Un conjunto de numeros, presentan ley de composición interna cuando realizando una operación entre dos números de ese conjunto se obtiene otro número de ese conjunto.

En los enteros dado un par ordenado de números enteros (ZxZ), con la suma y la multiplicación se obtiene un numero entero.

La operación “+” satisface:

*Esto caracteriza a (Z,+) como grupo abeliano.*

*La operación “.” Satisface:*

La suma y la multiplicación están relacionadas por el axioma de la propiedad distributiva:

Los axiomas mencionados califican a (Z, . , +) como anillo conmutativo con identidad.

Se dice que en el anillo de los enteros, no tiene divisores propios de 0 ya que no se cumple la existencia de elemento opuesto para la operación . .

Si a, b ∈ Z y b ≠ 0 decimos que b divide al entero a y lo simbolizamos b|a, si existe un entero n tal que a = b n. También podemos decir que b es un divisor de a, que a es un múltiplo de b, que b es un factor de a, o que a es divisible por b. Si a = 0 y b ≠ 0 decimos que b divide al entero 0 y lo simbolizamos b|0, porque existe un entero n = 0 tal que 0 = b 0. Luego, en Z, todo entero no nulo es un divisor del 0. Con la notación b a, que leemos b no divide al entero a, denotamos la negación de b|a.

Z no tiene divisores propios de cero. Z se denomina un dominio entero porque no tiene divisores propios del 0.

TEOREMA 3.1 Para a, b, c ∈ Z se verifican:

i) 1|a; a|0 y a|a, si a ≠ 0.

ii) Si a|b ∧ b|a entonces a = ± b, donde a ≠ 0 y b ≠ 0.

iii) Si a|b ∧ b|c entonces a|c, si a ≠ 0 y b ≠ 0.

iv) Si a|b entonces a|b c, si a ≠ 0.

v) Sean x, y, z enteros y a ≠ 0. Si z = x + y y a divide a dos de los enteros x, y, z, entonces divide al restante.

Esto significa que si a divide a dos enteros, entonces divide tanto a la suma como a la diferencia de dichos enteros.

vi) ∀ x, y ∈ Z si a ≠ 0 , a|b ∧ a|c entonces a|(x b + y c), es decir a divide a toda combinación lineal entera (con coeficientes enteros) de b y c.

Propiedad 3.2 Si n ∈ Z + y n es un número compuesto, entonces existe un número primo p tal que p|n. Es decir, todo número compuesto admite al menos un divisor que es un número primo.

Propiedad 3.3 Para verificar que un entero dado n > 1 es primo, basta con comprobar que ningún primo p tal que p ≤ n lo divide.

TEOREMA 3.2: Un legado de Euclides. Existen infinitos números primos.

TEOREMA 3.3: El algoritmo de la división. Si a, b ∈ Z con b > 0 entonces existen q, r ∈ Z, únicos, tales que a = b q + r con 0 ≤ r < b. Decimos que a es el dividendo, b es el divisor, q es el cociente y r es el resto de la división de a por b.

TEOREMA 3.4: El algoritmo de la división generalizado en Z. Sean a, b ∈ Z, b ≠ 0. Existen y son únicos, los enteros q, r tales que a = b q + r, con 0 ≤ r <|b|.

Definición 3.5 Sean a, b ∈ Z. Un entero positivo c es un divisor común de a y de b si c divide a ambos, es decir, si c|a y c|b

Definición 3.6 Sean a, b ∈ Z no ambos nulos; d ∈ Z + es el máximo común divisor de a y b si: i) d|a y d|b. ii) Para todo entero c tal que c|a y c|b entonces c|d. Indicamos al máximo común divisor d de a y b como d = mcd(a, b). Definimos el mcd(0, 0) = 0.

Propiedad 3.5 Sean a, b ∈ Z no ambos nulos. Se verifican:

1. mcd(a, b) = mcd(b, a)
2. mcd(a, b) = mcd(−a, b)
3. iii) mcd(a, b) = mcd(|a|, |b|)
4. mcd(a, 0) = |a|
5. ∀ k ∈ Z mcd(a, ka) = |a|
6. mcd(a, b) = mcd(b, r) siendo r el resto de dividir a por b, es decir, a = q b +r con 0 ≤ r

TEOREMA 3.5 Si a, b son enteros no ambos nulos, entonces su máximo común divisor d existe, es único y además existen enteros m0 , n0 tales que d = m0 a + n0 b.

Corolario 3.6 Para a y b ∈ Z y para n ∈ Z + U {0}, se verifica que: mcd(a n, b n) = n mcd(a, b).

Corolario 3.7 Para todo a, b, n enteros positivos, si n|a b y mcd(a, n) = 1, entonces n|b.

Propiedad 3.8 Para a, b enteros no nulos y d = mcd(a, b), se verifica que mcd(a/d, b/d) = 1.

TEOREMA 3.6: Algoritmo de Euclides

Definición 3.7 Una ecuación, en una o más variables, con la restricción de que sus soluciones sean números enteros se denomina ecuación diofántica.

La ecuación diofántica más simple es la ecuación diofántica lineal en dos variables a x + b y = c, donde a, b y c son enteros dados, con a y b no ambos nulos. Veamos bajo qué hipótesis, estas ecuaciones tienen soluciones enteras.

TEOREMA 3.7 Sean a, b, c enteros. La ecuación diofántica a x + b y = c tiene una solución entera x = x0 , y = y0 si y sólo si el mcd(a, b) divide a c.

Definición 3.8 Sean a, b ∈ Z no ambos nulos; c ∈ Z + es el mínimo común múltiplo de a y b si:

i) a|c y b|c,

ii) Para todo entero d tal que a|d y b|d entonces c|d.

Se indica c = mcm(a, b). Definimos el mcm(0, 0) = 0.

Propiedad 3.9 Sean a, b, c ∈ Z. Si a|c y b|c entonces mcm(a,b)|c

TEOREMA 3.8 Para a, b ∈ Z + se verifica que mcm(a, b) mcd(a, b) = a b

Propiedad 3.10 Si b y c son coprimos con a, entonces b c es coprimo con a.

Propiedad 3.11 Sean a y b coprimos y c un entero tal que c|a y c|b, entonces c = 1 o c = −1.

Propiedad 3.12 Sea p ∈ Z + . Si a, b ∈ Z, p es primo y p divide al producto ab entonces divide a uno de ellos. En símbolos, si p es primo y p|a b, entonces p|a o p|b.

TEOREMA 3.10: Teorema fundamental de la aritmética. Si n es un entero mayor que 1, entonces n es primo o puede escribirse de manera única en la forma n = p1 a 1 p2 a 2 ... pk a k donde p1 < p2 < ... < pk son números primos y los exponentes a1 , a2 , ..., ak son enteros positivos.