Unidad 1
TEORIA DE NÚMEROS

TEORIA DE NUMEROS

Parte de la matemática discreta que trata de las propiedades de los números enteros.

- N={0,1,2,3,…} Conjunto de los números naturales
- Z={…,-3,-2,-1,0,+1,+2,+3,…} Conjunto de los números enteros
- Z_+={1,2,3,…}
- Cómo representamos a estos números en una gráfica en la hoja?

"La matemática es la reina de las ciencias y la aritmética es la reina de las matemáticas."

Carl Friedrich Gauss

1,2,3…,100

$$\sum_{i=1}^{i=100} i$$

Teorema del Resto o Algoritmo de la División

- Dados dos enteros positivos a y b con $b > 0$, ***existen*** dos enteros q *(cociente)* y *r (resto)* ***únicos*** tales que:

  $a = b \, . \, q + r$ y

  $0 \leq r < | b |$

div y mod

Podemos ***definir*** dos nuevas operaciones :

- *div*

La operación div nos da el cociente entre a y b

$$a \; div \; b = q$$

- *mod*

La operación mod nos da el resto de dividir a y b

$$a \; mod \; b = r$$

Divisibilidad

Sean a y b dos números enteros, se dice que *a divide a b* y se escribe $a \mid b$ si existe un numero entero c tal que $b = a \cdot c$.
También decimos que *a* es un *divisor* de *b* o que *b* es *múltiplo* de *a* o que *a* es un *factor* de *b*

Cuales son los divisores de 120?
Porque?

Propiedades de la divisibilidad

- Teorema 1: La unidad divide a cualquier entero.

  $1 \mid a \quad$ para $a \in Z$

- Teorema 2: Todo entero divide a 0.

  $a \mid 0 \quad$ para $a \in Z$

Propiedades de la divisibilidad

- Teorema 3: Todo entero que es divisor de otros dos es divisor de la suma de ellos.

  Si $d \mid a$ y $d \mid b$ y entonces $d \mid a + b$

- Teorema 4: Todo entero que es divisor de otro es también divisor de los múltiplos de ese otro.

  Si $d \mid a$ entonces $d \mid n \times a$ para $n \in Z$

Propiedades de la divisibilidad

- Teorema 5: Todo entero que es divisor de otros dos es también divisor de su diferencia.

  Si $d \mid a$ y $d \mid b$ entonces $d \mid a - b$

- Teorema 6: Todo entero que es divisor de otros dos es también divisor del resto de la división de estos.
- Si $d \mid a$ y $d \mid b$ entonces $d \mid a \ \mathit{mod}\ b$

Divisor Común

- Sean a y b $\in$ Z. Se dice que un entero d es un divisor comun de a y b, siempre y cuando $d|a$ y $d|b$.

Máximo Común Divisor

- Dados dos números enteros positivos a y b se define el máximo común divisor de a y b y se escribe mcd (a,b) al mayor de los divisores comunes de a y b

- Cómo podemos resolver el problema de encontrar el mcd de dos números con lo que hemos aprendido hasta este momento?

- Existirán otros “algoritmos” que sean mas eficientes?

El algoritmo de Euclides

Nació en Alejandría en el 330 aC.

Lema:

- Dados dos enteros positivos a y b, a > b, entonces el mcd(a, b) = mcd(b, r), donde r es el resto de dividir a entre b.

$$\text{mcd}(a, b) = \text{mcd}(b, a \textit{ mod } b)$$

El algoritmo de Euclides

- Datos: a , $b \in Z$ y $a > b$

1. $a = b \times q_1 + r_1$ //Algoritmo de la División (a/b)
2. Si $r_1 = 0$

   $mcd(a,b) = b$ // $b \mid a$ b (divisor)

   Fin del proceso

   Si $r_1 \neq 0$

   $b = r_1 \times q_2 + r_2$ //Algoritmo de la División (b/r_1)
3. Si $r_2 = 0$

   $mcd(a,b) = r_1$ // $r_1 \mid b$ r_1 (divisor)

   Fin del proceso

   Si $r_2 \neq 0$

   $r_1 = r_2 \times q_3 + r_3$ //Algoritmo de la División (r_1/r_2)

El algoritmo de Euclides

Como podemos ver el proceso continua aplicando sucesivamente el algoritmo de la división entre restos r_i y r_{i-1}, hasta obtener un ultimo resto $r_n \neq 0$.

$$\ldots \qquad \ldots$$

$$r_{n-2} = r_{n-1} \times q_{n-1} + r_n \qquad 0 \leq r_n \leq r_{n-1}$$

$$r_{n-1} = r_n \times q_n \qquad r_n \mid r_{n-1} \qquad r_n \text{ (divisor)}$$

Luego por aplicación del Lema se tiene que:

$$\mathrm{mcd}(a,b)=\mathrm{mcd}(b,r_1)=\mathrm{mcd}(r_1,r_2)=\ldots$$

$$=\mathrm{mcd}(r_{n-2},r_{n-1})=\mathrm{mcd}(r_{n-1},r_n)=\mathrm{mcd}(r_n,0)=r_n$$

El ultimo resto distinto de cero es el mcd (a,b).

El algoritmo de Euclides

Ejemplo: Encontrar el máximo común divisor entre:

$a = 712710$

$b = 462$

Identifique los r_i del algoritmo

Los Números Primos

Definición: Un entero positivo $p \neq 1$ se dice que es *primo* si sus únicos divisores positivos son p y 1.

Todo número entero mayor que 1 y que no es primo se denomina ***compuesto***. En consecuencia:

$$n = n_1 \times n_2 \text{ , con } n_1 \text{ y } n_2 > 0$$

Primos Relativos

- Si dos enteros positivos a,b verifican que mcd(a,b) = 1 se dicen que son *primos relativos*.

Cuales de las siguientes parejas de números son primos relativos?

(3,15)
(5,18)
(12,35)
(23,59)

Algunos Lemas

- Lema 1: Un número primo p es primo relativo de un entero n o lo divide.

  Esto es consecuencia de que el mcd(p,n) es uno o p

  Lema 2: Un producto es divisible por un primo p solo si p divide a uno de los factores

  Lema 3: En un producto $q_1 \ldots q_r$ de primos q_i es divisible por un primo p solo si p es igual a algunos de los q_i

  Lema 4: Todo entero n > 1 es divisible por algún primo

Teorema Fundamental de la Aritmética

- Todo entero positivo puede ser escrito como producto de primos. Además la factorización es única, menos en el orden de los primos. En símbolos:

$$A = p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots p_n^{a_n}$$

Donde los a_n son números naturales y los p_n son números primos distintos

Cálculo del mcd por descomposición en factores primos

- Sean a y b dos enteros positivos. Por el TFA

  $a = 2^{e_2} 3^{e_3} 5^{e_5} 7^{e_7} \ldots$ y $b = 2^{f_2} 3^{f_3} 5^{f_5} 7^{f_7} \ldots$

- Supongamos que $a \mid b$. Sea p un primo y que aparece e_p veces en la factorización de a.
- Como $p^{e_p} \mid a$ y $a \mid b$ entonces $p^{e_p} \mid b$ y luego $p^{e_p} \mid p^{f_p}$. En consecuencia $e_p \leq f_p$.
- Si $d = mcd(a,b)$, entonces $d = 2^{x_2} 3^{x_3} 5^{x_5} 7^{x_7} \ldots$;

Donde $x_2 = min(e_2, f_2)$, $x_3 = min(e_3, f_3) \ldots$

Ejemplo: Encontrar el máximo común divisor entre:

$a = 712710$

$b = 462$

por el método de descomposición en sus factores primos.

- Teorema: Existen infinitos números primos.

- Teorema : Si n es un entero compuesto entonces tiene un divisor primo menor o igual que $\sqrt{n}$.

Demostración:

Si n es compuesto puede ser expresado como producto

$n = a \times b$, con a y b enteros positivos > 1.

Luego se debe cumplir que $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$,pues de no ser así $a \times b > \sqrt{n} \times \sqrt{n} = n$.

Por lo tanto n debe tener un divisor menor o igual que $\sqrt{n}$. Este número o bien es primo o por el TFA tiene un divisor primo. En ambos casos tiene un divisor primo $\leq \sqrt{n}$

Ejemplo: Es compuesto el número entero 187 ?

Ejemplo: Es compuesto el número entero 277 ?

Ejemplo: Es compuesto el número entero 1001 ?

Algoritmo

- Calculamos $\sqrt{n} = \sqrt{187} = 13{,}674$
- Tomamos el entero menor o igual a la raíz encontrada: 13
- Luego n si es compuesto debe tener un divisor primo menor o igual a 13.
- Los números primos menores o iguales a 13 son: 13, 11, 7, 5, 3, 2.
- Dividimos en consecuencia 187 por los primos anteriores y si alguna de ellos lo divide exactamente entonces

187 es compuesto

Formulación equivalente del Teorema:

- Si un entero n **no** tiene un divisor primo menor o igual a $\sqrt{n}$ entonces **no** es un número compuesto. Por lo tanto es un número primo

Múltiplos

- Sean a y d $\in$ Z. Si d | a entonces

$\exists c \in Z \,/\, a = c \times d$

y se dice que a es un múltiplo de d.

Los múltiplos de un número d son:

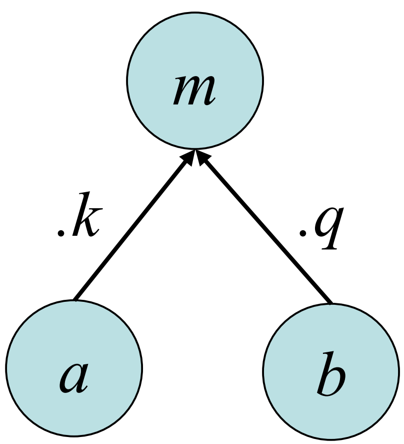
$0, \mp d, \mp 2d, \mp 3d, \ldots \mp kd$ con $k \in Z$

Múltiplo Común

Un número m se dice que es un múltiplo común de a y b cuando es divisible tanto por a como por b. Entonces:

$$a \mid m \text{ y } b \mid m$$

$$m = k.a \text{ y } m = q.b$$



Mínimo Común Múltiplo

- Dados dos números enteros positivos a y b se define el mínimo común múltiplo de a y b y se escribe *mcm(a.b)* al menor de los múltiplos comunes de a y b.

$$mcm(a,b) = {p_1}^{\max(a_1,b_1)} {p_2}^{\max(a_2,b_2)} {p_3}^{\max(a_3,b_3)} \ldots {p_n}^{\max(a_n,b_n)}$$

Ejemplo: Encontrar el mínimo común múltiplo entre:

$$a = 712710$$

$$b = 462$$

por el método de descomposición en sus factores primos.

Mínimo Común Múltiplo

- Teorema 7: Todo múltiplo común de un conjunto de números naturales $a_1, a_2, \ldots, a_n$ es divisible por su mcm.

Ejemplo:

$a_{1=}\ 24$

$a_{2=}\ 50$

$a_{3=}\ 14$

$a_{1=}\ 24 = 2^3 \times 3$

$a_{2=}\ 50 = 2 \times 5^2 \Longrightarrow mcm(24,50,17) = 8x25x7x3=4200$

$a_{3=}\ 14 = 2 \times 7$

Cual es el próximo múltiplo común de estos números?

Relación entre el *mcd* y el *mcm* de dos enteros *a y b*

$$mcd(a,b) \times mcm(a,b) = a \times b$$

Exprese con palabras la fórmula o expresión anterior

- Demostración:

Sean a y b ∈ N y **M=*mcm(a,b)*.** Claramente a.b es un múltiplo común de a y de b y por el teorema 7 M | a.b

Sea a.b = d.M con d ∈ N. [1]

(*Si comparamos esta igualdad con la tesis, vemos que lo que tenemos que demostrar es que* ***d*** *es el* ***mcd (a,b).*** *Para ello primero demostraremos que d es un divisor común de a y b y luego que d divide a todo el resto de los divisores comunes de a y b).*

Ya que M es un múltiplo común de a y b, se tiene que

M = k.a y M = q.b con k y b ∈ N.

Reemplazando en [1]: a.b = d.M = d.k.a = d.q.b. Entonces:

a=d.q y b=d.k

En consecuencia ***d es un divisor común de a y b***.

Sea t un divisor común de a y b. Entonces:

$$a = t.a_1 \qquad y \qquad b=t.b_1 \qquad [2]$$

Entonces $t.a_1.b_1$ es un múltiplo común de a y b. y por el teorema 7

$$M \mid t.a_1.b_1.$$

En consecuencia dado un entero u se tiene que

$$t.a_1.b_1 = M.u. \; [3]$$

Pero de [1] y [2] $\quad d.M = a.b = t^2.a_1.b_1$

Y reemplazando [3] en la igualdad anterior se obtiene

$$d.M = t.M.u$$

Luego d=t.u y en consecuencia $t \mid d$

Entonces d no solo es un divisor común de a y b. sino que además , ***todo divisor común de a y b divide a d***

lo que completa la demostración.

Problema

- En un vecindario, un camión de helados pasa cada 8 días y un *food truck* pasa cada dos semanas. Se sabe que 15 días atrás ambos vehículos pasaron en el mismo día.
- Raúl cree que dentro de un mes los vehículos volverán a encontrarse y Oscar cree esto ocurrirá dentro de dos semanas.
- ¿Quién está en lo cierto?