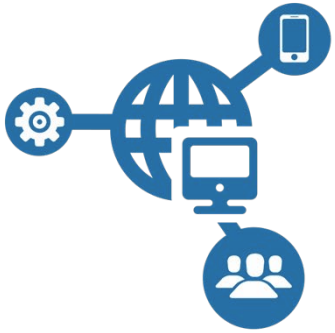

MAESTRÍA EN CIENCIAS EN INGENIERÍA Y TECNOLOGÍAS COMPUTACIONALES

Tema:

Resolución de Problemas

Teoría de Números

Cinvestav Tamaulipas

Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional
Cinvestav - Tamaulipas

Contenido

Temas a desarrollar de Teoría de Números

a. Números naturales

b. Divisibilidad

c. Máximo común divisor

d. Números primos

e. El teorema fundamental de la aritmética

Máximo común divisor

- Este concepto se basa en las proposiciones de la divisibilidad.
- Se consideran los divisores positivos
- La cantidad de divisores de un número es finita, por lo que siempre existirá un divisor máximo
- Sean **a** y **b** dos enteros, 1 siempre es un divisor común de **a** y **b**
- Si **a** es múltiplo de **b**, el conjunto de los divisores comunes de **a** y **b** coincide con el conjunto de los divisores de sólo **b**, entonces el divisor común de **a** y **b** es **b**
- Todo divisor común de **a** y **b** es divisor de **b**

Máximo común divisor

- Si **a = bq + c**, entonces el conjunto divisores comunes de **a** y **b** coincide con el conjunto de divisores comunes de **b** y **c**

  comundivisor(a, b) = comundivisor(b, c)

- Por la igualdad anterior, todo común divisor de **b** y **c** divide a **a** y es común divisor de **a** y **b**
- Sean 12 y 16, los divisores de cada uno son:

  12: 1, 2, 3, 4, 6

  16: 1, 2, 4, 8

  los divisores comunes son 1, 2 y 4

  El máximo común divisor de 12 y 16 es 4

- Si no hay factores primos comunes entre **a** y **b**, el mcd es 1, se dice que son **a** y **b** primos relativos

Máximo común divisor

- Si **a** = 0 = **b**, entonces por cualquier entero distinto de 0 divide a **a** y a **b,** por lo tanto no existe un entero mayor que divida a ambos.
- Supongamos que **a** o **b** es ≠ 0
- Supongamos **a** ≠ 0, todos los divisores de **a** son ≤ **|a|**. Así, el conjunto de **divisores comunes** de **a** y de **b** tiene un **elemento mayor**. A este entero se le llama **máximo común divisor** de **a** y **b**.
- Se representa como **mcd(a,b)**

Máximo común divisor

- Así, el máximo común divisor de **a** y **b** es un entero **g** que satisface:

  1) **g** | a y **g** | b, es decir, **g** es divisor común.

  2) Si **d** es cualquier entero tal que **d** | a y **d** | b,

     entonces d | **g**. Esto implica que en este caso

     |d| ≤ **|g|**, por lo que **g** es el **divisor común máximo**

- Para encontrar el máximo común divisor existen varios métodos: método del conjunto de divisores, el método de factorización completa, el método de la factorización simultánea y el algoritmo de Euclides

Máximo común divisor

- Teorema (Identidad de Bézout). Sean **a**, **b** dos enteros con uno de ellos distinto de cero, entonces:

  1) Existe un **máximo común divisor** de **a** y **b** y, a su vez, es la menor combinación lineal positiva de **a** y **b**, es decir, es de la forma **as** + **bt**, con **s**, **t** ∈ **Z**

  2) Cualesquiera dos **máximos comunes divisores** de **a** y **b** difieren sólo por el signo
- La propiedad 2) indica que al elegir el signo positivo se tiene un único máximo común divisor de **a** y **b**, que se denota **g = mcd(a, b)**.
- La propiedad 1) indica que el mcd de **a** y **b** se puede escribir de la forma g = mcd(a, b) = as + bt. **g** es el menor entero positivo que es combinación lineal de a y b

Máximo común divisor

- Dados dos enteros **a**, **b**, se dice que son **primos entre sí** si mcd(a, b) = 1.
- mcd(a, b, c, d, … k) = 1. Ej.

  (6, 10, 15) = 1, 6, 10 y 15 son primos entre sí
- Lo cual es la base para el siguiente teorema, que es fundamental para la aritmética
- Teorema. Si **a | bc** y mcd(a, b) = 1, entonces **a | c**.
- Demostración. Como 1 = mcd(a, b), entonces 1 es combinación lineal de **a** y **b**, tal que **1 = as + bt**. Multiplicando esta igualdad por c queda **c = c · 1 = acs + bct**, donde **a | acs** y **a | bct**, ya que a | bc. Se sigue que **a | acs + bct = c**, esto es, **a | c**

Máximo común divisor

- Proposición. Sean **a**, **b** dos enteros no nulos, entonces:

  mcd(a,b) = mcd(b,r)

  donde 0 < **r** < ***b*** tal que existe un entero **q** con

  a = bq + **r** (r es el resto de la división de a por b)
- Lo cual indica que es igual de válido calcular el mcd(a,b) que mcd(b,r), con la ventaja de que **r** es un entero de menor tamaño que el original **a**
- Esto es aprovechado por el algoritmo de Euclides para el cálculo del mcd

Máximo común divisor

Métodos para calcular el mcd

1) Método de factorización completa

1) Obtener la factorización completa de cada uno de los números.

Hacer divisiones enteras por números primos hasta llegar a 1. Ej.

36 / 2 = 18 18 / 2 = 9 9 / 9 = 1

la factorización de 36 es 36 = 2, 2, 9

2) Escribir la factorización completa usando potencias para los números repetidos.

Potenciación es la forma abreviada de escribir multiplicaciones consecutivas donde todos los factores son iguales. Ej.

$27 = 3 \times 3 \times 3 = 3^3$ $2^4 = 2 \times 2 \times 2 \times 2 = 16$

Máximo común divisor

1) Método de factorización completa

3) Escoger los factores comunes elevados al **menor exponente**

4) Multiplicar los factores comunes

- Calcular el máximo común divisor de 56 y 980

  56 / **2** = 28 / **2** = 14 / **2** = 7 / **7** = 1 = 2 x 2 x 2 x 7 = 2^3 x **7**

  980 = $\mathbf{2^2}$ x 5 x 7^2

  Factores comunes elevados al menor exponente 2^2 y 7

  Multiplicar los factores seleccionados: 2^2 x 7

  mcd(56, 980) = 2^2 x 7 = **28**

Máximo común divisor

2) Método de factorización simultánea

1) Colocar los números en fila
2) Trazar una línea vertical a la derecha de la fila
3) Identificar el menor número primo que es factor de todos los números en la fila y escribirlo a la derecha de la línea
4) Dividir los números en la fila por el factor identificado
5) Repetir el proceso hasta que los números no tengan ningún factor primo entre ellos
6) Multiplicar los factores identificados a la derecha de la línea vertical para obtener el máximo común divisor.

Máximo común divisor

2) Método de factorización simultánea

Calcular el mcd de 6, 12 y 18

6	12	18	2
3	6	9	3
1	2	3	

el **menor** número **primo** divisor de todos es 2

dividir los números por el factor anterior identificad

repetir hasta que no haya una factor primo entre los números, diferente a 1

multiplicar los factores identificados: 2 x 3

mcd(6, 12, 18) = 2 x 3 = 6

Máximo común divisor

3) El algoritmo de Euclides

- Para calcular el **mcd** de dos enteros **a** y **b** (ambos ≥ 0, suponemos **a** > **b**) se definen $\mathbf{q_i}$ y $\mathbf{r_i}$ recursivamente:

$a = bq_1 + r_1 \quad (0<r_1<b)$

$b = r_1q_2 + r_2 \quad (0<r_2<r_1)$

$r_1 = r_2q_3 + r_3 \quad (0<r_3<r_2)$

....

$r_{k-3} = r_{k-2}q_{k-1} + r_{k-1} \quad (0<r_{k-1}<r_{k-2})$

$r_{k-2} = r_{k-1}q_k \quad (r_k=0)$

Por lo que $mcd(a,b) = mcd(b,r_1) = mcd(r_1,r_2)$

$= \ldots = mcd(r_{k-2},r_{k-1}) = r_{k-1}$

mientras haya **r** y 0< **r** <b
hasta que no haya residuo
ese residuo es el mcd

Máximo común divisor

3) El algoritmo de Euclides

Calcular el mcd de 432 y 124

432 / 124 = 3 + 60

124 / 60 = 2 + 4

60 / 4 = 25 + 0

mcd(432,124) = mcd(124,60)

mcd(124,60) = mcd(60,4)

mcd(60,4) = mcd(25,0)

mcd(432,124) = mcd(25,0)

mcd(25,0) = 25

mcd(432,124) = 25

Máximo común divisor

3) El algoritmo de Euclides

```
procedure mcd(a, b)
      if a < b intercambiar(a,b) //a debe ser mayor
      while b ≠ 0
            r = a mod b
            a = b
            b = r
      endwhile
      return a
endprocedure
```

Máximo común divisor

- Observación. Sean **a,b** enteros no nulos, y sea **d = mcd(a,b)**. Entonces **d** es el menor entero positivo (no nulo) que puede expresarse en la forma
  b = ax + by con x,y ∈ **Z**

- El algoritmo de Euclides proporciona un método para calcular dos valores enteros ***x*** e ***y*** tales que **mcd(a,b) = ax + by**. El método consiste en ir despejando el resto de la última división, el que nos da el valor **mcd(a,b)**, hacia atrás hasta llegar a los valores **a** y **b** de partida.

Máximo común divisor

- Teorema. La ecuación $c = ax + by$, con $a, b, c \in Z$ tiene soluciones enteras si y sólo si $d \mid c$, si $d = mcd(a,b)$.
- Además, la solución general de esta ecuación es de la forma:

$$x = x_1 + (tb / d)$$

$$y = y_1 - (ta / d)$$

para todo valor **t** entero donde (x_1, y_1) es una solución particular cualquiera de la ecuación $c = ax + by$

Máximo común divisor

- Teorema

  Si **g** es el máximo común divisor de **b** y **c**, entonces existen los enteros $\mathbf{x_0}$ e $\mathbf{y_0}$ tales que

  $g = mcd(b,c) = bx_0 + cy_0$

- Demostración
- Considérense las combinaciones lineales **bx** + **cy**, donde **x** e **y** pueden ser todos los enteros {bx + cy}
- Se eligen $\mathbf{x_0}$ e $\mathbf{y_0}$ de tal manera que $\mathbf{bx_0 + cy_0}$ sea el **menor** entero positivo **l** en el conjunto. Así que

  $l = bx_0 + cy_0$

  $g = l$ $\quad\quad$ $g = mcd\ (b,c)$

Máximo común divisor

- Teorema. El máximo común divisor **g** de **b** y **c** puede caracterizarse de las formas siguientes:
  1. Es el menor valor positivo de **bx** + **cy**, donde **x** e **y** pueden ser cualquier entero positivo
  2. Es el común divisor positivo de **b** y **c**, el cual es divisible entre cada divisor común

Máximo común divisor

Ecuaciones diofánticas

- En honor a Diofanto, matemático griego
- Es cualquier ecuación algebraica, generalmente de varias variables, cuyos coeficientes son del conjunto de los números enteros **Z** o los números naturales **N**
- Se trata de ecuaciones cuyas soluciones son números enteros
- Las hay **lineales** (ax + by = c) y no lineales ($x^2 + y^2 = a$)
- Ejemplo X + Y = 5 (ax + by = c)

  * tiene infinitas soluciones en los números reales

  * "pero" si se restrige a los enteros positivos, hay 4 soluciones para (x,y): (1,4) (2,3) (3,2) (4,1).

Máximo común divisor

Ecuaciones diofánticas

- **ax + by =0** se denomina **ecuación lineal homogénea**, cuya solución general es x=b**k**, y =-a**k**, para cualquier número entero k
- Una ecuación diofántica lineal tendrá solución entera si y sólo si el mcd(a,b,c) = mcd(a,b)
- La solución general de una **ecuación lineal no homogénea** se obtiene sumando la solución general de su ecuación homogénea a una de las soluciones particulares
- El reto es encontrar las soluciones particulares

Máximo común divisor

Ecuaciones diofánticas

- Una manera de encontrar soluciones particulaes es aplicar el Teorema de Bezout
- Si d = mcd(a,b), entonces existes dos números enteros **p** y **q**, tales que **pa+qb=d**
- Ejemplo: Resolver la ecuación diofántica: 17x+5y =6

1- Comprobar que la ecuación tiene solución entera

mcd(17,5,6) = (17,5) = 1

2- Encontrar los valores de **x** e **y** de tal manera que se obtenga un múltiplo de 17 y otro 5 cuya diferencia sea 1, 6 o cualquier divisor de 6.

$x = 1, y = 3 \rightarrow 17 \bullet 1 - 5 \bullet 3 = 2$

Máximo común divisor

Ecuaciones diofánticas

2 es divisor de 6, así que si se multiplica por 3 en ambas partes de la ecuación:

$$3(17 \bullet 1 - 5 \bullet 3) = 3 \bullet 2 \rightarrow 17 \bullet 3 - 5 \bullet 9 = 6$$

3- La solución **particular** es $x = 3, y = -9$

4- Se busca la solución de la ecuación homogénea

$$17x + 5y = 0$$

$x = 5k, y = -17k$, con k un número entero cualquiera

5- Así la solución general de la ecuación diofántica es:

$(x,y) = (3,-9) + k(5,-17)$, para cualquier número entero k

Mínimo común múltiplo

Mínimo común múltiplo

- El mínimo común múltiplo de 2 o más números es el menor número, distinto de 0, que es múltiplo de esos números

Ejemplo

Los primeros múltiplos de 2 son: 0,2,4,**6**,8,10,12,14,16,..

Los primeros múltiplos de 3 son: 0,3,**6**,9,12,15,18,21,…

El número más pequeño en ambas listas es el 6, a ese número se le llama **mínimo común múltiplo** de 4 y 7

- El mínimo común múltiplo se representa como **mcm()**
- El mínimo común múltiplo de 2 y 3 se escribe mcm(2,3)=6
- El mínimo común múltiplo de 5, 10 y 15 se escribe mcm(5,10,15)=15

Mínimo común múltiplo

- No existe el **mayor** de los múltiplos comunes de un conjunto de números porque tanto los números naturales como sus múltiplos son infinitos.

Cálculo del mcm de dos o más números

- Crear una lista de múltiplos de varios números y buscar el número más pequeño que se encuentra en todas las listas
- Dos métodos más eficientes (similar a mcd):
  - factorización completa
  - factorización simultánea

Mínimo común múltiplo

- **Método de factorización completa**

1) Obtener la factorización completa de cada número
2) Escribir la factorización completa usando potencias para los números repetidos
3) Crear una lista con cada uno de los factores elevados a la **máxima potencia** con la que aparecen en las factorizaciones completas
4) Multiplicar los factores comunes

Mínimo común múltiplo

- **Método de factorización completa / Ejemplo**

Calcular el mínimo común múltiplo de 45, 60 y 80

1-2) Obtener la factorización completa de cada número usando potencias

45 = 3 * 15 = 3 * 3 * 5 = $\mathbf{3^2 * 5}$

60 = 2 * 30 = 2 * 2 * 15 = 2 * 2 * 3 * 5 = $\mathbf{2^2 * 3 * 5}$

80 = 2 * 40 = 2 * 2 * 20 = 2 * 2 * 2 * 10 = 2 * 2 * 2 * 2 * 5 = $\mathbf{2^4 * 5}$

3) Crear una lista con cada uno de los factores elevados a la máxima potencia con la que aparecen en las factorizaciones completas $\mathbf{3^2}$, $\mathbf{2^4}$, **5**

4) Multiplicar los factores comunes

$3^2 * 2^4 * 5 = 9 * 16 * 5 =$ **720** **mcm(45, 60 y 80) = 720**

Máximo común divisor

- **Método de factorización simultánea**

1) Colocar los números en fila
2) Trazar una línea vertical a la derecha de la fila
3) Identificar el menor número primo que es **divisor de al menos uno de los números** en la fila y escribirlo a la derecha de la línea
4) Dividir los números en la fila por el divisor identificado **si el número es divisible por ese divisor**
5) **Escribir debajo de cada número el mismo número si no es divisible por el divisor identificado**
6) Repetir el proceso con la nueva línea de números para identificar otros divisores hasta que los números de la línea sean todos 1
7) Multiplicar los factores identificados a la derecha de la línea vertical

Máximo común divisor

- **Método de factorización simultánea**

Calcular el mcd de 6, 15 y 18

6	15	18	2
3	15	9	3
1	5	3	3
1	5	1	5
1	1	1	

6 y 18 son divisible por 2, que es el **menor** número **primo** divisor, 15 pasa a la siguiente fila

todos son divisibles por 3, el menor divisor primo

sólo 3 es divisible por 3, el menor divisor primo, 5 pasa a la siguiente fila

sólo 5 es divisible por 5, el menor divisor primo

todos en la fila son 1

multiplicar los factores identificados: 2 x 3 x 3 x 5 = 90

mcm(6, 15, 18) = 90

Ejercicios

...