UNIVERSIDAD DE ORIENTE
NÚCLEO DE SUCRE
ESCUELA DE CIENCIAS
DEPARTAMENTO DE MATEMÁTICAS

ALGUNAS APLICACIONES DE LA CONGRUENCIA MODULAR EN LOS NÚMEROS ENTEROS

(Modalidad: Investigación)

M. SC. OSCAR ENRIQUE CASTRO PÉREZ

TRABAJO DE ASCENSO PRESENTADO COMO REQUISITO PARCIAL PARA ASCENDER A LA CATEGORÍA PROFESOR ASISTENTE

Cumaná, junio de 2021

DEDICATORIA

A:

Dios por darle sentido a mi existencia y por darme el aliento para seguir vivo.

Mis padres, a quienes les debo mi entrada a esta vida, los amo.

Mi esposa Rosianyi Tormes, ella representa ese lugar donde Dios y yo hacemos las paces, te amo.

AGRADECIMIENTOS

A:

Mi madre y a mi esposa por el amor que me dan, el cual es mi máxima inspiración.

Profesor Saúl Mosqueda, la Licda. Verónica González, Ing. Daniel Benavides, Licda. Angélica Arancibia y Ing. Claudio González, Licenciado Bautista Santiago, Licda. Francisca Suarez por su confianza y apoyo que siempre ha alimentado la fe en mí mismo.

Todo el personal del Departamento de Matemáticas de la Universidad de Oriente, profesores, secretarias y personal obrero que son el alma de la Universidad.

Todas las personas que de alguna u otra forma intervinieron en la realización de este trabajo.

ÍNDICE

RESUMEN

Se demuestra la relación entre la identidad de Bezout y los coprimos de un número natural dado. También, se construye un algoritmo que determina como son las soluciones, en $\mathbb{Z}$, de la identidad de Bezout $ax + by = 1$. Además, se deducen las soluciones en $\mathbb{Z}$, de $kx + my = n$, siempre que n sea múltiplo del máximo común divisor de los enteros positivos y distintos k y m. Lo que muestra la generalización de los resultados y que el algoritmo para encontrar los coprimos a n en $\mathbb{Z}_n$, no es optimizable, en el sentido del número finito de iteraciones necesarias para hallarlos.

INTRODUCCIÓN

La aritmética es el producto del perfeccionamiento de la idea de número en general, más aún, es parte misma de la evolución del hombre y de lo complejo en que se fue convirtiendo su intercambio con sus semejantes, esto último, justificaría el hecho de que usar al conjunto de los números naturales $\mathbb{N}$, para contar, pasara a un segundo plano y a medida que transcurriera el pasar de los siglos, el hombre convirtiese a $\mathbb{N}$ en una herramienta para enfrentar mayores abstracciones. Asimismo, surgen necesidades, donde $\mathbb{N}$, ya no es suficiente como herramienta y se deben recurrir a otras que conserven su esencia, (Flores, 1971). Por ello, se planteó, estudiar el anillo de los números enteros $\mathbb{Z}$, en particular, para cualquier valor natural *p* primo, hallar los inversos en el campo $\mathbb{Z}_p$ (generada por la relación de equivalencia congruencia modular en $\mathbb{Z}$). Específicamente, en el campo de los números reales $\mathbb{R}$ es un problema muy sencillo, hallar los inversos de los elementos no nulos, pero en el campo $\mathbb{Z}_p$, no es tan fácil.

En el presente trabajo se muestran las definiciones y algunos resultados útiles que describen el anillo $\mathbb{Z}$ (véase el capítulo que corresponde a los Preliminares) luego se profundiza en la congruencia modular en $\mathbb{Z}$, para presentar alguno de los resultados obtenidos en Castro, 2014 y en Castro et al 2015 (véase el capítulo que corresponde a El Producto Cartesiano De Conjuntos Finitos Y La Congruencia Modular En $\mathbb{Z}$), para finalmente, ampliar los resultados de aplicar la relación modular en el conjunto de los números enteros, de modo que se demuestra la relación entre la identidad de Bezout y los coprimos de un número natural dado, véase el capítulo titulado La Identidad De Bezout Y La Congruencia Modular En $\mathbb{Z}$, donde es importante destacar que se construyó un algoritmo basado en el resultado más importante del presente trabajo, que demuestra como son las soluciones en $\mathbb{Z}$, de la identidad de Bezout $ax + by = 1$, cuando los enteros positivos y distintos *a*, *b* son coprimos, de la cual, se pudo deducir las soluciones en $\mathbb{Z}$, de $kx + my = n$, siempre que *n* sea múltiplo del máximo común divisor

de los enteros positivos y distintos *k*, *m*. Además, se demostró que no se usaron los números enteros negativos, porque en la forma en que se definió al anillo $\mathbb{Z}$, permite describir a los enteros negativos, con los enteros positivos, lo que mostró la generalización de los resultados y que el algoritmo para encontrar los coprimos a *n* en $\mathbb{Z}_n$, no es optimizable, en el sentido del número finito de iteraciones necesarias para hallarlos.

1. PRELIMINARES

En el presente capítulo se describen las nociones básicas sobre las estructuras algebraicas básicas (grupo, anillos y campos) y sus propiedades, para luego detallar al el proceso de división y el orden en el anillo $\mathbb{Z}$.

1.1 EL ANILLO DE LOS NÚMEROS ENTEROS

Definición 1.1.1. (Herstein, 2008). Sean los conjuntos *A*, *B*, no vacíos; *B* tiene un *operador binario f* (*f* es un *operador* en *B*), si *f* es una función $f: B \times B \to A$.

Observación. De ahora en adelante, un operador $f: B \times B \to A$ se denotará por $*$, σ, λ, $+$, ó $\times$ y $f(a, b)$ en *A* se denotará por $a*b$, $a\ \sigma\ b$ $a\ \lambda\ b$, $a + b$ ó $a \times b$, con *a*, *b* en *B*.

Definición 1.1.2. (Lipschutz, 1975). Algunos axiomas de operadores binarios. Sea un conjunto *B*, no vacío, dotado de dos operaciones binarias denotadas por + y ×, tal que para cualesquiera $a, b, c \in B$ se cumple:

B_1. *Ley de Clausura* si y solo sí (*sii*) $a + b \in B$ y $a \times b \in B$ (usualmente, $a \times b = ab$).

B_2. *Ley Conmutativa sii* $a + b = b + a$ y $a \times b = b \times a$.

B_3. *Ley Asociativa sii* $(a + b) + c = a + (b + c)$ y $(a \times b) \times c = a \times (b \times c)$.

B_4. *Ley Distributiva sii* $a + (b \times c) = (a + b) \times (a + c)$ y $a \times (b + c) = (a \times b) + (a \times c)$.

B_5. *Elemento Neutro*: Existe un elemento $s \in B$ denominado *neutro* o *nulo* para el operador + tal que, $s + a = a + s = a$ y, análogamente, para el operador × existe el neutro o *identidad* $m \in B$ tal que, $m \times a = a \times m = a$.

Definición 1.1.3. (Herstein, 2008). Sea un conjunto *B*, no vacío y + un operador en *B*; (*B*, +) es un *grupo*, si para cualesquiera $a, b, c \in B$ se cumple, en la Definición 1.1.2: B_1 y B_3, existe $s \in B$ que cumple B_5 y para *a* existe el respectivo elemento $a' \in B$ denominado *inverso* u *opuesto* de *a*, tal que $a + a' = a' + a = s$. Además, si se cumple B_2 en la Definición 1.1.2 para + y con cualesquiera $a, b \in B$ se dice entonces

que $(B, +)$ es un grupo *abeliano* o *conmutativo*.

Teorema 1.1.1. (Rivero, 1996). En un grupo $(B, +)$:

a) El elemento neutro es único.

b) Cada elemento de B tiene un único inverso. En particular para cualquier $a, b \in B$ se tiene que $(a')' = a$, $(a + b)' = b' + a'$ y $s' = s$ con s el neutro en el grupo $(B, +)$.

Demostración. (Literal a). Sea el grupo $(B, +)$ entonces existe $s \in B$, el neutro para el operador + tal que, $s + a = a + s = a$ con cualquier $a \in B$. Supóngase por el contrario que el elemento neutro no es único para el operador + entonces existe $t \in B$, tal que $t + a = a + t = a$, con cualquier $a \in B$. Sin embargo, en particular para $t, s \in B$, $s = t + s = s + t = t$ (véase la Definición 1.1.3). Así, $s = t$ por transitividad de la igualdad, de lo cual se concluye que $s \in B$ es el único neutro.

(Literal b). Sea el grupo $(B, +)$ y $s \in B$ el neutro para el operador +. Supóngase por el contrario que cualquier elemento $a \in B$ no tiene un único opuesto $a' \in B$ para el operador +, tal que $a + a' = a' + a = s$ entonces para $a \in B$ existe $c \in B$, tal que $a + c = c + a = s$. Sin embargo, en particular para $a, a', c \in B$ y el neutro $s \in B$:

$a' = a' + s = a' + (a + c) = (a' + a) + c = s + c = c$ (véase la Definición 1.1.3).

Así, $a' = c$ por transitividad de la igualdad, de lo cual se concluye que $a' \in B$ es el único opuesto de $a \in B$.

Luego, para $a, b, a + b \in B$ se tiene que $a', b', (a + b)', a' + b', (a')' \in B$. Además, como $(b' + s) + b = b' + (s + b) = s$ y $b' + a'$ cumple con la definición de opuesto para $a + b$, ya que:

$$(b' + a') + a + b = b' + s + b = a + b + (b' + a')$$

pero $(a + b)'$es el opuesto de $a + b$ y tanto $(a')'$ como a son opuestos de a'. Así también, como el opuesto de todo elemento de B es único (Teorema 1.1.1), se tiene que $(a + b)' = b' + a'$ y $(a')' = a$.

Además, si s es el neutro en el grupo $(B, +)$ entonces sea s' el opuesto de s de modo que $s' + s = s = s + s'$ pero $s + s = s$; luego, nuevamente, como el opuesto de todo

elemento de B es único (Teorema 1.1.1), se tiene que $s' = s$. •

Teorema 1.1.2. (Rivero, 1996). Sea $(B,+)$ un grupo, $a + b = a + c$ $(c + a = b + a)$ *sii* $b = c$ para cualesquiera $a, b, c \in B$.

Demostración. (=>). Sea el grupo $(B,+)$ y $s \in B$ el neutro, entonces para cualesquiera $a, b, c \in B$, supóngase que $a + b = a + c$, así,

$$b' + a' + (a + c) = (a + c) + b' + a' = s \text{ (Teorema 1.1.1)}$$

pero

$$b = b + (b' + a' + (a + c)) = (s + a') + (a + c) = a' + (a + c) = s + c = c.$$

Así, por asociatividad de + y transitividad de la igualdad, $b = c$.

(<=). El teorema es cierto puesto que + es función.•

Teorema 1.1.3. (Castro, 2014). $(B, +)$ es un grupo conmutativo *sii* B tiene un operador + (que cumple la *ley de clausura*), cada elemento de B tiene opuesto, existe el neutro y para cualesquiera $a, b, c \in B$:

$$(a + b) + c = (b + c) + a$$

Demostración. Para el operador +, supóngase que $s \in B$ el neutro y que cada elemento de B tiene opuesto, falta demostrar que para cualesquiera $a, b, c \in B$:

$$a + b = b + a$$

y que

$$(a + b) + c = a + (b + c).$$

Pero

$$(a + b) + s = (b + s) + a$$

$$a + b = b + a$$

luego + tiene la propiedad conmutativa por lo que:

$$(a + b) + c = (b + c) + a$$

$$(a + b) + c = a + (b + c)$$

entonces + tiene la propiedad asociativa. •

Definición 1.1.4. (Herstein, 2008). Sea un conjunto B, no vacío y +, × dos operadores en B; $(B, +, \times)$ es un *anillo*, si $(B, +)$ es un grupo abeliano y con cualesquiera

a, b, $c \in B$ se cumple para $\times$ B_1, B_3 en la Definición 1.1.2, además que $a \times (b + c) = (a \times b) + (a \times c)$ y que $(b + c) \times a = (b \times a) + (c \times a)$.

Teorema 1.1.4. (Fraleigh, 1987). Sea el anillo $(B, +, \times)$ entonces para cualquier $a \in B$, $s \times a = a \times s = s$ con s el neutro del grupo $(B, +)$.

Demostración. Sea el anillo $(B, +, \times)$, si s es el neutro del grupo $(B, +)$, tal que para cualquier $a \in B$:

$$a \times s = a \times (s + s) = a \times s + a \times s \text{ ó } s \times a = (s + s) \times a = s \times a + s \times a$$

entonces de:

$$a \times s + s = a \times s + a \times s \text{ ó } s + s \times a = s \times a + s \times a$$

y el Teorema 1.1.2 se deduce para cualquier $a \in B$ que $s \times a = a \times s = s$, con s el neutro del grupo $(B, +)$. •

Teorema 1.1.5. (Rivero, 1996). Sea el anillo $(B, +, \times)$ entonces para cualquier $a, b \in B$ y sus opuestos en $(B, +)$ con respecto a $\times$ cumplen con:

a) $(a \times b)' = a \times b' = a' \times b$.

b) $a' \times b' = a \times b$.

Demostración. (Literal a). Sean $a, b \in B$, como $(B, +, \times)$ es un anillo $a \times b \in B$, por lo que $(a \times b)'$, a', b' también están en $(B, +)$ (Definición 1.1.3) y $a \times b + a \times b' = a \times (b + b') = a \times s = s$ (Definición 1.1.4 y Teorema 1.1.4). Análogamente, $a \times b' + a \times b = a \times (b' + b) = a \times s = s$ y como el opuesto es único en $(B, +)$ (Teorema 1.1.1), se deduce $(a \times b)' = a \times b'$.

Por otro lado, de manera semejante, se deduce que $(a \times b)' = a' \times b$ al considerase la Definición 1.1.3, la Definición 1.1.4, el Teorema 1.1.1 y el Teorema 1.1.4 en:

$a \times b + a' \times b = (a + a') \times b = s \times b = s$ y $a' \times b + a \times b = (a' + a) \times b = s \times b = s$.

(Literal b). Sean $a, b \in B$, como $(B, +, \times)$ es un anillo entonces a', b', $a \times b$, $a' \times b' \in B$, luego, $a' \times b + a' \times b' = a' \times b + a' \times b' = a' \times (b + b') = s = a' \times (b' + b) = a' \times b' + a' \times b$ (Definición 1.1.3, Definición 1.1.4, y Teorema 1.1.4). Luego, por lo demostrado en el Literal a), $(a \times b)' = a' \times b$ tiene un único opuesto $a \times b = a' \times b'$

(Teorema 1.1.1). •

Definición 1.1.5. (Herstein, 2008). Sea el anillo (B, +, ×), si se cumple que existe $m \in B$ para × en B_5 de la Definición 1.1.2, entonces (B, +, ×) es un *anillo con identidad*.

Teorema 1.1.6. (Castro, 2014). Sea (B, +, ×) un anillo con identidad, si s es el neutro del grupo (B, +) y $m \in B$ es la identidad para × entonces, $|B| > 1$ (orden usual en $\mathbb{R}$) => $s \neq m$.

Demostración. (B, +, ×) es un anillo con identidad, si s es el neutro del grupo (B, +) y $m \in B$ es la identidad para ×, tal que, $s + a = a + s = a = m \times a = a \times m$ con cualquier $a \in B$ (Definición 1.1.5). Supóngase por el contrario que $s = m$ entonces con cualquier $a \in B$ se tiene $a = a \times m = a \times s = s$ (Definición 1.1.3 y Teorema 1.1.4). Así, con cualquier $a \in B$, $a = s$ por transitividad de la igualdad, luego $B = \{s\}$ y $|B| = 1$. Por lo tanto, $s = m$ => $|B| = 1$ es cierto y como B es no vacío (Definición 1.1.3) entonces su contrarrecíproco es $|B| > 1$ => $s \neq m$, el cual queda demostrado por equivalencia lógica.•

Definición 1.1.6. (Herstein, 2008). Si (B, +, ×) es un anillo y si para × en la Definición 1.1.2 se cumple B_2 con cualesquiera $a, b \in B$ entonces (B, +, ×) es un *anillo conmutativo.*

Definición 1.1.7. (Herstein, 2008). Un anillo conmutativo (B, +, ×) es un *anillo entero*, un *dominio entero* o un anillo que *no tiene divisores de cero*, si para cualesquiera $a, b \in B$: $a \times b = s$ *sii* $a = s$ o $b = s$, con s el neutro del grupo (B, +).

Teorema 1.1.7. (Fraleigh, 1987). Sea (B, +, ×) un dominio entero y $a, b, c \in B$ si $a \neq s$, con s el neutro del grupo (B, +), entonces $a \times b = a \times c$ ($b \times a = c \times a$) *sii* $c = b$.

Demostración. (=>). Sean $a, b, c \in B$, si $a \neq s$, con s el neutro del grupo (B, +), tal que $a \times b = a \times c$ ($b \times a = c \times a$) *sii* $a \times (b - c) = s$ ($(b - c) \times a = s$) *sii* $b - c = s$ *sii* $b = c$ (Teorema 1.1.2, Definición 1.1.4, Teorema 1.1.5, Definición 1.1.7).

(<=). El teorema es cierto puesto que × es función.•

Teorema 1.1.8. (Fraleigh, 1987). Un anillo conmutativo $(B, +, \times)$ es un dominio entero, si y solo si para todo $a, b, c \in B$, con $a \neq s$ y s el neutro del grupo $(B,+)$ $a \times b = a \times c <=> c = b$.

Demostración. (=>). El teorema es cierto, véase el Teorema 1.1.7.

(<=). Sea $(B, +, \times)$ un anillo conmutativo, $a, b \in B$ y s el neutro del grupo $(B,+)$, si $a \neq s$ y $b \neq s$ entonces $a \times b \neq s$, ya que, si $a \times b = s = a \times s$ *sii* $b = s$ (Teorema 1.1.4, hipótesis y Teorema 1.1.7.) y además, $a \times b = s = s \times b$ *sii* $a = s$ (Teorema 1.1.4, hipótesis y Teorema 1.1.7) se contradice lo supuesto inicialmente. Así, su contrarrecíproco es para todo $a, b \in B$, si $a \times b = s$ entonces $a = s$ ó $b = s$, el cual queda demostrado por equivalencia lógica. Luego $(B, +, \times)$ es un dominio entero. •

Observación. Se asumirá que existe $(\mathbb{Z}, +, \times)$, con $|\mathbb{Z}| > 1$ (orden usual en el conjunto de los números reales, $\mathbb{R}$), un anillo entero con identidad que está dotado de los operadores *suma* (+) y *multiplicación* (×) (respectivamente, para a, b en $\mathbb{Z}$, $a + b$ y $a \times b = ab$), tal que $s = 0$, $a' = -a$ (neutro y opuesto para $(\mathbb{Z},+)$) y $m = 1$, neutro o unidad con respecto a la multiplicación, (Rivero, 1996). También, se asumirá, bajo los preceptos de Peano, que existe el conjunto *inductivo* más pequeño $\mathbb{N}$, llamado el conjunto de los *Números Naturales* (Flores, 1971), como subconjunto de $\mathbb{Z}$, de modo que $0 \notin \mathbb{N}$. Esto es, se asumirá, de ahora en adelante, que: $1 \in \mathbb{N}$ y para todo $a \in \mathbb{N}$ implica $a + 1 \in \mathbb{N}$ dada + en $\mathbb{Z}$, asimismo, $(\mathbb{Z}, +, \times)$ se denotará con el mismo símbolo $\mathbb{Z}$.

Definición 1.1.8. (Fraleigh, 1987). Si $(B, +, \times)$, con $|B| > 1$ es un anillo entero y si s es el neutro del grupo $(B, +)$ de modo que $(B - \{s\}, \times)$ también es un grupo entonces se dice que $(B, +, \times)$ es un *campo*.

Observación. $\mathbb{Z}$, no es un campo puesto que no necesariamente, todos sus elementos con respecto a la multiplicación poseen inverso. Un ejemplo de campo es el conjunto de los números racionales, $\mathbb{Q}$ o el conjunto de los números reales, $\mathbb{R}$, (Fraleigh, 1987).

Teorema 1.1.9. (Rivero, 1996). Sean a, b en $\mathbb{N}$, entonces

a) $a + b \in \mathbb{N}$.

b) $-a \notin \mathbb{N}$.

c) $ab \in \mathbb{N}$.

Demostración. (Literal a). *Asúmase el principio de inducción matemática*. Sean a, b en $\mathbb{N}$, fíjese a $b \in \mathbb{N}$, de modo que se aplique inducción sobre a para demostrar que $a + b \in \mathbb{N}$:

Sea $a = 1$ entonces como $b \in \mathbb{N}$. $1 + b = b + 1 \in \mathbb{N}$ (conmutatividad de + y $\mathbb{N}$ es el subconjunto inductivo de $\mathbb{Z}$). Por lo que $a + b \in \mathbb{N}$.

Supóngase que $a = k$ entonces $k + b \in \mathbb{N}$ (hipótesis inductiva) se demostrará para $a = k + 1$ que $a + b \in \mathbb{N}$. Así, como $k + b \in \mathbb{N}$ por hipótesis inductiva entonces $(k + 1) + b = (k + b) + 1 \in \mathbb{N}$ (conmutatividad y asociatividad de +). Por lo que para $a = k + 1$, $a + b \in \mathbb{N}$.

(Literal b). Sea $a \in \mathbb{N}$, supóngase por el contrario que $-a \in \mathbb{N}$, entonces por lo demostrado en el literal a, se concluye que $a + (-a) = 0 \in \mathbb{N}$, lo cual contradice lo asumido ($0 \notin \mathbb{N}$); por tanto $-a \notin \mathbb{N}$.

(Literal c). *Asúmase el principio de inducción matemática.* Sean a, b en $\mathbb{N}$, fíjese a $b \in \mathbb{N}$, de modo que se aplique inducción sobre a para demostrar que $ab \in \mathbb{N}$:

Sea $a = 1$ y $b \in \mathbb{N}$ entonces $1b = b \in \mathbb{N}$ (elemento identidad de × en $\mathbb{Z}$ y $\mathbb{N} \subset \mathbb{Z}$). Por lo que $ab \in \mathbb{N}$.

Supóngase que $a = k$ entonces $kb \in \mathbb{N}$ (hipótesis inductiva) se demostrará para $a = k + 1$ que $ab \in \mathbb{N}$. Así, como $kb \in \mathbb{N}$ por hipótesis inductiva entonces se tiene que $(k + 1)b = kb + b \in \mathbb{N}$ (distributividad a la izquierda de × sobre + en $\mathbb{Z}$ y por lo demostrado en el Literal a). Por lo que, para $a = k + 1$, $ab \in \mathbb{N}$. •

Observación. Existen elementos de $\mathbb{Z}$ que no están en $\mathbb{N} \cup \{0\}$. Esto es, $\mathbb{N} \cup \{0\}$ es un subconjunto propio de $\mathbb{Z}$ ó $\mathbb{Z} - (\mathbb{N} \cup \{0\}) \neq \varnothing$ y $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (\mathbb{Z} - (\mathbb{N} \cup \{0\}))$. Así, se asumirá que $\mathbb{Z} - (\mathbb{N} \cup \{0\})$ contiene, únicamente, a los opuestos de cada elemento del conjunto $\mathbb{N}$.

Definición 1.1.9. (Flores, 1971). $\mathbb{Z} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+$, con $\mathbb{Z}^- = \mathbb{Z} - (\mathbb{N} \cup \{0\})$ y $\mathbb{Z}^+ = \mathbb{N}$, donde $\mathbb{Z}$ es el conjunto de los *Números Enteros*, $\mathbb{Z}^-$ es el subconjunto de los *números enteros negativos* y $\mathbb{Z}^+$ es el subconjunto de los *números enteros positivos*.

1.2. ORDEN Y DIVISIÓN EN $\mathbb{Z}$

Definición 1.2.1. (Flores, 1971). Sean *a*, *b* en $\mathbb{Z}$, *a* es *menor o igual* que *b* y se escribe, respectivamente, $a < b$ ó $a = b$ ($a \leq b$) *sii* $b + (-a) = b - a \in \mathbb{Z}^+ \cup \{0\}$.

Teorema 1.2.1. (Rivero, 1996). Considérese la relación $\leq$ en $\mathbb{Z}$:

a) Para cualesquiera *a*, *b* en $\mathbb{Z}$, se cumple una y sólo una de las tres proposiciones: $a = b$, $a < b$ ó $b < a$. *Totalidad*.

b) Para todo *a* en $\mathbb{Z}$, $a \leq a$. *Reflexividad*.

c) Para cualesquiera *a*, *b* en $\mathbb{Z}$, si $a \leq b$ y $b \leq a$ implica $a = b$. *Antisimetría*.

d) Para cualesquiera *a*, *b*, *c* en $\mathbb{Z}$, si $a \leq b$ y $b \leq c$ implica $a \leq c$. *Transitividad*.

Demostración. (Literal a). Sean *a*, *b* en $\mathbb{Z}$, entonces existen $-a$, $-b$ en $\mathbb{Z}$, análogamente, existen $c = a - b$, $-c = b - a$, de modo que $-c$, $c \in \mathbb{Z} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+$ (conmutatividad y opuestos para + en $\mathbb{Z}$, Definición 1.1.9 y Teorema 1.1.5). Así, se cumple una y sólo una de las dos proposiciones siguientes: $-c$, $c \in \mathbb{Z}^- \cup \mathbb{Z}^+$, ó $-c$, $c \in \{0\}$ (por ser conjuntos disjuntos, Definición 1.1.9 y Teorema 1.1.1). Asimismo, para la proposición $-c$, $c \in \mathbb{Z}^- \cup \mathbb{Z}^+$ es cierta una y sólo una de las dos proposiciones siguientes: $-c \in \mathbb{Z}^-$ *sii* $c \in \mathbb{Z}^+$ ó $c \in \mathbb{Z}^-$ *sii* $-c \in \mathbb{Z}^+$ (Definición 1.1.9 y Teorema 1.1.9). Así, finalmente, es cierta una y sólo una de las siguientes proposiciones (Definición 1.2.1): $-c \in \mathbb{Z}^-$ *sii* $c \in \mathbb{Z}^+$ ($b < a$) ó $c \in \mathbb{Z}^-$ *sii* $-c \in \mathbb{Z}^+$ ($a < b$) ó $-c$, $c \in \{0\}$ ($a = b$). Esto es, Para cualesquiera *a*, *b* en $\mathbb{Z}$, se cumple una y sólo una de las tres proposiciones: $a = b$, $a < b$ ó $b < a$.

(Literal b). Sea $a \in \mathbb{Z}$ entonces existe $-a \in \mathbb{Z}$, de modo que $a - a = 0$ en $\mathbb{Z}^+ \cup \{0\}$ (opuesto para + en $\mathbb{Z}$ y Teorema 1.1.1). Así, Para todo $a \in \mathbb{Z}$, $a \leq a$ (Definición 1.2.1).

(Literal c). Sean a, b en $\mathbb{Z}$, si $a \leq b$ y $b \leq a$ entonces $b - a, a - b \in \mathbb{Z}^+ \cup \{0\}$ (Definición 1.2.1) pero $a - b + b - a = 0$, por lo que $a - b, b - a \notin \mathbb{Z}^+$ (opuesto para + en $\mathbb{Z}$, Teorema 1.1.1 y Teorema 1.1.9); así, $a - b = b - a = 0$, es decir, $a = b$. Por tanto, para cualesquiera a, b en $\mathbb{Z}$, si $a \leq b$ y $b \leq a$ implica $a = b$.

(Literal d). Sean a, b, c en $\mathbb{Z}$, si $a \leq b$ y $b \leq c$ entonces $b - a, c - b \in \mathbb{Z}^+ \cup \{0\}$ (Definición 1.2.1) pero $b - a + c - b = c - a$, por lo que si $b - a, c - b \in \mathbb{Z}^+$ entonces $c - a \in \mathbb{Z}^+$ (conmutatividad y opuesto para + en $\mathbb{Z}$, Teorema 1.1.1 y Teorema 1.1.9). Esto es, $a \leq c$ (Definición 1.2.1). Y, si $b - a = 0$ ó $c - b = 0$ entonces $a = b$ ó $c = b$, en cualquier caso $c - a \in \mathbb{Z}^+ \cup \{0\}$ (conmutatividad y opuesto para + en $\mathbb{Z}$, Teorema 1.1.2, Teorema 1.1.9, transitividad de la igualdad). Esto es, $a \leq c$ (Definición 1.2.1). Por tanto, para cualesquiera a, b en $\mathbb{Z}$, si $a \leq b$ y $b \leq c$ implica $a \leq c$.

Así, $\mathbb{Z}$ está *ordenado totalmente*. •

Teorema 1.2.2. (Flores, 1971). $a \in \mathbb{Z}^+$ *sii* $0 < 1 \leq a$.

Demostración. (=>). *Asúmase el principio de inducción matemática.* Sea a en $\mathbb{Z}^+$, de modo que se aplique inducción sobre a para demostrar que $1 \leq a$.

Sea $a = 1$ entonces como $1 - 1 = 0 \in \mathbb{Z}^+ \cup \{0\}$ (opuestos en + y Definición 1.1.9). Por lo que $1 \leq a$.

Supóngase que $a = k \in \mathbb{Z}^+$ entonces $1 \leq a$ (hipótesis inductiva), se demostrará para $a = k + 1 \in \mathbb{Z}^+$ que $1 \leq a$.

Sea $a = k + 1 \in \mathbb{Z}^+$, como $1 \leq k$ *sii* $k - 1 \in \mathbb{Z}^+ \cup \{0\}$ (hipótesis inductiva y Definición 1.2.1) se deduce que $k - 1 \in \mathbb{Z}^+$ ó $k - 1 = 0$. Así, si $k - 1 \in \mathbb{Z}^+$ implica que $(k + 1) - 1 = (k - 1) + 1 \in \mathbb{Z}^+$ (conmutatividad y asociatividad de + en $\mathbb{Z}$ y Definición 1.1.9) y $(k + 1) - 1 \in \mathbb{Z}^+ \cup \{0\}$ *sii* $1 \leq k + 1$ (Definición 1.2.1); pero, si $k - 1 = 0$ implica $k = 1$ (Teorema 1.1.1) y $(k + 1) - 1 = (k - 1) + 1 = 1 \in \mathbb{Z}^+$ (elemento neutro, conmutatividad y asociatividad de + en $\mathbb{Z}$ y Definición 1.1.9) y de igual modo

$(k + 1) - 1 \in \mathbb{Z}^+ \cup \{0\}$, es decir, $1 \leq k + 1$ (Definición 1.2.1). Por lo que $1 \leq a$.

(<=). Ahora bien suponga que para $a \in \mathbb{Z}$, $1 \leq a$, es decir, $a - 1 \in \mathbb{Z}^+ \cup \{0\}$ (Definición 1.2.1). Así, si $a - 1 \in \mathbb{Z}^+$ implica que $a = (a - 1) + 1 \in \mathbb{Z}^+$ (asociatividad y elemento neutro de + en $\mathbb{Z}$ y $\mathbb{Z}^+$ Definición 1.1.9); o, si $a - 1 = 0$ entonces $a = 1 \in \mathbb{Z}^+$ (Teorema 1.1.1). En ambos casos, se obtiene que $a \in \mathbb{Z}^+$.

Por otro lado nótese que $0 < 1$ *sii* $1 - 0 = 1 \in \mathbb{Z}^+$ (Teorema 1.1.6, Definición 1.1.9, Definición 1.2.1). Así, por lo demostrado anteriormente y el Teorema 1.2.1 se obtiene que $a \in \mathbb{Z}^+$ *sii* $0 < 1 \leq a$. •

Teorema 1.2.3. (Flores, 1971). Si $b \in \mathbb{Z}$ y $a \in \mathbb{Z}^+$, tal que $a \leq b \leq a + 1$ entonces $a = b$ ó $b = a + 1$.

Demostración. Sea $a \in \mathbb{Z}^+$ y suponga que existe $b \in \mathbb{Z}$, tal que $a \leq b \leq a + 1$. Así, $a \leq b$ *sii* $b - a \in \mathbb{Z}^+ \cup \{0\}$ y $b \leq a + 1$ *sii* $a + 1 - b \in \mathbb{Z}^+ \cup \{0\}$ (Definición 1.2.1). Nótese que si $a + 1 - b = 0$ ó $a - b = 0$ implica que $b = a + 1$ ó $b = a$ (Teorema 1.1.1). Sin embargo, supóngase que $b - a \in \mathbb{Z}^+$ y $a + 1 - b \in \mathbb{Z}^+$; pero $1 \leq a + 1 - b$ (Teorema 1.2.2), es decir, $a - b = (a + 1 - b) - 1 \in \mathbb{Z}^+ \cup \{0\}$ (Definición 1.2.1, elemento neutro, conmutatividad y asociatividad de + en $\mathbb{Z}$). Esto es, $b - a = 0$ ó $a - b \in \mathbb{Z}^+$ que, simultáneamente, con $b - a \in \mathbb{Z}^+$ contradicen que $0 \notin \mathbb{Z}^+$ (Definición 1.1.9). Luego, Si $b \in \mathbb{Z}$ y $a \in \mathbb{Z}^+$, tal que $a \leq b \leq a + 1$ entonces $a = b$ ó $b = a + 1$. •

Teorema 1.2.4. (Rivero, 1996). Sean a, b, c, d en $\mathbb{Z}$, entonces

a) $a, b \in \mathbb{Z}^-$ ó $a, b \in \mathbb{Z}^+$ <=> $ab \in \mathbb{Z}^+$.

b) $a \in \mathbb{Z}^+$ y $b \in \mathbb{Z}^-$ <=> $ab \in \mathbb{Z}^-$.

c) $a \leq b$ <=> $a + c \leq b + c$.

d) $a \leq b$ y $c \leq d$ => $a + c \leq b + d$

e) $a \leq b$ y $0 < c$ ó $b \leq a$ y $c < 0$ <=> $ac \leq bc$, con $c \neq 0$.

Demostración. (Literal a). (=>). Sean $a, b \in \mathbb{Z}^-$ entonces $-a, -b \in \mathbb{Z}^+$

(Definición 1.1.9), pero $-a\,(-b) = ab \in \mathbb{Z}^+$ (Teorema 1.1.5, Teorema 1.1.9).

(<=). Sean $a, b \in \mathbb{Z}$, tal que $ab \in \mathbb{Z}^+$ nótese que si se supone lo contrario a $a, b \in \mathbb{Z}^-$ ó $a, b \in \mathbb{Z}^+$, es decir, $a \in \mathbb{Z}^+$ y $b \in \mathbb{Z}^-$ (equivalente a suponer que $b \in \mathbb{Z}^+$ y $a \in \mathbb{Z}^-$) entonces $a \in \mathbb{Z}^+$ y $-b \in \mathbb{Z}^+$ (Definición 1.1.9 y Teorema 1.1.9) luego por lo demostrado previamente $-ab \in \mathbb{Z}^+$ y $-ab + ab = 0 \in \mathbb{Z}^+$, lo cual es una contradicción con respecto a la Definición 1.1.9. Así, $a, b \in \mathbb{Z}^+$ ó $a, b \in \mathbb{Z}^-$.

(Literal b). (=>). Sean $a \in \mathbb{Z}^+$ y $b \in \mathbb{Z}^-$ entonces $a \in \mathbb{Z}^+$ y $-b \in \mathbb{Z}^+$ (Definición 1.1.9 y Teorema 1.1.9), luego por lo demostrado en el literal a $a(-b) = -ab \in \mathbb{Z}^+$ entonces $ab \in \mathbb{Z}^-$.

(<=). Sean $a, b \in \mathbb{Z}$, tal que $ab \in \mathbb{Z}^-$, nótese que si se supone lo contrario a $a \in \mathbb{Z}^+$ y $b \in \mathbb{Z}^-$, es decir, $a, b \in \mathbb{Z}^-$ ó $a, b \in \mathbb{Z}^+$ entonces por lo demostrado en el literal a, $ab \in \mathbb{Z}^+$, lo cual contradice lo supuesto. Así, $a \in \mathbb{Z}^+$ y $b \in \mathbb{Z}^-$ (equivalente a suponer que $b \in \mathbb{Z}^+$ y $a \in \mathbb{Z}^-$).

(Literal c). Sean $a, b \in \mathbb{Z}$, sin pérdida de generalidad y por el orden total en $\mathbb{Z}$, $a \leq b$ *sii* $b + c - (a + c) = b - a \in \mathbb{Z}^+ \cup \{0\}$ (Teorema 1.1.5 y Definición 1.1.9), lo cual es equivalente a $a + c \leq b + c$ (Definición 1.2.1).

(Literal d). Sean $a, b, c, d \in \mathbb{Z}$, sin pérdida de generalidad y por el orden total en $\mathbb{Z}$, si $a \leq b$ y $c \leq d$ *sii* $b - a, d - c \in \mathbb{Z}^+ \cup \{0\}$ entonces considérese el Teorema 1.1.5, el Teorema 1.1.9 y la Definición 1.1.9 en los siguientes casos:

Si $b - a, d - c \in \mathbb{Z}^+$ entonces $b + d - (a + c) = b - a + d - c \in \mathbb{Z}^+$.

Si $b - a, d - c \in \{0\}$ entonces $b + d - (a + c) = 0$.

Si $b - a \in \{0\}$ y $d - c \in \mathbb{Z}^+$ entonces $b + d - (a + c) = d - c \in \mathbb{Z}^+$.

Si $b - a \in \mathbb{Z}^+$ y $d - c \in \{0\}$ entonces $b + d - (a + c) = b - a \in \mathbb{Z}^+$.

En todos los casos se concluye que $b + d - (a + c) \in \mathbb{Z}^+ \cup \{0\}$.

(Literal e). (=>). Sean $a, b, c \in \mathbb{Z}$, considérese $a \leq b$ y $0 < c$ entonces $b - a \in \mathbb{Z}^+ \cup \{0\}$ y $c \in \mathbb{Z}^+$ esto es equivalente a $b - a \in \mathbb{Z}^+$ ó $b - a = 0$ y $c \in \mathbb{Z}^+$. Asimismo, si se considera a $b \leq a$ y $c < 0$ *sii* $a - b \in \mathbb{Z}^+ \cup \{0\}$ y $c \in \mathbb{Z}^-$ esto es equivalente a $b - a \in \mathbb{Z}^-$ ó $b - a = 0$ y $c \in \mathbb{Z}^-$; en ambos casos se obtiene $bc - ac = (b - a)c \in \mathbb{Z}^+ \cup \{0\}$ (Definición 1.2.1, Teorema 1.1.4 y Teorema 1.1.9). Así, $ac \leq bc$.

(<=). Sean $a, b, c \in \mathbb{Z}$, de modo que $bc \leq ac$. Esto es, $bc - ac \in \mathbb{Z}^+ \cup \{0\}$ (Definición 1.2.1). Así, $bc - ac = (b - a)c \in \mathbb{Z}^+$ ó $(b - a)c = 0$; luego, si $c \neq 0$ entonces $b - a \in \mathbb{Z}^+$ y $c \in \mathbb{Z}^+$ ó $a - b \in \mathbb{Z}^-$ y $-c \in \mathbb{Z}^-$ ó $b = a$ (Definición 1.1.7, Teorema 1.1.4 y Teorema 1.2.1). Por tanto, $a \leq b$ y $0 < c$ ó $b \leq a$ y $c < 0$.•

Definición 1.2.2. (Rivero, 1996). Sea $A \neq \varnothing$ subconjunto de $\mathbb{Z}$ entonces $n \in \mathbb{Z}$ es una *cota superior* (*cota inferior*) de A *sii* $a \leq n$ ($n \leq a$) para todo $a \in A$.

Definición 1.2.3. (Rivero, 1996). Sea $A \neq \varnothing$ subconjunto de $\mathbb{Z}$ entonces, existe una *cota superior* (*cota inferior*) de A *sii* A está *acotado superiormente* (*acotado inferiormente*). Se dice que A está *acotado* si lo está superior e inferiormente.

Definición 1.2.4. (Rivero, 1996). Sea $A \neq \varnothing$ subconjunto de $\mathbb{Z}$ acotado superiormente (acotado inferiormente) y U el conjunto de las cotas superiores (L el conjunto de las cotas inferiores), entonces $x \in U$ ($x \in L$) es el *supremo* de A (es el *ínfimo* de A) *sii* $a \leq x$ ($x \leq a$) para todo $a \in A$. Si $x \in A$, se le denomina elemento *maximal* o *máximo* (elemento *minimal* o *mínimo*).

Observación. $\mathbb{Z}^+$ cumple el principio de *buen orden*, como consecuencia del *Lema de Zorn* (Fraleigh, 1987), es decir, cualquier subconjunto de $\mathbb{Z}^+$, tiene un elemento mínimo (nótese que $\mathbb{Z}^+$ está acotado inferiormente por 1, Teorema 1.2.2, y hereda la totalidad del orden de $\mathbb{Z}$, Teorema 1.2.1 y Teorema 1.2.3). Análogamente, como consecuencia del *Lema de Zorn*: todo subconjunto de $\mathbb{Z}^+$ acotado superiormente posee máximo (Teorema 1.2.1, Teorema 1.2.2, Teorema 1.2.3 y considérese que el conjunto de las cotas superiores de cualquier subconjunto de $\mathbb{Z}^+$, a su vez está acotado

inferiormente por el subconjunto y por el mínimo de dichas cotas). Por ejemplo, $s = 0$ es supremo de $\mathbb{Z}^-$ y su máximo es –1 (Teorema 1.2.2 y Teorema 1.2.4).

Definición 1.2.5. (Stark, 1984). Sean a, b en $\mathbb{Z}$, si $a \neq 0$ y existe $c := \frac{b}{a}$ en $\mathbb{Z}$, tal que $b = ac$ *sii* a es un *divisor* de b y se dirá que a *divide* a b, denotado por $a \mid b$. Asimismo, se dice que b es *múltiplo* de a y que b está *descompuesto en los factores* a y c.

Observación. Es usual describir el conjunto de divisores de cualquier elemento en $\mathbb{Z}$, como subconjunto de $\mathbb{Z}^+$ y nótese que, al menos, a =1 es un divisor para cualquier b en $\mathbb{Z}$, incluso, con la condición de que $b \neq 0$, los elementos b y $-b$ (alguno de los dos está en $\mathbb{Z}^+$) son divisores de b con c= 1, –1, respectivamente. Asimismo, cualquier $a \neq 0$ en $\mathbb{Z}$ divide a 0. También, nótese el conjunto de divisores de cualquier elemento en $\mathbb{Z}^+$ está acotado y nótese que el conjunto de múltiplos de cualquier elemento en $\mathbb{Z}^+$ está acotado inferiormente (Definición 1.2.4, Teorema 1.2.4).

Definición 1.2.6. (Rivero, 1996). Sean a, b, d en $\mathbb{Z}^+$, $d := (a, b)$ es el *Máximo Común Divisor* de a, b *sii* $d \mid a$, $d \mid b$ y si para cualquier c en $\mathbb{Z}^+$, tal que $c \mid a$ y $c \mid b$ entonces $c \mid d$.

Definición 1.2.7. (Rivero, 1996). Sean a, b, m en $\mathbb{Z}^+$, $m := [a, b]$, es el *Mínimo Común Múltiplo* de a, b *sii* $a \mid m$, $b \mid m$ y si para cualquier c en $\mathbb{Z}^+$, tal que $a \mid c$ y $b \mid c$ entonces $m \mid c$.

Teorema 1.2.5. (Epp, 2012). Sean a, b en $\mathbb{Z}^+$, tal que $a \mid b$ entonces $a \leq b$. En particular, si, además, $b \mid a$ entonces $a = b$.

Demostración. Sean a, b en $\mathbb{Z}^+$, si $a \mid b$ implica que $b = ac$, con c en $\mathbb{Z}^+$, (Definición 1.2.5). Además, c en $\mathbb{Z}^+$ implica que $1 \leq c$ (Teorema 1.2.2), luego por el Teorema 1.2.4 se obtiene $a \leq ca = b$. Por tanto, $a \leq b$.

Además, supóngase que $a \mid b$ y $b \mid a$ entonces, por lo expuesto anteriormente, se obtiene $a \leq b$ y $b \leq a$, de lo que se deduce $a = b$ (Teorema 1.2.4). •

Observación. Nótese que para a, b en $\mathbb{Z}^+$, si $1 = ab$ implica que $a \mid 1$ y que $b \mid 1$, pero 1 es divisor de cualquier entero entonces por el Teorema 1.2.5, se deduce que $a = 1$ y $b = 1$ (Epp, 2012).

Definición 1.2.8. (Stark, 1984). Sea p en $\mathbb{Z}^+$, $1 < p$ y $\{1, p\}$ es el único conjunto de divisores positivos de *p sii p* es *primo*.

Definición 1.2.9. (Stark, 1984). Sea c en $\mathbb{Z}^+$, $1 < c$ y c no es primo *sii c* es *compuesto*.

Observación. 1 no es compuesto ni primo (Definición 1.2.8 y Definición 1.2.9).

Teorema 1.2.6. (Castro, 2014). Sean b en $\mathbb{Z}$, a en $\mathbb{Z}^+$ y $a \mid b$ entonces para a y b fijos, existe un único c en $\mathbb{Z}$, tal que $b = ac$.

Demostración. Sean b en $\mathbb{Z}$ y a en $\mathbb{Z}^+$, suponga, para a y b fijos, que $a \mid b$, es decir, $b = ac$ para c en $\mathbb{Z}$ (Definición 1.2.5) y que por el contrario c en $\mathbb{Z}$ no es único para los valores a, b es decir, existe d en $\mathbb{Z}$, tal que $b = ad$. Así, $ad = ac$ ó $ad + (-ac) = 0$ (Teorema 1.1.2) y $a(d + (-c)) = 0$ ($\mathbb{Z}$ es un anillo y véase la Definición 1.1.4), de lo cual se deduce $d + (-c) = 0$ (a en $\mathbb{Z}^+$ y véase la Definición 1.1.7) y $d = c$ (Teorema 1.1.1). Así, para a en $\mathbb{Z}^+$, el elemento c en $\mathbb{Z}$ es el único elemento, tal que $b = ac$.•

Teorema 1.2.7. (Rivero, 1996). Sean b en $\mathbb{Z}$ y a en $\mathbb{Z}^+$ entonces, para a y b fijos, existen q, r en $\mathbb{Z}$ únicos, tal que $b = aq + r$ y $0 \leq r < a$.

Demostración. Sean b en $\mathbb{Z}$ y a en $\mathbb{Z}^+$, suponga que $a \mid b$ entonces el teorema se cumple (con $r = 0$ y $c = q$ en $\mathbb{Z}$ en la Definición 1.2.5 y en el Teorema 1.2.6).

Por otro lado, considerándose la Definición 1.2.5: sean b en $\mathbb{Z}$ y a en $\mathbb{Z}^+$, fijos, suponga que no se cumple que $a \mid b$ entonces no existe q en $\mathbb{Z}$, tal que $b - aq = 0$, $1 < a$ (de lo contrario, $a = 1$, sería divisor de b, Teorema 1.2.2) y $b \neq 0$ (de lo contrario, $b = 0$, tendría a todos los elementos distintos de cero de $\mathbb{Z}$ como divisores, entre ellos a, con q, $r = 0$, Teorema 1.1.4). Entonces, considerándose la Definición 1.2.1, el Teorema 1.2.1, el Teorema 1.2.2, el Teorema 1.2.3 y el Teorema 1.2.4, sean los

subconjuntos de $\mathbb{Z}$:

$$A = \{b - aq \in \mathbb{Z}^+ / q \in \mathbb{Z}\} \text{ y } B = \{q \in \mathbb{Z} / b - aq \in \mathbb{Z}^+\};$$

ambos son distintos del vacío, ya que si se fija a $0 < b$, con cualquier $q < 0$, se obtiene que $aq < 0$ y $0 < b - aq$. Asimismo, si se fija a $b < 0$, para $q = b$, $aq < 0$ y $b - aq = b - ab = b(1 - a)$ pero $1 - a < 0$, así, $0 < b - aq$. Además, A es subconjunto de $\mathbb{Z}^+$, en consecuencia, A tiene elemento mínimo r, es decir, existe $r = minA = b - aq$ para algún q en B (*Lema de Zorn*). Sin embargo, $q + 1$ no está en B, ya que si $q + 1 \in B$ entonces $q < q + 1$ y $aq - b < a(q + 1) - b$, por lo que $0 < b - a(q + 1) < b - aq$ y sería contradictorio que r sea mínimo en A, igualmente cualquier $h \in \mathbb{Z}$, tal que $q + 1 \leq h$, no está en B, por tanto, B está acotado superiormente, de modo que B tiene elemento máximo $q = maxB$ (*Lema de Zorn*).

Nótese que si $r = b - aq = a$ entonces $b = a(1 + q)$, lo cual contradice la negación de $a \mid b$ y si $a < r = b - aq$, se obtiene que $0 < b - a(q + 1)$ y similarmente se sigue la contradicción con $r = minA$. Así, q, r en $\mathbb{Z}$ son únicos (Definición 1.2.4 y Teorema 1.2.1) y además, $b = aq + r$ y $0 < r < a$.

Por tanto, para b en $\mathbb{Z}$ y a en $\mathbb{Z}^+$ fijos, existen q, r en $\mathbb{Z}$ únicos, tal que $b = aq + r$ y $0 \leq r < a$. •

2. EL PRODUCTO CARTESIANO DE CONJUNTOS FINITOS Y LA CONGRUENCIA MODULAR EN $\mathbb{Z}$

En el presente capítulo se demuestra que cualquier entero se puede expresar como una suma de productos de elementos de cualquier sucesión en $\mathbb{Z}^+ - \{1\}$. Luego se describe al anillo $\mathbb{Z}$, a través de sus particiones, en particular, la partición en $\mathbf{Z}_n$ y, a su vez, se demuestra que se puede describir a $\mathbf{Z}_n^m$ con $\mathbf{Z}_{n^m}$. Esto es, se puede describir a cualquier entero como una suma de productos de elementos de cualquier sucesión en $\mathbb{Z}^+ - \{1\}$.

2.1. BASES GENERALIZADAS

Teorema 2.1.1. (Castro *et al*, 2015). Sea $\{s_n\}_{n\in\mathbb{Z}^+}$ en $\mathbb{Z}^+ - \{1\}$, entonces para todo $a \in \mathbb{Z}^+ \cup \{0\}$ y algún $k \in \mathbb{Z}^+$:

$$a = \sum_{j=1}^{k} r_j q_{j-1}, \text{ con } r_j \in \mathbb{Z}^+ \cup \{0\} \text{ único, } r_j < s_j, \; q_j = \prod_{i=1}^{j} s_i \text{ y } q_0 = 1 \; \forall j = 1,2,..,k .$$

Demostración. Si $a = 0$ entonces para $k = 1$ y $r_1 = 0$ el teorema es cierto ($\{s_n\}_{n\in\mathbb{Z}^+} \subset \mathbb{Z}^+ - \{1\}$, Teorema 1.1.4, Teorema 1.1.6 y Definición 1.1.7).

Por otro lado, considerándose el Teorema 1.2.3 y que $1 \leq a$. *Asúmase el principio de inducción matemática*. Sea $\{s_n\}_{n\in\mathbb{Z}^+} \subset \mathbb{Z}^+ - \{1\}$, de tal manera que se aplique inducción sobre a en $\mathbb{Z}^+$, tal que para algún $k \in \mathbb{Z}^+$, existe r_j en $\mathbb{Z}$ único, de modo que $\forall j = 1,2,..,k : q_j = \prod_{i=1}^{j} s_i$, $q_0 = 1$, $0 \leq r_j < s_j$ y $a = \sum_{j=1}^{k} r_j q_{j-1}$.

Sea $a = 1$ entonces para $k = 1$ y $r_1 = 1$ único, el teorema se cumple ($\{s_n\}_{n\in\mathbb{Z}^+} \subset \mathbb{Z}^+ - \{1\}$, Definición 1.1.5 y considérese que existe la identidad y es único, puesto que es el neutro para × en $\mathbb{Z}$). Esto es,

$$a = \sum_{j=1}^{1} r_j q_{j-1} = r_1\, q_0 = r_1.1 = 1.$$

Asimismo, sea $a \in \mathbb{Z}^+$ supóngase cierto el teorema para cualquier b en $\mathbb{Z}$, de modo que $1 < b < a$. Así, para algún $m \in \mathbb{Z}^+$, existe r_j en $\mathbb{Z}$ único, tal que $0 \leq r_j < s_j$, $\forall j = 1,2,..,m$ y

$$b = \sum_{j=1}^{m} r_j q_{j-1}\text{, con } q_j = \prod_{i=1}^{j} s_i \text{ y } q_0 = 1 \text{ (hipótesis inductiva).}$$

Luego, se demostrará para a y algún $k \in \mathbb{Z}^+$, $q_j = \prod_{i=1}^{j} s_i$ y $q_0 = 1$ existe r_j en $\mathbb{Z}$ único, de modo que $\forall j = 1,2,..,k : 0 \leq r_j < s_j$ y

$$a = \sum_{j=1}^{k} r_j q_{j-1}\text{, con } q_j = \prod_{i=1}^{j} s_i \text{ y } q_0 = 1.$$

Primeramente, considérese el conjunto $A = \{ j \in \mathbb{Z}^+ \cup \{0\} / \ q_j \leq a\}$, el cual es distinto de vacío ($0 \in A$ e hipótesis inductiva). Además, A está acotado, superiormente, por a, ya que $\forall n \in \mathbb{Z}^+$, $q_n < q_{n+1}$, $n < q_n$ y $1 < s_n \Leftrightarrow 2 \leq s_n$ ($\{s_n\}_{n \in \mathbb{Z}^+} \subset \mathbb{Z}^+ - \{1\}$, Teorema 1.2.3 y Teorema 1.2.4).

Ahora bien, existe $d = maxA$ (consecuencia del *lema de Zorn*), así, $q_d \leq a < q_{d+1}$ (Teorema 1.2.3). Luego, como $q_d \in \mathbb{Z}^+$ ($1 < s_n$, $\forall n \in \mathbb{Z}^+$ y Teorema 1.2.2) existen h en $\mathbb{Z}^+$ y $t \in \mathbb{Z}^+ \cup \{0\}$, únicos, tal que $a = q_d h + t$ y $t < q_d$ ($1 < a$, Teorema 1.1.9 y Teorema 1.2.7). Además, por hipótesis inductiva, $t < a$ ($q_d \leq a$ y Teorema 1.2.1) y con $m = d$ entonces existe r_j en $\mathbb{Z}$ único, de modo que $\forall j = 1,2,...,d$, $0 \leq r_j < s_j$ y

$$t = \sum_{j=1}^{d} r_j q_{j-1}\text{, con } q_j = \prod_{i=1}^{j} s_i \text{ y } q_0 = 1.$$

Finalmente, considerándose que $q_d h \leq a = q_d h + t < q_{d+1}$, $0 < 1 < s_d$ y $q_{d+1} =$

$q_d s_{d+1}$ (Teorema 1.2.4) implica que $h < s_{d+1}$ y con $r_{d+1} = h$, se obtiene $\forall j = 1,2,..,d,d+1$, $0 \leq r_j < s_j$ y

$$a = r_{d+1}q_d + \sum_{j=1}^{d} r_j q_{j-1} = \sum_{j=1}^{d+1} r_j q_{j-1}, \text{ con } q_j = \prod_{i=1}^{j} s_i \text{ y } q_0 = 1.$$

Así, el teorema queda demostrado para $a \in \mathbb{Z}^+$, con $k = d + 1$.•

Observación. Escribir cualquier $a \in \mathbb{Z}^+ \cup \{0\}$ como:

$$a = \sum_{j=1}^{k} r_j q_{j-1},$$

con algún $k \in \mathbb{Z}^+$ y $\forall j = 1,2,..,k : r_j \in \mathbb{Z}^+ \cup \{0\}$ único (los *dígitos*), $r_j < s_j$, $q_j = \prod_{i=1}^{j} s_i$ y $q_0 = 1$ para $\{s_n\}_{n \in \mathbb{Z}^+}$ (la *base*) en $\mathbb{Z}^+ - \{1\}$ hace referencia a las *bases generalizadas* (Cilleruelo *et al*, 2010). También, garantiza la existencia de una biyección entre *a* y sus dígitos, lo cual brinda la ventaja de representar al entero *a* mediante los dígitos ($r_j \in \mathbb{Z}^+ \cup \{0\} \; \forall j = 1,2,..,k$). Esto es, se puede utilizar la notación de vector, (r_1, r_2, …, r_k), para *a*. Además, obsérvese que si $1 < b = s_n$, $\forall n \in \mathbb{Z}^+$ entonces se deduce la escritura usual de *a* en la base *b*.

2.2. RELACIÓN DE CONGRUENCIA MÓDULO EN $\mathbb{Z}$ Y EL TEOREMA DE FACTORIZACIÓN ÚNICA

Definición 2.2.1. (Fraleigh, 1987). Sea $c \in \mathbb{Z}^+$ para cada *a*, *b* en $\mathbb{Z}$, *a* es *congruente* con *b módulo c* y se escribe $a \equiv b$ (*mod*. *c*), *sii* $c \mid (a - b)$.

Teorema 2.2.1. (Rivero, 1996). Considérese $c \in \mathbb{Z}^+$ y la relación $\equiv$ (*mod*. *c*) en $\mathbb{Z}$:

a) Para todo *a* en $\mathbb{Z}$, $a \equiv a$. *Reflexividad*.

b) Para cualesquiera *a*, *b* en $\mathbb{Z}$, si $a \equiv b$ implica $b \equiv a$. *Simetría*.

c) Para cualesquiera *a*, *b*, *c* en $\mathbb{Z}$, si $a \equiv b$ y $b \equiv d$ implica $a \equiv d$. *Transitividad*.

Demostración. Primeramente, considérese a $c \in \mathbb{Z}^+$ para la demostración de cada literal.

(Literal a). Para cualquier $a \in \mathbb{Z}$ existe su opuesto $-a$, tal que $a - a = 0$ y a su vez, 0 = 0.c entonces c | $(a - a)$. Por tanto, $a \equiv a$ (*mod*. *c*).

(Literal b). Sean *a*, *b* en $\mathbb{Z}$, tal que $a \equiv b$ (*mod*. *c*), *sii* c | $(a - b)$ entonces existe *d* en $\mathbb{Z}$, tal que $a - b = d$c (Definición 1.2.5); pero también para los respectivo opuestos $b - a$ y $-d$ (Teorema 1.1.1 y Teorema 1.1.5), $b - a = -dc$, *sii c* | $(b - a)$. Esto es, b ≡ *a* (*mod*. *c*).

(Literal c) Sea *a*, *b*, *d* en $\mathbb{Z}$, $a \equiv b$ y $b \equiv d$ (*mod*. *c*) *sii c* | $(a - b)$ y *c* | $(b - d)$ entonces existen, respectivamente h' y *h* en $\mathbb{Z}$, tal que, $a - b = h$c y $b - d = h$c (Definición 1.1.5). Luego, $a - b + b - d = a - d = (h' + h)c$, por lo que *c* | $(a - d)$. Por tanto, $a \equiv d$ (*mod*. *c*).

Así, $\mathbb{Z}$ está dotado de una *relación de equivalencia*.•

Observación. Nótese que la relación de equivalencia en $\mathbb{Z}$ hace pensar que habrá elementos que no están relacionados. Sin embargo, los elementos que sí están relacionados pueden inferirse con un sólo elemento o un *representante*, tomando uno de ellos como tal.

Definición 2.2.2.. (Rivero, 1996). Una *partición* de un conjunto *A* es una colección de conjuntos $\{B_n\}_{n \in I}$, con I $\subseteq \mathbb{Z}^+$, tal que $\forall j, i \in I$, $B_i \cap B_j = \emptyset$, si $i \neq j$ y $\bigcup_{i \in I} B_i = A$.

Teorema 2.2.2. (Rivero, 1996). Sea $n \in \mathbb{Z}^+$ la relación de equivalencia ≡ (*mod*. *n*) induce una partición en $\mathbb{Z}$.

Demostración. Sea $n \in \mathbb{Z}^+$ y $\mathbb{Z}_n = \{[a]_n \subset \mathbb{Z} / a \in \mathbb{Z}, 0 \leq a < n\}$, con $[a]_n = \{x \in \mathbb{Z}, x \equiv a \ (mod.\ n)\}$, nótese que fijar $a \in \mathbb{Z}$, tal que $0 \leq a < n$, como representante del conjunto de elementos relacionados con *a*, es indistinto para la demostración (Definición 1.2.5, Definición 2.2.1, Teorema 1.2.7 y Teorema 2.2.1).

Así, $\mathbb{Z}_n$ es una partición de $\mathbb{Z}$, ya que:

Si $x \in [a]_n \cap [b]_n$ *sii* $x \equiv a$ y $x \equiv b$ (*mod. n*) y esto implica $a \equiv b$ (*mod. n*) (Teorema 2.2.1) cámbiese el representante del conjunto $[a]_n$ por *b* por lo que $[a]_n = [b]_n$. Por contrarrecíproco, al suponer que $[a]_n \neq [b]_n$ entonces $[a]_n \cap [b]_n = \emptyset$.

Asimismo, si $x \in \mathbb{Z}$ entonces, únicamente, existen *h*, $a \in \mathbb{Z}$, con $0 \leq a < n$, tal que $x - a = hn$ (Teorema 1.2.7), en consecuencia $x \in [a]_n$. Por tanto, *x* está en uno de los conjuntos cuyo representante es sólo uno de los elementos de $\mathbb{Z}_n$. Finalmente, como $[a]_n \subset \mathbb{Z}$ para cualquier $0 \leq a < n$ la unión de los elementos de $\mathbb{Z}_n$ forman a todo $\mathbb{Z}$.•

Observación. (Fraleigh, 1987). De ahora en adelante, se asume que $\mathbb{Z}_n = \{[a]_n \subset \mathbb{Z} \ / a \in \mathbb{Z},\ 0 \leq a < n\}$, con $n \in \mathbb{Z}^+$ y es denotado por el conjunto de enteros $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$ cuyos elementos se denominan *clase de equivalencia*.

Teorema 2.2.3. (Fraleigh, 1987). ($\mathbb{Z}_n$, σ) es un grupo conmutativo, tal que para *a*, *b* en $\mathbb{Z}_n$, se define $a \ \sigma \ b := r$ *sii* $a + b = qn + r$ y $q, r \in \mathbb{Z}$, con $0 \leq r < n$.

Demostración. Nótese que por definición de σ y el Teorema 1.2.7, σ es una función de $\mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$.

Igualmente, sea $a \in \mathbb{Z}_n$, como $0 \in \mathbb{Z}_n$, $0 \leq a < n$, considérese a $q = 0$ y $r = a$ (Teorema 2.1.1.) entonces $0 \ \sigma \ a = a \ \sigma \ 0 = a$. Por tanto, ($\mathbb{Z}_n$, σ) posee neutro.

Además, sea $a \in \mathbb{Z}_n$, como 0 es opuesto de sí mismo, supóngase $0 < a < n$, por lo que $-a < 0$ (Teorema 1.1.9, Teorema 1.2.1). Así, $0 < n - a < n$. Así, $n - a \in \mathbb{Z}_n$ (Definición 1.2.1, Teorema 1.2.4). Ahora bien, $a + n - a = n$, considerándose a $q = 1$ y $r = 0$ (Teorema 2.1.1.), se obtiene $(n - a) \ \sigma \ a = a \ \sigma \ (n - a) = 0$. Luego los elementos de ($\mathbb{Z}_n$, σ) poseen inverso.

Por otro lado, sean *a*, *b*, $c \in \mathbb{Z}_n$:

$$(a \ \sigma \ b) \ \sigma \ c = r_0 \ \sigma \ c = r_1 \text{ sii } a + b = q_0 n + r_0 \text{ y } r_0 + c = q_1 n + r_1$$

$$(b \sigma c)\ \sigma\ a = r_2\ \sigma\ a = r_3\ sii\ b + c = q_2 n + r_2 \text{ y } r_2 + a = q_3 n + r_3$$

con q_j, $r_j \in \mathbb{Z}$, $0 \leq r_j < n$ y $j = 1,2,3$. Sin embargo, por Teorema 1.1.1, Teorema 1.1.2, Teorema 1.1.5 y Teorema 2.1.1. se obtiene:

$a + b + c = (q_0 + q_1)n + r_1$, $a + b + c = (q_2 + q_3)n + r_3$, $(q_0 + q_1) = (q_2 + q_3)$ y $r_1 = r_3$. Esto es, $(a\ \sigma\ b)\ \sigma\ c = (b\ \sigma\ c)\ \sigma\ a$. Además, por Teorema 1.1.3, $(\mathbb{Z}_n, \sigma)$ cumple con la propiedad conmutativa y asociativa.•

Observación. Sea $(\mathbb{Z}_n, \sigma)$, con $n \in \mathbb{Z}^+$, el operador σ de modo que para a,b en $\mathbb{Z}_n$, $(a\ \sigma\ b)$ también se escribe $a + b$ (*mod*. n). Análogamente, se define ρ en $\mathbb{Z}_n$, tal que para a,b en $\mathbb{Z}_n$, $a\ \rho\ b := s\ sii\ ab = pn + s$ y $p, s \in \mathbb{Z}$, con $0 \leq s < n$. Igualmente, si $2 \leq n$, 1 es la identidad de $(\mathbb{Z}_n, \rho)$ y para a, b ,c se cumple que $(a\rho b)\rho c = (b\rho c)\rho a$ (Definición 1.1.9, Teorema 1.2.7). Esto es, $(\mathbb{Z}_n, \rho)$ cumple con la propiedad conmutativa y asociativa (véase la demostración del Teorema 1.1.3). Además, $a\ \rho\ b$ se escribe ab (*mod*. n). Finalmente, $a(b + c) = ab + ac$ (Definición 1.1.9, Teorema 1.2.7), es decir, se cumple la propiedad distributiva. Así, $(\mathbb{Z}_n, \sigma, \rho)$ es un anillo conmutativo con identidad y se denotará simplemente por $\mathbb{Z}_n$.

Teorema 2.2.4. (Castro, 2014). Sean $a, b \in \mathbb{Z}^+$, las siguientes proposiciones son equivalentes:

i. $ax + by = c$ (*Identidad de Bezout*) tiene infinitas soluciones en $\mathbb{Z}$.

ii. $c \in [0]_{(a,b)}$.

iii. $[c]_a \cap [0]_b \cup [0]_a \cap [c]_b \neq \emptyset$.

Demostración. (i => ii) Sean $a,b \in \mathbb{Z}^+$, si existen $x, y, c \in \mathbb{Z}$, tal que $ax + by = c$ y para (a ,b) existen $k, k' \in \mathbb{Z}^+$, tal que $a = (a,b)k$ y $b = (a,b)k'$ (Definición 1.2.6). Así, $c = ax + by = (a,b)(kx + k'y) + 0$, es decir, $c \in [0]_{(a,b)}$ (Definición 1.1.9 y Definición 2.2.1).

(ii => iii) Sea $P = \{ax + by \in \mathbb{Z}^+ / x, y \in \mathbb{Z}\} \neq \emptyset$, con $a, b \in \mathbb{Z}^+$, P está acotado

inferiormente por 0 (Definición 1.2.4, Teorema 1.2.2), entonces existen x_0, $y_0 \in \mathbb{Z}$ de modo que $ax_0 + by_0 = m = minP$ (consecuencia del *lema de Zorn*). Además, para (a, b) existen $k, k' \in \mathbb{Z}^+$, tal que $a = (a,b)k$ y $b = (a,b)k'$ entonces $(a,b)(kx_0 + k'y_0) = m$ *sii* $(a, b) \mid m$ (Definición 1.2.5).

Por otro lado, $a = mq + r$ y $b = mp + s$ con $0 \leq r, s < m$ (Teorema 1.2.7) pero $r = (1 - qx_0)a + b(-qy_0)$ y $s = (1 - px_0)a + b(-py_0)$ (Teorema 1.1.2, Teorema 1.1.4, Teorema 1.1.5, Definición 1.1.9). Esto es, $r, s = 0$ (puesto que $m = minP$) y $m \mid (a, b)$ (Definición 1.2.6). Así, $(a, b) = m$ (Teorema 1.1.7, Definición 1.1.9, Teorema 1.2.1, Teorema 1.2.2, Teorema 1.2.3, Teorema 1.2.4).

Ahora bien, $(a, b) \in P \subseteq D = \{ax + by \in \mathbb{Z} / x, y \in \mathbb{Z}\}$, luego para todo $n \in \mathbb{Z}$ $n(a, b) = anx_0 + bny_0$. Así, $[0]_{(a,b)} = D$ (Definición 2.2.1).

Finalmente, por lo expuesto anteriormente y si $c \in [0]_{(a,b)}$, existen $w, z \in \mathbb{Z}$, tal que $h = aw = bz + c$ ó $h = bz = aw + c$. Esto es $[c]_a \cap [0]_b \cup [0]_a \cap [c]_b \neq \emptyset$ (Teorema 1.1.1, Teorema 1.1.2, Teorema 1.1.5, Definición 2.2.1, Teorema 2.2.1 y Teorema 2.2.2).

(iii => i) Si $[c]_a \cap [0]_b \cup [0]_a \cap [c]_b \neq \emptyset$ entonces existen $x', y', x'', y'' \in \mathbb{Z}$ y $q \in [c]_a \cap [0]_b \cup [0]_a \cap [c]_b \neq \emptyset$, de modo que

$q = ax' + c = by' + 0$ ó $q = by'' + c = ax'' + 0$ (Definición 2.2.1),

implica que $x = -x'$ y $y = y'$ ó $x = x''$ y $y = -y''$ son soluciones de la identidad $ax + by = c$ (Definición 1.1.9). Además, para cualquier $w \in \mathbb{Z}$ implica que $x = -x' - bw$, $y = y' + aw \in \mathbb{Z}$ y, aplicando el Teorema 1.1.5 y propiedades del anillo $\mathbb{Z}$, se obtiene:

$ax + by = a(-x' - bw) + b(y' + aw) = -ax' - abw + by' + baw = a(-x') + by' = c.$

Análogamente, $x = x'' + bw$ y $y = -y'' - aw \in \mathbb{Z}$ y se obtiene:

$ax + by = a(x'' + bw) + b(-y'' - aw) = ax'' + abw - by'' - baw = ax'' + b(-y'') = c.$

Lo que demuestra que $ax + by = c$ tiene infinitas soluciones en $\mathbb{Z}$.•

Definición 2.2.3. (Rivero, 1996). Sean $a, b \in \mathbb{Z}$ son coprimos *sii* $(a,b) = 1$.

Teorema 2.2.5. (Rivero, 1996). Sean $a, b, c \in \mathbb{Z}$, si a,b son coprimos y $a \mid cb$ entonces $a \mid c$.

Demostración. Sean $a, b, c \in \mathbb{Z}$ supóngase que a, b son coprimos, esto es, $(a,b) = 1$ (Definición 2.2.3) y además, si $a \mid cb$ entonces existen $x, y \in \mathbb{Z}$, tal que $ax + by = 1$ (Teorema 2.2.4). Así, $cax + cby = c$ (Definición 1.1.9). Además, existe $k \in \mathbb{Z}^+$, tal que $cb = ka$ (Definición 1.2.5). Luego, $c = a(cx + ky)$ (Definición 1.1.9), por tanto $a \mid c$ (Definición 1.2.5). •

Teorema 2.2.6. (Rivero, 1996). *Teorema de Factorización Única*. Sea $a \in \mathbb{Z}^+$ y $1 < a$ entonces para algún $m \in \mathbb{Z}^+$, $a = \prod_{i=1}^{m} p_i$, donde $\{ p_i \}_{i=1}^{m}$ es una sucesión única de enteros primos.

Demostración. *Asúmase el principio de inducción matemática*. Sea $a \in \mathbb{Z}^+$ y $1 < a$, de tal manera que se aplique inducción sobre a para mostrar que con algún $m \in \mathbb{Z}^+$, $a = \prod_{i=1}^{m} p_i$, donde $\{ p_i \}_{i=1}^{m}$ es una sucesión única de enteros primos.

Como $1 < a$, si $a = 2$, nótese que 2 es primo (Teorema 1.2.3 y Definición 1.2.8). Por tanto, el teorema es cierto.

Asimismo, sea $a \in \mathbb{Z}^+$, supóngase que para cada $b \in \mathbb{Z}^+$, tal que $2 \leq b < a$ y $b = \prod_{i=1}^{k} p_i$, con algún $k \in \mathbb{Z}^+$, donde $\{ p_i \}_{i=1}^{k}$ es una sucesión única de enteros primos (Hipótesis Inductiva). Así, se demostrará para algún $m \in \mathbb{Z}^+$ que $a = \prod_{i=1}^{m} p_i$, donde $\{ p_i \}_{i=1}^{m}$ es una sucesión única de enteros primos.

Considérese que a es compuesto, de lo contrario, si a es primo el teorema es cierto. Entonces el conjunto de divisores de a tiene más de dos elementos (Definición 1.2.8 y

Definición 1.2.9). Sean c, $d \in \mathbb{Z}^+$, divisores de a, tal que $1 < c, d < a$ y $a = cd$ (Definición 1.2.5, Teorema 1.2.1). Por hipótesis inductiva, para $r, s \in \mathbb{Z}^+$

$$c = \prod_{i=1}^{r} p_i^{\bullet} \, , \; d = \prod_{i=1}^{s} p_i^{\bullet\bullet} \, ,$$

donde $\left\{ p_i^{\bullet} \right\}_{i=1}^{r}$ y $\left\{ p_i^{\bullet\bullet} \right\}_{i=1}^{s}$ son, respectivamente, sucesiones únicas de enteros primos. Por tanto,

$$a = \prod_{i=1}^{r} p_i^{\bullet} \prod_{i=1}^{s} p_i^{\bullet\bullet} = \prod_{i=1}^{m} p_i \text{ , con } m = r + s \in \mathbb{Z}^+,$$

donde $\left\{ p_i \right\}_{i=1}^{m}$ es una sucesión de enteros primos, tal que

$$p_i = \begin{cases} p_j^{\bullet}, & \text{si } j = i \\ p_j^{\bullet\bullet}, & \text{si } j = i - r \end{cases} .$$

Por otro lado, véase que si se escogen otros divisores de a la sucesión de primos siempre será la misma.

Considérese $2 \leq c', d' < a$, tal que $a = c'd'$ (Definición 1.2.5, Teorema 1.2.4) y por hipótesis inductiva $c' = \prod_{k=1}^{s'} p_k^{*}$, y $d' = \prod_{k=1}^{r'} p_k^{**}$, con $\left\{ p_k^{*} \right\}_{k=1}^{s'}$ y $\left\{ p_l^{**} \right\}_{l=1}^{r'}$ sucesiones únicas de enteros primos y $r', s' \in \mathbb{Z}^+$. Además, $c'd' = a = \prod_{i=1}^{m} p_i$, con $m \in \mathbb{Z}^+$, por lo que $p_i \left| \prod_{k=1}^{s'} p_k^{*} \prod_{l=1}^{r'} p_l^{**} \right.$, por cada $i = 1, 2, \ldots, m$. Y también, para todo $i = 1, 2, \ldots, m$, $k = 1, 2, \ldots, s'$ y $l = 1,2, \ldots, r'$,

$$\left(p_i, p_k^{*} \right) = \begin{cases} 1, & \text{si } p_i \neq p_k^{*} \\ p_i, & \text{si } p_i = p_k^{*} \end{cases} \text{ ó } \left(p_i, p_l^{**} \right) = \begin{cases} 1, & \text{si } p_i \neq p_l^{**} \\ p_i, & \text{si } p_i = p_l^{**} \end{cases} ;$$

de lo contrario, $\left\{ p_k^{*} \right\}_{k=1}^{s'}$, $\left\{ p_l^{**} \right\}_{l=1}^{r'}$ y $\left\{ p_i \right\}_{i=1}^{m}$ no serían sucesiones de enteros primos,

al tener un elemento con más de dos divisores (Definición 1.2.8). Así que $p_i \mid p_k^*$ ó $p_i \mid p_l^{**}$ para algún $k = 1, 2, \ldots, s'$ ó $l = 1, 2, \ldots, r'$ (Definición 1.2.5, Teorema 2.2.5). Ahora bien, supóngase para cualquier $i = 1, 2, \ldots, m$ que $p_i \neq p_k^*$ y $p_i \neq p_l^{**}$, con $k = 1, 2, \ldots, s'$ y $l = 1, 2, \ldots, r'$ entonces es imposible que $p_i \mid p_k^*$ ó $p_i \mid p_l^{**}$ (Definición 1.2.6 y Definición 1.2.8), lo cual contradice lo obtenido anteriormente. Por tanto, por cada $i = 1, 2, \ldots, m$, $p_i = p_k^*$ ó $p_i = p_l^{**}$ para algún k=1,2,…, s' ó l=1,2,…, r'. El mismo razonamiento se aplica, si se considera que existe otra *descomposición* de *a* en *factores primos* distinta a $\{ p_i \}_{i=1}^m$. Luego, $\{ p_i \}_{i=1}^m$ es una sucesión única de enteros primos. Esto es, *a* se descompone en una única factorización de enteros primos. •

Observación. (Fraleigh, 1987). Si *n* es primo, hágase todas las combinaciones posibles de algún *a* con cualquier *b*, *c* en $\mathbb{Z}_n - \{0\}$, obteniéndose $ba = ab \neq 0$ (*mod*. *n*) por lo que $\mathbb{Z}_n$ es un *anillo entero finito* (Teorema 2.2.3 y Teorema 2.2.6). Luego, para $b \neq c$ implica $ab \neq ac$ (*mod*. *n*) en $\mathbb{Z}_n - \{0\}$ y a su vez existe a^{-1} en $\mathbb{Z}_n - \{0\}$, tal que $a^{-1}a = aa^{-1} = 1$ (Teorema 1.1.8, clausura de ρ y $\left| \mathbb{Z}_n - \{0\} \right| = n - 1$), por lo que $\mathbb{Z}_n$ es un *campo*. Así, $\mathbb{Z}_p$ dotado de la multiplicación y la suma usuales en los números enteros y considerándose la relación de congruencia (*mod*. *p)*, es un *campo finito sii p* es primo.

2.3. EL GRUPO ABELIANO ($\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_n}$, σ)

Definición 2.3.1. (Fraleigh, 1987). El *producto cartesiano* $A_1 \times A_2 \times \ldots \times A_n$ de los conjuntos $A_1, A_2, \ldots, A_n$, es el conjunto de todas *n-adas ordenadas* y/o *vectores* $(a_1, a_2, \ldots, a_n)$, donde las *componentes* $a_i \in A_i$ para cada $i = 1, 2, \ldots, n$.

Observación. El producto cartesiano de un mismo conjunto *A* consigo mismo *k* veces se denota por A^k. Así, el *producto directo* de los grupos $\mathbb{Z}_n$ y $\mathbb{Z}_m$ es el grupo $(\mathbb{Z}_n \times \mathbb{Z}_m, \sigma)$, tal que $(z_1, z_2)\sigma(z_3, z_4) = (z_1 + z_3, z_2 + z_4)$ para (z_1, z_2), (z_3, z_4) en $\mathbb{Z}_n \times \mathbb{Z}_m$ y $1 < n, m$ (considérese para σ a (0,0) como el neutro, para cada (z_1, z_2) se tiene como opuesto $(n - z_1, m - z_2)$ y aplíquese los Teorema 1.1.3, Teorema 1.2.4 y Teorema 2.2.3),

donde se asume la operación suma módulo n y módulo m, respectivamente en cada componente, lo cual se puede extender al producto directo finito de grupos o a $\mathbb{Z}_n^k$ (asúmase *el principio de inducción*).

Definición 2.3.2. (Fraleigh, 1987). Un *isomorfismo* entre un grupo (G, σ) y otro grupo (H, λ) es una función biyectiva $\mu: G \rightarrow H$, tal que: $\mu(x \sigma y) = \mu(x) \lambda \mu(y)$ para todo $x, y \in G$ y se escribe $G \simeq H$

Teorema 2.3.1. (Castro *et al*, 2015). $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ \ldots \ x \mathbb{Z}_{m_n}, \sigma)$ es un grupo conmutativo, con $2 < n$,

$$\sigma: (\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n})^2 \rightarrow \mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ \ldots \ x \mathbb{Z}_{m_n},$$

tal que $(x_1, x_2, \ldots, x_n)\ \sigma\ (y_1, y_2, \ldots, y_n) = (z_1, z_2, \ldots, z_n)$, con $x_i, y_i \in \mathbb{Z}_{m_i}$, para todo $i = 1, 2, \ldots, n$, donde $z_i = x_i + y_i + r_i\ (mod.\ m_i)$ y

$$r_i = \begin{cases} 0, \text{ si } x_{i+1} + y_{i+1} + r_{i+1} < m_{i+1} \text{ ó } i = n \\ 1, \text{ si } m_{i+1} \leq x_{i+1} + y_{i+1} + r_{i+1} \end{cases}$$

Demostración. $\sigma: (\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n})^2 \rightarrow \mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}$ es un operador, ya que es una función ramificada con la congruencia módulo $m_i \in \mathbb{Z}^+$, con $i = 1, 2, \ldots, n$, cuyas condiciones dependen del operador suma y el orden en $\mathbb{Z}$, nótese la definición en el enunciado del teorema (Definición 1.1.9, Definición 1.2.1 y Definición 2.2.1). Así, $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma)$ también hereda la propiedad conmutativa de la congruencia módulo $m_i \in \mathbb{Z}^+$, con $i = 1, 2, \ldots, n$ (Teorema 2.2.3).

De ahora en adelante, considérese el operador suma y el orden en $\mathbb{Z}$ y las operaciones en los anillos $\mathbb{Z}_{m_1}, \mathbb{Z}_{m_2}, \ldots, \mathbb{Z}_{m_n}$.

Ahora bien, considerándose $(x_1, x_2, \ldots, x_n)\ \sigma\ (0, 0, \ldots, 0) = (z_1, z_2, \ldots, z_n)$, con $x_i, 0 \in \mathbb{Z}_{m_i}$ (Teorema 2.2.3), donde $z_i = x_i + 0 + r_i\ (mod.\ m_i)$ para todo $i = 1, 2, \ldots, n$, y

$$r_i = \begin{cases} 0, \text{ si } x_{i+1} + 0 + r_{i+1} < m_{i+1} \text{ ó } i = n \\ 1, \text{ si } m_{i+1} \leq x_{i+1} + 0 + r_{i+1} \end{cases}.$$

Pero $0 \in \mathbb{Z}$ (Definición 1.1.9), $0 < 1 < m_i$ para todo $i = 1, 2, \ldots, n$, y $r_n = 0$. Esto implica $z_n = x_n$ (*mod*. m_n), de modo que $r_{n-1} = 0$ y $z_{n-1} = x_{n-1}$ (*mod*. m_{n-1}), luego $r_{n-2} = 0$ y $z_{n-2} = x_{n-2}$ (*mod*. m_{n-2}) hasta $z_1 = x_1$ (*mod*. m_1). Esto es, $r_i = 0$ y $z_i = x_i$ (*mod*. m_i) para todo $i = 1, 2, \ldots, n$ y $(x_1, x_2, \ldots, x_n)\ \sigma\ (0,0,\ldots,0) = (x_1, x_2, \ldots, x_n)$. Así, $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma)$ posee neutro $(0, 0, \ldots, 0)$.

Asimismo, para $i = 1,2, \ldots, n$, si $x_i \in \mathbb{Z}_{m_i}$ y $x_i \neq 0$ entonces en $\mathbb{Z}_{m_i}$, existe su opuesto $m_i - x_i$, tal que $x_i + m_i - x_i = 0$ (*mod*. m_i) pero, si $x_i = 0$ entonces es opuesto de sí mismo, (Teorema 2.2.3). Además, $2 < n$ (hipótesis), considérese $m_t - x_t \in \mathbb{Z}_{m_j}$ y $m_j - x_j - 1 \in \mathbb{Z}_{m_j}$ para todo $j=1, 2, \ldots, t-1$, con $t = max\{i / x_i \neq 0\}$ (*lema de Zorn*). Luego, para $(x_1, x_2, \ldots, x_{n-1}, x_n)$ en $\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}$ se tiene:

$$(x_1, x_2, \ldots, x_{n-1}, x_n) = (x_1, \ldots, x_{t-1}, x_t, \ldots, x_n) = (x_1, \ldots, x_{t-1}, x_t, 0, \ldots, 0).$$

En consecuencia,

$$(x_1,\ldots, x_{t-1}, x_t,0,\ldots,0)\ \sigma\ (m_1-x_1-1,\ldots, m_{t-1} - x_{t-1}-1, m_t - x_t, 0,\ldots,0) =$$
$$(z_1,\ldots, z_{t-1}, z_t, 0,\ldots,0),$$

donde

$$z_j = m_j - 1 + r_j\ (mod.\ m_j) \text{ y } r_j = \begin{cases} 0, \text{ si } m_{j+1} - 1 + r_{j+1} < m_{j+1} \\ 1, \text{ si } m_{j+1} \leq m_{j+1} - 1 + r_{j+1} \end{cases},$$

para todo $j = 1, 2, \ldots, t - 2$.

Considerándose la Definición 1.1.9, el Teorema 2.2.3 y que, $r_t = 0$ y en $\mathbb{Z}$, $z_t = x_t + m_t - x_t + r_t = m_t$, por lo que $r_{t-1} = 1$ y $z_{t-1} = x_{t-1} + m_{t-1} - x_{t-1} - 1 + r_{t-1} = m_{t-1}$, en consecuencia, $r_{t-2} = 1$ y asimismo, $r_j = 1$ para todo $j=1, 2, \ldots, t - 1$, ya que recurrentemente, $z_j = m_j$. Esto es, $z_j = 0$ (*mod*. m_j) para todo $j = 1, 2, \ldots, t$ ó $(z_1,\ldots, z_{t-1}, z_t,0,\ldots,0) = (0,\ldots,0,0,\ldots,0)$. Así, en $\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}$, dada la arbitrariedad de $(x_1, x_2, \ldots, x_{n-1}, x_n)$ siempre se podrá encontrar su opuesto con el procedimiento descrito anteriormente. Es decir, existe el opuesto para cada

$(x_1, x_2, \ldots, x_{n-1}, x_n)$ en $\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}$.

Finalmente, sean $(x_1, x_2,\ldots,x_n),(y_1,y_2,\ldots,y_n),(z_1,z_2,\ldots,z_n)$ en $\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}$, considérese $[(x_1, x_2,\ldots, x_n)\ \sigma\ (y_1, y_2,\ldots, y_n)]\ \sigma\ (z_1, z_2,\ldots, z_n) = (v_1, v_2,\ldots, v_n)$, donde para cada $i = 1, 2, \ldots, n$: $v_i = (x_i + y_i + r_i) + z_i + s_i = x_i + y_i + z_i + r_i + s_i\ (mod.\ m_i)$,

$$r_i = \begin{cases} 0, \text{ si } x_{i+1} + y_{i+1} + r_{i+1} < m_{i+1} \text{ ó } i = n \\ 1, \text{ si } m_{i+1} \leq x_{i+1} + y_{i+1} + r_{i+1} \end{cases}$$

y

$$s_i = \begin{cases} 0, \text{ si } (x_{i+1} + y_{i+1} + r_{i+1}) + z_{i+1} + s_{i+1} < m_{i+1} \text{ ó } i = n \\ 1, \text{ si } m_{i+1} \leq (x_{i+1} + y_{i+1} + r_{i+1}) + z_{i+1} + s_{i+1} \end{cases}.$$

También, $(x_1, x_2,\ldots, x_n)\ \sigma\ [(y_1, y_2,\ldots, y_n)\ \sigma\ (z_1, z_2,\ldots, z_n)] = (w_1, w_2,\ldots, w_n)$, donde para cada $i = 1, 2, \ldots, n$: $w_i = x_i + (y_i + z_i + t_i) + u_i = x_i + y_i + z_i + t_i + u_i\ (mod.\ m_i)$,

$$t_i = \begin{cases} 0, \text{ si } y_{i+1} + z_{i+1} + t_{i+1} < m_{i+1} \text{ ó } i = n \\ 1, \text{ si } m_{i+1} \leq y_{i+1} + z_{i+1} + t_{i+1} \end{cases}$$

y

$$u_i = \begin{cases} 0, \text{ si } x_{i+1} + (y_{i+1} + z_{i+1} + t_{i+1}) + u_{i+1} < m_{i+1} \text{ ó } i = n \\ 1, \text{ si } m_{i+1} \leq x_{i+1} + (y_{i+1} + z_{i+1} + t_{i+1}) + u_{i+1} \end{cases}.$$

Además, para cada $i = 1, 2, \ldots, n$:

$$r_i + s_i = t_i + u_i = \begin{cases} 0, \text{ si } (x_{i+1} + y_{i+1} + z_{i+1} + t_{i+1} + u_{i+1} < m_{i+1}) \text{ ó } (i = n) \\ 1, \text{ si } (m_{i+1} \leq x_{i+1} + y_{i+1}) \text{ y } (x_{i+1} + y_{i+1} + z_{i+1} + t_{i+1} + u_{i+1} < 2m_{i+1}) \\ 2, \text{ si } 2m_{i+1} \leq x_{i+1} + y_{i+1} + z_{i+1} + t_{i+1} + u_{i+1} \end{cases}$$

Nótese que en para cada $i = 1, 2,\ldots, n$, $\mathbb{Z}$, $x_i + y_i + z_i + t_i + u_i < 3m_i - 3 + 2 = 3m_i - 1$ (Teorema 1.2.4), Así, $v_i = w_i$ para todo $i = 1,2,\ldots,n$. Esto es, en $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma)$ se cumple la propiedad asociativa.

Por tanto, $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma)$ es un grupo abeliano. •

Teorema 2.3.2. (Castro, 2014). Sea $n \in \mathbb{Z}^+$, (G, μ) un grupo y $A \neq \emptyset$, tal que

$|A| = |G| = n$ entonces existe un operador α en A, tal que $(G, \mu) \simeq (A, \alpha)$.

Demostración. Sea $n \in \mathbb{Z}^+$, (G, μ) un grupo y $A \neq \emptyset$, tal que $|A| = |G| = n$; defínase dos sucesiones finitas que enumeren uno a uno a los elementos de los conjuntos G y A. Sean respectivamente, $g:\{1, 2, \ldots, n\} \rightarrow G$ y $h:\{1, 2, \ldots, n\} \rightarrow A$ dichas sucesiones, ambas son funciones biyectivas.

Considérese la función inversa h^{-1} y $f = g \circ h^{-1}$: $A \rightarrow G$ que, a su vez, son funciones biyectivas, de modo que en A se define el operador α: $A \times A \rightarrow A$, tal que, para todo $b, c \in A$, $b \alpha c = f^{-1}(f(b) \mu f(c))$.

Por definición, α es cerrado en A (Definición 1.1.2).

Sea e el neutro en (G, μ) entonces existe algún $o \in A$, $f(o) = e$, tal que para todo $b \in A$, $b \alpha o = f^{-1}(f(b) \mu f(o)) = f^{-1}(f(b) \mu e) = f^{-1}(f(b)) = f^{-1}(e \mu f(b)) = f^{-1}(f(o) \mu f(b)) = o \alpha b$ y $f^{-1}(f(b)) = b = b \alpha o = o \alpha b$.

Asimismo, si $b \in A$ entonces $f(b) = d \in G$ y existen $b' \in A$ y $f(b') = d' \in G$, de modo que $d \mu d' = e$, a su vez, $b \alpha b' = f^{-1}(f(b) \mu f(b')) = f^{-1}(e) = f^{-1}(f(b') \mu f(b)) = b' \alpha b$. Y además, $b \alpha b' = b' \alpha b = f^{-1}(e) = o$.

Por otro lado, para $b, c, d \in A$, $(b \alpha c) \alpha d = f^{-1}[f[f^{-1}(f(b) \mu f(c))] \mu f[d]] = f^{-1}[(f(b) \mu f(c)) \mu f(d)] = f^{-1}[f(b) \mu (f(c) \mu f(d))]$

y

$$b \alpha (c \alpha d) = f^{-1}[f[b] \mu f[f^{-1}(f(c) \mu f(d))] = f^{-1}[f(b) \mu (f(c) \mu f(d))].$$

Luego, $(b \alpha c) \alpha d = b \alpha (c \alpha d)$.

Así, (A, α) es un grupo (Definición 1.1.3) y $f(b \alpha c) = f(b) \mu f(a)$. Esto es, f es un homomorfismo entre A y G. Por tanto $(G, \mu) \simeq (A, \alpha)$ (Definición 2.3.2.). •

Observación. α es el operador trivial que se puede construir en un conjunto con la misma cardinalidad de un grupo finito. Así, $(\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_n}, \alpha) \simeq \mathbb{Z}_{\prod_{i=1}^{n} m_i}$.

Teorema 2.3.3. (Castro *et al*, 2015). $(\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_n}, \sigma) \simeq \mathbb{Z}_{\prod_{i=1}^{n} m_i}$.

Siempre y cuando se considere estrictamente a

$$\mathbb{Z}_{m_i} = \{ [a]_{m_i} \subset \mathbb{Z} / a \in \mathbb{Z}, 0 \leq a < m_i \} := \{0, 1, 2, \ldots, m_i - 1\},$$

para todo $i = 1, 2, \ldots, n$.

Demostración. Sea $n \in \mathbb{Z}^+$, se demostrará que el producto cartesiano $\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}$, con el operador σ, es isomorfo a $\mathbb{Z}_{\prod_{i=1}^{n} m_i}$, tal que $1 < m_1, m_2, \ldots, m_n$.

Considérese la relación f: $\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n} \rightarrow \mathbb{Z}_{\varphi_1}$, tal que

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} x_i \varphi_{i+1} \ (mod.\ \varphi_1),$$

con $x_i \in \mathbb{Z}_{m_i}$, $\varphi_i = \prod_{j=i}^{n} m_j \ \forall i = 1,2,..,n$ y $\varphi_{n+1} = 1$; f es una función biyectiva (Teorema 2.1.1.); falta demostrar que f es un homomorfismo entre $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma)$ y $\mathbb{Z}_{\varphi_1}$.

Obsérvese que

$$f((x_1, x_2, \ldots, x_n)\sigma(y_1, y_2, \ldots, y_n)) = f(z_1, z_2, \ldots, z_n) = \sum_{i=1}^{n} z_i \varphi_{i+1} \ (mod.\ \varphi_1),$$

donde $z_i = x_i + y_i + r_i \ (mod.\ m_i)$ para $i = 1, 2, \ldots, n$.

Por otro lado,

$$f(x_1, x_2, \ldots, x_n) + f(y_1, y_2, \ldots, y_n) = \sum_{i=1}^{n} x_i \varphi_{i+1} + \sum_{i=1}^{n} y_i \varphi_{i+1} \ (mod.\ \varphi_1).$$

Además, si para todo $i = 1, 2, \ldots, n$ se considera, por hipótesis que estrictamente, $\mathbb{Z}_{m_i} = \{ [a]_{m_i} \subset \mathbb{Z} \ / \ a \in \mathbb{Z}, \ 0 \leq a < m_i \} := \{0, 1, 2, \ldots, m_i - 1\}$, la Definición 1.1.9, Teorema 1.2.3, el Teorema 1.2.4 y el Teorema 1.2.7, se obtiene $x_i + y_i < x_i + y_i + r_i < 2m_i$, $x_i + y_i = \gamma_i^1 m_i + k_i^1$, $x_i + y_i + r_i = \gamma_i^1 m_i + k_i^1 + r_i$, con $0 \leq k_i^1 < m_i$, y

$$\sum_{i=1}^{n} x_i\varphi_{i+1} + \sum_{i=1}^{n} y_i\varphi_{i+1} = \sum_{i=1}^{n}\left(x_i + y_i \right)\varphi_{i+1} = \sum_{i=1}^{n}\left(\gamma_i^1 m_i + k_i^1 \right)\varphi_{i+1} = \gamma_1^1 m_1\varphi_2 + \sum_{i=1}^{n}\left(k_i^1 + \gamma_{i+1}^1 \right)\varphi_{i+1}$$

tal que

$$\gamma_i^1 = \begin{cases} 0, \text{ si } x_i + y_i < m_i \text{ ó } i = n+1 \\ 1, \text{ si } m_i \le x_i + y_i \end{cases}.$$

Analogamente, para $i = 1, 2, \ldots, n$

$$\gamma_1^1\varphi_1 + \sum_{i=1}^{n}\left(k_i^1 + \gamma_{i+1}^1 \right)\varphi_{i+1} =$$

$$\gamma_1^1\varphi_1 + \sum_{i=1}^{n}\left(\gamma_i^2 m_i + k_i^2 \right)\varphi_{i+1} = \gamma_1^1\varphi_1 + \gamma_1^2 m_1\varphi_2 + \sum_{i=1}^{n}\left(k_i^2 + \gamma_{i+1}^2 \right)\varphi_{i+1},$$

con $0 \le k_i^1, k_i^2 < m_i$, tal que $k_n^2 = k_n^1$ y

$$\gamma_i^2 = \begin{cases} 0, \text{ si } k_i^1 + \gamma_{i+1}^1 < m_i \text{ ó } i = n, n+1 \\ 1, \text{ si } m_i = k_i^1 + \gamma_{i+1}^1 \end{cases}.$$

Así, sucesivamente en consecuencia

$$\gamma_1^1\varphi_1 + \gamma_1^2\varphi_1 + \sum_{i=1}^{n}\left(k_i^2 + \gamma_{i+1}^2 \right)\varphi_{i+1} = \ldots = \sum_{j=1}^{n}\gamma_1^j\varphi_1 + \sum_{i=1}^{n}\left(k_i^n + \gamma_{i+1}^n \right)\varphi_{i+1},$$

con $0 \le k_i^j < m_i$, tal que $k_i^j = k_i^{n-i+1}$, si $n - i + 1 < j$ ó $n - j + 1 < i$ para $i, j = 1, 2, \ldots, n$, ya que

$$\gamma_i^j = \begin{cases} 0, \text{ si } k_i^{j-1} + \gamma_{i+1}^{j-1} < m_i \text{ ó } n - j + 1 < i \\ 1, \text{ si } m_i = k_i^{j-1} + \gamma_{i+1}^{j-1} \end{cases}.$$

Es decir, $0 \le k_i^n = k_i^{n-i+1} < m_i$ para $1 < i$ de modo que

$$\sum_{i=1}^{n}\left(x_i + y_i \right)\varphi_{i+1} = \sum_{j=1}^{n}\gamma_1^j\varphi_1 + \sum_{i=1}^{n}\left(k_i^{n-i+1} \right)\varphi_{i+1}.$$

De forma semejante,

$$\sum_{i=1}^{n}\left(x_i + y_i + r_i \right)\varphi_{i+1} = \sum_{j=1}^{n}\gamma_1^j\varphi_1 + \sum_{i=1}^{n}k_i^{n-i+1}\varphi_{i+1} + \sum_{i=1}^{n}r_i\varphi_{i+1}.$$

Esto es,

$$\sum_{j=1}^{n}\gamma_1^j\varphi_1+\sum_{i=1}^{n}k_i^{n-i+1}\varphi_{i+1}+\sum_{i=1}^{n}r_i\varphi_{i+1}=\sum_{j=1}^{n-1}\gamma_1^j\varphi_1+\sum_{i=1}^{n}\left(k_i^{n-i+1}\right)\varphi_{i+1}+\gamma_1^n m_1\varphi_2+\sum_{i=1}^{n-1}r_i m_{i+1}\varphi_{i+2}+r_n$$

y con $r_n = 0$ se obtiene

$$\sum_{i=1}^{n}(x_i+y_i+r_i)\varphi_{i+1}=\sum_{j=1}^{n-1}\gamma_1^j\varphi_1+\left(k_1^n+\gamma_1^n m_1\right)\varphi_2+\sum_{i=2}^{n}\left(k_i^{n-i+1}+r_{i-1}m_i\right)\varphi_{i+1}\,.$$

Luego, por la unicidad de los coeficientes de cada término de la serie finita en $\mathbb{Z}_{\varphi_1}$ (hipótesis y Teorema 2.1.1.) y considerándose el Teorema 2.2.3 y el Teorema 2.3.1, se tiene

$$\sum_{i=1}^{n}(x_i+y_i)\varphi_{i+1}=\sum_{i=1}^{n}\left(k_i^{n-i+1}\right)\varphi_{i+1}\ (mod.\ \varphi_1)=$$

$$\sum_{i=1}^{n}\left(k_i^{n-i+1}\ (mod.\, m_i)\right)\varphi_{i+1}\ (mod.\,\varphi_1)\,.$$

También, para $i = 1, 2, \ldots, n$, $z_i = x_i + y_i + r_i\ (mod.\ m_i)$ y

$$r_i=\begin{cases}0, \text{ si } x_{i+1}+y_{i+1}+r_{i+1}<m_{i+1} \text{ ó } i=n\\ 1, \text{ si } m_{i+1}\le x_{i+1}+y_{i+1}+r_{i+1}\end{cases}$$

se tiene

$$\sum_{i=1}^{n}(z_i)\varphi_{i+1}=\sum_{i=1}^{n}\left(k_i^{n-i+1}\ (mod.\, m_i)\right)\varphi_{i+1}\ (mod.\,\varphi_1)\,.$$

Por tanto, $f((x_1, x_2,\ldots, x_n)\ \sigma\ (y_1,y_2,\ldots, y_n)) = f(x_1, x_2, \ldots, x_n) + f(y_1, y_2, \ldots, y_n)$. Esto es f es un homomorfismo y $(\mathbb{Z}_{m_1}x\mathbb{Z}_{m_2}x\ldots x\mathbb{Z}_{m_n}, \alpha) \simeq \mathbb{Z}_{\prod_{i=1}^{n}m_i}$.•

Observación. De ahora en adelante, al homomorfismo f del Teorema 2.3.3 se denotará por

$$f(x_1,x_2,\ldots,x_n) := (x_1, x_2, \ldots, x_n)_{10}\in \mathbb{Z}_{\prod_{i=1}^{n}m_i}\text{, con } (x_1, x_2, \ldots, x_n)\in \mathbb{Z}_{m_1}x\mathbb{Z}_{m_2}x\ldots x\mathbb{Z}_{m_n}$$

Si en el Teorema 2.3.3 se considera a f: $(\mathbb{Z}_{m_1} x\ \mathbb{Z}_{m_2}, \sigma) \rightarrow \mathbb{Z}_{m_1 m_2}$, tal que $(x_1, x_2)_{10} = m_2 x + y\ (mod.\ m_1 m_2)$, con $x_i \in \mathbb{Z}_{m_i}$ e i=1,2, f es un homomorfismo que admite la siguiente igualdad $(0, 0)_{10} = (dk_1k_2, dk_1k_2)_{10} = 0$ $(0 \equiv dk_1k_2\ (mod.\ m_i))$ y $(m_1, m_2) = d$ (Definición 1.2.6), tal que para $i = 1, 2$ $k_i \in \mathbb{Z}^+$ y $m_i = dk_i$. Pero véase, con $1 < m_i < dk_1k_2 < m_1m_2$ se obtiene

$$dk_1k_2m_2 + dk_1k_2 = k_2m_2m_1 + dk_1k_2 = dk_1k_2 \neq 0\ (mod.\ m_1m_2).$$

En fin, la hipótesis del Teorema 2.3.3 es necesaria puesto que, en este caso, por ejemplo, se requiere que cada componente del vector evaluado sea un elemento en el conjunto $\mathbb{Z}_{m_i}$, siempre y cuando se considere estrictamente, para todo i=1,2, …, n

$$\mathbb{Z}_{m_i} = \{[a]_{m_i} \subset \mathbb{Z} / a \in \mathbb{Z}, 0 \leq a < m_i\} := \{0, 1, 2, \ldots, m_i - 1\}.$$

Esto es, en el caso propuesto (dk_1k_2, dk_1k_2) no es preimagen de dk_1k_2 en $\mathbb{Z}_{m_1m_2}$; sino que (dk_1k_2, dk_1k_2) es preimagen única de $0 \in \mathbb{Z}_{m_1m_2}$ (cuya preimagen única es el equivalente de (dk_1k_2, dk_1k_2): $(0, 0)$ en $\mathbb{Z}_{m_1} x\ \mathbb{Z}_{m_2}$). Además, la preimagen única de $dk_1k_2 \in \mathbb{Z}_{m_1m_2}$ en $\mathbb{Z}_{m_1} x\ \mathbb{Z}_{m_2}$ es $(k_1, 0)$.

Notación. De ahora en adelante, para j = 1, 2,…, n, se representará a $x^k \in \mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}$, como $x^k = \left(x_1^k, x_2^k, \ldots, x_n^k\right) := x_1^k x_2^k \ldots x_n^k$, con $n \in \mathbb{Z}^+$, $k \in \mathbb{Z}$ $\prod_{j=1}^{n} m_j$ y $x_j^k \in \mathbb{Z}_{m_j}$ y a $x_1^k x_2^k \ldots x_n^k$ se le denominará la *cadena* de k ó x^k, indistintamente y a los elementos x_j^k de la cadena k se les denominará *componentes* de dicha cadena.

Observación. En el arreglo, vector o la *cadena* $x^k \in \mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}$, cada componente para j = 1, 2, …, n y r = 1, 2, …, n + 1, se obtiene:

$$x_j^k := c_{j+1} - m_j c_j, \text{ tal que } k = c_r\varphi_r + s \text{ (Teorema 1.2.7)}$$

con

$$\varphi_r = \prod_{j=r}^{n} m_j,\ \varphi_{n+1} = 1 \text{ y } 0 \leq s < \varphi_r.$$

Además:

$$(x^k)_{10} = k = \sum_{j=1}^{n} x_j^k \varphi_{j+1} \text{ (Teorema 2.3.3 y la existencia de } f^{-1}).$$

Finalmente, gracias al Teorema de Factorización Única (Teorema 2.2.6) se deduce, que por cada compuesto *n* se pueden construir distintos isomorfismos de $\mathbb{Z}_n$ (Teorema 2.3.3).

Por ejemplo, considérese escribir todos los elementos de $(\mathbb{Z}_2^4, \sigma) \simeq \mathbb{Z}_{16}$ entonces $\varphi_r = 2^{5-r}$, x^k, con $k = 0, 1, 2, \ldots, 15$ y $m_j = 2$, $j = 1, 2, 3, 4$ y $r = 1, 2, 3, 4, 5$. Así, para la expresión $k = c_r\varphi_r + s$, con $k = 0$ se tiene:

$c_1 = 0$, ya que $\varphi_1 = 16$, luego $0 = 0\text{x}16 + 0$,

$c_2 = 0$, ya que $\varphi_2 = 8$, luego $0 = 0\text{x}8 + 0$,

$c_3 = 0$, ya que $\varphi_3 = 4$, luego $0 = 0\text{x}4 + 0$,

$c_4 = 0$, ya que $\varphi_4 = 2$, luego $0 = 0\text{x}2 + 0$,

$c_5 = 0$, ya que $\varphi_5 = 1$, luego $0 = 0\text{x}1 + 0$,

Así,

$$x_1^0 = c_2 - 2c_1 = 0,\ x_2^0 = c_3 - 2c_2 = 0,\ x_3^0 = c_4 - 2c_3 = 0,\ x_4^0 = c_5 - 2c_4 = 0,$$

por lo que

$$x^0 = (0, 0, 0, 0) = 0000.$$

Para $k = 1$

$c_1 = 0$, ya que $1 = 0\text{x}16 + 1$,

$c_2 = 0$, ya que $1 = 0\text{x}8 + 1$,

$c_3 = 0$, ya que $1 = 0\text{x}4 + 1$,

$c_4 = 0$, ya que $1 = 0\text{x}2 + 1$,

$c_5 = 1$, ya que $1 = 1\text{x}1 + 0$,

Luego,

$$x_1^1 = c_2 - 2c_1 = 0,\ x_2^1 = c_3 - 2c_2 = 0,\ x_3^1 = c_4 - 2c_3 = 0, b_4^1 = c_5 - 2c_4 = 1,$$

por lo que

$$x^1 = (0, 0, 0, 1) = 0001.$$

Luego, para $k = 2, 3, \ldots, 15$ se obtienen:

$x^2 = (0, 0, 1, 0) = 0010$, $x^3 = (0, 0, 1, 1) = 0011$, $x^4 = (0, 1, 0, 0) = 0100$,

$x^5 = (0, 1, 0, 1) = 0101$, $x^6 = (0, 1, 1, 0) = 0110$, $x^7 = (0, 1, 1, 1) = 0111$,

$x^8 = (1, 0, 0, 0) = 1000$, $x^9 = (1, 0, 0, 1) = 1001$, $x^{10} = (1, 0, 1, 0) = 1010$,

$x^{11} = (1, 0, 1, 1) = 1011$, $x^{12} = (1, 1, 0, 0) = 1100$, $x^{13} = (1, 1, 0, 1) = 1101$,

$x^{14} = (1, 1, 1, 0) = 1110$ y $x^{15} = (1, 1, 1, 1) = 1111$.

En fin, sea $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma) \simeq \mathbb{Z}_{\varphi_1}$, siempre y cuando se considere estrictamente a $\mathbb{Z}_{m_i} = \{ [a]_{m_i} \subset \mathbb{Z} / a \in \mathbb{Z}, 0 \leq a < m_i \} := \{0, 1, 2, \ldots, m_i - 1\}$ para todo $p, q = 0, 1, 2, \ldots, \varphi_1 - 1$ entonces:

$$x^p \sigma x^q = x^{p+q\,(mod.\,\varphi_1)}$$ (Teorema 2.3.1 y Teorema 2.3.2).

3. LA IDENTIDAD DE BEZOUT Y LA CONGRUENCIA MODULAR EN $\mathbb{Z}$

Los inversos de los elementos distintos de cero en el campo $\mathbb{Z}_p$, con p primo, es un caso particular de los coprimos a n en $\mathbb{Z}_n$. En este capítulo se muestra un algoritmo para encontrar los coprimos a n en $\mathbb{Z}_n$, el cual no es optimizable, en el sentido del número finito de iteraciones necesarias para hallarlos.

3.1. ALGORITMO DE EUCLIDES.

Teorema 3.1.1. (Epp, 2012). Sean $a < b$ en $\mathbb{Z}^+$. Si $b = aq + r$ con $0 \leq r < 0$ entonces $(a, b) = (a, r)$.

Demostración. Sean $a < b$ en $\mathbb{Z}^+$, por el Teorema 1.2.7, existen q, r en $\mathbb{Z}$ únicos, tal que $b = aq + r$ y $0 \leq r < a$. Así, $b + a(-q) = r$ (propiedades en el anillo $\mathbb{Z}$). Además, si $c = (a, b)$ y por el Teorema 2.2.4 se tiene que $c \mid r$ y como $c \mid a$ entonces $c \mid d$, con $d = (a, r)$. (Definición 1.2.6). En consecuencia, $c \leq d$. (Teorema 1.2.5)

Por otro lado, existen enteros x y y, tales que $ax + by = c$, por lo que

$$c = ax + by = ax + (aq + r)y = a(x + qy) + ry.$$

Por tanto, $d \mid c$ (Teorema 2.2.4). A su vez, por el Teorema 1.2.5, $d \leq c$.

Finalmente, $c \leq d$ y $d \leq c$ implica que $(a, r) = (a, b)$ (Teorema 1.2.1).•

Observación. De lo expuesto anteriormente se deduce que $(a, 0) = a$ en $\mathbb{Z}^+$. Además, al aplicar el Teorema 1.2.7, para a, b en $\mathbb{Z}^+$, en un número finitos de pasos con los valores encontrados de q y r, hasta que $r = 0$, se deduce el máximo común divisor de a y b.

Algoritmo De Euclides Para Hallar El Máximo Común Divisor De Dos Números Enteros Positivos. (Epp, 2012). Dados dos números enteros a y b, con $0 < a < b$, este algoritmo calcula (a, b).

Entrada: a, b, enteros en $\mathbb{Z}^+$, con $0 < a < b$.

Inicio de Algoritmo.

Paso 1. Háganse $D = b$ y $d = a$.

Paso 2. Encuéntrense c y r, de modo que $D = dc + r$, $0 \leq r < d$.

Paso 3. Si $r \neq 0$, háganse, primeramente, $D = d$ y luego, $d = r$. Sino ejecútese el Paso 5.

Paso 4. Repítanse los pasos, desde el Paso 2.

Paso 5. $(a, b) = d$

Fin del Algoritmo.

Salida: el Máximo Común Divisor de a, b es d.

Ilustración. A continuación, se ilustra el algoritmo de Euclides para $a = 172$ y $b = 728$.

Entrada: $a = 728$, $b=172$, enteros en $\mathbb{Z}^+$, con $0 < 172 < 728$.

Inicio de Algoritmo.

Paso 1. Se hacen $D = 728$ y $d = 172$.

Paso 2. Aplicándose el algoritmo usual de la división, se encuentran los valores $c = 4$ y $r = 40$, de modo que $728 = 172(4) + 40$, $0 \leq 40 < 172$.

Paso 3. Como $40 \neq 0$, se hace, $D = 172$ y luego, $d = 40$.

Paso 4. Repitiéndose desde el Paso 2.

Paso 2. Aplicándose el algoritmo usual de la división, se encuentran los valores $c = 4$ y $r = 12$, de modo que $172 = 40(4) + 12$, $0 \leq 12 < 40$.

Paso 3. Como $12 \neq 0$, se hace, $D = 40$ y luego, $d = 12$.

Paso 4. Repitiéndose desde el Paso 2.

Paso 2. Aplicándose el algoritmo usual de la división, se encuentran los valores $c = 3$ y $r = 4$, de modo que $40 = 12(3) + 4$, $0 \leq 4 < 12$.

Paso 3. Como $4 \neq 0$, se hace, $D = 12$ y luego, $d = 4$.

Paso 4. Repitiéndose desde el Paso 2

Paso 2. Aplicándose el algoritmo usual de la división, se encuentran los valores $c = 3$ y $r = 0$, de modo que $12 = 4(3) + 0$,

$0 \leq 0 < 4$.

Paso 3. Como 0 = 0, Se ejecuta el Paso 5.

Paso 5. (728, 172) = 4.

Fin del Algoritmo.

Salida: el Máximo Común Divisor de $a = 728$ y $b = 172$ es $d = 4$.

Observación. Cualquier identidad $ax + by = c$, con a y b dos enteros positivos, tiene solución en $\mathbb{Z}$ *sii* c es múltiplo de (a, b) (Teorema 2.2.4). Asimismo, existen u y v en en $\mathbb{Z}$, tal que $au + bv = (a, b)$ o, análogamente, $\frac{a}{(a,b)}u + \frac{b}{(a,b)}v = 1$ (operando en el campo $\mathbb{Q}$). Donde, (a, b) se haya con el algoritmo de Euclides, entonces $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$. Además, al invertir el proceso anterior, partiendo de las soluciones enteras de $\frac{a}{(a,b)}u + \frac{b}{(a,b)}v = 1$ se obtienen, nuevamente, las soluciones enteras de $ax + by = c$. Entonces un problema interesante es hallar los valores u y v en función de los enteros $\frac{a}{(a,b)}$ y $\frac{b}{(a,b)}$. Lo que conlleva a una aplicación inmediata de lo anterior, la obtención de los inversos en el campo $\mathbb{Z}_p$, con p primo.

3.2. LOS COPRIMOS DE *n* EN $\mathbb{Z}_n$.

Teorema 3.2.1. Sean $a < b$ en $\mathbb{Z}^+$. $ax + by = 1$ tiene infinitas soluciones en los enteros *sii* existe un único entero $0 \leq t \leq \frac{a}{2}$, tal que $x = \frac{(a-t)b+1}{a} \in \mathbb{Z}$ y $y = t - a$ ó $x = \frac{tb+1}{a} \in \mathbb{Z}$ y $y = -t$, son soluciones de $ax + by = 1$.

Demostración. (<=). Sean $a < b$ en $\mathbb{Z}^+$. El teorema es cierto al evaluar, en la identidad de Bezout $ax + by = 1$ y operando en el campo $\mathbb{Q}$, los valores enteros $x = \frac{(a-t)b+1}{a}$ y $y = t - a$ ó $x = \frac{tb+1}{a}$ y $y = -t$ para algún entero $0 \leq t \leq \frac{a}{2}$, y por el Teorema 2.2.4, $ax + by = 1$ tiene infinitas soluciones.

(=>). Sea $a < b$ en $\mathbb{Z}^+$, si existen $x, y \in \mathbb{Z}$, tal que $ax + by = 1$ entonces $ax = kb + 1$, con $k = -y \in \mathbb{Z}$ (Teorema 1.1.2 y Teorema 1.1.5 en el anillo $\mathbb{Z}$), luego $ax \equiv 1 \ (mod.\ b)$, así existe $0 < w < b$, de modo que $x \equiv w$ y $aw \equiv 1 \ (mod.\ b)$ (Teorema

1.2.7, Definición 1.2.5, Definición 2.2.1, Teorema 2.2.2 y Teorema 2.2.4). Análogamente, $aw = qb + 1$, para algún entero no negativo q y considerándose el opuesto de w en $\mathbb{Z}_b - \{0\}$, $b - w \in \mathbb{Z}$ (Teorema 2.2.3), se obtiene $0 < a(b - w) = ab - aw = (a - q)b - 1$, lo que implica que $0 < 1 < (a - q)b$ y $0 < a - q$ (Teorema 1.2.1, Teorema 1.2.2 y propiedades del anillo $\mathbb{Z}$). Hágase $h = a - q$, así $a = h + q$, con $0 < h < \frac{a}{2}$ y $\frac{a}{2} < q < a$ ó con $0 \leq q \leq \frac{a}{2}$ y $\frac{a}{2} \leq h \leq a$, y escójase a q, tal que $0 \leq q \leq \frac{a}{2}$, entonces $aw + bz = 1$, si $w = \frac{qb+1}{a} \in \mathbb{Z}$ y $z = -q$. Pero si $\frac{a}{2} < q < a$, escójase $0 < h < \frac{a}{2}$ y como de $a = h + q$ se obtiene $q = a - h$, entonces $aw + bz = 1$, si $w = \frac{(a-h)b+1}{a} \in \mathbb{Z}$ y $z = h - a$. Por tanto, para $t = q$ ó $t = h$, $ax + by = 1$ tiene solución $x = \frac{tb+1}{a} \in \mathbb{Z}$ y $y = -t$ ó $x = \frac{(a-t)b+1}{a} \in \mathbb{Z}$ y $y = t - a$, con $0 \leq t \leq \frac{a}{2}$.

Finalmente, si existe $s \in \mathbb{Z}$, tal que $0 \leq s \leq \frac{a}{2}$ y $au + bv = 1$, $u = \frac{sb+1}{a} \in \mathbb{Z}$ y $v = -s$ ó $u = \frac{(a-s)b+1}{a} \in \mathbb{Z}$ y $v = s - a$, entonces $ax = tb + 1$ y $au = sb + 1$ ó $ax = (a - t)b + 1$ y $au = (a - s)b + 1$ (considérese operar usándose las propiedades del anillo $\mathbb{Z}$). Así, tomándose las igualdades $ax = tb + 1$ y $au = sb + 1$ y por la Definición 2.2.1 y el Teorema 2.2.1, se tiene que $tb + 1 \equiv sb + 1 \equiv 0$ *mod*. a, es decir, $tb \equiv sb$ *mod*. a ó $(t - s)b = ka$, para algún entero k, de lo que se deduce que $a \mid (t - s)b$ (Definición 1.2.5). Luego como, a y b son coprimos ($ax + by = 1$) y por el Teorema 2.2.5, entonces $a \mid (t - s)$. Por tanto, $t \equiv s$ *mod*. a (Definición 2.2.1). En consecuencia, t, s pertenecen a la misma clase en $\mathbb{Z}_a$ (Teorema 2.2.2). También, se deduce que el representante de s y t es el mismo (en este caso son ambos), porque $0 \leq s, t \leq \frac{a}{2} < a$ (orden usual en el campo $\mathbb{R}$). Esto es, dicho representante es único para valores enteros no negativos menores a a, entonces $s = t$ (Definición 2.2.1 y Teorema 2.2.3). Además, si $s \neq t$ entonces $s, t < 0$ ó $a \leq s, t$, lo cual, contradice lo obtenido para t y lo supuesto para s.

Análogamente, tomándose las igualdades $ax = (a - t)b + 1$ y $au = (a - s)b + 1$ y por la Definición 2.2.1 y el Teorema 2.2.1, se tiene que $(a - t)b + 1 \equiv (a - s)b + 1 \equiv 0$ *mod*. a, es decir, $tb \equiv sb$ *mod*. a. Si se argumenta de forma semejante a lo expuesto

anteriormente, se obtiene nuevamente que $s = t$. Así, en ambos casos se deduce que t es único.•

Observación. Nótese, que, en el Teorema 3.2.1, los valores enteros de t están acotados (Definición 1.2.4), tal que $0 \leq t \leq \frac{a}{2}$, de modo que se garantiza una solución de $ax + by = 1$ en los enteros, con $a < b$ en $\mathbb{Z}^+$, y dichas cotas no pueden ser aminoradas (en el caso de $\frac{a}{2}$) ni acrecentadas (en el caso de cero). Por ejemplo, para $2x + 9y = 1$, $0 \leq t \leq \frac{2}{2}$. Así, después de algunas iteraciones para $t \in \mathbb{Z}$, considerándose $0 \leq t \leq 1$, se obtienen los valores enteros $t = 0$ ó $t = 1$ (Teorema 1.2.2), de modo que:

$$x = \frac{tb+1}{a} = \frac{0(9)+1}{2} \notin \mathbb{Z}^+, \text{ con t = 0 y } x = \frac{tb+1}{a} = \frac{1(9)+1}{2} = 5 \in \mathbb{Z}^+,$$

y $y = -1$, con t = 1. Por tanto, $2(5 + 9w) + 9(-1 - 2w) = 1$, para cualquier $w \in \mathbb{Z}$.

Por otro lado, para la ecuación $x + 2y = 1$, $0 \leq t \leq \frac{1}{2}$ (Teorema 1.2.2), se obtiene, únicamente, que $t = 0$, de modo que:

$$x = \frac{tb+1}{a} = \frac{0(2)+1}{1} = 1 \in \mathbb{Z}^+.$$

y $y = 0$. Por tanto, $(1 + 2w) + 2(-w) = 1$, para cualquier $w \in \mathbb{Z}$.

Algoritmo Para Hallar Las Infinitas Soluciones Enteras De $ax + by = c$ **Siempre Que** $(a, b) \mid c$. Dados dos números enteros a y b, con $0 < a < b$, este algoritmo calcula las infinitas soluciones de $ax + by = c$ siempre que $(a, b) \mid c$.

Entrada: a, b, c enteros en $\mathbb{Z}^+$, con $0 < a < b$.

Inicio de Algoritmo.

Paso 1. Hállese (a, b) a través del algoritmo de Euclides.

Paso 2. Si (a, b) no divide a c, entonces $ax + by = c$ no tiene soluciones enteras. Fin del algoritmo. Sino continúese con el Paso 3.

Paso 3. Háganse $h = \frac{a}{(a,b)}$, $k = \frac{b}{(a,b)}$, $g = \frac{h}{2}$ y $t = 0$.

Paso 4. Si $t \leq g$ y $\frac{tk+1}{h} = \left\lfloor \frac{tk+1}{h} \right\rfloor$, háganse $u = \frac{tk+1}{h}$, $v = -t$ y $t = g + 1$ ó si $t \leq g$ y $\frac{(h-t)k+1}{h} = \left\lfloor \frac{(h-t)k+1}{h} \right\rfloor$, háganse $u = \frac{(h-t)k+1}{h}$, $v = h - t$ y

$t = g + 1$. Sino, háganse $t = t + 1$.

Paso 5. Si $t \leq g$, repítanse los pasos, desde el Paso 4. Sino las soluciones son $x = \frac{cu+bw}{(a,b)}$ y $y = \frac{cv-aw}{(a,b)}$, para cualquier entero w.

Fin del Algoritmo.

Salida: La ecuación $ax + by = c$ no tiene solución en los enteros o las soluciones de $ax + by = c$ son $x = \frac{cu+bw}{(a,b)}$ y $y = \frac{cv-aw}{(a,b)}$ para cualquier entero w.

Ilustración. A continuación, se ilustra el algoritmo anterior para la ecuación $15x + 24y = 9$.

Entrada: $a = 15$, $b = 24$, $c = 9$ enteros en $\mathbb{Z}^+$, con $0 < 15 < 24$.

Inicio de Algoritmo.

Paso 1. Aplicándose el algoritmo de Euclides, se obtiene $(15, 24) = 3$.

Paso 2. Como $(15, 24) = 3$ divide a $c = 9$, se continúa con el Paso 3.

Paso 3. Se hacen $h = \frac{a}{(a,b)} = \frac{15}{3} = 5$, $k = \frac{b}{(a,b)} = \frac{24}{3} = 8$, $g = \frac{5}{2}$ y $t = 0$.

Paso 4. Como $t = 0 \leq \frac{5}{2}$ y $\frac{tk+1}{h} = \frac{0(8)+1}{5} = \frac{1}{5} \neq 0 = \left\lfloor \frac{1}{5} \right\rfloor = \left\lfloor \frac{tk+1}{h} \right\rfloor$ y como $t = 0 \leq \frac{5}{2}$ y $\frac{(h-t)k+1}{h} = \frac{(5-0)8+1}{5} = \frac{41}{5} \neq 8 = \left\lfloor \frac{41}{5} \right\rfloor = \left\lfloor \frac{(h-t)k+1}{h} \right\rfloor$ se hace $t = 0 + 1 = 1$.

Paso 5. Como $t = 1 \leq \frac{5}{2}$, se repiten los pasos, desde el Paso 4.

Paso 4. Como $t = 1 \leq \frac{5}{2}$ y $\frac{tk+1}{h} = \frac{1(8)+1}{5} = \frac{9}{5} \neq 1 = \left\lfloor \frac{9}{5} \right\rfloor = \left\lfloor \frac{tk+1}{h} \right\rfloor$ y como $t = 1 \leq \frac{5}{2}$ y $\frac{(h-t)k+1}{h} = \frac{(5-1)8+1}{5} = \frac{33}{5} \neq 6 = \left\lfloor \frac{33}{5} \right\rfloor = \left\lfloor \frac{(h-t)k+1}{h} \right\rfloor$

se hace $t = 1 + 1 = 2$.

Paso 5. Como $t = 2 \leq \frac{5}{2}$, se repiten los pasos, desde el Paso 4.

Paso 4. Como $t = 2 \leq \frac{5}{2}$ y $\frac{tk+1}{h} = \frac{2(8)+1}{5} = \frac{17}{5} \neq 1 = \left\lfloor \frac{2(8)+1}{5} \right\rfloor = \left\lfloor \frac{tk+1}{h} \right\rfloor$

pero, como $t = 2 \leq \frac{5}{2}$ y

$$\frac{(h-t)k+1}{h} = \frac{(5-2)8+1}{5} = \frac{25}{5} = 5 = \left\lfloor\frac{25}{5}\right\rfloor = \left\lfloor\frac{(h-t)k+1}{h}\right\rfloor$$

se hace, $u = 5$, $v = t - h = 2 - 5 = -3$ y $t = g + 1 = \frac{5}{2} + 1 = \frac{7}{2}$.

Paso 5. Paso 5. Como $\frac{5}{2} < \frac{7}{2} = t$, las soluciones son

$x = \frac{cu+bw}{(a,b)} = \frac{9(5)+24w}{3} = 15 + 8w$ y $y = \frac{cv-aw}{(a,b)} = \frac{9(-3)-15w}{3} = -9 - 5w$

para cualquier entero w.

Fin del Algoritmo.

Salida: Las soluciones de $15x + 24y = 9$ son $x = 15 + 8w$ y $y = -9 - 5w$ para cualquier entero w.

Observación. Una ecuación de la forma $ax + ny = 1$, con $0 < a < n$ y soluciones enteras, es equivalente a la expresión $ax = n(-y) + 1$ ó $ax \equiv 1\ mod.\ n$ (Definición 2.2.1). Esto es, $ax \equiv 1$ es una ecuación en $\mathbb{Z}_n$, donde los valores a y x son coprimos de n. Además, si n es primo, y se aplica el algoritmo para hallar las soluciones enteras de la identidad de Bezout resultante, se obtendrán los inversos por cada entero conocido, $0 < a$, en el campo $\mathbb{Z}_n$.

CONCLUSIONES

Se mostró, independientemente, del Algoritmo de Euclides, el Teorema 1.2.7, usándose el Lema de Zorn y el orden usual en $\mathbb{Z}$. Asimismo, también se mostró la generalización de la escritura única de un entero como la suma de productos de elementos de una sucesión en $\mathbb{Z}^+ - \{1\}$ no necesariamente geométrica (base generalizada, véase el Teorema 2.1.1); lo cual fue necesario para exhibir una nueva operación en el producto cartesiano entre conjuntos de clases de equivalencia de $\mathbb{Z}$ (dada la partición generada por la relación de equivalencia congruencia módulo en $\mathbb{Z}$, véase el Teorema 2.3.1), obteniéndose, así el isomorfismo del Teorema 2.3.3. También, se exhibió que todo conjunto finito, tiene un operador implícito que lo transforma en grupo, ya que permite establecer un isomorfismo con $\mathbb{Z}_n$ (Teorema 2.3.2).

Como $\mathbb{Z}_n$ es un anillo admite una segunda operación, sólo que los coprimos a n, satisfacen la operación binaria cuya imagen es la identidad y como en el caso particular de $ax + by = 1$ (véase el Teorema 3.2.1), se demostró que el conjunto donde se encuentran las soluciones enteras, es más sencillo de encontrar que el conjunto que se describe en el Teorema 2.2.4 y en el método que también se describe, generalmente, en la literatura. En consecuencia, esto ayudó a encontrar los elementos que satisfacen las correspondencias del segundo operador con la identidad. Más aún, cuando n es primo se hallaron los inversos de los elementos distintos de cero, con respecto a la segunda operación del campo $\mathbb{Z}_n$, como se vio con el Algoritmo Para Hallar Las Infinitas Soluciones Enteras De $ax + by = c$, el Algoritmo de Euclides y el Teorema 3.2.1. Además, se demostró que el Algoritmo Para Hallar Las Infinitas Soluciones Enteras De $ax + by = c$, no es optimizable, en el sentido del número finito de iteraciones necesarias para hallar dichas soluciones.

RECOMENDACIONES

Estudiar el grupo $(\mathbb{Z}_{m_1} x \mathbb{Z}_{m_2} x \ldots x \mathbb{Z}_{m_n}, \sigma) \simeq \mathbb{Z}_{\prod_{i=1}^{n} m_i}$, con $n \in \mathbb{Z}^+$ para revisar las propiedades ganadas en dicho isomorfismo.

Programar el Algoritmo Para Hallar Las Infinitas Soluciones Enteras De $ax + by = c$.

BIBLIOGRAFÍA

Castro, O. 2014. *Funciones Booleanas con Buenas Propiedades Criptográficas*. (Tesis de Maestría). Universidad de Oriente.

Castro O., Villarroel F. y Brito Q. 2015. No Linealidad Distinta de Cero en Funciones Booleanas Balanceadas. *Saber, 27*: n° 4.

Cilleruelo J., Kiss S., Ruzsa I. y Vinuesa C. 2010. Generalization of a theorem of Erdos and Renyi on Sidon sets. *Random Structures and Algorithms, 37*: nº4.

Epp, S. 2012. *Matemáticas Discretas con Aplicaciones.* 4ta Edición. Cengage Learning. Mexico.

Flores, R. 1971. *Fundamentos de los Sistemas Numéricos.* Editorial Interamericana, S. A. México.

Fraleigh, J. 1987. *Álgebra Abstracta*. Addison-Wesley Iberoamericana S. A. Wilmington. Delaware.

Herstein, I. 2008. *Álgebra Moderna*. Trillas. México.

Lipschutz, S. 1975. *Teoría de Conjuntos y Temas Afines*. McGraw-Hill Inc. México.

Rivero F. 1996. *Algebra*. Talleres Gráficos Universitarios. ULA. Mérida. Venezuela.

Stark, H. 1984. *An Itroduction to Number Theory*. MIT Press. Massachusetts.

HOJA DE METADATOS

Hoja de Metadatos para Tesis y Trabajos de Ascenso – 1/6

Título	ALGUNAS APLICACIONES DE LA CONGRUENCIA MODULAR EN LOS NÚMEROS ENTEROS
Subtítulo	

Autor(es)

Apellidos y Nombres	**Código CVLAC / e-mail**	
CASTRO PÉREZ, OSCAR ENRIQUE	CVLAC	V-15.202.965
	e-mail	ocastro@udo.edu.ve
	e-mail	oecpmat@yahoo.com.mx

Palabras o frases claves:

Anillo de los Números Enteros, Bases Generalizadas, Identidad de Bezout, Coprimos.

Hoja de Metadatos para Tesis y Trabajos de Ascenso – 2/6

Líneas y sublíneas de investigación:

Área	Subárea
Ciencias	Matemáticas
	Matemáticas Discretas
	Teoría de Números

Resumen (Abstract):

Se demuestra la relación entre la identidad de Bezout y los coprimos de un número natural dado. También, se construye un algoritmo que determina como son las soluciones, en Z, de la identidad de Bezout $ax + by = 1$. Además, se deducen las soluciones en Z, de $kx + my = n$, siempre que n sea múltiplo del máximo común divisor de los enteros positivos y distintos k y m. Lo que muestra la generalización de los resultados y que el algoritmo para encontrar los coprimos a n en Z_n, no es optimizable, en el sentido del número finito de iteraciones necesarias para hallarlos.

Hoja de Metadatos para Tesis y Trabajos de Ascenso – 3/6

Contribuidores:

Apellidos y Nombres	ROL / Código CVLAC / e-mail	
	ROL	CA ☐ AS ☐ TU ☐ JU ☐
	CVLAC	
	e-mail	
	e-mail	
	ROL	CA ☐ AS ☐ TU ☐ JU ☐
	CVLAC	
	e-mail	
	e-mail	
	ROL	CA ☐ AS ☐ TU ☐ JU ☐
	CVLAC	
	e-mail	
	e-mail	

Fecha de discusión y aprobación:

Año	Mes	Día

Lenguaje: ESPAÑOL

Hoja de Metadatos para Tesis y Trabajos de Ascenso – 4/6

Archivo(s):

Nombre de archivo	Tipo MIME
TA_OCP.pdf	application/pdf.

Alcance:

Espacial: Nacional (Opcional)

Temporal: Intemporal (Opcional)

Título o Grado asociado con el trabajo:

No Aplica

Nivel Asociado con el Trabajo:

Profesor Asistente

Área de Estudio:

Teoría de Números

Institución(es) que garantiza(n) el Título o grado:

Universidad de Oriente

Hoja de Metadatos para Tesis y Trabajos de Ascenso – 5/6

UNIVERSIDAD DE ORIENTE
CONSEJO UNIVERSITARIO
RECTORADO

CU Nº 0975

Cumaná, 04 AGO 2009

Ciudadano
Prof. JESÚS MARTÍNEZ YÉPEZ
Vicerrector Académico
Universidad de Oriente
Su Despacho

Estimado Profesor Martínez:

Cumplo en notificarle que el Consejo Universitario, en Reunión Ordinaria celebrada en Centro de Convenciones de Cantaura, los días 28 y 29 de julio de 2009, conoció el punto de agenda ***"SOLICITUD DE AUTORIZACIÓN PARA PUBLICAR TODA LA PRODUCCIÓN INTELECTUAL DE LA UNIVERSIDAD DE ORIENTE EN EL REPOSITORIO INSTITUCIONAL DE LA UDO, SEGÚN VRAC Nº 696/2009".***

Leído el oficio SIBI – 139/2009 de fecha 09-07-2009, suscrita por el Dr. Abul K. Bashirullah, Director de Bibliotecas, este Cuerpo Colegiado decidió, por unanimidad, autorizar la publicación de toda la producción intelectual de la Universidad de Oriente en el Repositorio en cuestión.

Comunicación que hago a usted a los fines consiguientes.

UNIVERSIDAD DE ORIENTE
SISTEMA DE BIBLIOTECA
RECIBIDO POR
FECHA 5/8/09 HORA 5:30

Cordialmente,

JUAN A. BOLAÑOS CURIEL
Secretario

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD DE ORIENTE
SECRETARÍA
CONSEJO UNIVERSITARIO

C.C: *Rectora, Vicerrectora Administrativa, Decanos de los Núcleos, Coordinador General de Administración, Director de Personal, Dirección de Finanzas, Dirección de Presupuesto, Contraloría Interna, Consultoría Jurídica, Director de Bibliotecas, Dirección de Publicaciones, Dirección de Computación, Coordinación de Teleinformática, Coordinación General de Postgrado.*

JABC/YGC/maruja

Hoja de Metadatos para Tesis y Trabajos de Ascenso – 6/6

Articulo 41 del REGLAMENTO DE TRABAJO DE PREGRADO (vigente a partir del II Semestre 2009, según comunicación CU-034-2009): "Los trabajos de grados son de la exclusiva propiedad de la Universidad de Oriente, y solo podrá ser utilizados para otros fines con el consentimiento del Concejo de Núcleo respectivo, quien deberá participarlo previamente al Concejo Universitario, para su autorización".

OSCAR CASTRO
C.I. 15.202.965