagonal en los anillos de polinomios $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$, estudio que se basa en el capítulo anterior puesto que $\mathbb{Z}_n$ es un subanillo de $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$. Finalmente en el cuarto capítulo se estudia la extensión de la propiedad de la diagonal hacia la propiedad cúbica de la diagonal en los anillos $\mathbb{Z}_n$ en la cual se da respuesta a la pregunta ¿para cuáles n el 1 aparece en la tabla de multiplicación cúbica de $\mathbb{Z}_n$ unicamente en la diagonal principal o proviene de los planos coordenados?

Cabe resaltar que aunque el estudio de esta propiedad es reciente, ha ido evolucionando y a partir de ello han surgido nuevas investigaciones. Así por ejemplo se puede encontrar otros autores que estudian esta propiedad en otros anillos conmutativos como es el caso de Chebolu y colaboradores que en su artículo [5], la estudian en el contexto de álgebras de grupo o el estudio de Castillo y Caranguay en [3], que extienden esta propiedad para estudiar el concepto de k unidades módulo n. De esta manera el lector puede encontrar que el estudio de esta propiedad es un campo abierto en el que pueden surgir futuras investigaciones.

Capítulo 1

Preliminares

En este capítulo se presentan algunas definiciones y teoremas relacionados con la Teoría de Números, Teoría de Grupos y Teoría de Anillos, los cuales se utilizan a lo largo de este trabajo. Aunque aquí no se exponen sus demostraciones, se las puede encontrar en los siguientes libros, ver [2, 7, 12, 1, 9, 13, 11]. El objetivo es contribuir a la comprensión de cada uno de estos temas ya que ayudarán al desarrollo de los siguientes capítulos.

1.1. Teoría de Números

1.1.1. Divisibilidad

Teorema 1.1 (Algoritmo de la división)**.** *Dados enteros a y b, con $b > 0$, existen enteros únicos q y r tales que*

$$a = bq + r, \quad 0 \leq r < b.$$

Los enteros q y r se llaman el cociente y el residuo, respectivamente, en la división de a por b.

Corolario 1.1. *Si a y b son enteros, con $b \neq 0$, entonces existen enteros únicos q y r tales que*

$$a = bq + r, \quad 0 \leq r \leq |b|.$$

Definición 1.1 (Divisibilidad)**.** Sean a, b enteros donde $a \neq 0$. Se dice que a divide a b si existe un entero k tal que $b = ak$. En tal caso se denota $a|b$ y se dice que a es un divisor de b o que b es un múltiplo de a. Para indicar que a no divide a b se escribe $a \nmid b$.
Es fácil verificar que para todo entero k, $1|k$ y que si $k \neq 0$, $k|k$.

De la anterior definición se tiene que si a es un divisor de b, entonces b también es divisible por $-a$, es decir, los divisores de un entero vienen por pares. Por esta razón los resultados y definiciones se limitarán a los divisores positivos, aunque algunos de ellos se podrían enunciar también para divisores negativos.

Teorema 1.2. *Sean a, b y c enteros entonces*

1. *Si $a \neq 0$ entonces $a|0, a|a, a|(-a)$,*
2. *$1|a$, $(-1)|a.$,*
3. *Si $a|b$ entonces $a|bc$,*
4. *Si $a|b$ y $c|d$ entonces $ac|bd$,*
5. *Si $a|b$ y $b|c$ entonces $a|c$,*
6. *Si $a|b$ y $a|c$ entonces para todo $x, y \in \mathbb{Z}$, se tiene $a|(bx + cy)$,*
7. *Si $a|b$ y $b \neq 0$ entonces $|a| \leq |b|$,*
8. *Si $a|b$ y $b|a$ entonces $a = b$ o $a = (-b)$.*

Definición 1.2 (Máximo común divisor)**.** Sean a y b enteros con al menos uno de ellos diferente de cero, se denomina a $m > 0$ como el máximo común divisor de a y b si $m|a$, $m|b$ y para todo d tal que $d|a$ y $d|b$ se tiene que $d|m$. Se denota con $\gcd(a, b)$ al máximo común divisor de a y b.

El siguiente teorema presenta una caracterización del máximo común divisor de a y b en términos de combinación lineal.

Teorema 1.3. *Sean a y b enteros, con al menos uno de ellos diferente de cero, y sea $\gcd(a, b) = d$, entonces d es el menor entero positivo que se puede expresar como una combinación lineal de a y b y se denota*

$$d = min\left\{ax + by \in \mathbb{Z}^+ : x, y \in \mathbb{Z}\right\}$$

Definición 1.3 (Primos relativos)**.** Se dice que dos enteros a y b son primos relativos si $\gcd(a, b) = 1$; es decir, si el único factor común positivo que tienen es 1.

Definición 1.4 (Mínimo común múltiplo)**.** Sean a y b enteros, el mínimo común múltiplo de a y b, denotado por $lcm(a, b)$ es el entero positivo m tal que $a|m$ y $b|m$. Además si existe un $c > 0$ tal que $a|c$ y $b|c$ entonces $m \leq c$.

1.1.2. Congruencias

Definición 1.5 (Congruencia)**.** Se dice que a y b son congruentes módulo $n \neq 0$, lo que se denota por $a \equiv b$ mód n, si n divide a $a - b$.

En caso que $n \nmid (a - b)$ entonces se dice que a y b son incongruentes módulo n, y se escribe $a \not\equiv b(\text{mód} n)$.

Teorema 1.4. *Sean a y b enteros, $a \equiv b(\text{mód}n)$ si y sólo si a y b dejan el mismo residuo cuando se dividen por n.*

El siguiente teorema presenta algunas propiedades de las congruencias, las cuales son muy útiles en lo que sigue.

Teorema 1.5. *Si $a \equiv b(\text{mód}n)$ y $c \equiv d(\text{mód}n)$ entonces*

1. *Para todo par de enteros r y $s, ar + cs \equiv br + ds(\text{mód}n)$.*
2. *$ac \equiv bd(\text{mód}n)$.*
3. *Para todo entero $k, ak \equiv bk(\text{mód}n)$.*
4. *Para todo entero $r, a + r \equiv b + r(\text{mód}n)$.*
5. *Para todo entero $r, ar \equiv br(\text{mód}n)$.*

1.1.3. Números primos

Definición 1.6. Un entero $p > 1$ es un número primo si sus únicos divisores positivos son 1 y el mismo.

Teorema 1.6 (Lema de Euclides)**.** *Si p es primo y $p|ab$ entonces $p|a$ o $p|b$*

Teorema 1.7 (Euclides)**.** *Existen infinitos números primos*

Por otro lado se tienen en cuenta las siguientes definiciones.

Definición 1.7 (Función de Euler)**.** Para un entero positivo n, se denota por $\phi(n)$ el número de enteros positivos menores o iguales que n que son primos relativos con n.

Definición 1.8 (Unidades módulo n)**.** Para cada $n > 1$ se denota con $\mathcal{U}_n$ al conjunto de todos los enteros positivos menores que n y primos relativos con n.

1.2. Teoría de Grupos

1.2.1. Grupos y Subgrupos

Definición 1.9 (Operación binaria)**.** Sea G un conjunto diferente de vacío; una operación binaria en G (usualmente llamada multiplicación) es una función de $G \times G$ en G que asigna a cada par de elementos (a, b) de G un elemento en G denotado por ab.

Definición 1.10 (Grupo)**.** Sea G un conjunto con una operación binaria $\cdot$, se dice que $(G, \cdot)$ es un grupo, si satisface las siguientes condiciones.

- **Asociativa**: para cualesquier $a, b, c \in G$ se tiene que

$$a(bc) = (ab)c.$$

- **Identidad**: existe un elemento e llamado identidad o elemento neutro en G tal que

$$ae = ea = a, \text{ para todo } a \in G.$$

- **Inverso**: para cada elemento a en G, existe un elemento b en G (llamado inverso de a) tal que

$$ab = ba = e.$$

De esta manera un grupo es un conjunto con una operación binaria, asociativo, con identidad en el que cada elemento tiene inverso.

Definición 1.11 (Tabla de Cayley)**.** Sea $G = \{g_1, g_2, ..., g_n\}$ un conjunto y $\cdot$ una operación binaria de G. La tabla de Cayley de $(G, \cdot)$ es una matriz de tamaño $n \times n$, tal que tal que en la (i, j)-ésima entrada aparece el resultado de la operación $g_i \cdot g_j$.

Definición 1.12 (Grupo Abeliano)**.** Un grupo G se denomina abeliano o conmutativo si cumple que $ab = ba$ para todo par de elementos $a, b \in G$.

Definición 1.13 (Grupo cíclico)**.** Un grupo G se denomina cíclico si existe un $g \in G$ tal que $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.

Definición 1.14 (Orden de un grupo)**.** El número de elementos de un grupo (finito o infinito) se denomina su orden y se denota $|G|$.

Definición 1.15 (Orden de un elemento)**.** El orden de un elemento g de un grupo G es el menor entero positivo n tal que $g^n = e$ (en notación aditiva es el menor entero positivo n tal que $ng = 0$). Se denota con $|g|$.

Teorema 1.8. *Si d es un divisor positivo de n, el número de elementos de orden d en un grupo cíclico de orden n es $\phi(d)$.*

La demostración del anterior teorema se puede encontrar en [9, pag. 79].

Ejemplo 1.1. El conjunto $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ para $n \geq 1$ es un grupo cíclico con la adición modulo n.

Definición 1.16 (Subgrupo)**.** Si un subconjunto no vacío H de un grupo G también es un grupo bajo la operación de G, se dice que H es un subgrupo de G y se denota $H \leq G$.

1.2.2. Isomorfismo de Grupos

Definición 1.17 (Isomorfismo de Grupos)**.** Un isomorfismo ϕ de un grupo G a un grupo $\bar{G}$ es una función uno a uno de G sobre $\bar{G}$ que preserva la operación del grupo; esto es.

$$\phi(ab) = \phi(a)\phi(b) \text{ para todo } a, b \text{ en } G.$$

Si hay un isomorfismo de G a $\bar{G}$, se dice que G y $\bar{G}$ son isomorfos y se denota $G \approx \bar{G}$.

1.2.3. Producto directo externo

Definición 1.18 (Producto directo externo)**.** Sea $G_1, G_2, \ldots, G_n$ una colección finita de grupos. El producto directo externo de $G_1, G_2, \ldots, G_n$ escrito como $G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, g_2, \ldots, g_n) : g_i \in G_i\}$ donde la operación se realiza componente a componente; esto es

$$(g_1, g_2, \ldots, g_n) \cdot (h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n),$$

y la operación en la i-ésima coordenada es la del grupo G_i.

Teorema 1.9. *Sean G y H grupos cíclicos finitos entonces $G \oplus H$ es cíclico si y solo si $|G|$ y $|H|$ son primos relativos.*

Corolario 1.2. *Sea $m = n_1n_2 \cdots n_k$ entonces*

$$\mathbb{Z}_m \approx \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$$

si y solo si n_i y n_j son primos relativos cuando $i \neq j$.

1.3. Teoría de Anillos

1.3.1. Anillos y Subanillos

Definición 1.19 (Anillo)**.** Un anillo $(R, +, \cdot)$ es un conjunto R con dos operaciones binarias, adición (denotada por $a + b$) y multiplicación (denotada por ab), tal que para todo $a, b, c \in R$ se cumple lo siguiente.

1. $a + b = b + a$,
2. $(a + b) + c = a + (b + c)$,
3. existe un elemento 0 en R tal que $a + 0 = 0 + a = a$,
4. para cada elemento $a \in R$, existe un elemento $-a \in R$ tal que $a + (-a) = 0$,
5. $a(bc) = (ab)c$,

6. $a(b+c) = ab + ac$ y $(b+c)a = ba + ca$.

Así un anillo es un grupo Abeliano bajo la adición, tal que la multiplicación es asociativa y distributiva tanto por izquierda como por derecha.

Definición 1.20 (Anillo conmutativo)**.** Un anillo R se denomina conmutativo si $ab = ba$ para todo par de elementos $a, b \in R$.

Además no todo anillo tiene una identidad multiplicativa, por tanto es necesario dar la siguiente definición.

Definición 1.21 (Anillo con identidad)**.** Un anillo R se denomina anillo con identidad, si tiene un elemento $1 \neq 0$ tal que $r1 = 1r = r$ para todo $r \in R$.

Ejemplo 1.2. El conjunto $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ bajo la suma y la multiplicación módulo n es un anillo conmutativo con identidad 1.

Cabe aclarar que en este trabajo se estudia los anillos conmutativos con identidad.

Definición 1.22 (Subanillo)**.** Un subconjunto no vacío S de un anillo R es un subanillo de R, si S es un anillo bajo las operaciones de R.

Definición 1.23. Sea R un anillo con identidad, se dice que a es una unidad (elemento invertible) de R si existe $b \in R$ tal que $ab = 1$ y $ba = 1$.

Definición 1.24. Sea R un anillo. Se denota con $\mathcal{U}(R)$ el conjunto de las unidades (los elementos invertibles) de R. Denotado por

$$\mathcal{U}(R) = \{a \in R : a \text{ es una unidad}\}.$$

1.3.2. Homomorfismo e isomorfismo

Definición 1.25 (Homomorfismo e isomorfismo de anillos)**.**

Un homomorfismo de anillos ϕ de un anillo R a un anillo S es una función de R a S que preserva las operaciones; esto es, para todo $a, b \in R$ se tiene que.

$$\phi(a+b) = \phi(a) + \phi(b),$$
$$\phi(ab) = \phi(a)\phi(b).$$

Ademas, si R y S tienen identidad se pide que $\phi(1_R) = 1_S$.

Si un homomorfismo de anillos es biyectivo entonces se llamará **isomorfismo de anillos**.

1.3.3. Dominio entero y divisores de cero

Definición 1.26 (Divisores de cero)**.** Un divisor de cero es un elemento a no nulo de un anillo conmutativo R tal que existe un elemento b no nulo en R para el que $ab = 0$.

Definición 1.27 (Dominio entero)**.** Un dominio entero es un anillo conmutativo con identidad, sin divisores de cero.

1.3.4. Ideales y anillos factores

Definición 1.28 (Ideal)**.** Un subanillo A de un anillo R se denomina un ideal de R si para todo $r \in R$ y todo $a \in A$ tanto ar como ra están en A.

Definición 1.29 (Ideal primo)**.** Un ideal primo A de un anillo conmutativo R es un ideal propio de R tal que $a, b \in R$ y $ab \in A$ implica que $a \in A$ o $b \in A$.

Definición 1.30 (Ideal maximal)**.** Un ideal maximal de un anillo conmutativo R es un ideal propio A de R, tal que si B es un ideal de R y $A \subseteq B \subseteq R$, entonces $B = A$ o $B = R$.

Teorema 1.10 (Anillo factor o anillo cociente)**.** *Sea R un anillo y sea A ideal de R. El conjunto de clases $\{r + A : r \in R\}$ es un anillo bajo las operaciones*

$$(s + A) + (t + A) = (s + t) + A \quad y \quad (s + A)(t + A) = st + A.$$

Teorema 1.11. *Sean R un anillo conmutativo con identidad y A un ideal de R. Entonces R/A es un dominio entero si y solo si A es primo.*

1.3.5. Nilpotente y nilradical

Definición 1.31 (Nilpotente)**.** Sean R un anillo y $a \in R$. Se dice que a es un elemento nilpotente si $a^n = 0$ para algún entero positivo n.

Definición 1.32 (Nilradical)**.** El nilradical de un anillo conmutativo R es el conjunto de todos los elementos nilpotentes de R.

El siguiente resultado relaciona los elementos nilpotentes con los ideales primos de un anillo, su demostración se puede encontrar en [7, Prop. 12, p. 674].

Proposición 1.1. *El nilradical N de un anillo conmutativo R es la intersección de todos los ideales primos de R.*

1.3.6. Suma directa externa de anillos

Definición 1.33. Sean $R_1, R_2, \ldots, R_n$ anillos. El anillo

$$R_1 \dot{\oplus} R_2 \dot{\oplus} \cdots \dot{\oplus} R_n = \{(a_1, a_2, \ldots, a_n) : a_i \in R_i, 1 \leq i \leq n\},$$

con la adición y multiplicación definida componente a componente se denomina la suma directa externa de los anillos $R_1, R_2, \ldots, R_n$.

1.3.7. Anillos de polinomios

Definición 1.34 (Anillo de polinomios sobre R)**.** Sea R un anillo conmutativo. El conjunto formado por

$$R[x] = \left\{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : a_i \in R, n \text{ es un entero no negativo } \right\}.$$

se denomina anillo de polinomios sobre R en la indeterminada x.

Definición 1.35. Sean R un anillo conmutativo, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ y $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ elementos de $R[x]$. Entonces la suma y el producto de polinomios se define.

$$f(x) + g(x) = (a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \cdots + (a_1 + b_1)x + a_0 + b_0,$$

donde $s = \text{máx}\{m, n\}$, $a_i = 0$ para $i > n$, y $b_i = 0$ para $i > m$. Además,

$$f(x)g(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_1 x + c_0,$$

donde $c_k = a_k b_0 + a_{k-1}b_1 + \cdots + a_1 b_{k-1} + a_0 b_k$ para $k = 0, \ldots, m+n$.

Adicionalmente se puede probar el siguiente resultado.

Teorema 1.12. *Si D es un dominio entero, entonces $D[x]$ es un dominio entero.*

La demostración de este teorema se puede encontrar en [9, Teorema 16.1, p. 296]

Capítulo 2

Propiedad de la diagonal en anillos $\mathbb{Z}_n$

En este capítulo se presenta el estudio de la propiedad de la diagonal que surge a partir del artículo, ver [4] "What is special about the divisors of 24?", del Profesor Sunil K. Chebolu de la Universidad Estatal de Ilinois.

2.1. Propiedad de la Diagonal

El Profesor Sunil K. Chebolu menciona [4] que en una clase de Teoría de Números su estudiante Elliott Mahler al observar las siguientes tablas de Cayley

$\mathbb{Z}_2=$

$\cdot$	0	1
0	0	0
1	0	1

$\mathbb{Z}_3=$

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4=$

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_5=$

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Tabla 2.1: Tablas de Cayley multiplicativas para $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4$ y $\mathbb{Z}_5$.

notó que en las tres primeras, es decir para $\mathbb{Z}_2, \mathbb{Z}_3$ y $\mathbb{Z}_4$, el 1 siempre aparece en la diagonal principal; mientras que para $\mathbb{Z}_5$ esto no sucede. A partir de lo anterior formuló la siguiente pregunta: ¿para qué valores de n, los 1's están únicamente en la diagonal principal y nunca fuera de ella?

La respuesta a este interrogante dio origen al siguiente teorema, el cual es el teorema principal de este capítulo.

Teorema 2.1. *La tabla multiplicativa de Cayley para $\mathbb{Z}_n$ los 1's únicamente aparecen en la diagonal principal si y solo si n es un divisor de 24.*

Antes de presentar las cinco demostraciones diferentes que probarán el teorema principal es necesario tener en cuenta la siguiente proposición.

Proposición 2.1. *Sea n un entero positivo entonces las siguientes afirmaciones son equivalentes.*

1) Los 1's en la tabla multiplicativa de Cayley para $\mathbb{Z}_n$ están únicamente en la diagonal principal.

2) Si a es un elemento invertible en $\mathbb{Z}_n$, entonces $a^2 = 1$ en $\mathbb{Z}_n$.

3) Si a es un entero positivo que es primo relativo con n, entonces $n|a^2 - 1$.

4) Si p es un primo que no divide a n, entonces $n|p^2 - 1$.

Demostración.

- 1) $\Rightarrow$ 2)
  Sea a es un elemento invertible en $\mathbb{Z}_n$; luego existe $b \in \mathbb{Z}_n$, tal que $ab \equiv 1(\text{mód}\, n)$. Es decir, el 1 está en la tabla multiplicativa de Cayley en la intersección de la fila que contiene a a y la columna que contiene a b. Ahora, por hipótesis se tiene que todos los unos deben estar en la diagonal principal, de ahí que a y b deben ser iguales, esto es $a^2 \equiv 1(\text{mód}\, n)$.

- 2) $\Rightarrow$ 3)
  Sea a un entero positivo primo relativo con n. Entonces a es un elemento invertible en $\mathbb{Z}_n$. Luego por la hipótesis $a^2 = 1$ en $\mathbb{Z}_n$.

- 3) $\Rightarrow$ 4)
  Sea p un primo que no divide a n. Entonces p y n son primos relativos, así $n|p^2 - 1$.

- 4) $\Rightarrow$ 1)
  Sean a y b en $\mathbb{Z}_n$ tal que en la tabla de Cayley la entrada correspondiente a la coordenada (a, b) es 1. Esto significa que $ab = 1$ en $\mathbb{Z}_n$. En particular, esto implica que a es invertible en $\mathbb{Z}_n$, lo cual es equivalente a tener $\gcd(a, n) = 1$.

  De esta manera si $a = 1$ entonces $b = 1$ y así $a = b$. Luego el 1 aparece en la diagonal principal.

  Si $a > 1$ entonces se considera su factorización prima $a = p_1^{c_1} p_2^{c_2} \dots p_r^{c_r}$, puesto que a es primo relativo con n se tiene que ninguno de los p_i dividen a n.

  Por hipótesis se tiene que $p_i^2 \equiv 1(\text{mód}\, n)$ para todo i.

Luego $a^2 = (p_1^{c_1} p_2^{c_2} \dots p_r^{c_r})^2 = (p_1^2)^{c_1} (p_2^2)^{c_2} \dots (p_r^2)^{c_r} \equiv 1^{c_1} 1^{c_2} \dots 1^{c_r} \equiv 1 (\text{mód} n)$.

Esto implica que $a^2 = 1$ en $\mathbb{Z}_n$ y así $a = b$. Por lo tanto, el 1 aparece unicamente en la diagonal principal.

□

2.2. Tablas multiplicativas de Cayley para los divisores de 24

En esta sección se va a demostrar el recíproco del Teorema 2.1, es decir la implicación « si n es un divisor de 24 entonces n tiene la propiedad de la diagonal», por medio de las tablas multiplicativas de Cayley. Por esta razón en lo que sigue se muestra cada uno de los divisores de 24 con sus respectivas tablas multiplicativas de Cayley; en las cuales se puede apreciar que cada una de ellas cumple con la propiedad de la diagonal.

$\mathbb{Z}_1 = \{1\}$

$\mathbb{Z}_2 =$

·	0	1
0	0	0
1	0	1

$\mathbb{Z}_3 =$

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4 =$

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_6 =$

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\mathbb{Z}_8=$

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

$\mathbb{Z}_{12}=$

$\cdot$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

$\mathbb{Z}_{24} =$

·	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2	0	2	4	6	8	10	12	14	16	18	20	22	0	2	4	6	8	10	12	14	16	18	20	22
3	0	3	6	9	12	15	18	21	0	3	6	9	12	15	18	21	0	3	6	9	12	15	18	21
4	0	4	8	12	16	20	0	4	8	12	16	20	0	4	8	12	16	20	0	4	8	12	16	20
5	0	5	10	15	20	**1**	6	11	16	21	2	7	12	17	22	3	8	13	18	23	4	9	14	19
6	0	6	12	18	0	6	12	18	0	6	12	18	0	6	12	18	0	6	12	18	0	6	12	18
7	0	7	14	21	4	11	18	**1**	8	15	22	5	12	19	2	9	16	23	6	13	20	3	10	17
8	0	8	16	0	8	16	0	8	16	0	8	16	0	8	16	0	8	16	0	8	16	0	8	16
9	0	9	18	3	12	21	6	15	0	9	18	3	12	21	6	15	0	9	18	3	12	21	6	15
10	0	10	20	6	16	2	12	22	8	18	4	14	0	10	20	6	16	2	12	22	8	18	4	14
11	0	11	22	9	20	7	18	5	16	3	14	**1**	12	23	10	21	8	19	6	17	4	15	2	13
12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12
13	0	13	2	15	4	17	6	19	8	21	10	23	12	**1**	14	3	16	5	18	7	20	9	22	11
14	0	14	4	18	8	22	12	2	16	6	20	10	0	14	4	18	8	22	12	2	16	6	20	10
15	0	15	6	21	12	3	18	9	0	15	6	21	12	3	18	9	0	15	6	21	12	3	18	9
16	0	16	8	0	16	8	0	16	8	0	16	8	0	16	8	0	16	8	0	16	8	0	16	8
17	0	17	10	3	20	13	6	23	16	9	2	19	12	5	22	15	8	**1**	18	11	4	21	14	7
18	0	18	12	6	0	18	12	6	0	18	12	6	0	18	12	6	0	18	12	6	0	18	12	6
19	0	19	14	9	4	23	18	13	8	3	22	17	12	7	2	21	16	11	6	**1**	20	15	10	5
20	0	20	16	12	8	4	0	20	16	12	8	4	0	20	16	12	8	4	0	20	16	12	8	4
21	0	21	18	15	12	9	6	3	0	21	18	15	12	9	6	3	0	21	18	15	12	9	6	3
22	0	22	20	18	16	14	12	10	8	6	4	2	0	22	20	18	16	14	12	10	8	6	4	2
23	0	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	**1**

2.3. Demostraciones del teorema principal

En las siguientes subsecciones se van a presentar las cinco demostraciones del teorema principal a partir de los siguientes resultados de la teoría de números: el Teorema Chino de los restos, la estructura de las unidades, el Teorema de Dirichlet sobre primos en progesiones aritméticas, el Teorema de Bertrand- Chebyshev y el Teorema de Erdös- Ramanujan.

Es necesario resaltar que las cinco demostraciones que se estudiarán a continuación en realidad demostrarán que si n tiene la propiedad de la diagonal entonces n es un divisor de 24.

2.3.1. Teorema Chino de los restos

En esta sección se presenta una demostración del Teorema 2.1 usando el Teorema Chino de los restos. Este teorema fue estudiado por primera vez por el matemático chino Sun Tzu en el siglo III y originalmente se establece en su forma clásica como la solución a un sistema de congruencias lineales dado. Por una solución de la congruencia $ax \equiv b(\text{mód} n)$ se entiende como un entero x_0 tal que $ax_0 \equiv b\,(\text{mód} n)$. La solución de un sistema de congruencias lineales se puede encontrar por medio del Teorema Chino de los Restos, el cual se puede plantear de la siguiente manera.

Teorema 2.2. *Sean $n_1, n_2, \ldots, n_r$ enteros positivos tales que n_i, n_j son primos relativos entre sí para $i \neq j$. Entonces el sistema de congruencias lineales*

$$\begin{aligned} x &\equiv a_1 \,(\text{mód} n_1), \\ x &\equiv a_2 \,(\text{mód} n_2), \\ &\vdots \\ x &\equiv a_r \,(\text{mód} n_r), \end{aligned}$$

tiene solución única módulo $n_1 n_2 \cdots n_r$.

En este caso se desea interpretar el anterior teorema desde el punto de vista de la teoría de anillos, en el cual si $R_1, R_2, \ldots, R_n$ son anillos, entonces $R_1 \oplus R_2 \oplus \cdots \oplus R_n$, denota el producto directo externo de R_i está dado por el conjunto de n-uplas $(r_1, r_2, \ldots, r_n)$ con $r_i \in R_i$. Teniendo en cuenta lo anterior se presenta la otra versión del Teorema Chino de los restos con la que se va a demostrar el teorema principal de este capítulo.

Teorema 2.3 (Teorema Chino de los restos)**.** *Sean a, b enteros positivos primos relativos entre sí, entonces $\mathbb{Z}_{ab} \approx \mathbb{Z}_a \oplus \mathbb{Z}_b$ como anillos.*

En este estudio no se va a tratar la demostración de este teorema sin embargo la misma se puede encontrar en [7, p. 265]. Antes de realizar la demostración del teorema principal es necesario tener en cuenta los siguientes lemas.

Lema 2.1. *Sean G y H grupos tales que $G \approx H$. Si G tiene la propiedad de la diagonal, entonces H tiene la propiedad de la diagonal.*

Demostración. Sean $\psi : G \to H$ un isomorfismo de grupos y $x \in G$. Si G tiene la propiedad de la diagonal entonces $x^2 = 1$. Por otro lado, sea $y \in H$ tal que $y = \psi(x)$. Luego, $y^2 = \psi(x)^2 = \psi(x^2) = \psi(1) = 1$. Por tanto, H tiene la propiedad de la diagonal. □

Definición 2.1. Sea R un anillo con identidad. Se dice que $a \in R$ es una involución si $a^2 = 1$.

La definición anterior, lleva a establecer que para que un anillo R tenga la propiedad de la diagonal es equivalente a que todas sus unidades sean involuciones; este resultado se presenta a continuación.

Afirmación 1. Sea R un anillo con identidad. Entonces R tiene la propiedad de la diagonal si y solo si toda unidad en este anillo es una involución.

Lema 2.2. *Sean $R_1, R_2, \ldots, R_n$ una colección finita de anillos con identidad. Entonces el producto directo externo $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ tiene la propiedad de la diagonal si y solo si R_i tiene la propiedad de la diagonal para cada $1 \leq i \leq n$.*

Demostración. Sea $x \in \mathcal{U}(R_i)$, se tiene que $(1, 1, \ldots, x_i, \ldots 1) \in \mathcal{U}(R_1 \oplus R_2 \oplus \cdots \oplus R_n)$ donde x_i es la i-ésima entrada.

Por hipótesis $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ tiene la propiedad de la diagonal entonces $(1, 1, \ldots, x_i, \ldots 1)^2 = (1, 1, \ldots, 1, \ldots, 1)$. Luego $x_i^2 = 1$. De ahí que R_i tiene la propiedad de la diagonal para cada $1 \leq i \leq n$.

En la otra implicación, sea $(x_1, x_2, \ldots, x_n) \in \mathcal{U}(R_1 \oplus R_2 \oplus \cdots \oplus R_n)$. Luego se sabe que $x_i \in \mathcal{U}(R_i)$. Entonces $x_i^2 = 1$ para todo i. Es decir, $(x_1, x_2, \ldots, x_n)^2 = (x_1^2, x_2^2, \ldots, x_n^2) = (1, 1, \ldots, 1)$.

Por lo tanto $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ tiene la propiedad de la diagonal. □

A continuación se realiza la demostración del teorema principal.

Demostración del Teorema 2.1 usando el Teorema Chino de los restos. Sea $n \in \mathbb{Z}^+$ con la propiedad de la diagonal, entonces se consideran los siguientes casos.

- **Caso 1**. Si n es impar. Entonces $\gcd(2, n) = 1$, por el item 4 de la proposición 2.1, se tiene que $n|2^2 - 1$; es decir, $n|3$. Lo cual indica que $n = 1$ o $n = 3$.

- **Caso 2**. Si $n = 2^t$ donde t es algún entero positivo.
  Puesto que el $\gcd(3, n) = 1$ y la proposición 2.1, se tiene que $n|3^2 - 1$; esto es $n|8$. De ahí que $n = 2, 4$ u 8.

- **Caso 3**. Si $n = 2^t k$ donde t es un entero positivo y $k > 1$ es impar.
  Por el Teorema 2.3 se tiene que $\mathbb{Z}_n \approx \mathbb{Z}_{2^t} \oplus \mathbb{Z}_k$. Dado que $\mathbb{Z}_n$ tiene la propiedad de la diagonal, entonces por el Lema 2.1, se sigue que $\mathbb{Z}_{2^t} \oplus \mathbb{Z}_k$ tiene la propiedad de la diagonal. Luego el Lema 2.2 implica que, cada uno de los términos de este producto directo externo tienen esta propiedad. Ahora por el primer caso $k = 3$ y por el segundo caso $1 \leq t \leq 3$. Es decir que

t	k	$n = 2^t k$
1	3	6
2	3	12
3	3	24

De los anteriores casos se deduce que si n tiene la propiedad de la diagonal entonces $n = 1, 2, 3, 4, 6, 8, 12$ o 24, esto es n es un divisor de 24. □

2.3.2. Estructura algebraica de las unidades para $\mathbb{Z}_n$

En esta sección se presenta la demostración del Teorema 2.1 a partir de la estructura de las unidades, la cual está dada de la siguiente manera.

Teorema 2.4. *Sea $n = {p_1}^{c_1} {p_2}^{c_2} \ldots {p_k}^{c_k}$ la factorización prima de un entero positivo $n > 1$, entonces $\mathcal{U}(n) \approx \mathcal{U}({p_1}^{c_1}) \oplus \mathcal{U}({p_2}^{c_2}) \oplus \cdots \oplus \mathcal{U}({p_k}^{c_k})$ como grupos.*

Cabe aclarar que no se va a realizar la demostración de este teorema, pero se la puede encontrar en [12, p. 124]. A partir del resultado anterior y del Lema 2.2, se puede obtener la siguiente proposición.

Proposición 2.1. *Sea $n = {p_1}^{c_1}{p_2}^{c_2}\cdots{p_k}^{c_k}$. Entonces n tiene la propiedad de la diagonal si y solo si $p_i^{c_i}$ tiene la propiedad de la diagonal.*

De esta manera, para estudiar los n que satisfacen la propiedad de la diagonal, basta con encontrar aquellas potencias de primos p^c que la satisfacen. Para esto, se utilizará la estructura de $\mathcal{U}(p^c)$, resultado que se presenta a continuación.

Teorema 2.5 (Estructura algebraica de las unidades)**.** *Sean p un primo y c un entero positivo. Entonces*

$$\mathcal{U}(p^c) \approx \begin{cases} C_1, & \text{si } p^c = 2^1, \\ C_2, & \text{si } p^c = 2^2, \\ C_2 \oplus C_{2^{c-2}}, & \text{si } p^c = 2^c \text{ donde } c \geq 3, \\ C_{\phi(p^c)}, & \text{si } p \text{ es impar}, \end{cases}$$

donde C_k es el grupo cíclico de orden k y ϕ es la función de Euler.

Observe que el isomorfismo que se presenta es un isomorfismo de grupos y además aunque en este estudio no se presenta la demostración de esta estructura, se puede encontrar en [12, p.124].

Teniendo en cuenta el teorema 2.5, se realiza la demostración del teorema para p^c.

Teorema 2.6. *Sean p un primo y c un entero positivo. Si p^c tiene la propiedad de la diagonal, entonces satisface que.*

1. *$p = 2$ y $0 \leq c \leq 3$,*
2. *$p = 3$ y $c = 1$.*

Demostración. Suponga que p^c tiene la propiedad de la diagonal. Por hipótesis, se tiene que $a^2 = 1$ para todo $a \in \mathcal{U}(p^c)$, entonces la demostración se resume en identificar para cuales grupos dados por el Teorema 2.5 satisfacen que sus elementos tienen orden a lo más 2.

- C_1 es el grupo cíclico que tiene un elemento, el cual es de orden 1; esto significa que cumple con la propiedad de la diagonal.
- $C_2 = \langle a \rangle = \{1, a\}$. Luego $a^2 = 1$ y $1^2 = 1$. De ahí que cumple con la propiedad de la diagonal. Así en este caso, $p = 2$ y $c = 2$.

- $C_2 \oplus C_{2^{c-2}}$, donde $c \geq 3$
  Sean $C_2 = \langle a \rangle = \{1, a\}$ y $C_{2^{c-2}} = \langle b \rangle = \left\{1, b, b^2, \ldots, b^{2^{c-2}-1}\right\}$. Si se toma $(x, y) \in C_2 \oplus C_{2^{c-2}}$ entonces $x \in C_2$ y $y \in C_{2^{c-2}}$ lo que significa que $x \in \{1, a\}$, $y = b^k$ para algún $0 \leq k \leq 2^{c-2} - 1$. Puesto que p^c tiene la propiedad de la diagonal entonces $(x, y)^2 = (1, 1)$ si y solo si $x^2 = 1$ y $y^2 = 1$, lo que implica que $b^{2k} = 1$. De ahí $2^{c-2} | 2k$ para cualquier k. En particular cuando $k = 1$, esto lleva a que $c - 2 \leq 1$. Por tanto, el hecho de que $C_2 \oplus C_{2^{c-2}}$ tiene la propiedad de la diagonal implica que $c = 3$.

- $C_{\phi(p^c)}$, donde p es un primo impar y $c \in \mathbb{Z}^+$.

  Puesto que $\phi(p^c) = p^{c-1}(p-1)$, y como el orden de cualquier elemento debe ser a lo más 2 entonces se tiene lo siguiente

  $$p^{c-1}(p-1) \leq 2.$$

  Se tienen los siguientes casos

  - Si $p > 3$, entonces $p^{c-1}(p-1) > 2$, lo cual es una contradicción.
  - Si $p = 3$, entonces $3^{c-1}(3-1) \leq 2$, implica que $3^{c-1} \leq 1$. Lo que significa que $c = 1$. Luego $p^c = 3$.

□

Ahora se realiza la demostración del teorema principal a partir del Teorema 2.4.

Demostración de Teorema 2.1 a partir de la estructura algebraica de las unidades. De los teoremas 2.5 y 2.6, se observa que la descomposición prima de n es la siguiente $n = 2^u 3^v$ donde $0 \leq u \leq 3$ y $0 \leq v \leq 1$, la que corresponde exactamente con aquella de los divisores de 24. □

2.3.3. Teorema de Dirichlet

En esta sección se presenta la demostración del Teorema 2.1 a partir del Teorema de Dirichlet acerca de primos en una progresión aritmética; el cual se conoce como el Teorema de Dirichlet y tiene el siguiente enunciado.

Teorema 2.7 (Teorema de Dirichlet)**.** *Dado cualquier par de números enteros s, t primos relativos entre sí, la progresión aritmética $\{sx + t : x \in \mathbb{Z}^+\}$ contiene un número infinito de números primos.*

Este teorema fue conjeturado por el matemático Adrien-Marie Legendre y demostrado por Peter Gustav Lejeune Dirichlet en el año 1837 por medio de las L-series de Dirichlet. En este trabajo no se estudiará su demostración, pero se puede encontrar una discusión en [12, p.401].

Demostración del Teorema 2.1 usando el Teorema de Dirichlet. Sea $n \in \mathbb{Z}^+$ con la propiedad de la diagonal. Considere la progresión aritmética $S = \{qx + 2 : x \in \mathbb{Z}^+\}$ donde $q > 3$ y el $\gcd(q, 2) = 1$, además suponga que q es un divisor primo de n. Por el Teorema de Dirichlet se tiene que en S existen infinitos primos, entonces se escoge un primo $p \in S$ tal que $p \nmid n$. De ahí que existe $b \in \mathbb{Z}^+$ tal que $pb \equiv 1(\text{mód}n)$. Puesto que n tiene la propiedad de la diagonal y por la Proposición 2.1, se tiene que $n|p^2 - 1$.

Puesto que $q|n$ y como $n|p^2 - 1$, entonces $q|p^2 - 1$, es decir $q|(p - 1)(p + 1)$. Por el Lema de Euclides, ver Lema 1.6, $q|p - 1$ o $q|p + 1$, de esta forma existe $x \in \mathbb{Z}$ tal que

$$p - 1 = qx \text{ o } p + 1 = qx$$
$$p = qx + 1 \text{ o } p = qx - 1$$

Esto es una contradicción al hecho que $p \in S$. Por tanto no existe un primo que divida a n tal que $q > 3$. Luego $q \leq 3$.

Esto significa que los divisores primos de n pueden ser unicamente 2 o 3. Esto implica que $gcd(n, 5) = 1$, lo que por la Proposición 2.1, $n|5^2 - 1 = 24$. Es decir, n es un divisor de 24.

□

2.3.4. Teorema de Bertrand-Chebyshev

En esta sección se va a demostrar el Teorema 2.1 por medio del Teorema de Bertrand-Chebyshev el cual afirma que.

Teorema 2.8 (Teorema de Bertrand-Chebyshev)**.** *Sea $n \geq 2$ un entero, entonces existe al menos un número primo p tal que $n < p < 2n$.*

Fue conjeturado por Bertrand en el año 1845 aunque no consiguió hacer ninguna demostración. Después de cinco años (1850) Chebyshev presentó una demostración analítica a este teorema, sin embargo Erdös en 1932 dio otra demostración de este teorema usando algunas propiedades de coeficientes binomiales. Con respecto a la demostración presentada por Erdös se puede encontrar en [8], puesto que en este estudio no se presentará.

Para demostrar el Teorema 2.1 usando el Teorema de Bertrand-Chebyshev se utilizará la siguiente definición.

Definición 2.2 (Función Piso)**.** La función piso se aplica a un número real x y retorna el mayor entero menor o igual que x, es decir

$$\begin{aligned} \lfloor x \rfloor : &\mathbb{R} \to \mathbb{Z} \\ &x \to y = \lfloor x \rfloor = \text{máx}\{k \in \mathbb{Z} \mid k \leq x\}. \end{aligned}$$

A continuación se presentará la demostración del Teorema 2.1 a partir del Teorema de Bertrand-Chebyshev.

Demostración del Teorema 2.1 usando el Teorema de Bertrand-Chebyshev. Sea $n \in \mathbb{Z}^+$ con la propiedad de la diagonal y sea p un primo tal que $p \not| n$. Entonces $\gcd(p, n) = 1$, y por la Proposición 2.1, $n|p^2 - 1$ entonces $p^2 - 1 \geq n$, lo que significa que $p \geq \sqrt{n+1}$.

El contra recíproco de la anterior afirmación dice que si $p < \sqrt{n+1}$ entonces $p|n$. Por el Teorema de Bertrand-Chebyshev se sabe que existe un primo p tal que $n < p < 2n$. Se asume que $\frac{\sqrt{n+1}}{4} \geq 5$ y se consideran los siguientes dos intervalos

$$\left(\frac{\sqrt{n+1}}{4}, \frac{\sqrt{n+1}}{2}\right), \left(\frac{\sqrt{n+1}}{2}, \sqrt{n+1}\right).$$

Por el Teorema 2.8, existen primos P_1 y P_2 tales que

$$\left\lfloor \frac{\sqrt{n+1}}{4} \right\rfloor < P_1 < \left\lfloor \frac{\sqrt{n+1}}{2} \right\rfloor \text{ y } \left\lfloor \frac{\sqrt{n+1}}{2} \right\rfloor < P_2 < \left\lfloor \sqrt{n+1} \right\rfloor.$$

De esta manera se tiene que $P_1 < P_2 < \sqrt{n+1}$.

Puesto que $\frac{\sqrt{n+1}}{4} \geq 5$ entonces $P_2 > P_1 > 5$, de ahí que $2, 3, 5 \leq \frac{\sqrt{n+1}}{4} < \sqrt{n+1}$ entonces $2, 3, 5, P_1, P_2$ dividen a n. Esto implica que $lcm(2, 3, 5, P_1, P_2)|n$, es decir que $30P_1P_2 \leq n$.

Como $\frac{\sqrt{n+1}}{4} < P_1$ y $\frac{\sqrt{n+1}}{2} < P_2$ se sigue que

$$\begin{aligned} 30\left(\frac{\sqrt{n+1}}{4}\right)\left(\frac{\sqrt{n+1}}{2}\right) &\leq n \\ 15(n+1) &< 4n \\ 11n &< -15 \\ n &< \frac{-15}{11}. \end{aligned}$$

Lo cual es una contradicción a que $n \in \mathbb{Z}^+$.

Por lo tanto, se considera $\frac{\sqrt{n+1}}{4} < 5$ y además $\sqrt{n+1} > 7$.

De $\frac{\sqrt{n+1}}{4} < 5$ implica que $n \leq 398$ *(2.2.1)* y de $\sqrt{n+1} > 7$, se tiene que $2, 3, 5, 7$ dividen a n. Luego $lcm(2, 3, 5, 7)|n$. Así $210|n$.

Si $210|n$ entonces $n = 210t$ donde $t \in \mathbb{Z}^+$. Se considera los siguientes casos.

- **Caso 1**. Si $t = 1$ entonces $n = 210$. Esto implica que $210 < 398$, es decir cumple con la condición *(2.2.1)*.
- **Caso 2**. Si $t = 2$ entonces $n = 420$. Implica que $420 > 398$. Lo cual lleva a contradecir la condición *(2.2.1)*.

Por tanto se toma el caso 1, pero se tiene que $11 \cdot 191 = 2101$ es decir, $11 \cdot 191 = 2101 \equiv 1(\text{mód}210)$. Luego no cumple con la propiedad de la diagonal.

De esta manera se considera $\frac{\sqrt{n+1}}{4} < 5$ y $\sqrt{n+1} \leq 7$.

Similarmente, cuando $\sqrt{n+1} \leq 7$ se tiene que $n \leq 48$. Se consideran los siguientes dos casos.

- **Caso 1**. Cuando $\sqrt{n+1} > 5$ entonces $2, 3, 5$ dividen a n. Así $lcm(2,3,5)|n$. Luego $30|n$.

  Si $30|n$ entonces $n = 30t$ donde $t \in \mathbb{Z}^+$, se tiene en cuenta lo siguiente.

  - Si $t = 1$ entonces $n = 30$. Esto implica que n cumple con $n \leq 48$.
  - Si $t = 2$ entonces $n = 60$. Contradice el hecho de que $n \leq 48$.

  Luego se toma cuando $t = 1$, pero $7 \cdot 13 = 91$ es decir, $7 \cdot 13 = 91 \equiv 1(\text{mód}30)$, así no cumple con la propiedad de la diagonal.

  Por tanto se descarta este caso y se tiene en cuenta el siguiente.

- **Caso 2**. Cuando $\sqrt{n+1} \leq 5$. Lo que significa que $n \leq 24$.

Así $n \leq 24$, pero existen algunos en este intervalo que no cumplen con la propiedad de la diagonal, para los cuales en la siguiente tabla se presenta una pareja (a, b) tal que $ab \equiv 1$ mód n pero $a \not\equiv b$ mód n.

n	$\mathbb{Z}_n$	(a, b)
5	$\mathbb{Z}_5$	$3 \cdot 2 = 6 \equiv 1(\text{mód}5)$
7	$\mathbb{Z}_7$	$5 \cdot 3 = 15 \equiv 1(\text{mód}7)$
9	$\mathbb{Z}_9$	$2 \cdot 5 = 10 \equiv 1(\text{mód}9)$
10	$\mathbb{Z}_{10}$	$7 \cdot 3 = 21 \equiv 1(\text{mód}10)$
11	$\mathbb{Z}_{11}$	$8 \cdot 7 = 56 \equiv 1(\text{mód}11)$
13	$\mathbb{Z}_{13}$	$9 \cdot 3 = 27 \equiv 1(\text{mód}13)$
14	$\mathbb{Z}_{14}$	$5 \cdot 3 = 15 \equiv 1(\text{mód}14)$
15	$\mathbb{Z}_{15}$	$8 \cdot 2 = 16 \equiv 1(\text{mód}15)$
16	$\mathbb{Z}_{16}$	$13 \cdot 5 = 65 \equiv 1(\text{mód}16)$
17	$\mathbb{Z}_{17}$	$6 \cdot 3 = 18 \equiv 1(\text{mód}17)$
18	$\mathbb{Z}_{18}$	$11 \cdot 5 = 55 \equiv 1(\text{mód}18)$
19	$\mathbb{Z}_{19}$	$5 \cdot 4 = 20 \equiv 1(\text{mód}19)$
20	$\mathbb{Z}_{20}$	$7 \cdot 3 = 21 \equiv 1(\text{mód}20)$
21	$\mathbb{Z}_{21}$	$11 \cdot 2 = 22 \equiv 1(\text{mód}21)$
22	$\mathbb{Z}_{22}$	$9 \cdot 5 = 45 \equiv 1(\text{mód}22)$
23	$\mathbb{Z}_{23}$	$8 \cdot 3 = 24 \equiv 1(\text{mód}23)$

Tabla 2.2: Contraejemplos de la propiedad de la diagonal para algunos $n \leq 24$.

Por lo tanto, como se muestra en la Sección 2.2, los n que cumplen con la propiedad de la diagonal son $n = 1, 2, 3, 4, 6, 8, 12$ y 24, que son exactamente los divisores de 24. □

2.3.5. Teorema de Erdös y Ramanujan

En esta sección se va a realizar la demostración del Teorema principal, 2.1 por medio del Teorema de Erdös y Ramanujan, el cual afrima lo siguiente.

Teorema 2.9 (Teorema de Erdös-Ramanujan)**.** *Sea n un número entero mayor o igual que 6, entonces hay por lo menos dos números primos entre n y $2n$.*

Este teorema es una extensión del Teorema de Bertrand- Chebyshev anteriormente mencionado; aunque en 1852 Chebyshev presentó la demostración de este teorema, se tuvo que esperar un siglo (1919) para que Ramanujan presentara una demostración usando algunas propiedades de la función Gamma y la fórmula de la Stirling y trece años más (1932) para que Paul Erdös presentara otra demostración de este teorema, la cual utiliza propiedades de los coeficientes binomiales. La demostración realizada por Ramanujan se puede encontrar en [14], debido a que no se presentará en este estudio.

Demostración del Teorema 2.1 usando el Teorema de Erdös-Ramanujan. Sean $n \in \mathbb{Z}^+$ con la propiedad de la diagonal y el primo p tal que $p \nmid n$. Entonces, por la Proposición 2.1 se tiene que $n|p^2-1$, esto es $p^2-1 \geq n$ o equivalentemente $p \geq \sqrt{n+1}$.

Tomando el contra recíproco se tiene que si $p < \sqrt{n+1}$, entonces $p|n$.

Considere el siguiente intervalo $\left(\frac{\sqrt{n+1}}{2}, \sqrt{n+1}\right)$.

Si $\frac{\sqrt{n+1}}{2} \geq 6$, por el Teorema de Erdös y Ramanujan este intervalo tiene al menos dos primos P_1 y P_2 tales que $\left\lfloor \frac{\sqrt{n+1}}{2} \right\rfloor < P_1, P_2 < \lfloor \sqrt{n+1} \rfloor$.

Puesto que $\frac{\sqrt{n+1}}{2} \geq 6$, los primos $2, 3, 5 < \frac{\sqrt{n+1}}{2} < \sqrt{n+1}$. Es decir, $(2)(3)(5)\left(\frac{\sqrt{n+1}}{2}\right)^2 \leq n$.

Esto implica que $lcm(2, 3, 5, P_1, P_2)$ dividen a n; de ahí que $30P_1P_2 \leq n$.

Además $\frac{\sqrt{n+1}}{2}$ es menor que P_1 y P_2, entonces

$$\begin{aligned} 30\left(\frac{\sqrt{n+1}}{2}\right)^2 &\leq n \\ 30\left(\frac{n+1}{4}\right) &\leq n \\ 30(n+1) &\leq 4n \\ n &\leq \frac{-15}{13}. \end{aligned}$$

Esto contradice el hecho de que $n \in \mathbb{Z}^+$.

Por lo tanto se considera $\frac{\sqrt{n+1}}{2} < 6$ y $\sqrt{n+1} > 7$.

Si $\frac{\sqrt{n+1}}{2} < 6$ implica que $n \leq 142$ y si $\sqrt{n+1} > 7$, entonces $2, 3, 5, 7$ dividen a n. Luego $lcm(2, 3, 5, 7)|n$. Así $210|n$.

Si $210|n$ entonces $n = 210t$ donde $t \in \mathbb{Z}^+$. Pero si $t = 1$ entonces $n = 210$, esto contradice el hecho que $n \leq 142$. Por lo tanto se considera $\sqrt{n+1} \leq 7$. Esto implica que $n \leq 48$, se analiza los siguientes casos

- **Caso 1:**. Si $\sqrt{n+1} > 5$, entonces $2, 3, 5$ dividen a n. De ahí que $lcm(2, 3, 5)|n$. Luego $30|n$.

  Si $30|n$ entonces $n = 30t$ donde $t \in \mathbb{Z}^+$

  - Si $t = 1$ entonces $n = 30$. Luego n cumple con que $n \leq 48$.
  - Si $t = 2$ entonces $n = 60$. Esto contradice el hecho de que $n \leq 48$.

  Por tanto se toma cuando $t = 1$, pero se tiene que $7 \cdot 13 = 91$ es decir, $7 \cdot 13 = 91 \equiv 1(\,\text{mód}\,30)$. Luego no cumple con la propiedad de la diagonal.

  De esta manera se descarta el anterior caso.

- **Caso 2:**. Si $\sqrt{n+1} \leq 5$. Entonces $n \leq 24$.

De ahí que $n \leq 24$. Luego por la Tabla 2.2 y por la Sección 2.2 se tiene que los n que cumplen con la propiedad de la diagonal son los divisores de 24. □

Capítulo 3

Propiedad de la diagonal en anillos $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$

Este capítulo está enfocado en el estudio de la propiedad de la diagonal en los anillos $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$ que está basado en el artículo,"What is special about the divisors of 12?", del Profesor Sunil K. Chebolu y Michael Mayers, en el año 2012, ver [6]. Este artículo es consecuencia de "What is special about the divisors of 24?"[4], que fue estudiado en el capítulo anterior.

3.1. Propiedad de la diagonal

En el anterior capítulo se estudió la propiedad de la diagonal para anillos $\mathbb{Z}_n$, donde se observó que aquellos que la cumplían son los divisores de 24 y se podía representar en tablas multiplicativas de Cayley para $\mathbb{Z}_n$; en este caso se va a estudiar las condiciones que el anillo de polinomios $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$ debe cumplir para que los 1's estén en la diagonal principal.

Aquí se debe tener en cuenta que realizar la tabla multiplicativa de Cayley para $\mathbb{Z}_n[x]$ es imposible puesto que su tamaño es infinito; por tanto el trabajo se centrará en utilizar propiedades de los anillos en general, las cuales posteriormente se aplicarán al anillo $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$.

Antes de presentar el teorema principal de este capítulo es necesario tener en cuenta algunas definiciones, lemas y proposiciones, que se utilizarán en la demostración de ese teorema.

Lema 3.1. *Sea R un anillo conmutativo con identidad. Si u es una unidad en R y r es un elemento nilpotente en R, entonces $u + r$ es una unidad en R.*

Demostración. Sea k el entero positivo tal que $r^k \neq 0$ y $r^{k+1} = 0$. Entonces el inverso de $u + r$ está

dado por $v = u^{-1} \sum_{i=0}^{k} (-1)^i (ru^{-1})^i$, puesto que

$$\begin{aligned}(u+r)v &= uu^{-1} \sum_{i=0}^{k} (-1)^i (ru^{-1})^i + ru^{-1} \sum_{i=0}^{k} (-1)^i (ru^{-1})^i \\ &= 1 - ru^{-1} + \left(ru^{-1}\right)^2 - \cdots + (-1)^k \left(ru^{-1}\right)^k + \\ &\qquad ru^{-1} - \left(ru^{-1}\right)^2 - \cdots + (-1)^{k-1} \left(ru^{-1}\right)^k + (-1)^k \left(ru^{-1}\right)^{k+1} \\ &= 1.\end{aligned}$$

□

Definición 3.1. Un anillo R se denomina anillo reducido si no tiene elementos nilpotentes distintos de cero.

Ejemplo 3.1. Los anillos $\mathbb{Z}_2$, $\mathbb{Z}_3$ y $\mathbb{Z}_6$ son anillos reducidos porque no tienen elementos nilpotentes diferentes de cero. En cambio el anillo $\mathbb{Z}_4$ no es un anillo reducido porque tiene el elemento nilpotente 2, tal que $2^2 = 4 \equiv 0(\text{mód}4)$.

El siguiente es un resultado muy conocido del cual puede encontrarse una discusión en [7, Apéndice 1].

Lema 3.2 (Lema de Zorn)**.** *Sea S un conjunto no vacío parcialmente ordenado. Si toda cadena T de S tiene una cota superior en S, entonces S tiene al menos un elemento maximal.*

Este lema se utilizará en la demostración del siguiente teorema.

Teorema 3.1. *Todo anillo conmutativo R con identidad 1, tiene al menos un ideal maximal.*

Demostración. Sea S el conjunto de todos los ideales propios de R que no contienen al 1. Se asigna un orden a S mediante la inclusión; puede verificarse que esta relación de inclusión es una relación de orden parcial. Además, S es diferente del vacío porque el ideal generado por 0, pertenece a S. Para aplicar el Lema de Zorn se debe demostrar que toda cadena de S tiene una cota superior en S.

Sea $(I_\alpha)_{\alpha \in K}$ una cadena de ideales de S, para cada par de índices $\alpha, \beta \in K$ se tiene que $I_\alpha \subset I_\beta$ o $I_\beta \subset I_\alpha$. Sea $A = \bigcup_\alpha I_\alpha, \alpha \in K$ entonces A es un ideal y $1 \notin A$ porque $1 \notin I_\alpha$ para todo $\alpha \in K$. Luego $A \in S$ y además A es una cota superior de la cadena. Por tanto, por el Lema de Zorn S tiene un elemento maximal. □

Teorema 3.2. *Sea R un anillo conmutativo. Todo ideal maximal de R es un ideal primo.*

Demostración. Sea M es un ideal maximal entonces $R/M = \{a + m : a \in R\}$ es un cuerpo. Suponga que $ab \in M$. Luego $(a + M)(b + M) = ab + M = M$ y como R/M es un domino entero se tiene que $a + M = M$ o $b + M = M$, así $a \in M$ o $b \in M$. Por lo tanto, M es un ideal primo. □

Teorema 3.3. *Sea R un anillo conmutativo. Un polinomio $f(x_1, x_2, \ldots, x_m)$ es una unidad en $R[x_1, x_2, \ldots, x_m]$ si y solo si el término constante de f es una unidad en R y todos los otros coeficientes de f son nilpotentes en R.*

Demostración. Para realizar la demostración se tiene en cuenta los siguientes dos casos.

- **Caso particular**. Supongamos que R es un dominio entero y f es una unidad en $R[x_1, x_2, \ldots, x_m]$ entonces existe un polinomio $g \in R[x_1, x_2, \ldots, x_m]$ tal que $fg = 1$.
  Como R es un dominio entero, se tiene que $deg(fg) = deg(f) + deg(g)$. Luego comparando grados se tiene que $deg(f) + deg(g) = 0$. De ahí que f y g son polinomios constantes, lo que confirma el resultado.

- **Caso general**. Se considera el siguiente homomorfismo

$$\begin{aligned} \varphi : R[x_1, x_2, \ldots, x_m] &\to R \\ \varphi(g) &\to g(0, 0, \ldots, 0). \end{aligned}$$

  De esta manera, para $g \in R[x_1, x_2, \ldots, x_m]$ su imagen bajo el homomorfismo φ es el término constante de g. Sea f una unidad en $R[x_1, x_2, \ldots, x_m]$. Como todo homomorfismo de anillos envía unidades a unidades, entonces $\varphi(f)$ es una unidad, esto es el término constante de f es una unidad.

  Para ver que los otros coeficientes de f son nilpotentes, se considera el siguiente homomorfismo. Por los teoremas 3.1 y 3.2 se puede tomar un ideal primo p arbitrario de R. Sea

$$\psi : R[x_1, x_2, \ldots, x_m] \to (R/p)\,[x_1, x_2, \ldots, x_m],$$

  que reduce los coeficientes de un polinomio módulo p.

  Dado que p es un ideal primo de R entonces R/p es un dominio entero. Como $\psi(f)$ es una unidad en $(R/p)\,[x_1, x_2, \ldots, x_m]$ y R/p es un dominio entero, entonces por el caso particular $\psi(f)$ es una constante; es decir, sus coeficientes de todos los términos grado mayor que cero son nulos. De ahí que todos los coeficientes de los términos de grado mayor que cero de f pertenecen a p.
  Puesto que la escogencia del ideal primo p fue arbitraria, se tiene que todos los coeficientes de los términos de grado mayor que cero de f pertenecen a la intersección de todos los ideales primos y por la Proposición 1.1 esto es precisamente el nilradical de R. En consecuencia, los coeficientes de los términos de grado mayor que cero de f son nilpotentes.

El recíproco se obtiene del Lema 3.1. □

Apartir de los resultados anteriores se presenta el teorema principal de este capítulo.

Teorema 3.4. *Para cualquier entero positivo m, $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$ tiene la propiedad de la diagonal si y solo si n es un divisor de* 12.

Demostración. Suponga que n es un entero positivo para el cual $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$ tiene la propiedad de la diagonal. Como $\mathbb{Z}_n$ es un subanillo de $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$, se sigue que $\mathbb{Z}_n$ tiene la propiedad de la diagonal, así del Teorema 2.1 se tiene que n debe ser un divisor de 24.

Dado que 8 y 24 son los únicos números que dividen a 24 y no a 12 entonces la demostración se reduce a demostrar lo siguiente.

a) $\mathbb{Z}_8[x_1, x_2, \ldots, x_m]$ y $\mathbb{Z}_{24}[x_1, x_2, \ldots, x_m]$ no tienen la propiedad de la diagonal.

b) $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$ tiene la propiedad de la diagonal cuando n es un divisor de 24 diferente a 8 y 24.

Demostración de a) Para demostrar que $\mathbb{Z}_8[x_1, x_2, \ldots, x_m]$ y $\mathbb{Z}_{24}[x_1, x_2, \ldots, x_m]$ no tienen la propiedad de la diagonal es suficiente con encontrar en ambos anillos una unidad que no sea involución.

- Sea el elemento nilpotente $2x_1$ del anillo $\mathbb{Z}_8[x_1, x_2, \ldots, x_m]$. Por el Lema 3.1, se tiene que $u = 1 + 2x_1$ es una unidad, sin embargo.

$$u^2 - 1 = (1 + 2x_1)^2 - 1 = 1 + 4x_1 + 4{x_1}^2 - 1 = 4x_1 + 4{x_1}^2 = 4(x_1 + {x_1}^2) \neq 0.$$

  Luego u no es una involución.

- Similarmente, como $6x_1$ es un elemento nilpotente en $\mathbb{Z}_{24}[x_1, x_2, \ldots, x_m]$, se tiene que $u = 1 + 6x_1$ es una unidad, que no es una involución, puesto que

$$u^2 - 1 = (1 + 6x_1)^2 - 1 = 1 + 12x_1 + 36{x_1}^2 - 1 = 12x_1 + 36{x_1}^2 = 12(x_1 + 3{x_1}^2) \neq 0.$$

Demostración de b) Se va a demostrar que cuando n es divisor diferente de 8 y 24, todas las unidades u en $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$ son involuciones; es decir $u^2 = 1$.

Por la Definición 3.1, los anillos $\mathbb{Z}_2, \mathbb{Z}_3$ y $\mathbb{Z}_6$ son reducibles y por el Teorema 3.3, las unidades en $\mathbb{Z}_2[x_1, x_2, \ldots, x_m], \mathbb{Z}_3[x_1, x_2, \ldots, x_m]$ y $\mathbb{Z}_6[x_1, x_2, \ldots, x_m]$ son exactamente las unidades en $\mathbb{Z}_2, \mathbb{Z}_3$ y $\mathbb{Z}_6$ respectivamente. Además, por el capítulo anterior $\mathbb{Z}_2, \mathbb{Z}_3$ y $\mathbb{Z}_6$ tienen la propiedad de la diagonal entonces los anillos de polinomios también la tienen.

En cuanto a los anillos de polinomios $\mathbb{Z}_4[x_1, x_2, \ldots, x_m]$ y $\mathbb{Z}_{12}[x_1, x_2, \ldots, x_m]$ se desarrolla a continuación.

Por un lado en $\mathbb{Z}_4[x_1, x_2, \ldots, x_m]$ el único elemento nilpotente es 2, y además las unidades en $\mathbb{Z}_4$ son 1 y -1 entonces las unidades u en $\mathbb{Z}_4[x_1, x_2, \ldots, x_m]$ están dadas por $u = 2h - 1$ y $u = 2h + 1$ donde h es un polinomio arbitrario. Luego $u^2 = 1$ en $\mathbb{Z}_4[x_1, x_2, \ldots, x_m]$. Por tanto u es una involución en $\mathbb{Z}_4[x_1, x_2, \ldots, x_m]$.

Por otro lado el único elemento nilpotente en $\mathbb{Z}_{12}[x_1, x_2, \ldots, x_m]$ es 6, por tanto todas las unidades u son de la forma $u = 6h + r$ donde h es un polinomio arbitrario y r es una unidad en $\mathbb{Z}_{12}$. Luego

$$u^2 = (6h + r)^2 = 36h^2 + 12hr + r^2 = r^2 \in \mathbb{Z}_{12}[x_1, x_2, \ldots, x_m].$$

Además $\mathbb{Z}_{12}$ tiene la propiedad de la diagonal entonces $r^2 \equiv 1(\text{mód}12)$. Por tanto u es una involución en $\mathbb{Z}_{12}[x_1, x_2, \ldots, x_m]$.

Finalmente de los incisos a) y b) se deduce que el anillo de polinomios $\mathbb{Z}_n[x_1, x_2, \cdots, x_m]$ cumple con la propiedad de la diagonal siempre y cuando n sea un divisor de 12. □

Capítulo 4

Propiedad cúbica de la diagonal para los anillos $\mathbb{Z}_n$

El estudio de este capítulo se centra en la propiedad cúbica para los anillos $\mathbb{Z}_n$ el cual está basado en el artículo, "Sophie Germain primes and involutions of $\mathbb{Z}_n^\times$", de los autores Karenna Genzlinger y Keir Lockridge, del año 2015, ver [10].

4.1. Propiedad cúbica de la diagonal

Dado un entero positivo n, la tabla de multiplicación cúbica de $\mathbb{Z}_n$ es un cubo $[0, n-1]^3$ cuya entrada en la coordenada (i, j, k) es el producto $ijk(\text{ mód } n)$. Así se puede plantear la pregunta ¿para cuáles n la tabla de multiplicación cúbica de $\mathbb{Z}_n$ tiene los 1's unicamente en la diagonal principal?

Sin embargo, puede probarse que la respuesta para esta pregunta es $n = 1$ o $n = 2$, dado que de otra manera $(-1)(-1)1 = 1$ lleva a un 1 fuera de la diagonal principal. En consecuencia, se hace una modificación a este interrogante con el objetivo de que pueda ser más interesante.

Antes de presentar la modificación al interrogante, se tiene en cuenta la siguiente definición.

Definición 4.1 (Plano coordenado)**.** Se dice que la coordenada (i, j, k) correspondiente al producto $ijk(\text{ mód } n)$ de la tabla de multiplicación cúbica de $\mathbb{Z}_n$ pertenece a un plano coordenado si una de sus entradas es congruente con 1 módulo n; es decir, si $i \equiv 1(\text{mód}n)$ o $j \equiv 1(\text{mód}n)$ o $k \equiv 1(\text{mód}n)$.

Ejemplo 4.1. La entrada $(1, 5, 5) \in (\mathbb{Z}_6)^3$ está en un plano coordenado ya que su producto es $1 \cdot 5 \cdot 5 = 25 \equiv 1(\text{mód}6)$. Así $1 \equiv 1(\text{mód}6)$. De la misma forma las entradas $(5, 1, 5)$ y $(5, 5, 1)$ pertenecen a un plano coordenado.

De esta manera, en este capítulo se estudia la pregunta ¿para cuáles n el 1 aparece en la tabla de multiplicación cúbica de $\mathbb{Z}_n$ en la diagonal principal o proviene de los planos coordenados?

Para presentar el resultado que caracteriza la propiedad cúbica de la diagonal, es necesario lo siguiente.

En primer lugar se recuerda que con $\mathcal{U}(R)$ se denota el conjunto de unidades en R, ver Definición 1.24. Además, en lo que sigue se representará la tabla cúbica de la diagonal, como se muestra a continuación.

$\mathcal{U}(R)$		$\cdots$	$\boldsymbol{k}$	$\cdots$
$\vdots$	$\vdots$			
	$\boldsymbol{j}$			
	$\vdots$			
$\boldsymbol{i}$	$\vdots$			
	$\boldsymbol{j}$		$ijk(\text{mód}n)$	
	$\vdots$			
$\vdots$	$\vdots$			
	$\boldsymbol{j}$			
	$\vdots$			

Tabla 4.1: Representación de la tabla de multiplicación cúbica de $\mathbb{Z}_n$.

Por ejemplo, si $\mathcal{U}(R) = \{a, b, c\}$, la tabla cúbica de la diagonal estaría dada así

$\mathcal{U}(R)$		$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$
$\boldsymbol{a}$	$\boldsymbol{a}$	a^3	a^2b	a^2c
	$\boldsymbol{b}$	aba	ab^2	abc
	$\boldsymbol{c}$	aca	acb	ac^2
$\boldsymbol{b}$	$\boldsymbol{a}$	ba^2	bab	bac
	$\boldsymbol{b}$	b^2a	b^3	b^2c
	$\boldsymbol{c}$	bca	bcb	bc^2
$\boldsymbol{c}$	$\boldsymbol{a}$	ca^2	cab	cac
	$\boldsymbol{b}$	cba	cb^2	cbc
	$\boldsymbol{c}$	c^2a	c^2b	c^3

Tabla 4.2: Ejemplo de tabla cúbica cuando $\mathcal{U}(R) = \{a, b, c\}$.

Cabe resaltar que como $\mathbb{Z}_n$ es un anillo conmutativo, la entrada $abc(\text{ mód } n)$ correspondiente a la coordenada (a, b, c) en la anterior representación es la misma a la que le corresponde a la coordenada (a, c, b).

La representación de esta tabla en esta manera permitirá realizar el recíproco del teorema de la propiedad de la diagonal.

Ejemplo 4.2. El anillo $\mathbb{Z}_{12}$ no cumple con la propiedad cúbica de la diagonal puesto que para la coordenada $(7, 5, 11)$ se tiene que $7 \cdot 5 \cdot 11 = 385 \equiv 1(\text{mód}12)$, de esta manera el 1 cae por fuera de

la diagonal y no proviene de ningún plano coordenado.

Para ejemplificarlo se muestra a continuación su respectiva tabla cúbica de la diagonal.

$\mathcal{U}(\mathbb{Z}_{12})$		**1**	**5**	**7**	**11**
1	**1**	1	5	7	11
	5	5	1	11	7
	7	7	11	1	5
	11	11	7	5	1
5	**1**	5	1	11	7
	5	1	5	7	11
	7	11	7	5	1
	11	7	11	1	5
7	**1**	7	11	1	5
	5	11	7	5	1
	7	1	5	7	11
	11	5	1	11	7
11	**1**	11	7	5	1
	5	7	11	1	5
	7	5	1	11	7
	11	1	5	7	11

Tabla 4.3: Tabla de multiplicación cúbica para $\mathbb{Z}_{12}$

Teorema 4.1 (Propiedad cúbica de la diagonal)**.** *Los* 1*'s en la tabla de multiplicación cúbica para* $\mathbb{Z}_n$ *se encuentran en la diagonal principal o en los planos coordenados (donde una de la tres coordenadas es 1) si y solo si* n *es un divisor de* 4 *o* 6*.*

Demostración. En primer lugar se realiza el recíproco del teorema. Cuando $n = 1$ o $n = 2$ que corresponden a $\mathcal{U}(\mathbb{Z}_1)$ y $\mathcal{U}(\mathbb{Z}_2)$ cumplen trivialmente la propiedad cúbica de la diagonal. Por otro lado para $n = 3, 4$ y 6 se puede dar la tabla de multiplicación cúbica. Como se muestra a continuación en cada caso se verifica la propiedad cúbica de la diagonal.

$\mathcal{U}(\mathbb{Z}_3)$		**1**	**2**
1	**1**	1	2
	2	2	1
2	**1**	2	1
	2	1	2

$\mathcal{U}(\mathbb{Z}_4)$		**1**	**3**
1	**1**	1	3
	3	3	1
3	**1**	3	1
	3	1	3

$\mathcal{U}(\mathbb{Z}_6)$		**1**	**5**
1	**1**	1	5
	5	5	1
5	**1**	5	1
	5	1	5

Tabla 4.4: Tablas de multiplicación cúbica para $\mathbb{Z}_3, \mathbb{Z}_4$ y $\mathbb{Z}_6$.

Para probar el reciproco se encontrará el número de 1's que aparecen en la tabla de multiplicación cúbica de $\mathbb{Z}_n$, pero que no están en ninguno de los planos coordenados. Para realizar esto se

consideran los siguientes conjuntos.

$$A = \left\{(a,b,c) \in \mathcal{U}(\mathbb{Z}_n)^3 : abc = 1\right\},$$
$$B = \left\{(1,b,c) \in \mathcal{U}(\mathbb{Z}_n)^3 : bc = 1 \text{ y } b \neq 1, c \neq 1\right\} \cup \left\{(a,1,c) \in \mathcal{U}(\mathbb{Z}_n)^3 : ac = 1 \text{ y } a \neq 1, c \neq 1\right\}$$
$$\cup \left\{(a,b,1) \in \mathcal{U}(\mathbb{Z}_n)^3 : ab = 1 \text{ y } a \neq 1, b \neq 1\right\} \cup \{(1,1,1)\},$$
$$C = \left\{(a,a,a) \in \mathcal{U}(\mathbb{Z}_n)^3 : a^3 = 1 \text{ y } a \neq 1\right\}$$

Dado que n satisface la propiedad cúbica de la diagonal, se tiene que el conjunto A sirve para contar el número de 1's que están en la diagonal principal o en un plano coordenado; además se puede observar que $A = B \cup C$, y que además B y C son disjuntos.

El número de elementos de cada conjunto se presenta en lo que sigue.

$|A| = \phi(n)^2$ porque $(ab)c = 1$ implica que c se puede ver como el inverso de ab. De esta manera los que varían son a y b, y cada uno puede tomar $\phi(n)$ valores. Es decir, $|A| = \phi(n)^2$.

Por otro lado, el $|\{(1,b,c) : bc = 1, b \neq 1 \text{ y } c \neq 1\}| = \phi(n) - 1$ porque al ser $bc = 1$, entonces c es el inverso multiplicativo de b; luego aquel que está variando es b y puede tomar $\phi(n) - 1$ valores diferentes, puesto que $b \neq 1$.

De la misma forma se tiene que

$$|\{(a,1,c) : ac = 1, a \neq 1 \text{ y } c \neq 1\}| = \phi(n) - 1 \text{ y}$$

$$|\{(a,b,1) : bc = 1, a \neq 1 \text{ y } b \neq 1\}| = \phi(n) - 1,$$

y adicionalmente $|\{(1,1,1)\}| = 1$.

De ahí que $|B| = 3(\phi(n) - 1) + 1$.

De esta manera el número de 1's que aparecen en la tabla de multiplicación cúbica de $\mathbb{Z}_n$, pero que no están en ninguno de los planos coordenados, está dado por

$$|C| = |A| - |B| = \phi(n)^2 - (3(\phi(n) - 1) + 1) = \phi(n)^2 - 3\phi(n) + 2.$$

Ahora se desea encontrar los valores de n donde esta cantidad es igual al número de elementos de orden multiplicativo precisamente 3, puesto que la entrada $(1,1,1)$ se ha omitido. Dicho de otra manera lo que se pretende es encontrar los valores de n tal que $\phi(n)^2 - 3\phi(n) + 3$ sea igual al número de elementos cuyo orden divida a 3. Para ello se considera $\mathcal{U}(\mathbb{Z}_{p^k})$ donde p es un número primo y k es un entero positivo. Se consideran los siguientes casos.

- **Caso 1:** $p \equiv 2(\text{mód}3)$. Suponga que existe un elemento a de orden 3 entonces $3|\phi(p^k) = (p-1)p^{k-1}$ luego por el Lema de Euclides $3|p-1$ o $3|p^{k-1}$. Luego se tiene que $p \equiv 1(\ \text{mód } 3)$ o $p \equiv 0(\text{mód}3)$, lo que lleva a una contradicción. Por lo tanto no existe un elemento de orden 3. Luego existe un sólo elemento cuyo orden divide a 3.

- **Caso 2:** $p \equiv 1(\text{mód}3)$ con $p > 2$. Como $\mathcal{U}(\mathbb{Z}_{p^k})$ es cíclico y su orden está dado por $\phi(p^k) = (p-1)p^{k-1}$, por el Teorema 1.8 el número de elementos de orden 3 en $\mathcal{U}(\mathbb{Z}_{p^k})$ es $\phi(3) = 3-1 = 2$. Luego se tienen 2 elementos de orden 3 y un elemento de orden 1.

  De esta manera hay 3 elementos cuyo orden divide a 3.

- **Caso 3:** $p = 3$ y $k = 1$. El conjunto $\mathcal{U}(\mathbb{Z}_{p^k})$ tiene 2 elementos los cuales son el 1 y el 2. Puesto que el orden de 1 es 1 y el orden de 2 es 2, luego se tiene que solo hay un elemento que divide a 3.

- **Caso 4:** $p = 3$ y $k \geq 2$. Similarmente al caso 2, $\mathcal{U}(\mathbb{Z}_{p^k})$ es cíclico entonces $3|p^{k-1}$. Así $\phi(3) = 3 - 1 = 2$. Luego se tienen 2 elementos de orden 3 y un elemento de orden 1.

  De esta forma, hay 3 elementos cuyo orden es divisor de 3.

Luego si la factorización prima de $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$, por el Teorema Chino de los Restos $\mathbb{Z}_n \approx \mathbb{Z}_{p_1}^{k_1} \oplus \mathbb{Z}_{p_2}^{k_2} \oplus \cdots \oplus \mathbb{Z}_{p_r}^{k_r}$. Como consecuencia de los casos estudiados anteriormente, en particular los casos 2 y 4, el número de elementos cuyo orden es divisor de 3 está dado por $3^{r+\epsilon}$, donde r representa el número de divisores primos de n congruentes con 1 módulo 3 y $\epsilon = 1$ si 9 divide a n o $\epsilon = 0$ en caso contrario.

Por lo tanto, se debe estudiar la ecuación $\phi(n)^2 - 3\phi(n) + 3 = 3^{r+\epsilon}$.

Suponga que $r + \epsilon \geq 2$. Esto implica que si $3|3^{r+\epsilon}$ entonces $3|\phi(n)$ y por tanto 9 divide a $\phi(n)^2$. Esto significa que 9 divide a $\phi(n)^2 - 3\phi(n)$. Luego 9 debe dividir a $3^{r+\epsilon} - 3$. Puesto que $r + \epsilon \geq 2$ entonces 9 divide a $3^{r+\epsilon}$, pero 9 no puede dividir a 3. Por lo tanto $r + \epsilon < 2$, de ahí que $r + \epsilon \in \{0, 1\}$ y así $\phi(n)^2 - 3\phi(n) + 3 = 1$ o $\phi(n)^2 - 3\phi(n) + 3 = 3$.

Observe que la ecuación $\phi(n)^2 - 3\phi(n) + 3 = 3$, no tiene solución porque ϕ no puede tomar los valores 0 y 3. Por otro lado, para la ecuación $\phi(n)^2 - 3\phi(n) + 3 = 1$, la soluciones son $\phi(n) = 1$ o $\phi(n) = 2$

Suponga que existe un primo $p \geq 5$ tal que $p|n$ y que $n = p^k q$ donde $k, q \in \mathbb{Z}^+$ y además $\gcd(p, q) = 1$, entonces $\phi(n) = \phi(p^k)\phi(q) = \phi(q)(p-1)p^{k-1} \geq p - 1 \geq 4$. Esto implica que en la factorización prima de n, no pueden aparecer primos mayores o iguales que 5, así $n = 2^\alpha 3^\beta$.

Ahora se analiza entre que valores deben estar α y β.

Si $\alpha \geq 3$ entonces $\phi(2^\alpha) = 2^{\alpha-1} \geq 2^{3-1} = 4 > 2$. Esto contradice el hecho que $\phi(n)$ tiene que ser a lo más 2. Luego $\alpha \leq 2$.

De la misma forma se realiza para β. Si $\beta \geq 2$ entonces $\phi(3^\beta) = (2)3^{\beta-1} \geq (2)3^{2-1} = 6 > 2$. Esto es una contradicción. Luego $\beta \leq 1$.

De lo anterior $\alpha \leq 2$ y $\beta \leq 1$.

Por lo tanto, la factorización prima de n está dada por $n = 2^\alpha 3^\beta$ donde $0 \leq \alpha \leq 2$ y $0 \leq \beta \leq 1$. La siguiente tabla ayuda a ejemplificar los valores que debe tomar n para que cumpla con la propiedad cúbica de la diagonal.

n	α	β	$\phi(2^\alpha)\phi(3^\beta) = \phi(n)$
1	0	0	$\phi(2^0)\phi(3^0) = \phi(1) = 1$
2	1	0	$\phi(2^1)\phi(3^0) = \phi(2) = 1$
3	0	1	$\phi(2^0)\phi(3^1) = \phi(3) = 2$
4	2	0	$\phi(2^2)\phi(3^0) = \phi(4) = 2$
6	1	1	$\phi(2^1)\phi(3^1) = \phi(6) = 2$

Tabla 4.5: Valores n para los cuales $\phi(n) = 1$ o $\phi(n) = 2$.

Cabe resaltar que si se toma $n = 12 = 2^2 3$ entonces

$$\phi(2^2 3) = \phi(2^2)\phi(3) = 4 > 2.$$

Esto es una contradicción. Luego $n|6$ o $n|4$.

Con lo anterior se finaliza la demostración, y se concluye que los valores de n que cumplen la propiedad cúbica de la diagonal son los divisores de 4 o 6. □

Conclusiones

- En este trabajo se recopilaron los resultados que permitieron realizar el estudio de la propiedad de la diagonal en los anillos $\mathbb{Z}_n$, en los anillos de polinomios $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$ y la extensión a la propiedad cúbica de la diagonal. Para esto, se organizaron de manera sistemática de tal manera que sea de mayor comprensión para el lector. Cabe resaltar que las pruebas presentadas han sido reelaboradas de manera detallada, dado que en los textos estudiados se omiten pasos que restan claridad a dichas pruebas.

- Aunque en este trabajo se estudió la propiedad de la diagonal en algunos anillos conmutativos, se puede investigar en otros anillos conmutativos como es el caso del trabajo presentado por S.K Chebolu et al. [5], en el cual se estudió la propiedad de la diagonal en el contexto de álgebras de grupo. Adicionalmente, en este artículo los autores analizan generalizaciones de la propiedad de la diagonal en cuerpos finitos y álgebras de grupo. Así mismo esta propiedad se puede extender para estudiar el concepto de k unidades módulo n, como se hace en el trabajo de J. Castillo y J. Caranguay en [3].

- Se puede pensar en estudiar esta propiedad en anillos no conmutativos. De esta forma es un campo en el que se pueden desarrollar futuras investigaciones.

- En el Capítulo 2, Sección 2.2 se pudo observar las tablas multiplicativas de Cayley para los anillos $\mathbb{Z}_n$ y en el Capítulo 4 las tablas cúbicas de la diagonal; si bien en las primeras se realiza la tabla completa para cada anillo y en las segundas se toma las unidades del anillo, esto puede llevar a que el lector piense que se están utilizando enfoques diferentes, sin embargo cabe resaltar que las tablas multiplicativas de Cayley podrían reducirse de tamaño si solamente se hubieran considerado las unidades para su construcción, pero esto no se hizo con el ánimo de mantener la idea que generó el problema originalmente.

Referencias

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Avalon Publishing, 1994.

[2] D. M. Burton. *Elementary Number Theory*. Library of Congress Cataloging-in-Publication Data, 5 edition, 1980.

[3] J. H. Castillo and J. F. Caranguay. The set of k-units modulo n. *arXiv:1708.06812*, 2017.

[4] S. K. Chebolu. What is special about the divisors of 24? *Math. Mag.*, 85(5):366–372, 2012.

[5] S. K. Chebolu, K. Lockridge, and G. Yamskulna. Characterizations of Mersenne and 2-rooted primes. *Finite Fields Appl.*, 35:330–351, 2015.

[6] S. K. Chebolu and M. Mayers. What is special about the divisors of 12? *Math. Mag.*, 86(2):143–146, 2013.

[7] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[8] P. Erdös. Beweis eines satzes von tschebyschef. *Acta Litt. Univ. Sci., Szeged, Sect. Math.*, 5:194–198, 1932.

[9] J. A. Gallian. *Contemporay Abstract Algebra*. Cengage Learning, seventh edition, 2009.

[10] K. Genzlinger and K. Lockridge. Sophie germain primes and involutions of $\mathbb{Z}_n^x$. *Involve*, 8(4):653–663, 2015.

[11] T. Koshy. *Elementary Number Theory with Applications*. Library of Congress Cataloging-in-Publication Data, 2 edition, 2007.

[12] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[13] C. Polcino Milies and S. K. Sehgal. *An introduction to group rings*, volume 1 of *Algebra and Applications*. Kluwer Academic Publishers, Dordrecht, 2002.

[14] S. Ramanujan. A proof of Bertrand's postulate [J. Indian Math. Soc. **11** (1919), 181–182]. In *Collected papers of Srinivasa Ramanujan*, pages 208–209. AMS Chelsea Publ., Providence, RI, 2000.

Índice alfabético