Capítulo 2

Números Enteros

Notemos que las ecuaciones del tipo $a + x = b$, con $a, b \in \mathbb{N}$, pueden tener solución vacía en el conjunto de los numeros naturales. Para que este tipo de ecuación siempre tenga solución no vacía, es necesario construir un conjunto $\mathbb{Z}$ llamado de los números enteros.

Definición 7 *Sean $x, y, z \in \mathbb{N}$.*

Se dice que la diferencia o resta entre x e y es z si y sólo si x es igual a $y + z$, es decir,

$$x - y = z \text{ si y sólo si } x = y + z$$

Observación: El símbolo "$x - y$"se lee x menos y.

Propiedad 38 *Sean $x, y, z \in \mathbb{N}$.*

1. *Si $x - y = p,\ p \in \mathbb{N}$ entonces se tiene*
$$(x - y)z = xz - yz.$$
2. *Si $x - y = p,\ p \in \mathbb{N}$ entonces se tiene*
$$(x - y) + z = (x + z) - y.$$

Demostración:

1. Sea $x - y = p,\ p \in \mathbb{N}$, luego tenemos que $x = y + p$ de este modo
$$xz = (y + p)z = yz + pz$$
y por lo tanto
$$xz - yz = pz = (x - y)z.$$
2. Sean $x - y = p,\ p \in \mathbb{N}$
Luego tenemos que
$$x = y + p$$
de donde
$$x + z = y + p + z$$
Por lo tanto
$$(x + z) - y = p + z = (x - y) + z$$

□

Definición 8 *En el conjunto* $\mathbb{N} \times \mathbb{N}$ *se define la siguiente relación*[1]*:*

Sean $a, b, c, d \in \mathbb{N}$*, entonces diremos que los pares ordenados* (a, b) *y* (c, d) *están relacionados, lo que denotaremos por*

$$(a, b) \sim (c, d) \quad \textit{si y sólo si } a + d = b + c.$$

Teorema 39 *La relación* $\sim$ *es una relación de equivalencia en* $\mathbb{N} \times \mathbb{N}$*.*

Demostración: Sean $a, b, c, d, e, f \in \mathbb{N}$

Refleja: Como $a + b = b + a$ se tiene que $(a, b) \sim (b, a)$
Simétrica: Supongamos $(a, b) \sim (c, d)$, luego tenemos que

$$\begin{array}{rrcl} & a+d & = & b+c \\ \Rightarrow & b+c & = & a+d \\ \Rightarrow & c+b & = & d+a \\ \Rightarrow & (c,d) & \sim & (a,b) \end{array}$$

Transitiva: Supongamos $(a, b) \sim (c, d) \wedge (c, d) \sim (e, f)$, d lo cual se obtiene que

$$\begin{array}{rccccl} & (a+d=b+c) & \wedge & (c+f=d+e) & & \\ \Rightarrow & a+d+f=b+c+f & \wedge & c+f=d+e & & \text{Reemplazando} \\ \Rightarrow & a+f+d & = & b+d+e & & \text{Cancelado} \\ \Rightarrow & a+f & = & b+e & & \\ \Rightarrow & (a,b) & \sim & (e,f) & & \end{array}$$

□

Definición 9 *Sean* $(a, b) \in \mathbb{N} \times \mathbb{N}$*.*

Se define la clase de equivalencia de (a, b) *como el conjunto de todos los pares ordenados de* $\mathbb{N} \times \mathbb{N}$ *que están relacionados con el par ordenado* (a, b)*, y la denotaremos por* $\overline{(a, b)}$*. El par* (a, b) *se llama representante de la clase de equivalencia de* (a, b)*.*

$$\overline{(a, b)} = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid (x, y) \sim (a, b)\}.$$

Ejemplo 14

$$\begin{array}{rcl} \overline{(1,0)} & = & \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid (x,y) \sim (1,0)\} \\ & = & \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid x+0 = y+1\} \\ & = & \{(1,0),(2,1),(3,2),\ldots\}. \end{array}$$

Definición 10 *El conjunto formado por todas las clases de equivalencia definidas sobre el conjunto* $\mathbb{N} \times \mathbb{N}$*, es llamado conjunto de los números enteros y a cada clase de equivalencia número entero.*

El conjunto de los números enteros se anota

$$\mathbb{Z} = \{\overline{(a, b)} \mid a, b \in \mathbb{N}\}.$$

[1]Para más detalles ver el capítulo de **Relaciones** del curso de Matemáticas Generales.

Sistema de Representante

Por teorema (23) tenemos que, dado $a, b \in \mathbb{N}$ se tiene que $a \geq b \ \veebar \ a < b$.
Luego $(a, b) \in \overline{(a-b, 0)}$, cuando $a \geq b$ y en el otro caso tenemos que $(a, b) \in \overline{(0, b-a)}$.
Es decir,

$$\overline{(a,b)} = \begin{cases} \overline{(a-b,0)} & \text{si} \quad a \geq b \\ \\ \overline{(0,b-a)} & \text{si} \quad a < b \end{cases}$$

Además se tiene que

$$\begin{array}{rcl} \overline{(n,0)} = \overline{(m,0)} & \Rightarrow & n = m \\ \overline{(0,n)} = \overline{(0,m)} & \Rightarrow & n = m \\ \overline{(n,0)} = \overline{(0,m)} & \Rightarrow & n = m = 0 \end{array}$$

Así tenemos que cada elemento $\overline{(a,b)} \in \mathbb{Z}$ admite una único elemento de las siguientes formas

$$\overline{(n,0)} \quad \vee \quad \overline{(0,m)}$$

donde $n \in \mathbb{N}, m \in \mathbb{N}^*$.

De este modo tenemos que

$$\{\overline{(n,0)}, \overline{(0,m)} \mid n \in \mathbb{N}, m \in \mathbb{N}^*\}$$

es un sistema de representante

2.1. Suma y Producto en $\mathbb{Z}$

Teorema 40 *Sean $(a,b),(c,d),(e,f),(g,h) \in \mathbb{N} \times \mathbb{N}$ tales que $(a,b) \sim (c,d)$ y $(e,f) \sim (g,h)$ entonces tenemos*

$$\begin{array}{rcl} (a+e \ , \ b+f) & \sim & (c+g \ , \ d+h) \\ (a \cdot e + b \cdot f \ , \ a \cdot f + b \cdot e) & \sim & (c \cdot g + d \cdot h \ , \ c \cdot h + d \cdot g) \end{array}$$

Demostración:

1. **Suma**

   Supongamos $(a,b) \sim (c,d)$ y $(e,f) \sim (g,h)$ entonces

$$\begin{array}{rcccc} & a+d = b+c & \wedge & e+h = f+g \\ \Rightarrow & (a+d)+(e+h) & = & (b+c)+(f+g) \\ \Rightarrow & (a+e)+(d+h) & = & (b+f)+(c+g) \\ \Rightarrow & (a+e, b+f) & \sim & (c+g, d+h) \\ \Rightarrow & \overline{(a+e, b+f)} & = & \overline{(c+g, d+h)}. \end{array}$$

2. Producto

   Supongamos $(a,b) \sim (c,d)$ y $(e,f) \sim (g,h)$ entonces

   $$(1) \quad a+d = b+c \ \wedge \ (2) \quad e+h = f+g$$

   La primera ecuación amplificamos por e, f, y la segunda ecuación por c, d

   $$\begin{array}{rcl} ae+de & = & be+ce \\ bf+cf & = & af+df \\ ce+ch & = & cf+cg \\ df+dg & = & de+dh \end{array}$$

   Sumando las ecuaciones resultantes obtenemos

   $$ae+\underline{de}+bf+\underline{cf}+\underline{ce}+ch+\underline{df}+dg = be+\underline{ce}+af+\underline{df}+\underline{cf}+cg+\underline{de}+dh$$

   Cancelando se tiene

   $$(ae+bf)+(ch+dg) = (be+af)+(cg+dh)$$

   de lo cual tenemos

   $$(a\cdot e+b\cdot f \ , \ a\cdot f+b\cdot e) \sim (c\cdot g+d\cdot h \ , \ c\cdot h+d\cdot g)$$

□

Observación: El teorema anterior nos permite definir la suma y el producto en $\mathbb{Z}$ del siguiente modo:

Definición 11 *Sean $\overline{(a,b)}$ y $\overline{(c,d)} \in \mathbb{Z}$, se definen*

1. **Suma**
   $$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}.$$
2. **Producto**
   $$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)}.$$

Teorema 41 *El conjunto de los números enteros con la suma y el producto definido tiene la estructura de un anillo conmutativo. De otro modo $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo, es decir*

1. *Propiedades de la suma en $\mathbb{Z}$*

   i) Asociatividad
   $$(\forall x,y,z \in \mathbb{Z})((x+y)+z = x+(y+z)).$$

   ii) Existencia de elemento neutro
   $$(\exists! e \in \mathbb{Z})(\forall x \in \mathbb{Z})(x+e = e+x = x).$$

   iii) Existencia de elemento inverso
   $$(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x+y = y+x = e).$$

   iv) Conmutatividad
   $$(\forall x,y \in \mathbb{Z})(x+y = y+x).$$

2. *Propiedades del producto en* $\mathbb{Z}$

   i) Asociatividad

   $$(\forall x, y, z \in \mathbb{Z})((x \cdot y) \cdot z = x \cdot (y \cdot z)).$$

   ii) Existencia de elemento neutro

   $$(\exists! e \in \mathbb{Z})(\forall x \in \mathbb{Z})(x \cdot e = e \cdot x = x).$$

   iii) Conmutatividad

   $$(\forall x, y \in \mathbb{Z})(x \cdot y = y \cdot x).$$

3. *El producto en* $\mathbb{Z}$ *es distributivo respecto a la suma*

   $$x \cdot (y + z) = x \cdot y + x \cdot z \quad \forall x, y, z \in \mathbb{Z}.$$

Demostración:

1. Propiedades de la suma en $\mathbb{Z}$

   i) Sean $x = \overline{(a,b)}, y = \overline{(c,d)}, z = \overline{(e,f)} \in \mathbb{Z}$.

   Entonces

   $$\begin{aligned}
   (x+y)+z &= [\overline{(a,b)} + \overline{(c,d)}] + \overline{(e,f)} \\
   &= \overline{(a+c, b+d)} + \overline{(e,f)} \\
   &= \overline{((a+c)+e, (b+d)+f)} \\
   &= \overline{(a+(c+e), b+(d+f))} \\
   &= \overline{(a,b)} + \overline{(c+e, d+f)} \\
   &= \overline{(a,b)} + [\overline{(c,d)} + \overline{(e,f)}] \\
   &= x + (y+z).
   \end{aligned}$$

   ii) Sean $x = \overline{(a,b)}$ cualquiera y determinemos $e = \overline{(u,v)}$ de modo que

   $$\begin{aligned}
   & \overline{(a,b)} + \overline{(u,v)} = \overline{(a,b)} \\
   \Leftrightarrow\ & \overline{(a+u, b+v)} = \overline{(a,b)} \\
   \Leftrightarrow\ & (a+u, b+v) \sim (a,b) \\
   \Leftrightarrow\ & (a+u)+b = (b+v)+a \\
   \Leftrightarrow\ & a+u = v+a \\
   \Leftrightarrow\ & u = v.
   \end{aligned}$$

   Por lo tanto existe $e = \overline{(u,u)}$, el cual por comodidad lo denotaremos por $\overline{(0,0)}$.

iii) Sea $x = \overline{(a,b)}$, queremos encontrar un elemento $y = \overline{(c,d)}$ de modo que se verifique la siguiente relación

$$\begin{array}{rrcl} & x+y & = & e \\ \Leftrightarrow & \overline{(a,b)} + \overline{(c,d)} & = & \overline{(0,0)} \\ \Leftrightarrow & \overline{(a+c,b+d)} & = & \overline{(0,0)} \\ \Leftrightarrow & (a+c,b+d) & \sim & (0,0) \\ \Leftrightarrow & a+c & = & b+d \\ \Leftrightarrow & c+a & = & d+b \\ \Leftrightarrow & (c,d) & \sim & (b,a) \\ \Leftrightarrow & \overline{(c,d)} & = & \overline{(b,a)}. \end{array}$$

Por lo tanto tenemos que $y = \overline{(b,a)}$.

Notación: De acuerdo a lo anterior cada elemento en $\mathbb{Z}$ tiene un inverso. En adelante anotaremos como $-x$ el inverso de $x \in \mathbb{Z}$. Según esto $-\overline{(a,b)} = \overline{(b,a)}$ y siempre tendremos que $x + (-x) = e$, además naturalmente $-(-x) = x, \forall x \in \mathbb{Z}$.

iv) La conmutatividad queda como ejercicio

2. Propiedades del producto en $\mathbb{Z}$

i) Sean $x = \overline{(a,b)}, y = \overline{(c,d)}, z = \overline{(e,f)} \in \mathbb{Z}$. Entonces

$$\begin{array}{rcl} (x \cdot y) \cdot z & = & [\overline{(a,b)} \cdot \overline{(c,d)}] \cdot \overline{(e,f)} \\ & = & \overline{(ac+bd, ad+bc)} \cdot \overline{(e,f)} \\ & = & \overline{((ac+bd)e + (ad+bc)f, (ac+bd)f + (ad+bc)e)} \\ & = & \overline{((ac)e + (bd)e + (ad)f + (bc)f, (ac)f + (bd)f + (ad)e + (bc)e)} \\ & = & \overline{(a(ce) + b(de) + a(df) + b(cf), a(cf) + b(df) + a(de) + b(ce))} \\ & = & \overline{(a(ce) + a(df) + b(cf) + b(de), a(cf) + a(de) + b(ce) + b(df))} \\ & = & \overline{a(ce+df) + b(cf+de), a(cf+de) + b(ce+df)} \\ & = & \overline{(a,b)} \cdot \overline{(ce+df, cf+de)} \\ & = & \overline{(a,b)} \cdot [\overline{(c,d)} \cdot \overline{(e,f)}] \\ & = & x \cdot (y \cdot z). \end{array}$$

ii) Sean $x = \overline{(a,b)}$,

$$\overline{(a,b)} \cdot \overline{(1,0)} = \overline{(a \cdot 1 + b \cdot 0, a \cdot 0 + b \cdot 1)} = \overline{(a,b)}.$$

Además

$$\overline{(1,0)} \cdot \overline{(a,b)} = \overline{(1 \cdot a + 0 \cdot b, 0 \cdot a + 1 \cdot b)} = \overline{(a,b)}.$$

iii) Sea $x = \overline{(a,b)}, y = \overline{(c,d)}$

Luego

$$\begin{array}{rcl} x \cdot y & = & \overline{(a,b)} \cdot \overline{(c,d)} \\ & = & \overline{(ac+bd, ad+bc)} \\ & = & \overline{(ca+db, cb+da)} \\ & = & \overline{(c,d)} \cdot \overline{(a,b)} \\ & = & y \cdot x. \end{array}$$

3. Distributividad

   Sean $x = \overline{(a,b)}, y = \overline{(c,d)}, z = \overline{(e,f)}$

   Entonces

$$\begin{aligned} x \cdot (y+z) &= \overline{(a,b)} \cdot (\overline{(c,d)} + \overline{(e,f)}) \\ &= \overline{(a,b)} \cdot \overline{(c+e, d+f)} \\ &= \overline{(a(c+e)+b(d+f), a(d+f)+b(c+e))} \\ &= \overline{(ac+ae+bd+bf, ad+af+bc+be)} \\ &= \overline{((ac+bd)+(ae+bf), (ad+bc)+(af+be))} \\ &= \overline{(ac+bd, ad+bc)} + \overline{(ae+bf, af+be)} \\ &= \overline{(a,b)} \cdot \overline{(c,d)} + \overline{(a,b)} \cdot \overline{(e,f)} \\ &= x \cdot y + x \cdot z. \end{aligned}$$

□

Teorema 42 *Ley de cancelación para la suma en $\mathbb{Z}$, es decir*

$$(\forall x, y, z \in \mathbb{Z})((x + y = x + z) \Rightarrow y = z).$$

Demostración: Sean $x = \overline{(a,b)}, y = \overline{(c,d)}, z = \overline{(e,f)} \in \mathbb{Z}$.

Luego

$$\begin{aligned} & \overline{(a,b)} + \overline{(c,d)} = \overline{(a,b)} + \overline{(e,f)} \\ \Rightarrow\ & \overline{(a+c, b+d)} = \overline{(a+e, b+f)} \\ \Rightarrow\ & a+c+b+f = b+d++a+e \\ \Rightarrow\ & c+f = d+e \quad \text{(Ley de cancelación en } \mathbb{N}) \\ \Rightarrow\ & \overline{(c,d)} = \overline{(e,f)}. \end{aligned}$$

□

Teorema 43 *Ley de cancelación para el producto en $\mathbb{Z}$, es decir*

$$(\forall x \in \mathbb{Z} - \{0\})(\forall y, z \in \mathbb{Z})((x \cdot y = x \cdot z) \Rightarrow y = z).$$

o bien

$$(\forall x, y, z \in \mathbb{Z})((x \cdot y = x \cdot z \wedge x \neq 0) \Rightarrow y = z).$$

Demostración: Sean $x = \overline{(a,b)}, y = \overline{(c,d)}, z = \overline{(e,f)} \in \mathbb{Z}$.

Luego

$$\begin{aligned} & \overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a,b)} \cdot \overline{(e,f)} \\ \Rightarrow\ & \overline{(ac+bd, ad+bc)} = \overline{(ae+bf, af+be)} \\ \Rightarrow\ & ac+bd+af+be = ad+bc+ae+bf \\ \Rightarrow\ & a(c+f)+b(d+e) = a(d+e)+b(c+f) \\ \Rightarrow\ & a(c+f)-b(c+f) = a(d+e)-b(d+e) \quad (a > b, \text{ es decir, } a-b \in \mathbb{N}) \\ \Rightarrow\ & (a-b)(c+f) = (a-b)(d+e) \\ \Rightarrow\ & c+f = d+e \\ \Rightarrow\ & \overline{(c,d)} = \overline{(e,f)} \\ \Rightarrow\ & y = z. \end{aligned}$$

□

Observación: ¿En que casos $\overline{(a,b)}$ admite un inverso multiplicativo?
Consideremos $\overline{(a,b)}$ y sea $\overline{(c,d)}$ tal que

$$\begin{array}{rrcl} & \overline{(a,b)}\cdot\overline{(c,d)} & = & \overline{(1,0)} \\ \Leftrightarrow & \overline{(ac+bd,ad+bc)} & = & \overline{(1,0)} \\ \Leftrightarrow & ac+bd & = & ad+bc+1 \\ \Leftrightarrow & ac+bd-ad-bc & = & 1 \\ \Leftrightarrow & a(c-d)-b(c-d)=1 & \vee & b(d-c)-a(d-c)=1 \\ \Leftrightarrow & (a-b)(c-d)=1 & \vee & (b-a)(d-c)=1. \end{array}$$

Ahora bien, tenemos tres casos:

1. $a>b$, entendiendo $a-b\in\mathbb{N}$ luego

$$\begin{array}{rrcl} & (a-b)(c-d) & = & 1 \\ \Rightarrow & a-b=1 & \vee & c-d=1 \\ \Rightarrow & a=b+1 & \vee & c=d+1. \end{array}$$

   Por lo tanto $\overline{(a,b)}=\overline{(b+1,b)}=\overline{(1,0)}$ admite inverso multiplicativo y este es

$$\overline{(c,d)}=\overline{(d+1,d)}=\overline{(1,0)}.$$

2. $a<b$ entonces $b-a\in\mathbb{N}$ luego $(b-a)(d-c)=1$ y en este caso

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

   admite inverso multiplicativo el cual esta dado por

$$\overline{(0,1)}.$$

3. $a=b$ entonces $0=1$ y por lo tanto $\overline{(a,a)}$ con $a\in\mathbb{N}$ no tiene inverso multiplicativo.

Resumiendo tenemos que $\overline{(a,b)}$ admite inverso multiplicativo si

$$\overline{(a,b)}=\overline{(1,0)} \quad \vee \quad \overline{(a,b)}=\overline{(0,1)}.$$

La unidades de $\mathbb{Z}$ es

$$\mathcal{U}(\mathbb{Z})=\{\overline{(1,0)}\ ,\ \overline{(0,1)}\}$$

Identificación con el Sistema de Representante

Con el sistema de representante, se tiene que

$$\begin{array}{rcl} \overline{(n,0)}+\overline{(m,0)} & = & \overline{(n+m,0)} \\ \overline{(n,0)}\cdot\overline{(m,0)} & = & \overline{(n\cdot m,0)} \end{array}$$

Y para los otros tenemos

$$\begin{aligned} \overline{(0,n)} + \overline{(0,m)} &= \overline{(0,n+m)} \\ \overline{(0,n)} \cdot \overline{(0,m)} &= \overline{(n \cdot m, 0)} \end{aligned}$$

Usando lo anterior podemos identificar

$$\overline{(n,0)} = n; \qquad \overline{(0,m)} = -m$$

Con esta identificación se tiene que compatible con la suma y el producto de los números naturales.

A partir de esto, podemos considerar la siguiente correspondencia o contención

$$\begin{aligned} \mathbb{N} &\subset \mathbb{Z} \\ n &\equiv \overline{(n,0)} \end{aligned}$$

Notación: $\mathbb{Z}^+ = \mathbb{N}^*; \quad -\mathbb{N} = \{-n \mid n \in \mathbb{N}\}; \quad \mathbb{Z}^- = -\mathbb{Z}^+.$

Con las notaciones anteriores tenemos

$$\mathbb{Z} = \mathbb{N} \cup -\mathbb{N} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+,$$

además $\mathbb{N} \cap -\mathbb{N} = \{0\}$.

Propiedad 44 *Sean $x \in \mathbb{Z}$ entonces se tiene*

$$x \cdot 0 = 0.$$

Demostración: Sea $x \in \mathbb{Z}$, entonces

$$\begin{aligned} x \cdot 0 &= x \cdot (0+0) \\ x \cdot 0 &= x \cdot 0 + x \cdot 0 \\ 0 &= x \cdot 0 \quad \text{(sumando inverso aditivo de } x \cdot 0). \end{aligned}$$

□

Teorema 45 *Para todo $x, y, z \in \mathbb{Z}$ se verifica:*

1. $x \cdot (-y) = -(x \cdot y)$.
2. $(-x) \cdot y = -(x \cdot y)$.
3. $(-x) \cdot (-y) = x \cdot y$.

Demostración: Sean $x, y, z \in \mathbb{Z}$

1. Consideremos
$$x \cdot y + x \cdot (-y) = x \cdot (y + (-y)) = x \cdot 0 = 0,$$
así tenemos que $x \cdot (-y)$ es el inverso aditivo de $x \cdot y$, lo cual es equivalente a demostrar (1).

2. Análogo al caso (1).

3. De acuerdo a (1) y (2) tenemos (3) como sigue

$$(-x)\cdot(-y) \underbrace{=}_{\text{por (2)}} -(x\cdot(-y)) \underbrace{=}_{\text{por (1)}} -(-(x\cdot y)) = x\cdot y.$$

para la última igualdad, tenga presente que el inverso aditivo de a es $-a$, de otro modo el inverso de $-a$ es a y también $-(-a)$, luego son iguales

Notación: Para $a, b \in \mathbb{Z}$ anotaremos $a+(-b)$ como $a-b$, cuya notación es compatible con la dada anteriormente para el conjunto $\mathbb{N}$.

Teorema 46 *La ecuación $a+x=b$ con $a, b \in \mathbb{Z}$ tiene única solución. La cual esta dada por $x=b-a$.*

Demostración: Sea

$$\begin{array}{rrcll} & a+x & = & b & \\ \Leftrightarrow & (a+x)+(-a) & = & b+(-a) & \text{(sumando el inverso aditivo de } a) \\ \Leftrightarrow & (a+(-a))+x & = & b-a & \\ \Leftrightarrow & 0+x & = & b-a & \\ \Leftrightarrow & x & = & b-a. & \end{array}$$

□

Definición 12 *Sea A un anillo, $x \in A,\ x \neq 0$.*

Se dice que x es un divisor de cero derecho si y sólo si existe $y \in A,\ y \neq 0$ tal que $yx = 0$

Se dice que x es un divisor de cero izquierdo si y sólo si existe $y \in A,\ y \neq 0$ tal que $xy = 0$

Teorema 47 *El anillo $\mathbb{Z}$ no tiene divisores de cero, es decir,*

$$(\forall x, y \in \mathbb{Z})(\ xy = 0 \Rightarrow (x = 0 \vee y = 0)\ )$$

Demostración: Si $x, y \in \mathbb{N}$, por teorema 31, la propiedad se cumple.

Supongamos ahora $x \in \mathbb{N}, y \in -\mathbb{N}$, luego tenemos $-y = z \in \mathbb{N}$.

$$xz = x(-y) = -(xy) = -0 = 0$$

Por la primera parte tenemos que $x = 0 \vee z = 0$, como $-y = z = 0$ entonces $y = 0$. Por lo tanto

$$x = 0 \vee y = 0$$

Los otros caso son similares. □

2.2. Orden en $\mathbb{Z}$

Definición 13 *Sean $x, y \in \mathbb{Z}$*

Se dice que x es menor o igual que y si y sólo si existe $n \in \mathbb{N}$ tales que $x + n = y$, es decir,

$$(x \leq y) \Leftrightarrow (\exists n \in \mathbb{N})(x + n = y)$$

de modo equivalente

$$(x \leq y) \Leftrightarrow (y - x \in \mathbb{N}).$$

Teorema 48 *La relación "$\leq$" es una relación de orden en $\mathbb{Z}$.*

Demostración: Sean $x, y, z \in \mathbb{Z}$
Refleja:

$$x \leq x \text{ pues } x - x = 0 \in \mathbb{N}.$$

Antisimétrica: Supongamos $x \leq y$ e $y \leq x$, es decir $y - x \in \mathbb{N}$ y $x - y \in \mathbb{N}$, puesto que

$$(x - y) + (y - x) = x + ((-y) + y) + (-x) = 0$$

tenemos que

$$x - y = -(y - x)$$

de esto

$$y - x \in \mathbb{N} \quad \wedge \quad y - x \in -\mathbb{N}$$

es decir,

$$y - x \in (\mathbb{N} \cap -\mathbb{N}),$$

pero

$$\mathbb{N} \cap -\mathbb{N} = \{0\},$$

de otro modo

$$y - x \in \{0\},$$

esto es

$$y - x = 0 \Leftrightarrow x = y.$$

Transitiva: Supongamos $x \leq y$ e $y \leq z$, es decir, $y - x \in \mathbb{N}$ y $z - y \in \mathbb{N}$, ahora bien como

$$(y - x) + (z - y) \in \mathbb{N}$$

pero

$$(y - x) + (z - y) = z - x$$

tenemos entonces que

$$z - x \in \mathbb{N}$$

con lo cual

$$x \leq z.$$

□

Teorema 49 *La relación "$\leq$" es compatible con la suma $(+)$ y el producto $(\cdot)$ en $\mathbb{Z}$, esto es:*

1. $(\forall x, y \in \mathbb{Z})(\forall z \in \mathbb{Z})(\, x \leq y \;\Rightarrow\; x + z \leq y + z\,)$.
2. $(\forall x, y \in \mathbb{Z})(\forall z \in \mathbb{N})(\, x \leq y \;\Rightarrow\; x \cdot z \leq y \cdot z\,)$.
3. $(\forall x, y \in \mathbb{Z})(\forall z \in -\mathbb{N})(\, x \leq y \;\Rightarrow\; x \cdot z \geq y \cdot z\,)$.

Demostración: Sea $x, y, z \in \mathbb{Z}$

1. Supongamos $x \leq y$, ahora bien

$$\begin{array}{ll} & x \leq y \\ \Rightarrow & y - x \in \mathbb{N} \\ \Rightarrow & (y - x) + (z - z) \in \mathbb{N} \\ \Rightarrow & (y + z) - (x + z) \in \mathbb{N} \\ \Rightarrow & x + z \leq y + z. \end{array}$$

2. Supongamos $x \leq y$ e $z \in \mathbb{N}$

$$\begin{array}{ll} & x \leq y \;\wedge\; z \in \mathbb{N} \\ \Rightarrow & y - x \in \mathbb{N} \;\wedge\; z \in \mathbb{N} \\ \Rightarrow & (y - x) \cdot z \in \mathbb{N} \\ \Rightarrow & y \cdot z - x \cdot z \in \mathbb{N} \\ \Rightarrow & x \cdot z \leq y \cdot z. \end{array}$$

3. Supongamos $x \leq y$ e $z \in -\mathbb{N}$

$$\begin{array}{ll} & x \leq y \;\wedge\; z \in -\mathbb{N} \\ \Rightarrow & y - x \in \mathbb{N} \;\wedge\; (-z) \in \mathbb{N} \\ \Rightarrow & (y - x) \cdot (-z) \in \mathbb{N} \\ \Rightarrow & -y \cdot z + x \cdot z \in \mathbb{N} \\ \Rightarrow & x \cdot z - y \cdot z \in \mathbb{N} \\ \Rightarrow & x \cdot z \geq y \cdot z. \end{array}$$

□

2.3. Divisibilidad

Dada dos rueda dentada, una con 54 diente y la otra con 28 diente, inicia su giro después de ¿cuántas vueltas como mínimo debe girar de modo que vuelva a la posición origina o de partida?

En esta sección debemos tener presente en forma especial el Principio de Inducción Teorema 34 y Principio del Buen Orden Teorema 33

Definición 14 *Sean $a, b \in \mathbb{Z}$, $a \neq 0$.*
Diremos que "a" divide a "b", si existe $q \in \mathbb{Z}$ tal que

$$b = aq.$$

Notación: a divide a b, se denota por $a|b$, y cuando a no divide a b, se denota por $a \nmid b$.

Teorema 50 *Sean $a, b, c \in \mathbb{Z}$*

1. *Si $a|b$ entonces $(\forall c \in \mathbb{Z})(a|bc)$.*
2. *Si $(a|b \wedge b|c)$ entonces $a|c$.*
3. *Si $(a|b \wedge a|c)$ entonces $(\forall m, n \in \mathbb{Z})(a|(mb + nc))$.*
4. *Si $(a|b \wedge b|a)$ entonces $(a = b \vee a = -b)$.*
5. *Si $(a|b \wedge a > 0 \wedge b > 0)$ entonces $a \leq b$.*

Notación: La expresión $a = \pm b$ significa $(a = b \vee a = -b)$.

Demostración: Demostraremos sólo (3) y (5), quedando las demás como ejercicio.

(3) Si $a|b$ y $a|c$ entonces existen $q, q' \in \mathbb{Z}$ tal que

$$b = aq \quad \wedge \quad c = aq'. \tag{2.1}$$

Sean $n, m \in \mathbb{Z}$ y notemos que por (2.1)

$$\begin{aligned} mb + nc &= m(aq) + n(aq') \\ &= a(mq + nq'), \end{aligned}$$

ahora bien, definiendo $s = mq + nq' \in \mathbb{Z}$, tenemos que $mb + nc = as$, es decir, $a|(mb + nc)$.

(5) Si $a|b$ entonces existe $q \in \mathbb{Z}$ tal que

$$b = aq.$$

Ahora como $a > 0$ y $b > 0$, se tiene que q es positivo, más aún $q \geq 1$, luego

$$b - a = aq - a = a(q - 1) \geq 0,$$

es decir,

$$b - a \geq 0 \Leftrightarrow b \geq a.$$

Ejemplo 15 *Demostrar que*

$$(\forall n \in \mathbb{N})(6|(n^3 - n))$$

Solución: La demostración la realizaremos usando el principio de inducción.

Definamos la función proposicional $p(n) = 6|(n^3 - n)$

Primer paso: $p(0) = 6|0$, verdadero.

Segundo paso: Supongamos $p(n) = 6|(n^3 - n)$ es verdadero, es decir, existe $k \in \mathbb{Z}$, tal que $n^3 - n = 6k$.

Por demostrar que $p(n+1)$ es verdadero. Lo cual significa que $6|((n+1)^3 - (n+1))$, lo cual es equivalente a demostrar $(n+1)^3 - (n+1) = 6 \cdot q; \quad \text{con } q \in \mathbb{Z}$.

Para ello veamos lo siguiente:

$$\begin{aligned}(n+1)^3 - (n+1) &= n^3 + 3 \cdot n^2 + 3 \cdot n + 1 - n - 1 \\ &= n^3 - n + 3 \cdot n^2 + 3 \cdot n \\ &= 6 \cdot k + 3 \cdot n \cdot (n+1)\end{aligned}$$

Pero de la suma de los primeros n naturales obtenemos que $(\forall n \in \mathbb{N})(2|n \cdot (n+1))$ que se puede reescribir del siguiente modo $(\forall n \in \mathbb{Z})(\exists r \in \mathbb{Z})(n \cdot (n+1) = 2 \cdot r)$, queda como ejercicio su demostración, reemplazando este resultado, tenemos

$$\begin{aligned}(n+1)^3 - (n+1) &= 6 \cdot k + 3 \cdot 2 \cdot r \\ &= 6 \cdot k + 6 \cdot r \\ &= 6 \cdot (k + r)\end{aligned}$$

Luego

$$6|((n+1)^3 - (n+1))$$

y por teorema de inducción, obtenemos

$$(\forall n \in \mathbb{N})(6|(n^3 - n)).$$

Ejercicio 16 *Demostrar*

$$(\forall n \in \mathbb{Z})(\ 2|n \cdot (n+1))$$

Teorema 51 (Algoritmo de la División) *Sean $a, b \in \mathbb{Z}, a > 0$. Entonces existen únicos enteros q y r tales que:*

$$b = qa + r,$$

donde $0 \leq r < a$.

Además si $a \nmid b$ entonces $0 < r < a$.

Demostración: Consideremos el conjunto

$$A = \{b - qa \mid q \in \mathbb{Z}\} \cap \mathbb{N}.$$

Como $a, b \in \mathbb{Z}$ se tiene tres caso y verificando cada uno de ello se comprueba que el conjunto es no vacío.

Luego por el Teorema Buen Orden (33) existe un elemento mínimo de A, el cual llamaremos r. Por definición de A, se tiene que $r \geq 0$.

Supongamos que $r \geq a$, entonces

$$r = b - qa \geq \quad a,$$

de donde $b - (q+1)a \geq 0$, es decir, $b - (q+1)a \in A$.

Ahora bien como

$$b - (q+1)a \leq b - qa = r,$$

se tiene que r no es el menor elemento de A, lo cual es una contradicción, por lo tanto $r < a$ y en consecuencia que

$$0 \leq r < a.$$

Para mostrar la unicidad de q y r, supongamos que existe otro par de elementos q' y r' que satisfacen las hipótesis del teorema. Tenemos entonces que $aq + r - aq' - r' = 0$, luego $a(q - q') = r' - r$, es decir, $a|(r' - r)$. Ahora bien si $r' \neq r$, por el teorema (50) parte (5), se tiene que $(r' - r) \geq a > 0$, lo cual es una contradicción pues $-a < r' - r < a$, por lo tanto $r' = r$. Pero entonces $a(q - q') = 0$ y $a \neq 0$, así $q = q'$.

Corolario 52 *Sean a, x enteros positivos, con $a > 1$. Entonces x tiene una única representación de la forma*

$$x = b_0 + b_1 a + \cdots b_n a^n,$$

con $n \geq 0$, $0 < b_n < a$ y $0 \leq b_i < a$, para $0 \leq i \leq n-1$.

Demostración: Usaremos inducción sobre la existencia de la representación de x.

Si $x = 1$, tomamos $b_0 = 1$ y $n = 0$ y el resultado es válido.

Supongamos que cualquier entero $m < x$, puede ser representado de manera única en la forma

$$r_0 + r_1 a + \cdots + r_k a^k,$$

donde $0 < r_i < a, 0 \leq i \leq k$ y $r_k > 0$.

Por el algoritmo de la división $x = qa + r$ con $0 \leq r < a$.

Si $q \geq x$, amplificando por a obtenemos $aq \geq ax$ pero $ax > x$, luego tenemos que $aq > x$ sumando r obtenemos $aq + r > x + r \geq x$ lo cual es imposible. Por lo tanto, $q < x$

Veamos ahora, si $q = 0$, tenemos que

$$x = r + 0 \cdot a,$$

luego obtenemos la representación que buscada, es decir, $p(x)$ es verdadero .

Finalmente, falta el caso que $0 < q < x$.

Por hipótesis de inducción tenemos que, existen k, $0 \leq r_i < a$ y $0 < r_k$ tales que

$$q = r_0 + r_1 a + \cdots r_k a^k.$$

Entonces, reemplazando se tiene

$$x = aq + r = r_k a^{k+1} + \cdots r_0 a + r,$$

haciendo un cambio de indices apropiado, obtenemos que

$$x = b_0 + b_1 a + \cdots b_n a^n.$$

Luego existe la representación

Ahora para demostrar la unicidad de esta representación, supongamos que existe otra representación, es decir

$$x = b_0 + b_1 a + \cdots + b_n a^n = c_0 + c_1 a + \cdots + c_j a^j,$$

tenemos entonces que

$$0 = h_0 + h_1 a + \cdots + h_s a^s,$$

donde $|h_i| < a$, para $0 \leq i \leq s,\ h_s \neq 0, s \geq 0$.

Ahora bien como $|h_i| < a$, entonces $|h_i| \leq a - 1$ y así

$$\begin{aligned} a^s &\leq |h_s a^s| \\ &= |h_o + h_1 a + \cdots + h_{s-1} a^{s-1}| \\ &\leq |h_0| + |h_1| a + \cdots + |h_{s-1}| a^{s-1} \\ &\leq (a-1) + (a-1)a + \cdots + (a-1)a^{s-1} \\ &= (a-1)(1 + a + \cdots + a^{s-1}) \\ &= a^s - 1 \end{aligned}$$

lo cual es una contradicción y en consecuencia se tiene al unicidad. □

2.3.1. Representaciones de Números Enteros

$$\begin{aligned} 122 &= 3 \cdot 40 + 2 \\ 40 &= 3 \cdot 13 + 1 \\ 13 &= 3 \cdot 4 + 1 \\ 4 &= 3 \cdot 1 + 1 \\ 1 &= 3 \cdot 0 + 1 \end{aligned}$$

$$\begin{aligned} 122 &= 3 \cdot 40 + 2 \\ &= 3 \cdot (3 \cdot 13 + 1) + 2 \\ &= 3^2 \cdot 13 + 1 \cdot 3 + 2 \\ &= 3^2(3 \cdot 4 + 1) + 1 \cdot 3 + 2 \\ &= 3^3 \cdot 4 + 1 \cdot 3^2 + 1 \cdot 3 + 2 \\ &= 3^3(3 \cdot 1 + 1) + 1 \cdot 3^2 + 1 \cdot 3 + 2 \end{aligned}$$

Luego

$$\begin{aligned} 122 &= 1 \cdot 3^4 + 1 \cdot 3^3 + 1 \cdot 3^2 + 1 \cdot 3 + 2 \\ 122 &= (1\ 1\ 1\ 1\ 2)_3 \quad \text{(base 3)} \\ 122 &= 1 \cdot 10^2 + 2 \cdot 10 + 2 = (122)_{10} \quad \text{(base 10)} \end{aligned}$$

Veamos ahora el 7 en base 3

$$7 = 2 \cdot 3^1 + 1 \cdot 3^0$$

Al sumar $\begin{array}{r} (1\ 1\ 1\ 1\ 2)_3 \\ +\quad\quad (2\ 1)_3 \\ \hline (1\ 1\ 2\ 1\ 0)_3 \end{array}$ Verificando con las potencias tenemos

$$\begin{aligned}
&(1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+1\cdot 3+2)+(2\cdot 3+1)\\
&1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+(1+2)3\cdot 3\\
&1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+(3+1)3+0\\
&1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+1\cdot 3^2+1\cdot 3+0\\
&1\cdot 3^4+1\cdot 3^3+(1+1)3^2+1\cdot 3+0\\
&1\cdot 3^4+1\cdot 3^3+2\cdot 3^2+1\cdot 3+0
\end{aligned}$$

Ahora revisemos la multiplicación

$$(1\ 1\ 1\ 1\ 2)_3\times(2\ 1)_3=(1\ 0\ 1\ 1\ 1\ 2\ 2)_3$$

$$\begin{array}{r} \underline{1\ 1\ 1\ 1\ 2}\times 2\ 1 \\ 1\ 1\ 1\ 1\ 2 \\ \underline{1\ 0\ 0\ 0\ 0\ 1\ \ } \\ (1\ 0\ 1\ 1\ 1\ 2\ 2)_3 \end{array}$$

Con la aritmética habitual.

$$\begin{array}{rcl} (1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+1\cdot 3+2) & \times & (2\cdot 3+1) \\ 1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+1\cdot 3+2 & & \\ \underline{2\cdot 3^5+2\cdot 3^4+2\cdot 3^3+2\cdot 3^2+4\cdot 3} & & \\ 2\cdot 3^5+3\cdot 3^4+3\cdot 3^3+3\cdot 3^2+5\cdot 3+2 & & \\ 1\cdot 3^6+0\cdot 3^5+1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+2\cdot 3+2 & & \end{array}$$

2.4. Regla de Divisibilidad

Debemos tener presente que todo natural se puede escribir en base 10 en forma única, corolario 52

$$n=a_ma_{m-1}a_{m-2}\dots a_1a_0=a_m10^m+a_{m-1}10^{m-1}+a_{m-2}10^{m-2}+\cdots+a_110+a_0$$

donde los a_i son dígitos.

Además recordemos el corolario $a|n\wedge a|y\Rightarrow a|(n-y)$, que en nuestro caso lo aplicaremos para $n=x+y$, es decir $n|x$

2.4.1. Divisibilidad por 2

Dado $n=a_m10^m+a_{m-1}10^{m-1}+a_{m-2}10^{m-2}+\cdots+a_110+a_0$, con los a_i dígitos.

Además se tiene que $2|10^i$, para todo $i>0$.

Luego se tiene que

$$2|(a_m10^m+a_{m-1}10^{m-1}+a_{m-2}10^{m-2}+\cdots+a_110).$$

de lo cual se tiene

Propiedad 53 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$2|n \Leftrightarrow 2|a_0 \Leftrightarrow a_0 \text{ es par}$$

Ejemplo 17 *El número* $n = 8334216$ *es divisible por* 2*, ya que* $a_0 = 6$ *número par.*

2.4.2. Divisibilidad por 3

Dado $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$, con los a_i dígitos.
Es fácil demostrar por inducción que $3|(10^i - 1)$, para todo $i > 0$.
Luego se tiene que

$$3|(a_m(10^m - 1) + a_{m-1}(10^{m-1} - 1) + a_{m-2}(10^{m-2} - 1) + \cdots + a_1(10 - 1))$$

además

$$n = (a_m + a_{m-1} + \cdots + a_1 + a_0) + (a_m(10^m - 1) + a_{m-1}(10^{m-1} - 1) + \cdots + a_1(10 - 1))$$

de lo cual se tiene

Propiedad 54 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$3|n \Leftrightarrow 3|(a_m + a_{m-1} + a_{m-2} + \cdots + a_1 + a_0)$$

Ejemplo 18 *El número* $n = 134718$ *es divisible por* 3*, ya que* $1 + 3 + 4 + 7 + 1 + 8 = 24$ *es divisible por* 3*.*

2.4.3. Divisibilidad por 4

Sea $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$, con los a_i dígitos.
Es fácil demostrar que $4|10^i$, con $i > 1$ y además se tiene que $10 = 4 \cdot 2 + 2$. De lo cual se obtiene

$$4|(a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 8)$$

además

$$n = (2a_1 + a_0) + (a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 8)$$

de lo cual se tiene

Propiedad 55 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$4|n \Leftrightarrow 4|(2a_1 + a_0)$$

Ejemplo 19 *El número* $n = 231528$ *es divisible por* 4*, ya que* $2 \cdot 2 + 8 = 12$ *es divisible por* 4*.*

2.4.4. Divisibilidad por 5

Sea $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$, con los a_i dígitos.
Es fácil demostrar que $5|10^i$, con $i > 0$.
De lo cual se obtiene

$$5|(a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10)$$

además

$$n = (a_0) + (a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10)$$

de lo cual se tiene

Propiedad 56 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$5|n \Leftrightarrow 5|a_0$$

Ejemplo 20 *El número* $n = 5689425$ *es divisible por* 5*, ya que* 5 *es divisible por* 5*.*

2.4.5. Divisibilidad por 6

Propiedad 57 *Sea* $n \in \mathbb{N}^*$*, luego*

$$6|n \;\Leftrightarrow\; 2|n \wedge 3|n$$

2.4.6. Divisibilidad por 8

Sea $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$, con los a_i dígitos.
Es fácil demostrar que: $8|10^i$, con $i > 2$ y además $10^2 = 8 \cdot 12 + 4$, $10 = 8 \cdot 1 + 2$. De lo cual se obtiene

$$8|(a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} \cdots + a_2 96 + a_1 8)$$

además

$$n = (4a_2 + 2a_1 + a_0) + (a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_2 96 + a_1 8)$$

de lo cual se tiene

Propiedad 58 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$8|n \Leftrightarrow 8|(4a_2 + 2a_1 + a_0)$$

Ejemplo 21 *El número* $n = 231528$ *es divisible por* 8*, ya que* $4 \cdot 5 + 2 \cdot 2 + 8 = 32$ *es divisible por* 8*.*

2.4.7. Divisibilidad por 9

Sea $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$, con los a_i dígitos.
Es fácil demostrar que $9|(10^i - 1)$, con $i > 0$.
De lo cual se obtiene

$$9|(a_m(10^m - 1) + a_{m-1}(10^{m-1} - 1) + a_{m-2}(10^{m-2} - 1) + \cdots + a_1 9)$$

además

$$n = (a_m + a_{m-1} + \cdots + a_1 + a_0) + (a_m(10^m - 1) + a_{m-1}(10^{m-1} - 1) + \cdots + a_1 9)$$

de lo cual se tiene

Propiedad 59 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$9|n \Leftrightarrow 9|(a_m + a_{m-1} + a_{m-2} + \cdots + a_1 + a_0)$$

Ejemplo 22 *El número* $n = 245718$ *es divisible por* 3, *ya que* $2 + 4 + 5 + 7 + 1 + 8 = 27$ *es divisible por* 9.

2.4.8. Divisibilidad por 11

Sea $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$, con los a_i dígitos.
Se sabe que $11|(10^i - (-1)^i)$, para todo $i \geq 0$. De lo cual se obtiene

$$9|(a_m(10^m - (-1)^m) + a_{m-1}(10^{m-1} - (-1)^{m-1}) + \cdots + a_1(10 + 1))$$

además

$$n = (a_m(-1)^m + \cdots + a_1(-1)^1 + a_0) + (a_m(10^m - (-1)^m) + \cdots + a_1(10 + 1))$$

de lo cual se tiene

Propiedad 60 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$11|n \Leftrightarrow 11|(a_m(-1)^m + a_{m-1}(-1)^{m-1} + a_{m-2}(-1)^{m-2} + \cdots + a_2(-1)^2 + a_1(-1)^1 + a_0)$$

Ejemplo 23 *El número* $n = 245718$ *es divisible por* 11, *ya que* $-2 + 4 - 5 + 7 - 1 + 8 = 11$ *es divisible por* 11.

2.5. Máximo Común Divisor

Definición 15 (Divisor Común) *Sean* $a, b, c \in \mathbb{Z}$.

Se dice que a *es un divisor común de* b *y* c *si y sólo si* $a|b$ *y* $a|c$.

En general dados $x_1, x_2, \ldots, x_n \in \mathbb{Z}$, *se dice que* a *es divisor común de* $x_1, x_2, \ldots, x_n$ *si y sólo si* $a|x_1 \wedge a|x_2 \wedge \cdots \wedge a|x_n$.

Definición 16 (Máximo Común Divisor) *Sean a, b dos enteros no nulos. El máximo común divisor entre a y b es el mayor divisor común positivo de a y b, el cual denotaremos por (a, b).*

En general dados $x_1, x_2, \ldots, x_n \in \mathbb{Z}^*$, el máximo común divisor de $x_1, x_2, \ldots, x_n$ es el mayor divisor común de $x_1, x_2, \cdots, x_n$, el cual denotamos por $(x_1, x_2, \ldots, x_n)$

Teorema 61 (Bézout) *Sean a, b dos enteros no nulos.*

Si $g = (a, b)$, entonces existen $x_0, y_0 \in \mathbb{Z}$ tales que

$$g = ax_0 + by_0.$$

Demostración: Consideremos el conjunto

$$A = \{ax + by \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}^*.$$

La considerar $x = a$, e $y = b$, el conjunto es no vacío, luego por el Teorema del Buen Orden (33). El conjunto A posee un primer elemento, el que denotaremos por d.

Ahora bien como $d \in A$, se tiene que existen enteros x_0, y_0 tales que $d = ax_0 + by_0$, luego por el algoritmo de la división $a = qd + r$, con $0 \leq r < d$. Entonces,

$$r = a - qd = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0).$$

Si $r > 0$ entonces $r \in A$, pero $r < d$, lo cual contradice la minimalidad de d, por lo tanto $d|a$. Análogamente se demuestra que $d|b$ y así se obtiene que d es un divisor común de a y b.

Para verificar que d es el mayor divisor común positivo de a y b, sea $t \geq 1$ otro divisor común. Por el teorema (50) parte (3), $t|(ax + by)$, para cualquier $x, y \in \mathbb{Z}$, en particular $t|d$, luego $0 < t \leq d$. □

Corolario 62 *Sean $a, b \in \mathbb{Z}^*$ entonces*

1. $(a, b) = \text{mín}\{ax + by \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}^*$.
2. $(a, b) = (|a|, |b|)$.

Teorema 63 *Sean $a, b, c \in \mathbb{Z}^*$, tales que $a|b$ y $a|c$, entonces $a|(b, c)$*

Demostración: Si $a|b$ y $a|c$, entonces por el teorema (50) parte (3) tenemos que $a|(mb+nc)$, para cualquier par de enteros n, m y luego por el teorema (61), se tiene que $a|(b, c)$ □

Corolario 64 *Sean $a_1, a_2, \cdots, a_n \in \mathbb{Z}^*$ entonces*

1. $(a_1, a_2, \cdots, a_n) = (a_1, (a_2, \cdots, a_n))$.
2. *Existen $x_1, x_2, \cdots, x_n \in \mathbb{Z}$ tales que*

$$(a_1, a_2, \cdots, a_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

Teorema 65 *Para todo $a, b \in \mathbb{Z}^*$, $m \in \mathbb{Z}^+$, se tiene que*

$$(ma, mb) = m(a, b)$$

Demostración: Del corolario (62) tenemos que:

$$\begin{aligned}(ma, mb) &= \text{mín}\{(ma)x + (mb)y > 0 \mid x, y \in \mathbb{Z}\} \\ &= \text{mín}\{m(ax + by) > 0 \mid x, y \in \mathbb{Z}\} \\ &= m \cdot \text{mín}\{ax + by > 0 \mid x, y \in \mathbb{Z}\} \\ &= m(a, b).\end{aligned}$$

□

Ejercicio 24 *Sean $a \in \mathbb{Z}^+$, $b \in \mathbb{Z}^*$ entonces*

$$(a, ab) = a(1, b) = a$$

Corolario 66 *Si $d|a$ y $d|b$, $d > 0$, entonces*

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b).$$

En particular se tiene que $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.

Demostración: El resultado es consecuencia directa del teorema (65) tomando

$$m = d, a = \frac{a}{d} \text{ y } b = \frac{b}{d}.$$

□

Corolario 67 *Si $c|ab$ y $(b, c) = 1$, entonces $c|a$.*

Demostración: Por el teorema (65), tenemos que

$$(ab, ac) = a(b, c) = a. \tag{2.2}$$

Ahora bien como $c|ab$ y $c|ac$, por el teorema (63) tenemos que $c|(ab, ac)$, pero de (2.2) se tiene que $c|a$. □

Definición 17 *Sean a, b dos enteros no ambos nulos. Se dice que a y b son primos relativos si y sólo si $(a, b) = 1$.*

Teorema 68 *Sean a, b, c enteros no ambos nulos. Si $(a, c) = 1$ y $(b, c) = 1$, entonces $(ab, c) = 1$.*

Demostración: Si $(a, c) = 1$ y $(b, c) = 1$, por el teorema (61) obtenemos que existen enteros x_0, x_1, y_0, y_1 tales que

$$\begin{aligned}ax_0 + cy_0 &= 1 \\ bx_1 + cy_1 &= 1,\end{aligned}$$

de donde se obtiene que

$$(ab)(x_0x_1) + c(y_1 + y_0 - cy_0y_1) = 1. \tag{2.3}$$

Por otro lado, sabemos que $(ab, c)|ab$ y $(ab, c)|c$. Luego por el teorema (50) parte (3) se tiene que $(ab, c)|(abx + cy)$, para todo $x, y \in \mathbb{Z}$, en particular para $x = x_0x_1$ e $y = y_1 + y_0 - my_0y_1$. Así

$$(ab, c)|((ab)(x_0x_1) + c(y_1 + y_0 - my_0y_1)),$$

pero por (2.3) obtenemos que $(ab, c)|1$ y en consecuencia que $(ab, c) = 1$. □

Teorema 69 *Para todo $a, b \in \mathbb{Z}^*$, $k \in \mathbb{Z}$, se tiene que*

$$(a, b) = (a, b + ak).$$

Demostración: En primer lugar notemos que $(a, b)|a$ y $(a, b)|b$, ahora bien, por el teorema (50) parte (1), se tiene que $(a, b)|ak$, para todo $k \in \mathbb{Z}$, tenemos así que $(a, b)|ak$ y $(a, b)|b$, luego por el teorema (50) parte (3) obtenemos que $(a, b)|(b + ak)$. De lo anterior tenemos que $(a, b)|a$ y $(a, b)|b + ak$ y por lo tanto

$$(a, b)|(a, b + ak). \tag{2.4}$$

Por otro lado $(a, b + ak)|a$ y $(a, b + ak)|b + ak$, por el teorema (50) parte (1), se tiene que $(a, b + ak)|ak$, para todo $k \in \mathbb{Z}$. En virtud del teorema (50) parte (3), obtenemos que $(a, b + ak)|(b + ak - ak)$. Luego se tiene que $(a, b + ak)|b$ y $(a, b + ak)|a$, con lo cual

$$(a, b + ak)|(a, b). \tag{2.5}$$

Ahora de (2.4) y (2.5) se tiene que $(a, b) = (a, b + ak)$. □

Ejemplo 25 *Calcular $(45, 18)$ y $(72, 15)$*

Solución: En el primer caso

$$(45, 18) = (45 - 18 \cdot 2, 18) = (9, 18) = (9, 9 \cdot 2) = 9(1, 2) = 9.$$

Ene segundo

$$(72, 15) = (72 - 60, 15) = (12, 15) = (12, 3) = 3.$$

♡

Teorema 70 (Algoritmo de Euclides) *Sean a y b enteros, con $a > 0$. Aplicando repetidamente el teorema (51), obtenemos la siguiente secuencia de ecuaciones:*

$$\begin{aligned}
b &= aq_1 + r_1, \quad 0 < r_1 < a \\
a &= r_1q_2 + r_2, \quad 0 < r_2 < r_1 \\
&\vdots \\
r_{j-2} &= r_{j-1}q_j + r_j, \quad 0 < r_j < r_{j-1} \\
r_{j-1} &= r_jq_{j+1.}
\end{aligned}$$

Entonces $(a,b) = r_j$, resto inmediatamente anterior al resto que se anula. Además los valores de x_0 e y_0 tales que

$$(a,b) = ax_0 + by_0$$

pueden ser obtenidos de $r_{j-1}, \ldots, r_2, r_1$ en esta secuencia de ecuaciones.

Demostración: es inmediata de teorema 69, ya que

$$(b,a) = (b - aq_1, a) = (r_1, a) = (r_1, r_2) = \cdots = (r_j, r_{j_1}) = r_j(1, q_{j+1})$$

La segunda parte se obtiene, al despejar los restos y reemplazando recursivamente se obtiene el resultado deseado □

Observación: Veamos el despeje en un ejemplo pequeño. El cálculo anterior se realiza despejando y reemplazando, para ello lo haremos en el siguiente ejemplo

$$\begin{aligned} b &= aq_1 + r_1, \quad 0 < r_1 < a \\ a &= r_1q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2 \\ r_2 &= r_3q_4 + 0 \end{aligned}$$

$$\begin{aligned} r_3 &= r_1 - r_2q_3 \text{ reemplazo } r_2 \\ &= r_1 - (a \cdot 1 - r_1q_2)q_3 \text{reordenado} \\ &= a \cdot (-q_3) + r_1(1 + q_2q_3) \text{ reemplazo } r_1 \\ &= a \cdot (-q_3) + (b - aq_1)(1 + q_2q_3) \text{reordenado} \\ &= a(-q_3 - q_1 - q_1q_2q_3) + b(1 + q_2q_3) \end{aligned}$$

de otro modo

$$\begin{pmatrix} b & 1 & 0 \\ a & 0 & 1 \end{pmatrix} \underset{F_{21}(-q_1)}{\sim} \begin{pmatrix} r_1 & 1 & -q_1 \\ a & 0 & 1 \end{pmatrix} \underset{F_{12}(-q_2)}{\sim} \begin{pmatrix} r_1 & 1 & -q_1 \\ r_2 & -q_2 & 1 + q_1q_2 \end{pmatrix}$$

$$\underset{F_{21}(-q_3)}{\sim} \begin{pmatrix} r_3 & 1 + q_2q_3 & -q_1 - q_3 - q_1q_2q_3 \\ r_2 & -q_2 & 1 + q_1q_2 \end{pmatrix} \underset{F_{12}(-q_4)}{\sim} \begin{pmatrix} r_3 & 1 + q_2q_3 & -q_1 - q_3 - q_1q_2q_3 \\ 0 & * & * \end{pmatrix}$$

Ejemplo 26 *Encontrar el máximo común divisor (MCD) en cada caso*

a) $(5, 19)$ Apliquemos el algoritmo de la división

$$\begin{aligned} 19 = 5 \cdot 3 + 4 \quad &\text{o bien} \quad 4 = 19 - 5 \cdot 3 \\ 5 = 4 \cdot 1 + 1 \quad &\text{o bien} \quad 1 = 5 - 4 \cdot 1 \\ 4 = 1 \cdot 4 + 0 \end{aligned}$$

Por lo tanto $(5, 19) = 1$. Además

$$1 = 5(1) - 4(1) = 5(1) - (19 - 5 \cdot 3)(1) = 19(-1) + 5(1 + 3) = 19(-1) + 5(4)$$

b) $(2,5,19)$ Para ello $(2,5,19) = (2,(5,19)) = (2,1) = 1$ Por lo tanto $(2,5,19) = 1$

c) $(5748,-7207)$

Para determinar el MCD no se considera los signos corolario 62.

$$\begin{aligned}
7207 &= 5748\cdot 1 + 1459 \quad \text{o bien} \quad 1459 = 7207 - 5748\cdot 1\\
5748 &= 1459\cdot 3 + 1371 \quad \text{o bien} \quad 1371 = 5748 - 1459\cdot 3\\
1459 &= 1371\cdot 1 + 88 \quad \text{o bien} \quad 88 = 1459 - 1371\cdot 1\\
1371 &= 88\cdot 15 + 51 \quad \text{o bien} \quad 51 = 1371 - 88\cdot 15\\
88 &= 51\cdot 1 + 37 \quad \text{o bien} \quad 37 = 88 - 51\cdot 1\\
51 &= 37\cdot 1 + 14 \quad \text{o bien} \quad 14 = 51 - 37\cdot 1\\
37 &= 14\cdot 2 + 9 \quad \text{o bien} \quad 9 = 37 - 14\cdot 2\\
14 &= 9\cdot 1 + 5 \quad \text{o bien} \quad 5 = 14 - 9\cdot 1\\
9 &= 5\cdot 1 + 4 \quad \text{o bien} \quad 4 = 9 - 5\cdot 1\\
5 &= 4\cdot 1 + 1 \quad \text{o bien} \quad 1 = 5 - 4\cdot 1\\
4 &= 1\cdot 4
\end{aligned}$$

Por lo tanto $(5748,-7207) = 1$

Observación: La aritmética anterior se puede reescribir del siguiente modo

$$\begin{pmatrix} 7207 & 1 & 0\\ 5748 & 0 & 1\end{pmatrix} \underset{F_{21}(-1)}{\sim} \begin{pmatrix} 1459 & 1 & -1\\ 5748 & 0 & 1\end{pmatrix} \underset{F_{12}(-3)}{\sim} \begin{pmatrix} 1459 & 1 & -1\\ 1371 & -3 & 4\end{pmatrix}$$
$$\underset{F_{21}(-1)}{\sim} \begin{pmatrix} 88 & 4 & -5\\ 1371 & -3 & 4\end{pmatrix} \underset{F_{12}(-15)}{\sim} \begin{pmatrix} 88 & 4 & -5\\ 51 & -63 & 79\end{pmatrix}$$
$$\underset{F_{21}(-1)}{\sim} \begin{pmatrix} 37 & 67 & -84\\ 51 & -63 & 79\end{pmatrix} \underset{F_{12}(-1)}{\sim} \begin{pmatrix} 37 & 67 & -84\\ 14 & -130 & 163\end{pmatrix}$$
$$\underset{F_{21}(-2)}{\sim} \begin{pmatrix} 9 & 327 & -410\\ 14 & -130 & 163\end{pmatrix} \underset{F_{12}(-1)}{\sim} \begin{pmatrix} 9 & 327 & -410\\ 5 & -457 & 573\end{pmatrix}$$
$$\underset{F_{21}(-1)}{\sim} \begin{pmatrix} 4 & 784 & -983\\ 5 & -457 & 573\end{pmatrix} \underset{F_{12}(-1)}{\sim} \begin{pmatrix} 4 & 784 & -983\\ 1 & -1241 & 1556\end{pmatrix}$$
$$\underset{F_{21}(-1)}{\sim} \begin{pmatrix} 0 & * & *\\ 1 & -1241 & 1556\end{pmatrix}$$

Note que

$$(-1241)\cdot(7207) + (1556)\cdot(5748) = 1 \text{ o bien } (1241)\cdot(-7207) + (1556)\cdot(5748) = 1$$

2.6. Números Primos

Definición 18 *Sea $p \in \mathbb{Z}$, tal que $p \notin \{-1,0,1\}$*

Se dice que p es número primo, si y sólo si los únicos divisores dde él son ± 1 y $\pm p$. En caso contrario se dice que p es un número compuesto.

Ejemplo 27 *Algunos primos positivos son*

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31, \cdots$$

No se conoce la formula general de esta sucesión, pero son infinitos.

Propiedad 71 *Sean $a, b, p \in \mathbb{Z}^*$, tal que p es primo*

$$\textit{Si } p|ab \textit{ entonces } p|a \textit{ o } p|b$$

Demostración: Si p divide a a listo. Por ello suponemos que p no divide a a, entonces p y a son primos relativos y por la Teorema 61 existen x e y enteros tales que $px + ay = 1$. Multiplicando por b se obtiene $pbx + aby = b$, y puesto que los dos sumandos del lado izquierdo son divisibles por p, el término de la derecha también es divisible por p. □

Teorema 72 (Fundamental de la Aritmética) *Todo numero entero positivo mayor que uno, puede ser escrito como producto de números primos positivos. Más aún, dicha factorización es única salvo el orden de los factores.*

Demostración:

Existencia de la descomposición: Suponemos que existe algún entero positivo que no puede representarse como producto de primos. Entonces debe haber un mínimo número n con esa propiedad (principio del Buen Orden). Este número n no puede ser 1, por la convención anterior. Tampoco puede ser un primo, porque todo primo es el producto de un único número primo: él mismo. Así pues, $n = ab$, donde a y b son enteros positivos menores que n. Como n es el mínimo entero positivo para el que falla el teorema, tanto a como b pueden escribirse como producto de primos. Pero entonces $n = ab$ también puede escribirse como producto de primos, lo que es contradictorio.

Unicidad de la descomposición: Dados dos productos de primos que tengan igual resultado, tómese un primo p del primer producto. Divide al primer producto, y por lo tanto también al segundo. Por la propiedad anterior, p debe dividir al menos a un factor del segundo producto; pero los factores son todos primos, así que p debe ser igual a uno de los factores del segundo producto. Se puede entonces cancelar a p de ambos productos. Siguiendo de esta forma se cancelarán todos los factores de ambos productos, con lo cual éstos deben coincidir exactamente □

Teorema 73 *Existen infinitos números primos.*

Demostración: Supongamos que existe sólo una cantidad finita de números primos, digamos $p_1, p_2, \ldots, p_n$.

Consideremos el número

$$P = p_1 \cdot p_2 \cdots p_n + 1.$$

Es claro que $P > p_j$, para $1 \leq j \leq n$, luego P no es primo. Por otra parte P no es divisible por ninguno de los p_j, para $1 \leq j \leq n$, pero por el teorema (72), P debe ser divisible por algún primo, lo cual es claramente una contradicción.

Propiedad 74 *Sea a un entero positivo tal que para todo primo $p \leq \sqrt{a}$ no se cumple $p|a$, entonces a es primo*

Demostración: Supongamos que a es un número compuesto, es decir, tal que no es divisible por algún primo p, con $p \leq \sqrt{a}$ y $a = b \cdot c$ con $1 < b < a,\ 1 < c < a$.

Podemos suponer sin perdida de generalidad que $b \leq c$. multiplicando por b obtenemos

$$b^2 \leq b \cdot c = a.$$

Luego $b \leq \sqrt{a}$. Pero esto es una contradicción porque:

Si b es primo llegamos a una contradicción por suponer que a no es divisible por algún primo $p \leq \sqrt{a}$.

Si b es compuesto llegamos a una contradicción, pues b compuesto podría expresarse como producto de primos, y siendo p uno de ellos: $b|a$, $p|b$ por lo tanto $p|a$, siendo $p < b \leq \sqrt{a}$. Luego a es primo. □

Ejemplo 28 $\sqrt{19} = 4,35\cdots$, *inspeccione con* 2 *y* 3 *como ninguno lo divide, entonces* 19 *es primo*

Propiedad 75 *Sean $a, b \in \mathbb{Z}^+$ tales que*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},\ b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$$

con p_i primos distintos $\alpha_i,\ \beta_i \in \mathbb{N}_0$, entonces

$$(a, b) = p_1^{\text{mín}\{\alpha_1,\beta_1\}} p_2^{\text{mín}\{\alpha_2,\beta_2\}} \cdots p_n^{\text{mín}\{\alpha_n,\beta_n\}}$$

Demostración: Sabemos que $a = (a, b)k_1,\ b = (a, b)k_2$, luego en (a, b), los únicos primos que pueden aparecer en la descomposición son los primos p_i. Por lo tanto

$$(a, b) = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$$

De la primera ecuación tenemos que

$$\alpha_i = \lambda_i + \gamma_i,\ \beta_i = \lambda_i + \gamma_i',$$

es decir,

$$\alpha_i \geq \lambda_i,\ \beta_i \geq \lambda_i,$$

de lo cual, se tiene

$$\text{mín}\{\alpha_i, \beta_i\} \geq \lambda_i,$$

Como (a, b) es el máximo con es condición, se obtiene que

$$(a, b) = p_1^{\text{mín}\{\alpha_1,\beta_1\}} p_2^{\text{mín}\{\alpha_2,\beta_2\}} \cdots p_n^{\text{mín}\{\alpha_n,\beta_n\}}$$

□

Ejemplo 29 *Sea p un número primo. Demostrar que si $p|a \ \wedge\ p|(a^2 + b^2)$ entonces $p|b$*

Solución: Sabemos que $p|a$ luego tenemos que $p|a^2$, así $p|a^2 \wedge p|(a^2+b^2)$ de lo cual obtenemos que

$$p|(a^2+b^2)-a^2$$

Por ende tenemos que $p|b^2$, de este modo en la descomposición en primo de b tiene que estar el primo p, por lo tanto $p|b$

Observación: Note que si $a^2+b^2=c^2$, el ejemplo anterior, nos dice que:

Si $p|a \wedge p|c$ entonces $p|b$.

Además si se define $a=x^2-y^2, b=2x^2y^2, c=x^2+y^2$ entonces son ternas pitagóricas

2.7. Mínimo Común Múltiplo

Definición 19 (Múltiplo Común) *Sean $a,b,c \in \mathbb{Z}$.*

Se dice que c es un múltiplo común de a y b si $a|c$ y $b|c$.

En general dados $x_1,x_2,\ldots,x_n \in \mathbb{Z}$, se dice que a es un múltiplo común de $x_1,x_2,\ldots,x_n$ si y sólo si $x_1|a \wedge x_2|a \wedge \cdots \wedge x_n|a$.

Definición 20 (Mínimo Común Múltiplo) *Sean $a,b \in \mathbb{Z}^*$.*

El mínimo común múltiplo entre a y b, es el menor múltiplo común positivo de a y b, el cual denotaremos por $[a,b]$.

En general dados $x_1,x_2,\ldots,x_n \in \mathbb{Z}^*$, el mínimo común múltiplo de $x_1,x_2,\ldots,x_n$ es el menor múltiplo común de $x_1,x_2,\cdots,x_n$, el cual denotamos por $[x_1,x_2,\ldots,x_n]$

Propiedad 76 *Sean $a,b \in \mathbb{Z}^*$ entonces*

$$[a,b]=[|a|,|b|].$$

Propiedad 77 *Sean $a,b \in \mathbb{Z}^+$ tales que*

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n},\ b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$$

con p_i primos distintos $\alpha_i,\ \beta_i \in \mathbb{N}_0$, entonces

$$[a,b]=p_1^{\text{máx}\{\alpha_1,\beta_1\}}p_2^{\text{máx}\{\alpha_2,\beta_2\}}\cdots p_n^{\text{máx}\{\alpha_n,\beta_n\}}$$

Demostración: Sabemos que $[a,b]=ak_1,\ [a,b]=bk_2$, luego en $[a,b]$, a lo menos aparecer en la descomposición los primos p_i. Por lo tanto

$$(a,b)=p_1^{\lambda_1}p_2^{\lambda_2}\cdots p_n^{\lambda_n}c$$

con c, tal que $(c,p_i)=1$.

De la primera ecuación tenemos que

$$\lambda_i=\alpha_i+\gamma_i,\ \lambda_i=\beta_i+\gamma_i',$$

es decir,

$$\lambda_i \geq \alpha_i,\ \lambda_i \geq \beta_i,$$

de lo cual, se tiene

$$\lambda_i \geq \text{máx}\{\alpha_i, \beta_i\},$$

Como $[a, b]$ es el mínimo con es condición, se obtiene que $c = 1$ y

$$[a, b] = p_1^{\text{máx}\{\alpha_1,\beta_1\}} p_2^{\text{máx}\{\alpha_2,\beta_2\}} \cdots p_n^{\text{máx}\{\alpha_n,\beta_n\}}$$

□

Propiedad 78 *Si m es múltiplo común de a y b, entonces $[a, b]|m$.*

Propiedad 79 *Sean $a_1, a_2, \cdots, a_n \in \mathbb{Z}^*$ entonces*

$$[a_1, a_2, \cdots, a_n] = [a_1, [a_2, \cdots, a_n]]$$

Teorema 80 *Si a, b son enteros no nulos,*

$$[a, b] = \frac{|ab|}{(a, b)}.$$

Corolario 81 *Sea $m \in \mathbb{Z}^+$, entonces $[ma, mb] = m[a, b]$.*

Demostración: Del teorema (80), tenemos que

$$[ma, mb] = \frac{|mamb|}{(ma, mb)} = m^2 \frac{|ab|}{(ma, mb)},$$

luego por el teorema (65) se tiene que $(ma, mb) = m(a, b)$, así obtenemos que

$$[ma, mb] = m\frac{|ab|}{(a, b)} = m[a, b].$$

□

Ejemplo 30 *Encontrar el mínimo común múltiplo MCM de:*

a) $[10, 18]$

Calculemos el máximo común divisor

$$\begin{pmatrix} 18 & 1 & 0 \\ 10 & 0 & 1 \end{pmatrix} \underset{F_{21}(-1)}{\sim} \begin{pmatrix} 8 & 1 & -1 \\ 10 & 0 & 1 \end{pmatrix} \underset{F_{12}(-1)}{\sim} \begin{pmatrix} 8 & 1 & -1 \\ 2 & -1 & 2 \end{pmatrix} \underset{F_{21}(-4)}{\sim} \begin{pmatrix} 0 & * & * \\ 2 & -1 & 2 \end{pmatrix}$$

Luego

$$(10, 18) = 2 \text{ y } 18(-1) + 10(2) = 2$$

Como

$$[10, 18] = \frac{|10 \cdot 18|}{(10, 18)} = \frac{180}{2} = 90$$

Por lo tanto $[10, 18] = 90$

b) $[-2, 3, 18]$.

Veamos primero

$$[-2, 3, 18] = [-2, [3, 18]] = [-2, 18] = 18$$

Ya que

$$\begin{aligned} 18 &= 3 \cdot 6 + 0 \\ [3, 18] &= \frac{|3 \cdot 18|}{3} = 18 \end{aligned}$$

Además

$$\begin{aligned} 18 &= 2 \cdot 9 + 0 \\ [-2, 18] &= \frac{|-2 \cdot 18|}{(-2, 18)} = 18 \end{aligned}$$

2.8. Ecuaciones Diofánticas Lineales

El nombre de ecuaciones diofánticas proviene de Diofanto (Matemático de la antigua Grecia), y su origen está ligado a la siguiente pregunta: ¿Cuantos números naturales son necesarios para expresar un número natural cualquiera como suma de cuadrados $n = x^2 + y^2 + z^2 ...$?.

Note que

$$3 = x^2 + y^2 \qquad 7 = x^2 + y^2 + z^2$$

no tiene soluciones en los enteros

La respuesta que los antiguos griegos dieron a esta pregunta fue:

"siempre es posible, si el número de términos es cuatro´´

Definición 21 *Una ecuación diofántica lineal, es una ecuación de la forma*

$$ax + by = c,$$

donde x, y son incógnitas y $a, b \in \mathbb{Z}^*, c \in \mathbb{Z}$. El conjunto solución es

$$S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid ax + by = c \}$$

En general, sean $a_1, a_2, a_3, ...a_n \in \mathbb{Z}^*$ y $b \in \mathbb{Z}$, con $x_1, x_2, x_3, ...x_n$ incógnitas entonces la ecuación

$$a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n = b$$

es llamada ecuación diofántica lineal. El conjunto solución es

$$S = \{x \in \mathbb{Z}^n \mid a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n = b \}$$

Teorema 82 *$a_1, a_2, a_3, ...a_n \in \mathbb{Z}^*$ y $b \in \mathbb{Z}$. La ecuación*

$$a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n \quad = \quad b, \tag{2.6}$$

tiene solución en $\mathbb{Z}$ si y sólo si $(a_1, a_2, a_3, \cdots, a_n)|b$.

Demostración: Supongamos que $(a_1, a_2, a_3, \cdots, a_n) \mid b$, entonces existe k tal que $b = (a_1, a_2, a_3, \cdots, a_n)k$, además existe $y_1, y_2, \cdots, y_n$ enteros tales que

$$a_1y_1 + a_2y_2 + a_3y_3 + \cdots + a_ny_n = (a_1, a_2, a_3, \cdots, a_n)$$

Amplificando, obtenemos

$$a_1(y_1k) + a_2(y_2k) + a_3(y_3k) + \cdots + a_n(y_nk) = (a_1, a_2, a_3, \cdots, a_n)k = b$$

luego la ecuación tiene solución.

Supongamos que tiene solución enteras de (2.6), luego existe $z_1, z_2, \cdots, z_n$ enteros tales que

$$a_1z_1 + a_2z_2 + a_3z_3 + \cdots + a_nz_n = b$$

Pero por teorema (50), tenemos que $(a_1, a_2, a_3, \cdots, a_n)|(a_1z_1 + a_2z_2 + a_3z_3 + \cdots + a_nz_n)$, luego $(a_1, a_2, a_3, \cdots, a_n)|b$. □

Teorema 83 *Sean $a, b \in \mathbb{Z}^*, c \in \mathbb{Z}$. La ecuación*

$$ax + by \quad = \quad c, \tag{2.7}$$

Si (2.7) es soluble y $x_0, y_0 \in \mathbb{Z}$ es una solución, entonces todas las soluciones están dadas por

$$x = x_0 - \frac{tb}{(a,b)} \quad \wedge \quad y = y_0 + \frac{ta}{(a,b)},$$

donde t recorre todos los enteros.

De otro modo

$$S = \left\{ \left(x_0 - \frac{tb}{(a,b)}, y_0 + \frac{ta}{(a,b)} \right) \in \mathbb{Z}^2 \mid t \in \mathbb{Z} \right\}$$

Demostración:

Sea $m = (a, b)$ y que x, y es otra solución, además de x_0, y_0. Entonces

$$ax_0 + by_0 = c = ax + by,$$

así

$$a(x_0 - x) = b(y - y_0) \quad \Leftrightarrow \quad \frac{a}{m}(x_0 - x) = \frac{b}{m}(y - y_0). \tag{2.8}$$

Luego por el corolario (66) tenemos que $\left(\frac{a}{m}, \frac{b}{m}\right) = 1$, ahora bien por el corolario (67), obtenemos que

$$\frac{b}{m}|(x_0 - x) \quad \text{y} \quad \frac{a}{m}|(y - y_0). \tag{2.9}$$

Así, de (2.8) y (2.9) se tiene que existe un entero t tal que

$$x_0 - x = \frac{tb}{m} \quad \wedge \quad y - y_0 = \frac{ta}{m},$$

es decir

$$x = x_0 - \frac{tb}{m} \quad \wedge \quad y = y_0 + \frac{ta}{m}. \tag{2.10}$$

Claramente para cualquier $t \in \mathbb{Z}$, (2.10) define una solución de (2.7). Para ver esto basta reemplazar los valores de x e y en (2.7) con lo cual se obtiene una tautología. □

Ejemplo 31 *Determinar la solución general de la ecuación diofántica lineal*

$$10 \cdot x - 32 \cdot y = 2.$$

Solución: Determinemos el máximo común divisor

$$\begin{aligned} 32 &= 10 \cdot 3 + 2 \\ 10 &= 2 \cdot 5 \end{aligned}$$

Por lo tanto $(10, 32) = 2$, de lo cual tenemos

$$\begin{aligned} 2 &= 32 - 10 \cdot 3 \\ 2 &= 10 \cdot (-3) - 32 \cdot (-1) \end{aligned}$$

es decir, $x_0 = -3$, $y_0 = -1$ es una solución particular

La solución general es:

$$x = -3 - \frac{32}{2} \cdot t \ \wedge \ y = -1 - \frac{10}{2} \cdot t \quad \forall t \in \mathbb{Z}$$

El conjunto solución de la ecuación diofántica es

$$S = \{(-3 - 16 \cdot t \ , \ -1 - 5 \cdot t) \mid t \in \mathbb{Z}\}$$

Propiedad 84 *Sean $a_1, a_2, a_3, ...a_n \in \mathbb{Z}^*$ y $b \in \mathbb{Z}$, tal que $(a_1, a_2) = 1 = a_1 z_1 + a_2 z_2$.*

La ecuación diofántica

$$a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n = b,$$

es soluble y las soluciones son

$$\begin{aligned} x_1 &= z_1(b - a_3x_3 - a_4x_4 \cdots - a_nx_n) + a_2t \\ x_2 &= z_2(b - a_3x_3 - a_4x_4 \cdots - a_nx_n) - a_1t \end{aligned}$$

con $t, x_3, x_4, x_5, ...x_n \in \mathbb{Z}$.

Ejemplo 32 *Determinar la solución general de la ecuación diofántica lineal*

$$10x + 7y + 5z = 2.$$

Solución: Note que la ecuación es igual a

$$7y + 5z = 2 - 10x.$$

El máximo común divisor, entre 5 y 7 es 1, para ello

$$\begin{aligned} 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

Por lo tanto

$$5(3) + 7(-2) = 1$$

Amplificando por $2 - 10x$, tenemos una solución particular

$$5(6 - 30x) + 7(-4 + 20x) = 2 - 10x$$

La solución general es:

$$y = 6 - 30x - 7t \ \wedge \ z = -4 + 20x - 5t \qquad \forall t \in \mathbb{Z}$$

El conjunto solución de la ecuación diofántica es

$$S = \{(x, 6 - 30x - 7t \ , \ -4 + 20x - 5t) \mid x, t \in \mathbb{Z}\}$$

Propiedad 85 *Sean $a_1, a_2, a_3, ...a_n \in \mathbb{Z}^*$ y $b \in \mathbb{Z}$, tal que $(a_1, a_2) = d = a_1 z_1 + a_2 z_2$ y $(a_1, a_2, \cdots, a_n) = 1$.*

La ecuación diofántica

$$a_1 x_1 + a_2 x_2 + a_3 x_3 + \cdots + a_n x_n \ = \ b,$$

se resuelve usando la variable auxiliar x_0 y

$$\begin{aligned} x_1 &= z_1 x_0 + \tfrac{a_2}{d} t \\ x_2 &= z_2 x_0 - \tfrac{a_1}{d} t \\ d x_0 + a_3 x_3 + \cdots + a_n x_n &= b \end{aligned}$$

con $t, x_3, x_4, x_5, ...x_n \in \mathbb{Z}$.

Ejemplo 33 *Determinar la solución general de la ecuación diofántica lineal*

$$10x + 6y + 15z = 13.$$

Solución: Note que la ecuación es igual a

$$10x + 6y = 13 - 15z$$

Como el máximo común divisor, entre 10 y 6 es 2, luego existe r entero (variable auxiliar) tal que

$$10x + 6y = 2r = 13 - 15z$$

es decir

$$\begin{array}{|rcl} 10x + 6y & = & 2r \\ 13 - 15z & = & 2r \\ \hline \end{array}$$

Para la primera ecuación, una solución particular al máximo común divisor es

$$10(-1) + 6(2) = 2$$

amplificando obtenemos

$$10(-r) + 6(2r) = 2r$$

Y la solución es

$$\begin{array}{rcl} x & = & -r + 3t \\ y & = & 2r - 5t \end{array}$$

con $t \in \mathbb{Z}$.

La otra ecuación es

$$2r + 15z = 13$$

Una solución particular es $r = -1,\ z = 1$. Luego la general esta dada por:

$$\begin{array}{rcl} r & = & -1 + 15u \\ z & = & 1 - 2u \end{array}$$

con $u \in \mathbb{Z}$.

Reemplazando la variable auxiliar obtenemos

$$\begin{array}{rcl} x & = & 1 - 15u + 3t \\ y & = & -2 + 30u - 5t \\ z & = & 1 - 2u \end{array}$$

con $t, u \in \mathbb{Z}$.

$$S = \{(1 - 15u + 3t,\ -2 + 30u - 5t,\ 1 - 2u) \mid u, t \in \mathbb{Z}\}$$

Ejemplo 34 *Determinar la solución general de la ecuación diofántica lineal*

$$10x + 6y + 15z + 70w = 13.$$

Solución: Notemos que $(10,6)=2,\ (15,70)=5$. Consideremos las variables auxiliares u,l

$$\begin{aligned} 10x+6y &= 2u \\ 15z+70w &= 5l \end{aligned}$$

Reemplazando obtenemos $2u+5l=13$.

Para resolver las ecuaciones notemos que

$$10(-1)+6(2)=2\ \ 15(5)+70(-1)=5$$

amplificando obtenemos

$$10(-u)+6(2u)=2u\ \ 15(5l)+70(-l)=5l$$

Y la solución es

$$\begin{aligned} x &= -u+3t \\ y &= 2u-5t \\ z &= 5l+14r \\ w &= -l-3r \end{aligned}$$

Además las soluciones de $2u+5l=13$, son

$$\begin{aligned} u &= -1+5q \\ l &= 3-2q \end{aligned}$$

Reemplazando las variables auxiliares obtenemos,

$$\begin{aligned} x &= 1-5q+3t \\ y &= -2+10q-5t \\ z &= 15-10q+14r \\ w &= -3+2q-3r \end{aligned}$$

con $t,q,r\in\mathbb{Z}$.

$$S=\{(1-5q+3t,\ -2+10q-5t,\ 15-10q+14r,\ -3+2q-3r)\mid t,q,r\in\mathbb{Z}\}$$

2.9. Ejercicios Desarrollados

Ejemplo 35 *Demostrar que el cuadrado de cualquier entero de la forma* $5\cdot k+1$ *es de la misma forma.*

Solución:

$$\begin{aligned} (5\cdot k+1)^2 &= 25\cdot k^2+10\cdot k+1 \\ &= 5\cdot(5\cdot k^2+2\cdot k)+1 \\ &= 5\cdot r+1;\quad r=5\cdot k^2+2\cdot k \end{aligned}$$

Ejemplo 36 *Demostrar que el cuadrado de un entero impar es de la forma* $8 \cdot k + 1$.

Solución: Sea n un número impar entonces $n = 2 \cdot k + 1; \quad k \in \mathbb{Z}$
Por demostrar que $n^2 = 8 \cdot k' + 1$

$$\begin{aligned} n^2 &= (2 \cdot k + 1)^2 \\ &= 4 \cdot k^2 + 4 \cdot k + 1 \\ &= 4 \cdot k \cdot (k + 1) + 1 \end{aligned}$$

Recuerde que ($2|n \cdot (n + 1)$) o bien $(\forall n \in \mathbb{Z})(\exists r \in \mathbb{Z}) n \cdot (n + 1) = 2 \cdot r$), reemplazando obtenemos

$$\begin{aligned} n^2 &= 4 \cdot 2 \cdot r + 1 \\ &= 8 \cdot r + 1 \end{aligned}$$

Ejemplo 37 *Si* $a|b$ *y* $b|c$ *entonces* $a|c$.

Solución: $a|b \Leftrightarrow (\exists q \in \mathbb{Z})(b = a \cdot q)$ y $b|c \Leftrightarrow (\exists k \in \mathbb{Z})(c = b \cdot k)$.
Por demostrar que $a|c \Leftrightarrow (\exists r \in \mathbb{Z})(c = a \cdot r)$.

$$\begin{aligned} c &= b \cdot k \\ &= a \cdot q \cdot k \end{aligned}$$

Por lo tanto $a|c$

Ejemplo 38 *Si* $(b \cdot c)|a$ *entonces* $b|a$ *y* $c|a$.

Solución: $(b \cdot c)|a \Leftrightarrow a = b \cdot c \cdot q; \quad q \in \mathbb{Z}$
Por demostrar que $(b|a \Leftrightarrow a = b \cdot r;\ r \in \mathbb{Z})$ y $(c|a \Leftrightarrow a = c \cdot s;\ s \in \mathbb{Z})$

$$\begin{aligned} a &= b \cdot c \cdot q \\ &= b \cdot r; \quad r = c \cdot q \end{aligned}$$

Por lo tanto $b|a$
De igual manera

$$\begin{aligned} a &= b \cdot c \cdot q \\ &= c \cdot b \cdot q \\ &= c \cdot s; \quad s = b \cdot q \end{aligned}$$

Por lo tanto $c|a$.

Ejemplo 39 *Si* $(a, b \cdot c) = 1$ *entonces* $(a, b) = 1$ *y* $(a, c) = 1$.

Solución: $(a, b \cdot c) = 1 \Leftrightarrow$ existen $x, y \in \mathbb{Z}$ tal que $1 = a \cdot x + b \cdot c \cdot y$

Por demostrar que $((a, b) = 1 \Leftrightarrow \exists x_0, y_0 \in \mathbb{Z}$ tal que $1 = a \cdot x_0 + b \cdot y_0)$ y $((a, c) = 1 \Leftrightarrow \exists x_1, y_1 \in \mathbb{Z}$ tal que $1 = a \cdot x_1 + c \cdot y_1)$

$$\begin{aligned} 1 &= a \cdot x + b \cdot c \cdot y \\ &= a \cdot x + b \cdot y_0; \quad y_0 = c \cdot y \end{aligned}$$

Por lo tanto $(a, b) = 1$

$$\begin{aligned} 1 &= a \cdot x + b \cdot c \cdot y \\ &= a \cdot x + c \cdot b \cdot y \\ &= a \cdot x + c \cdot y_0; \quad y_0 = b \cdot y \end{aligned}$$

Por lo tanto $(a, c) = 1$

Ejemplo 40 *Si $a|c$, $b|c$ y $(a, b) = 1$ entonces $(a \cdot b)|c$.*

Solución: Por hipótesis tenemos que $(a, b) = 1 \Leftrightarrow$ existen $x_0, y_0 \in \mathbb{Z}$ tal que $1 = a \cdot x_0 + b \cdot y_0$, $a|c \Leftrightarrow c = a \cdot r; \quad r \in \mathbb{Z}$, $b|c \Leftrightarrow c = b \cdot s; \quad s \in \mathbb{Z}$

Por demostrar que $a \cdot b|c \Leftrightarrow c = a \cdot b \cdot k; \quad k \in \mathbb{Z}$

$$\begin{aligned} 1 &= a \cdot x + b \cdot y \quad / \cdot c \\ c &= c \cdot a \cdot x + c \cdot b \cdot y \\ &= a \cdot b \cdot s \cdot x + b \cdot a \cdot r \cdot y \\ &= a \cdot b \cdot (s \cdot x + r \cdot y) \\ &= a \cdot b \cdot k; \quad k = s \cdot x + r \cdot y \end{aligned}$$

Por lo tanto $a \cdot b|c$

Ejemplo 41 *Determinar todos los $x, y \in \mathbb{Z}$ que cumplan con: $x + y = 100$ y $(x, y) = 3$*

Solución: $(x, y) = 3 \Leftrightarrow 3|x$ y $3|y$

$3|x \Leftrightarrow x = 3 \cdot q; \quad q \in \mathbb{Z}$; $3|y \Leftrightarrow y = 3 \cdot k; \quad k \in \mathbb{Z}$

$$\begin{aligned} x + y &= 3 \cdot q + 3 \cdot k \\ 100 &= 3 \cdot (q + k) \end{aligned}$$

Luego $3|100$, lo que es contradictorio, por lo tanto no existen $x \in \mathbb{Z}$ tal que $x + y = 100$ y $(x, y) = 3$

Ejercicio 42 *Sean $a, b, c \in \mathbb{Z}^*$, tales que $(a, b) = (a, c) = (b, c) = 1$ y $a^2 + b^2 = c^2$.*

Demostrar que

1. *si a es par entonces $(c - b, c + b) = 2$*
2. *si a es impar entonces $(c - a, c + a) = 2$*

3. *Si* $a = 2x,\ c+b = 2y,\ c-b = 2z, (y,z) = 1$ *entonces existe* u, v *tales que* $y = u^2 \wedge z = v^2$
4. *Si* $a = 2x,\ c+b = 2u^2,\ c-b = 2v^2$ *entonces* $c = u^2+v^2,\ b = u^2-v^2,\ a = 2u^2v^2$

Ejercicio 43 *Resolver la siguientes ecuaciones diofánticas*

1. $3x + 5y = 7$
2. $135x + 142y = 7$
3. $442x + 663y = 13$
4. $1527x - 3452y = 21$
5. $3x + 5y + 7z = 123$
6. $13x + 15y + 7z = 12$
7. $135x + 142y + 726z = 41$
8. $442x + 663y - 221z = 629$
9. $10x + 6y + 15z = 213$
10. $273x + 195y + 105z = 57$