

# Teoría de números

Juan Antonio Ríos Briceño

17 de mayo de 2009



# Índice general

<b>1. Aritmetica y Álgebra</b>	<b>5</b>
1.1. Valor absoluto . . . . .	5
<b>2. Divisibilidad</b>	<b>7</b>
2.1. Conceptos basicos . . . . .	7
2.2. Maximo comun divisor . . . . .	10



# Capítulo 1

## Aritmetica y Álgebra

En este capítulo trataremos algunos temas de álgebra y aritmetica los cuales son necesarios par poder entender los siguientes temas de la teoría de números.

### 1.1. Valor absoluto

El valor absoluto de un número real es su valor numérico sin su signo, sea este positivo (+) o negativo (-); es decir, su distancia al cero en la recta numerica.

**Definición 1. 1** Formalmente el valor absoluto esta definido como:  $a$ , si  $a \geq 0$  y como  $-a$  si  $a < 0$ . En simbolos el valor absoluto de un número  $a$  se puede poner como  $|a|$ .

**Ejemplos:**

1.  $|1| = 1$ .
2.  $|-2| = 2$ .
3.  $|0| = 0$ .
4.  $|-10| = 10$ .
5.  $|30| = 30$ .

**Propiedades:**

1.  $|a| \geq 0$ , para todo  $a$  real.
2.  $|a| = 0$ , si y solo si,  $a = 0$ .
3.  $|ab| = |a||b|$ , para todo  $a, b$  reales.
4.  $|\frac{a}{b}| = \frac{|a|}{|b|}$  para todo  $a, b$  reales.

**Otras propiedades:**

1.  $|a + b| \leq |a| + |b|$ , para todo  $a, b$  reales. (**Desigualdad del triángulo**)
2.  $|a| \leq b$ , si y solo si,  $-b \leq a \leq b$ .
3.  $|a| \geq b$ , si y solo si,  $a \geq b$  o  $a \leq -b$ .

# Capítulo 2

## Divisibilidad

### 2.1. Conceptos básicos

Uno de los conceptos necesarios para entender todo lo referente a la teoría de números, es el concepto de divisibilidad, por eso veremos la siguiente definición:

**Definición 1. 2** Sean  $a$  y  $b$  dos números enteros. Decimos que  $a$  divide a  $b$  (lo que en símbolos es  $a|b$ ) si existe un entero  $c$  tal que  $b = ac$ .

Nota:  $a$  no divide a  $b$  lo podemos escribir en símbolos como  $a \nmid b$ .

**Nota:** Cuando  $a \neq 0$ ,  $a|b$  es equivalente a que  $\frac{b}{a}$  sea entero, ya que la ecuación  $b = ax$  cuando  $a \neq 0$  tiene solución única la cual está dada por  $x = \frac{b}{a}$  (despejando  $x$ ) por lo que existe un entero  $c$  tal que  $b = ac$ , solamente si pasa  $c = \frac{b}{a}$ , es decir solamente si  $\frac{b}{a}$  es entero.

**Ejemplos:**

1.  $4|12$  ya que  $12 = 4 \cdot 3$ .
2.  $5 \nmid 6$  ya que no existe un entero  $c$  tal que  $6 = 5c$ .
3.  $2009|0$  ya que  $0 = 2009 \cdot 0$ .
4.  $0|0$  ya que  $0 = 0 \cdot 0$ .
5.  $1|2009$  ya que  $2009 = 2009 \cdot 1$ .

**Propiedades:**

1. Para todo  $a$  entero se tiene que  $a|a$ .
2. Si  $a|b$ , entonces  $a|bc$  para todo entero  $c$ .
3. Para  $a$  y  $b$  enteros,  $a|b$  si y solo si  $|a||b|$
4. Si  $a|b$  con  $b \neq 0$ , entonces  $|a| \leq |b|$ .
5. Si  $a|b$  y  $b|a$ , entonces  $b = \pm a$ .
6. Si  $a|b$  y  $b|c$ , entonces  $a|c$ .
7. Si  $a|b$  y  $a|c$ , entonces  $a|(b + c)$ .

**Definición 1. 3** Si  $a$  y  $b$  son enteros, todo número que pueda expresarse de la forma  $ax + by$  (para  $x$  y  $y$  enteros) se llama *combinación lineal (entera)* de  $a$  y  $b$ .

**Ejemplos:**

1. 2 es combinación lineal de  $a = 1$  y  $b = 0$  ya que  $2 = a \cdot 2 + b \cdot 0$ .
2. 13 es combinación lineal de  $a = 2$  y  $b = 3$  ya que  $12 = a \cdot 5 + b \cdot 1$ .
3. 3 no es combinación lineal de  $a = 2$  y  $b = 4$  ya que  $ax + by$  para todo entero  $x, y$  es múltiplo de 2 (ya que 2 y 4 son múltiplos de 2) y el número 3 no lo es.

**Teorema 1. 1** Si un número divide a un conjunto de enteros, entonces divide a cualquier combinación lineal de los mismos, esto es, Si  $a|x_1, a|x_2, \dots, a|x_n$ , entonces

$$a|(c_1x_1 + c_2x_2 + \dots + c_nx_n)$$

para cualesquiera enteros  $c_1, c_2, \dots, c_n$ .

**Teorema 1. 2 (Algoritmo de la división)** Sean  $a$  y  $b \neq 0$  dos enteros. Entonces existen enteros únicos  $q$  y  $r$  tales que  $a = bq + r$  y  $0 \leq r < |b|$ , si  $a \nmid b$ , entonces  $r$  satisface las desigualdades más fuertes  $0 < r < |b|$ .

**Ejemplos:**

1.  $a = 5, b = 3$ . Usando el algoritmo de la división  $a = b \cdot 1 + 2$ .
2.  $a = 17, b = 5$ . Usando el algoritmo de la división  $a = b \cdot 3 + 2$ .
3.  $a = 20, b = 4$ . Usando el algoritmo de la división  $a = b \cdot 5 + 0$ .
4.  $a = 3, b = 18$ . Usando el algoritmo de la división  $a = b \cdot 0 + 3$ .
5.  $a = -12, b = 7$ . Usando el algoritmo de la división  $a = b \cdot (-2) + 2$ .

**Definición 1. 4** Un número positivo se llama número primo si tiene exactamente dos divisores positivos distintos. Un número mayor a 1 que no es primo se denomina compuesto.

**Teorema 1. 3** Todo número mayor a 1 es divisible por algún primo.

**Teorema 1. 4** Todo número mayor que 1 puede escribirse como producto de primos, es decir, un número  $n > 1$  puede escribirse de la forma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$$

donde cada  $p_j$  es un primo.

**Teorema 1. 5 (Teorema Fundamental de la Aritmetica)** Todo número se puede factorizar de manera única como producto de primos.

**Teorema 1. 6 (Euclides)** Hay una cantidad infinita de primos.

**Ejercicios**

**Ejercicio 1. 1** Sea  $a \neq 1$ . Demuestre la identidad

$$1 + a + a^2 + \dots + a^{n-1} = \frac{a^n - 1}{a - 1}$$

**Ejercicio 1. 2** Demuestre la identidad:

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \dots + xy^{n-2} + y^{n-1})$$

**Ejercicio 1. 3** Demuestre que para todo  $n$  entero positivo impar se tiene que:

$$1 + 2 + \dots + (n - 1) + n | 1^k + 2^k + \dots + (n - 1)^k + n^k$$

**Ejercicio 1. 4** Prueba que  $c|ax + by$  para todo  $x, y$  enteros, si y solo si,  $c|a$  y  $c|b$ .

**Ejercicio 1. 5** Prueba que si  $a - c|ab + cd$ , entonces  $a - c|ad + bc$

**Ejercicio 1. 6** Obtenga la factorización en primos de 89999.

**Ejercicio 1. 7** Demostrar que el unico primo de la forma  $n^4 + 4$  es 5.

**Ejercicio 1. 8** Demuestra que:

$$1 + x + x^2 + \dots + x^9 | 1 + x^{1111} + x^{2222} + \dots + x^{9999}$$

## 2.2. Maximo comun divisor

Un entero  $d$  es un divisor común de  $a$  y  $b$  si  $d|a$  y  $d|b$ , Puesto que solamente existe un número finito de divisores de cualquier entero distinto de cero, solamente existe un número finito de divisores comunes de  $a$  y de  $b$ , excepto el caso cuando  $a$  y  $b$  son cero.

**Definición 2. 5** Si por lo menos uno de  $a$  y  $b$  es distinto de cero, el mayor entre sus divisores comunes (este existe ya que el número de divisores comunes es finito) se llama Máximo Común Divisor de  $a$  y  $b$  y se denota por  $(a, b)$ .

Notemos que  $(a, b) \geq 1$  ya que  $1|n$  para todo  $n$  entero.

**Propiedades:**

1.  $(a, 1) = (a, -1) = 1$ , para todo entero  $a$
2.  $(a, a) = a$  para todo  $a \neq 0$  entero.
3.  $(a, 0) = a$  para todo  $a \neq 0$  entero.
4.  $(a, b) = (b, a)$ .

5.  $(a, b) = (a, b - a)$ .

**Teorema 2. 7** Si  $a = bq + r$  con  $0 \leq r < b$  entonces  $(a, b) = (r, b)$ .

**Teorema 2. 8** Sean  $a$  y  $b$  enteros no ambos cero y considerese los números positivos de la forma  $ax + by$ , sea  $d$  el menor de los números de esta forma