Capítulo

1

Los Números Enteros

1.1 Introducción

En este capítulo nos dedicaremos al estudio de los números enteros los cuales son el punto de partida de toda la teoría de números. Estudiaremos una serie de propiedades básicas de este conjunto, que son fundamentales para el posterior desarrollo de esta materia, como lo son el algoritmo de la división y el teorema de la factorización única.

Advertimos al lector sobre la necesidad de estudiar cuidadosamente el material expuesto en todas estas secciones de este capítulo, antes de pasar a los siguientes.

El enfoque usado en estas notas consiste en exponer inicialmente las propiedades básicas de los enteros, y a partir de éstas, ir deduciendo propiedades más avanzadas, como proposiciones, teoremas,..etc. En ningún momento nos planteamos dar un tratamiento formal y riguroso del tema de los números enteros, cosa que esta fuera del alcance de este curso. Para un estudio completo acerca de la construcción de los enteros a partir de los naturales, ver [**?**].

1.2 Definiciones Básicas

Supondremos que el lector está familiarizado con la notación de conjunto y además maneja los conceptos de pertenencia, inclusión, unión e intersección.

Definición 1.2.1 *Sean A y B dos conjuntos, una* **función de A en** *B, es una ley que asocia a cada elemento a de A, un único elemento b de B.*

Usamos la letra f para indicar la función, o bien el símbolo $f : A \longrightarrow B$. El elemento b se llama la **imagen** de a bajo la función f, y será denotada por $f(a)$.

Definición 1.2.2 *Sea $f : A \longrightarrow B$ una función y E un subconjunto de A, entonces la* **Imagen de E** *bajo f es el conjunto*

$$f(E) = \{b \in B \mid b = f(c), \text{ para algún } c \text{ en } E\}.$$

Es claro que $f(E)$ es un subconjunto de B.

Definición 1.2.3 *Sea $f : A \longrightarrow B$ una función y G es un subconjunto de B, la* **imagen inversa de G** *bajo f es el conjunto*

$$f^{-1}(G) = \{d \in A \mid f(d) \in G\}.$$

Definición 1.2.4 *Una función $f : A \longrightarrow B$ se dice* **Inyectiva** *si para todo b en B, $f^{-1}(\{b\})$ posee a lo sumo un elemento.*

Observación: Otra forma de definir la inyectividad de una función es la siguiente: Si cada vez que tengamos un par de elementos a y b en A, entonces si estos elementos son diferentes, sus imágenes deben ser diferentes.

Ejemplo: La función $F : \mathbb{N} :\longrightarrow \mathbb{N}$, donde $\mathbb{N}$ denota al conjunto de los números naturales, dada por $F(n) = 2n$, es inyectiva. ¿Podría el lector dar una demostración de este hecho?

Definición 1.2.5 *Sea $f : A \longrightarrow B$ una función. Diremos que f es* **Sobreyectiva** *si $f(A) = B$.*

Observación: El conjunto imagen de A, se llama también el **rango de la función**. Luego f es sobreyectiva si su rango es igual al conjunto de llegada.

Ejemplo: La función del ejemplo anterior no es sobreyectiva ¿Porqué?

Ejemplo: Sea $g : \mathbb{N} \longrightarrow \mathbb{N}$ dada por $g(n) = n + 1$. Entonces esta función tampoco es sobreyectiva. Sin embargo si denotamos por $\mathbb{Z}$ al conjunto de los enteros y $G : \mathbb{Z} \longrightarrow \mathbb{Z}$, mediante $G(z) = z + 1$, entonces G si es una función sobreyectiva.

Definición 1.2.6 *Una función $f : A \longrightarrow B$ se dice* **biyectiva** *si f es inyectiva y sobreyectiva.*

Definición 1.2.7 *Sea A un conjunto cualquiera, una* **relación en A**, *es un subconjunto R del producto cartesiano $A \times A$.*

Si el par (a, b) está en R, diremos que a **está relacionado con** b, y lo denotamos por $a \sim b$, ó aRb.

Definición 1.2.8 *Una relación R sobre A, se dice que es de* **equivalencia**, *si satisface las tres condiciones*

1. *Reflexiva*
   $a \sim a$ para todo a en A.

2. *Simétrica*
   $a \sim b$ implica $b \sim a$, para todos a y b en A.

3. *Transitiva*
   Si $a \sim b$ y $b \sim c$, entonces $a \sim c$, para todos a, b y c en A.

Para cada a en A, el conjunto

$$[a] = \{b \in A \mid b \sim a\}$$

se llama **la clase de equivalencia de a**.

Definición 1.2.9 *Una* **operación binaria** *sobre un conjunto A, es una función $g : A \times A \longrightarrow A$.*

La imagen del elemento (a, b) bajo la función g se denota por $a * b$.

Ejemplos de operaciones son la suma y producto de números enteros. También se pueden definir operaciones en forma arbitraria. Por ejemplo, si $\mathbb{N}$ es el conjunto de números naturales, podemos construir la operación

$$* : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

$$(a, b) \longrightarrow a * b = ab + 1.$$

1.3 Propiedades de los Enteros

Nosotros supondremos que el lector está familiarizado con el sistema de los números enteros $\ldots -2, -1, 0, 1, 2, 3, \ldots$, el cual denotaremos por $\mathbb{Z}$, así como también, con las propiedades básicas de adición y multiplicación. Podemos dar algunas de estas propiedades como axiomas y deducir otras, a partir de las primeras, como teoremas.

I) **Axiomas de Suma**

Existe una operación binaria en $\mathbb{Z}$, llamada la **suma de enteros**, la cual será denotada por $+$ y satisface :

1. **Cerrada**
   Para a y b números enteros, $a + b$ es un número entero

2. **Conmutativa**
   $a + b = b + a$, para todos a y b enteros .

3. **Asociativa**
   $(a + b) + c = a + (b + c)$, para todos a, b y c enteros.

4. **Elemento neutro**
   Existe un elemento en $\mathbb{Z}$ llamado el cero, el cual se denota por 0, y satisface:
   $$0 + a = a + 0 = a$$
   para todo a entero.

5. **Elemento opuesto**
   Para todo a en $\mathbb{Z}$ existe un elemento, llamado el opuesto de a, el cual denotamos por $-a$, y que satisface:
   $$a + (-a) = -a + a = 0$$

II) **Axiomas de Multiplicación**

Existe una operación binaria en $\mathbb{Z}$, llamada **producto de números enteros**, la cual se denota por $\cdot$, y satisface:

1. **Cerrada**
   Para a y b números enteros, $a \cdot b$ es un número entero

2. **Asociativa**
   Para a, b y c enteros

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

3. **Conmutativa**
   Para a y b enteros

$$a \cdot b = b \cdot a$$

4. **Elemento neutro**
   Existe un entero, llamado el uno y denotado por 1, tal que para todo entero a se tiene

$$1 \cdot a = a \cdot 1 = a$$

III) **Axioma de distributividad**
Para a, b y c enteros se cumple que

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

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

Antes de pasar a ver otros axiomas de los números enteros, como son los axiomas de orden, necesitamos la siguiente definición.

Definición 1.3.1 *Una* **relación de orden** *en un conjunto A, es una relación R sobre A, con las siguientes propiedades:*

1. *Propiedad simétrica*
   Para todo a en A, se verifica aRa.

2. *Propiedad Transitiva*
   Para a, b y c en A se verifica: Si aRb y bRc, entonces aRc

3. *Propiedad antisimétrica*
   Si aRb y bRa entonces $a = b$.

Ejemplo: La relación "Menor o igual que", en el conjunto de los enteros, es ciertamente, una relación de orden. Esto puede ser verificado sin ninguna dificultad por el lector.

A continuación daremos una forma, quizás un poco rigurosa, de introducir esta relación, usando la suma de enteros y la existencia de un conjunto P. (Conjunto de enteros positivos).

IV) **Axiomas de Orden**

Existe un conjunto de enteros, llamados **enteros positivos**, el cual denotaremos por P, y que satisface:

1. Para todos a y b en P, $a+b$ y $a.b$ están en P.
2. 1 está en P.
3. **Ley de tricotomía**
   Para todo entero a se tiene una y sólo una de las siguientes:
   i) a está en P, ii) $-a$ está en P, iii) $a=0$.

Usando los axiomas de orden, se define la siguiente relación en el conjunto de los enteros:

Definición 1.3.2 *Sean a y b dos enteros, diremos que a* **es menor o igual que** *b, y lo denotamos por $a \leq b$, si y sólo si $b-a$ es positivo o cero.*

Definición 1.3.3 *Sean a y b dos enteros, diremos que a* **es menor que** *b, y lo denotamos por $a < b$ si y sólo si $a \leq b$ y $a \neq b$.*

También diremos que: a **es mayor o igual a** b, y lo denotamos por $a \geq b$ si b es menor o igual que a.

Igualmente, diremos que a es **mayor que** b, y se denota por $a > b$, si b es menor que a.

Observación: El conjunto P de enteros positivos es igual al conjunto de los números naturales $\mathbb{N} = \{1, 2, 3, \ldots\}$, como veremos a continuación:

Notemos en primer lugar que 1 está en P (Axioma 2 de orden). Por la primera parte del axioma 1, se sigue que $2 = 1 + 1$, también está en P. De igual manera $3 = 2 + 1$, está en P, ... y así sucesivamente. De esta forma se concluye que el conjunto de los números naturales está en P. ¿Habrán otros elementos en P además de estos? La respuesta a esta pregunta, la podremos obtener como una consecuencia del teorema del mínimo elemento.

1.4 Axioma del Elemento Mínimo

Los axiomas estudiados hasta ahora no son suficientes para caracterizar el conjunto de los números enteros, en el sentido de determinar, sin ningún tipo de duda, todas y cada una de sus propiedades. A manera de ejemplo, la propiedad de infinitud de los enteros, no se puede derivar de ninguno de los axiomas o propiedades antes vistas. De aquí se concluye que es necesario incluir más axiomas, si se quiere tener un sistema completo, suficientemente bueno como para deducir, esta y otras propiedades que caracterizan a los enteros.

Definición 1.4.1 *Sea A un conjunto no vacío de $\mathbb{Z}$, entonces diremos que un entero a es una* **cota superior** *para A, si se cumple:*

$$n \leq a, \text{ para todo } n \text{ en } A \ .$$

Definición 1.4.2 *Diremos que un conjunto A está* **acotado superiormente***, si A posee una cota superior.*

Definición 1.4.3 *Sea A un conjunto no vacío de $\mathbb{Z}$. Un elemento a del conjunto A se dice* **elemento maximal** *, si $n \leq a$ para todo n en A.*

Observación: La diferencia entre las definiciones **??** y **??** radica en lo siguiente: Un conjunto A de enteros puede tener una cota superior a, pero, posiblemente a no es un elemento del conjunto A, por tanto a no es un elemento maximal.

Definición 1.4.4 *Sea A un conjunto no vacío de $\mathbb{Z}$. Un entero b se llama* **cota inferior** *para el conjunto A, si se cumple:*

$$b \leq x, \text{ para todo } x \text{ en } A$$

Definición 1.4.5 *Sea A un conjunto no vacío de $\mathbb{Z}$. Un elemento a de A se llama* **elemento minimal***(o elemento mínimo), si satisface:*

$$a \leq x, \text{ para todo } x \text{ en } A \ .$$

La misma observación que hicimos para el elemento maximal, se aplica al elemento minimal.

Axioma del mínimo elemento

Todo conjunto no vacío de números enteros positivos, posee un elemento minimal.

El axioma del mínimo elemento, es equivalente a otro axioma, llamado Principio de Inducción, el cual damos a continuación:

Principio de Inducción

Sea $P(n)$ una proposición que depende de un entero positivo n, y supongamos que:

1. $P(1)$ es cierta.
2. Si $P(k)$ es cierta, para un entero k, entonces $P(k+1)$ también es cierta.

Luego $P(n)$ es cierta para todo entero positivo n.

A partir del principio de inducción es posible probar una gran cantidad de fórmulas o identidades, que involucran un número positivo n.

Ejemplo: Probar la fórmula:

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2} \tag{1.1}$$

Demostración:

A fin de utilizar el principio de inducción, haremos una proposición que depende de n, y la llamaremos $P(n)$. Luego probaremos que esta proposición satisface las condiciones 1) y 2) del principio, con lo cual se estará verificando para todo n. Por lo tanto hacemos:

$$\text{P(n)} = \text{“la fórmula (}\mathbf{??}\text{) vale para todo } n\text{”}.$$

Notemos en primer lugar, que $P(1)$ se reduce a afirmar lo siguiente:

$$1 = \frac{1(1+1)}{2}$$

lo cual es evidentemente cierto.

Sea ahora, k un entero y supóngase que $P(k)$ es cierto, esto es:

$$1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}.$$

Partiendo de esta ecuación, y sumando $k + 1$ a ambos lados, se tiene

$$1 + 2 + 3 + \ldots + k + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

Luego podemos sumar los dos términos en el lado derecho de la ecuación para obtener:

$$1 + 2 + 3 + \ldots + k + (k+1) = \frac{(k+1)(k+2)}{2}$$

Vemos entonces que esta última fórmula es igual a (**??**), con $n = k + 1$. Por lo tanto $P(k+1)$ es cierto, si se asume que $P(k)$ es cierto. Esto, unido a la veracidad de P(1), nos permite afirmar la validez de $P(n)$ para todo n.

♠

Ejemplo: Consideremos el **triángulo de Pascal:**

$$
\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
 & & & & \ldots & & & &
\end{array}
$$

donde todos los elementos situados sobre los lados oblicuos son iguales a uno, y cada elemento interior es igual a la suma de los dos elementos adyacentes sobre la fila anterior.

Podemos denotar por $C(n, r)$ al elemento del triángulo de Pascal situado en la fila n y en la posición r (dentro de esta fila).

Luego se tendrá

$$C(0,0) = 1$$

$$C(1,0) = 1, \quad C(1,1) = 1$$

$$C(2,0) = 1, \quad C(2,1) = 2, \quad C(2,2) = 1$$

$$\ldots$$

y así sucesivamente.

En general se tiene la fórmula

$$C(n, r) = C(n-1, r-1) + C(n-1, r)$$

Este tipo de fórmula, en donde un elemento se define en función de los anteriores se llama **fórmula de recurrencia**. La posibilidad de definir elementos enteros mediante esta técnica de la recurrencia se debe al principio de inducción, ver [**?**].

Existe otra forma de expresar los coeficientes del triángulo de Pascal, explícitamente en función de n, la cual probaremos usando inducción. Más precisamente:

Proposición 1.4.1 *Si n es un entero positivo, entonces se tiene*

$$C(n,r) = \frac{n!}{(n-r)!\ r!} \qquad 0 \leq r \leq n. \tag{1.2}$$

Demostración:

Denotaremos por $P(n)$ la proposición (**??**), y probaremos que $P(n)$ es cierta para todo n, usando el principio de inducción.

El primer paso de la inducción corresponde a $n = 0$, lo cual nos da:

$$1 = C(0,0) = \frac{0!}{(0-0)!\ 0!}$$

siendo esto cierto, se tiene que $P(0)$ es cierto.

Sea n un entero positivo cualquiera, y supongamos que la relación (**??**) sea cierta. Luego debemos probar $P(n+1)$:

$$C(n+1,r) = \frac{(n+1)!}{(n+1-r)!\ r!} \qquad 0 \leq r \leq n+1$$

Sea r entero positivo, $0 < r < n+1$. Luego usando la fórmula de recurrencia para $C(n+1,r)$ se obtiene:

$$\begin{aligned} C(n+1,r) &= C(n,r) + C(n,r-1) \\ &= \frac{n!}{(n-r)!r!} + \frac{n!}{(n-r+1)!\ (r-1)!} \\ &= \frac{(r+1)!}{(n+1-r)!\ r!} \end{aligned}$$

Si $r = 0$, se tiene:

$$C(n+1,0) = 1 = \frac{(n+1)!}{(n+1-0)!\ 0!}$$

Si $r = n+1$ se tiene:

$$C(n+1,n+1) = 1 = \frac{(n+1)!}{((n+1)-(n+1))!\ (n+1)!}$$

Por lo tanto, hemos demostrado la veracidad de $P(n+1)$, a partir de la veracidad de $P(n)$. Luego la fórmula (**??**) es cierta para todo n. ♠

Observación: Los números $C(n,r)$ son los coeficientes de la expansión del binomio $(x+y)^n$ y por ello se les llama **coeficientes binomiales**

Ejercicios

1) (Binomio de Newton) Sean x e y números reales cualesquiera y sea n un entero positivo. Probar

$$(x+y)^n = \sum_{r=1}^{n} \left(\begin{array}{c} n \\ r \end{array} \right) x^{n-r} y^r$$

2) La **sucesión de Fibonacci**. La sucesión a_n definida por recurrencia $a_0 = 0$, $a_1 = 1 \ldots, a_{n+1} = a_n + a_{n-1}$, se denomina sucesión de Fibonacci. Demostrar, usando inducción sobre n, que el término general de esta sucesión viene dado por:

$$a_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$$

3) **El Número de Oro:**

El número $\varphi = (\frac{1+\sqrt{5}}{2})$ que aparece en la sucesión de Fibonacci, se llama el Número de Oro y posee propiedades muy interesantes. Este se obtiene como el cociente de los lados del rectángulo de lados a y b, tal que es proporcional al rectángulo de lados b, $a+b$. Esto es

$$\frac{b}{a} = \frac{a+b}{b}$$

Probar que el radio $\dfrac{b}{a}$ es igual a φ.

4) Si a_n es el término enésimo de la sucesión de Fibonacci, probar

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \varphi$$

5) Usando el principio de inducción, probar las fórmulas

1. $1 + 2^2 + 3^2 + \ldots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$
2. $1 + 3 + 5 + 7 + \ldots + 2n - 1 = n^2$
3. $1 + 2 + 2^2 + 2^3 + \ldots + 2^{n-1} = 2^n - 1$

6) Probar

$$\left(\begin{array}{c} n \\ 0 \end{array}\right) + \left(\begin{array}{c} n \\ 1 \end{array}\right) + \cdots + \left(\begin{array}{c} n \\ n \end{array}\right) = 2^n$$

7) Probar

$$\left(\begin{array}{c} n \\ 0 \end{array}\right)^2 + \left(\begin{array}{c} n \\ 1 \end{array}\right)^2 + \cdots + \left(\begin{array}{c} n \\ n \end{array}\right)^2 = \left(\begin{array}{c} 2n \\ n \end{array}\right)$$

8) Probar que no existe un número entero x con la propiedad:

$$0 < x < 1.$$

Ayuda: Suponiendo que tal x exista, consideremos el conjunto de enteros positivos $\{x, x^2, \ldots\}$, el cual es distinto del vacío y no tiene elemento minimal. Esto contradice el axioma del mínimo elemento.

9) Usando el ejercicio anterior, probar que si n es un número entero cualquiera, entonces no existe entero x con la propiedad:

$$n < x < n + 1$$

10) Probar el principio de inducción a partir del principio del mínimo elemento.

11) Probar que el conjunto de los números enteros no está acotado superiormente.

12) Probar que en $\mathbb{Z}$ valen las dos leyes de cancelación, es decir, para todo a, b y c en $\mathbb{Z}$, con $a \neq 0$, se tiene

$$ab = ac \Longrightarrow b = c$$

$$ba = ca \Longrightarrow b = c$$

13) Probar que si a y b son dos enteros diferentes de cero, entonces

$$ab = 0 \Longrightarrow a = 0 \quad \text{ó} \quad b = 0$$

14) Demuestre que no existe un entero $a \neq 0$, con la propiedad.

$$a + x = x,$$

para todo x entero.

15) Probar que toda función inyectiva $f : A \to A$, donde A es conjunto finito, es sobre.

16) Demuestre que cualquier elemento $a \in \mathbb{Z}$ satisface:
i) $a^m.a^n = a^{m+n}$
ii) $(a^n)^m = a^{nm}$,
para todos m y n enteros.

17) Una **partición** en un conjunto A, es una familia de subconjuntos $\{A_i\}$ de A, tales que.
i) $A_i \cap A_j \neq \emptyset$, para $i \neq j$.
ii) $\bigcup_{i \geq 1} A_i = A$.

Probar que toda relación de equivalencia en A determina una partición

18) Demuestre que cualquier conjunto de números enteros acotado superiormente posee un máximo.

19) Demuestre que si a es un entero positivo y b es un entero negativo, entonces ab es negativo.

20) Demuestre que si a y b son impares, entonces su producto es un número impar.

1.5 Máximo Común Divisor

En esta sección estudiaremos el famoso teorema de la división de los números enteros, y algunos resultados importantes que se derivan del mismo.

Teorema 1.5.1 *Sea a un entero positivo, y b un entero arbitrario. Entonces existen enteros p y q, únicos, tales que*

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

El entero q se llama el **cociente** *y r se llama el* **resto**

Demostración:

Primero, probaremos que q y r existen, y posteriormente, probaremos que ellos son únicos.

En primer lugar, si $b = 0$, tomamos $q = r = 0$.

Sea b distinto de cero y consideremos el conjunto

$$D = \{b - ua \mid u \text{ es un entero}\}$$

Este conjunto contiene enteros positivos, pues si $b > 0$, basta tomar $u = 0$.

Si por el contrario $b < 0$, hacer $u = b$, con lo cual $b - ba > 0$, y $b - ba \in D$.

Por lo tanto el conjunto D^+, de elementos no negativos de D es diferente del vacío.

Por el axioma del mínimo elemento, este conjunto posee un elemento minimal r el cual pertenece a D^+.

Así pues, existe un entero q, tal que

$$r = b - qa,$$

o bien

$$b = qa + r, \quad 0 \leq r.$$

Si suponemos $r \geq a$, se tiene $r - a \geq 0$ y por lo tanto

$$b - qa - a = b - (q + 1)a \geq 0.$$

Esto es,

$$b - (q+1)a \in D^+$$

y

$$b - (q+1)a < r,$$

lo cual contradice la minimalidad del elemento r. Luego se debe tener $r < a$.

Unicidad:

Supongamos que existen otro par de enteros q' y r' los cuales satisfacen

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

Probaremos que $q = q'$, para lo cual supondremos que $q' > q$. Luego se tiene

$$0 = b - b = (q'a + r') - (qa + r) = (q' - q)a - (r - r'),$$

de donde se obtiene

$$(q' - q)a = r - r' \geq a.$$

lo cual es una contradicción, pues $r - r' < a$. Similarmente si suponemos $q > q'$ llegamos a la misma contradicción. Por lo tanto, se debe tener $q = q'$, y de esto se sigue $r = r'$.

♠

Definición 1.5.1 *Sea a un entero positivo, y b un entero cualquiera. Diremos que a* **divide a** *b, y lo denotamos por $a \mid b$, si existe otro entero c tal que $b = ac$.*

También se dice que b **es divisible por** a, o bien a **es un divisor de** b. El concepto de divisibilidad es uno de los más importantes en toda la teoría de números. Uno de los problemas aún no resueltos, consiste en hallar todos los divisores de un número cualquiera dado.

Algunas de las propiedades básicas de la divisibilidad, se exponen en la siguiente proposición.

Proposición 1.5.1 *Sean a, b y c enteros distintos de cero. Entonces*

1. $1 \mid a$
2. $a \mid 0$
3. $a \mid a$
4. *Si* $a \mid b$ *y* $b \mid c$, *entonces* $a \mid c$.
5. *Si* $a \mid b$ *y* $a \mid c$, *entonces* $a \mid bx + cy$, *para todo par de enteros* x *e* y.

Demostración:
Ejercicio. ♠

Definición 1.5.2 *Sean* a *y* b *dos enteros positivos. Un entero positivo* d, *se dice* **Máximo Común Divisor** *entre* a *y* b, *si y sólo si satisface*

1. $d \mid a$ *y* $d \mid b$
2. *Si* c *es otro entero positivo con la condición :*

$$c \mid a \quad \text{y} \quad c \mid b, \quad \text{entonces} \quad c \mid d.$$

El entero positivo d, se denota por $d = (a, b)$. De acuerdo a la definición, se tiene que el Máximo Común Divisor d, es el mayor de los divisores comunes de a y b.

Ejemplo: Hallar el Máximo Común Divisor entre 12 y 18.
En primer lugar, buscamos por tanteo, todos los divisores comunes de ambos números

Divisores de 12 : 1, 2, 3, 4, 6 y 12.
Divisores de 18 : 1, 2, 3, 6, 9 y 18.

Es evidente que el mayor divisor común es 6, y por lo tanto concluimos

$$(12, 18) = 6.$$

Existe un método práctico para calcular el Máximo Común Divisor entre dos números, el cual está basado en el algoritmo de división. Este método, llamado **Método de Euclides para el M.C.D.** consiste en una serie de divisiones sucesivas y, el Máximo Común Divisor se obtiene como uno de los restos en el proceso de división. Además de dar una forma constructiva de calcular el M.C.D., permite al mismo tiempo dar una demostración de la existencia de éste.

Teorema 1.5.2 Método de Euclides

Dados dos enteros positivos a y b, el Máximo Común Divisor entre ellos, $d = (a, b)$, siempre existe.

Demostración:

Podemos suponer, sin pérdida de generalidad que $b > a > 0$. Luego por el teorema de división, existen enteros q_1 y r_1 tales que

$$b = q_1 a + r_1, \quad 0 \leq r_1 < a.$$

Si $r_1 = 0$, entonces $b = q_1 a$ y por lo tanto $(b, a) = a$, con lo cual queda demostrado el teorema.

Si $r \neq 0$, podemos aplicar de nuevo el teorema de la división, para obtener un par de enteros q_2, r_2 tales que

$$a = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1$$

Continuando de esta manera, se obtiene una sucesión de enteros positivos decrecientes: $r_1 > r_2 > \ldots > 0$. Es evidente que esta sucesión es finita y por lo tanto existe n, tal que $r_n \neq 0$ y $r_{n+1} = 0$. Luego existen enteros $q_1, q_2, \ldots q_{n+1}, r_1, r_2, \ldots, r_n$ que cumplen las relaciones:

$$\begin{aligned} b &= aq_1 + r_1, \quad 0 < r_1 < b \\ a &= r_1q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} \end{aligned}$$

Afirmamos que $(a, b) = r_n$.

En primer lugar, notemos que de la última ecuación se tiene que r_n divide a r_{n-1} . Por lo tanto, $r_n \mid (r_{n-1}q_n + r_n)$, es decir r_n divide a r_{n-2}. Continuando de esta manera, llegamos finalmente, a que r_n divide a todos los demás r_i . En particular

$$r_n \mid r_1 \quad y \quad r_n \mid r_2, \quad \text{implica que} \quad r_n \mid r_1q_2 + r_2$$

luego $r_n \mid a$.

Igualmente, usando $r_n \mid a$ y $r_n \mid r_1$ se deduce $r_n \mid b$.

Finalmente, si c es un entero positivo que divide a a y a b, se tiene

$$c \mid b - aq_1,$$

o sea, $c \mid r_1$. Continuando de esta manera, se tiene que $c \mid r_i$ para todo i y por tanto $c \mid r_n$.

Con esto hemos demostrado las dos condiciones de la definición de Máximo Común Divisor para r_n y por lo tanto $(a, b) = r_n$.

♠

Ejemplo: Podemos calcular el Máximo Común Divisor entre 672 y 38, usando el método anterior, para lo cual haremos las divisiones correspondientes. Luego

$$672 = 17 \cdot 38 + 26$$

$$38 = 1 \cdot 26 + 12$$

$$26 = 2 \cdot 12 + 2$$
$$12 = 6 \cdot 2$$

El último resto diferente de cero es 2, luego $(672, 38) = 2$.

En la demostración del teorema anterior, obtuvimos las ecuaciones

$$\begin{aligned} r_1 &= b - aq_1 \\ r_2 &= a - r_1 q_2 \\ &\vdots \\ r_{n-1} &= r_{n-3} - r_{n-2} q_{n-1} \\ r_n &= r_{n-2} - r_{n-1} q_n \end{aligned}$$

Observamos que el Máximo Común Divisor entre a y b, dado por r_n viene expresado en función de r_{n-2} y r_{n-1}. Ahora bien, en la penúltima ecuación se puede reemplazar r_{n-1} en función de r_{n-2} y r_{n-3}. Continuando de esta forma, podemos ir sustituyendo los valores de r_i en función de los anteriores, hasta que tengamos r_n en función de a y b. Así pues hemos demostrado el siguiente resultado:

Teorema 1.5.3 *El Máximo Común Divisor entre dos enteros a y b, se expresa como combinación lineal de a y b. Es decir, existen enteros x e y tales que*

$$(a, b) = ax + by$$

Ejemplo: Podemos expresar el Máximo Común Divisor entre 672 y 38 como combinación lineal de ambos, para lo cual usamos las cuatro ecuaciones del ejemplo anterior.

$$\begin{aligned} 2 &= 26 - 2 \cdot 12 \\ 2 &= 26 - 2 \cdot (38 - 26) \\ 2 &= 3 \cdot 26 - 2 \cdot 38 \\ 2 &= 3 \cdot (672 - 17 \cdot 38) - 2 \cdot 38 \\ 2 &= 3 \cdot 672 - 53 \cdot 38 \end{aligned}$$

Una de las aplicaciones de mayor utilidad que ofrece el teorema de la división, es la representacion de cualquier número mediante combinación lineal de potencias de 10.

Teorema 1.5.4 *Si b es un entero positivo, entonces existen enteros únicos $r_0, r_1, \ldots, r_n$ tales que*

$$b = r_n 10^n + r_{n-1} 10^{n-1} + \ldots + r_1 10 + r_0$$

con $0 \leq r_i < 10$ para todo i.

Demostración:

Usaremos inducción sobre b. Si $b = 1$ es cierto. Supongamos el resultado cierto para todo entero menor que b, y probaremos la afirmación para b. Podemos dividir b entre 10 para obtener enteros únicos q y r_0 tales que

$$b = q \cdot 10 + r_0, \quad 0 \leq r_0 < 10$$

Como q es menor que b, aplicamos la hipótesis de inducción a q. Luego existen enteros únicos $r_1, r_2, \ldots, r_n$, con $0 \leq r_i < 10$, tales que

$$q = r_n 10^{n-1} + \ldots + r_2 10 + r_1$$

Por lo tanto

$$b = (r_1 + r_2 10 + \ldots + r_n 10^{n-1})10 + r_0$$

$$= r_n 10^n + \ldots + r_1 10 + r_0$$

Es claro que todos los r_i son únicos. Con esto termina la demostración.

♠

Definición 1.5.3 *Dos enteros positivos a y b, se dicen* **primos relativos** *si el Máximo Común Divisor entre ellos es uno.*

Ejemplo: Los enteros 20 y 9 son primos relativos, pues $(20, 9) = 1$. Nótese que 20 y 9 no son números primos.

El siguiente resultado, que caracteriza las parejas de enteros primos relativos, será de mucha utilidad en el futuro:

Teorema 1.5.5 *Dos enteros positivos a y b son primos relativos, si y sólo si existen enteros x e y tales que*

$$ax + by = 1$$

Demostración:

Es claro que existen enteros x e y, tal que

$$ax + by = 1$$

pues 1 es el Máximo Común Divisor entre a y b.

Por otro lado, si suponemos $ax + by = 1$, para algunos enteros x e y, podemos probar $(a, b) = 1$. En efecto, si c es un divisor de a y b, se tendrá que c divide a $ax + by$, o sea c divide a 1. Luego $c = 1$, y por lo tanto el Máximo Común Divisor entre a y b es 1.

♠

Definición 1.5.4 *Sean a y b dos enteros positivos, el* **mínimo común múltiplo** *entre a y b, es otro entero positivo c, el cual satisface:*

1. *$a \mid c$ y $b \mid c$*
2. *Si e es otro entero, tal que $a \mid e$ y $b \mid e$, se tiene $c \mid e$.*

De la definición anterior se sigue que c es el menor múltiplo común entre a y b.

Usaremos la notación :

$$[a, b] = \text{mínimo común múltiplo entre } a \text{ y } b.$$

Proposición 1.5.2 *Sean a, b, y c tres enteros positivos, tales que $(a, b) = 1$ y $a \mid bc$. Luego $a \mid c$.*

Demostración:

Por el teorema anterior, existen enteros x e y tales que

$$ax + by = 1$$

Multiplicando por c tenemos

$$cax + cby = c$$

Por hipótesis, sabemos que $a \mid bc$, luego $a \mid cby$. También se tiene $a \mid cax$, y por lo tanto concluimos

$$a \mid cax + cby$$

lo cual implica que $a \mid c$.

♠

Para finalizar esta sección, daremos una serie de propiedades fundamentales del Máximo Común Divisor:

Proposición 1.5.3 *Sean a, b y c enteros positivos. Entonces*

1. *Si m es otro entero tal que $m \mid a$ y $m \mid b$ se tiene*

$$\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{(a,b)}{m}$$

2. *Si n es cualquier entero*

$$(na, nb) = n(a, b)$$

3. *Si $(a, b) = d$, entonces*

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

4. *Si x es cualquier entero, entonces*

$$(b, a + bx) = (a, b)$$

Demostración:
1) Sea $d = (a, b)$, y probaremos

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

Notemos en primer lugar que d/m es un entero. En efecto se tiene $ax + by = d$, y por lo tanto

$$\frac{a}{m}x + \frac{b}{m}y = \frac{d}{m}$$

en el lado izquierdo de la ecuación tenemos un entero, luego d/m es entero.

Por otra parte, como d divide a a, se tiene que d/m divide a a/m. Igualmente se tendrá que d/m divide a b/m.

Finalmente, si c es otro entero que divide a a/m y b/m, se tendrá

$$\frac{a}{m} = cj \quad y \quad \frac{b}{m} = ck$$

para algunos enteros j y k.

Multiplicando ambas ecuaciones por m nos da

$$a = mcj \quad y \quad b = mck$$

de donde obtenemos

$$mc \mid a \quad y \quad mc \mid b$$

Usando la definición de Máximo Común Divisor para d, se tiene que d divide a mc, y por lo tanto d/m divide a c.

Así pues, hemos probado 1).

2) Usando 1) se tiene

$$(a, b) = \left(\frac{an}{n}, \frac{bn}{n}\right) = \frac{(an, bn)}{n}$$

luego

$$n(a, b) = (an, bn)$$

3) Usar 1) con $m = (a, b)$.

4) Observar que $(a, b) \mid a$ y $(a, b) \mid b$. Luego $(a, b) \mid ax + b$.
Si c es un entero que divide tanto a b como a $a + bx$, se tendrá

$$c \mid ((a + bx) - bx)$$

y en consecuencia $c \mid a$.

Luego c divide al máximo común divisor entre a y b, el cual es d. Así pues, hemos probado $(b, a + bx) = (a, b) = d$.

♠

Ejemplo:

$$(200, 300) = (2, 3)100 = 100.$$

Ejercicios

1) Usando el algoritmo de Euclides, hallar
a) (122,648)
b) (715,680)
c) (1581,206)
d) (3742, 843)
e) (120, 560)
f) (458, 1290).

2) Demuestre que si $(a, b) = 1$, entonces:

$$(a - b, a + b) = 1, \quad \text{ó} \quad 2.$$

3) Demuestre que si $ax + by = m$, entonces $(a, b) \mid m$.

4) Demuestre que si $(b, c) = 1$, entonces para todo entero positivo a, se tiene $(a, bc) = (a, b)(a, c)$.

5) El Máximo Común Divisor para tres números enteros positivos a, b y c, denotado por (a, b, c) se define como el entero positivo d que satisface:

1. $d \mid a, \quad d \mid b, \quad y \quad d \mid c$

2. Si f es otro entero tal que $f \mid a$, $f \mid b$ y $f \mid c$ entonces $f \mid d$.

Probar que $(a, b, c) = ((a, b), c) = (a, (b, c))$.

6) Hallar el Máximo Común Divisor de
   a) (23,12,18)
   b) (90, 80, 56)
   c) (65, 20, 190).

7) Hallar una solución en números enteros de la ecuación

$$21x + 25y = 1$$

8) Probar que el mínimo común múltiplo entre dos enteros a y b siempre existe.

9) Demostrar la fórmula

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

10) Usando la fórmula anterior, calcular
   a) [12,28]
   b) [120,50]
   c) [34,62]
   d) [88, 340].

1.6 Teorema de Factorización Unica

Definición 1.6.1 *Un entero positivo p, distinto de 1, se dice que es* **primo** *si los únicos divisores de p son 1 y p.*

Ejemplo: Los números 2, 3, 19 son primos.

Los números enteros positivos que no son primos, se les llama **compuestos**, como por ejemplo 6. Es decir, todo número compuesto es de la forma

$$m = m_1 m_2,$$

donde $1 < m_1 < m$ y $1 < m_2 < m$.

Los números primos y su distribución dentro de los números enteros, han sido estudiados desde la antigüedad. Ellos han ejercido una atracción fascinante sobre los matemáticos, debido a la forma tan irregular como aparecen en la sucesión de los enteros. Muchos matemáticos han tratado en vano de hallar una fórmula que genere exclusivamente números primos. Así por ejemplo, Pierre Fermat conjeturó que todo número de la forma

$$s(n) = 2^{2^n} + 1$$

era primo. Esto lo comprobó para n= 1,2,3 y 4. Sin embargo en 1732 Leonhard Euler demostró que $s(5)$ no era primo.

Existe una gran cantidad de problemas, aún no resueltos, sobre los números primos. Algunos de ellos serán tratados en las próximas secciones.

El método más elemental para hallar la sucesión de los primos, es el llamado **Criba de Eratóstenes**. Este consiste en colocar los números enteros positivos en orden creciente, formando diez columnas de la siguiente forma

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

.....

Entonces comenzamos por eliminar de la lista todos los números pares, luego los múltiplos de tres, luego los de cinco, ... y así sucesivamente, hasta agotar todos los números compuestos. Es evidente que los restantes números en la lista serán todos los números primos.

Teorema 1.6.1 *Todo número entero positivo, mayor que uno, puede ser factorizado como un producto de números primos.*

Demostración:

Sea m el número en cuestión. Usaremos inducción sobre m, para probar la proposición "m puede ser factorizado como un producto de primos".

En primer lugar, la proposición es cierta para $m = 2$, pues 2 mismo es un número primo. Supóngase la veracidad de la proposición, para todo número menor que un cierto k, es decir, todo número menor que k y mayor o igual a dos, puede ser factorizado como producto de primos.

Consideremos ahora k. Si k es primo, entonces no hay nada que probar y el resultado será cierto para k. Si por el contrario, k resulta ser compuesto, entonces tenemos

$$k = m_1 m_2$$

donde $2 \leq m_1 < k$ y $2 \leq m_2 < k$.

Podemos entonces aplicar la hipótesis de inducción, tanto a m_1 como a m_2, es decir cada uno de ellos se factoriza como un producto de primos. Luego

$$m_1 = p_1 p_2 \dots p_s$$

$$m_2 = q_1 q_2 \dots q_t$$

donde los p_i, q_j son números primos.

Por lo tanto tenemos

$$k = m_1 m_2 = p_1 p_2 \dots p_s q_1 q_2 \dots q_t$$

esto es, un producto de primos.

♠

Observación: Es posible tener algunos primos repetidos en la factorización de un número compuesto. Por ejemplo $24 = 2.2.2.3$. En todo caso, podemos agrupar aquellos primos iguales usando potenciación. Esto es todo entero positivo n puede ser escrito de la forma

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} \tag{1.3}$$

donde los p_i son todos primos diferentes y los α_i son mayores o iguales a uno.

La siguiente proposición es fundamental para la demostración del teorema de factorización única.

Proposición 1.6.1 *Sean $p, p_1, p_2, , \ldots p_n$ números primos, tales que $p \mid p_1.p_2 \ldots p_n$. Entonces $p = p_i$ para algún i.*

Demostración:

Usaremos inducción sobre n.

Para $n = 1$, el resultado es cierto. Supongamos que p es distinto de p_1, entonces tenemos

$$(p, p_1) = 1 \quad y \quad p \mid p_1(p_2 p_3 \ldots p_n)$$

Luego por la proposición 2 se obtiene

$$p \mid p_2.p_3 \ldots p_n$$

Usando la hipótesis de inducción, se concluye que $p = p_i$ para algún i.

♠

Teorema 1.6.2 *Todo número entero positivo n, tiene una factorización única de la forma*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$$

Demostración:

Supongamos que n tiene dos factorizaciones distintas

$$n = p_1^{\alpha_1} \ldots p_s^{\alpha_s} = q_1^{\beta_1} \ldots q_t^{\beta_t} \tag{1.4}$$

Probaremos en primer lugar que $s = t$ y posteriormente probaremos que para todo i, con $1 \leq i \leq s$, se tiene

$$p_i = q_j, \quad \text{para algún} \quad j \ \text{ y } \quad \alpha_i = \beta_j.$$

Usaremos inducción sobre n. Si $n = 1$, entonces la tesis del teorema se cumple.

Supongamos que el teorema es cierto para todo entero positivo k, con $k < n$ y probemos el resultado para n.

Sea entonces n como en (1.4). Notemos que p_1 divide al producto de primos $q_1^{\beta_1} \dots q_t^{\beta_t}$, luego por el lema anterior p_1 debe ser igual a alguno de ellos, digamos q_i. Podemos entonces cancelar p_1 en ambos lados de (**??**), con lo cual tendremos que n/p_1 posee dos factorizaciones. Si se aplica entonces la hipótesis de inducción se obtiene el resultado.

♠

Uno de los primeros resultados acerca de los números primos, y que aparece demostrado en *Los Elementos* de Euclides, es el siguiente.

Teorema 1.6.3 *Existen infinitos números primos.*

Demostración:

Supóngase que hay solamente un número finito de primos, digamos $p_1, p_2, \dots, p_n$. Entonces el número

$$x = p_1 p_2 \dots p_n + 1$$

puede ser factorizado como producto de primos.

Sin embargo, ningún primo p_i, de los antes mencionados, puede estar entre los factores de x, pues p_i no divide a x; ¿Por qué?

♠

Ejercicios

1) Hallar la descomposición en factores primos de
   a) 165
   b) 670
   c) 124
   d) 1567
   e) 444.

2) Por medio de la Criba de Eratóstenes, hallar todos los primos menores que 200.

3) Probar que si n no es primo, entonces n tiene un divisor primo, el cual es menor o igual a $\sqrt{n}$.

4) Usando el resultado anterior, implemente un algoritmo de computación para determinar cuándo un número es primo.

5) Determine cuáles de los siguientes números son primos:
   a) 941
   b) 1009
   c) 1123
   d) 1111
   e) 671
   f) 821.

6) Algunos primos son de la forma $4k + 1$, como por ejemplo, 5, 17, 101, ... etc. Probar que hay infinitud de ellos.

7) Demostrar que $2^{524} - 1$ no es primo.

8) Sea

$$a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$$

y

$$b = p_1^{\beta_1} \dots p_n^{\beta_n},$$

entonces probar

$$(a, b) = p_1^{\delta_1} \dots p_n^{\delta_n}$$

donde $\delta_i = min\{\alpha_i, \beta_i\}$.

$$[a, b] = p_1^{\gamma_i} \dots p_n^{\gamma_n}$$

donde $\gamma_i = max\{\alpha_i, \beta_i\}$

9) Use el ejercicio anterior para hallar
   a) $(240, 45)$
   b) $[240, 45]$.
   c) $[1650, 7800]$
   d) $[235, 7655]$

10) Probar que $\sqrt{5}$ es un número irracional.