Centro de
Investigación en
Computación

Maths Problems

Problemas matemáticos

Teoría y ejemplos

Course

Analysis and design of algorithms

Instructor

Acosta Bermejo Raúl

Lecture notes

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

Intro

Introducción

Repaso de matemáticas

GCD (*Greatest Common Divisor*)

MCD (Máximo Común Divisor)

GCD

MCD

Definición

El MCD de dos o más números enteros, es el número entero más grande que los divide sin dejar residuo**.**

Ejemplo:

mcd(36, 60) = 12

Ya que 36/12= 3 y 60/12=5

12 es divisible por 1, 2, 3, 4, 6 y 12 que son divisores comunes de 36 y 60 pero son menores.

GCD

MCD

Algoritmo No. 1

Por descomposición de factores primos

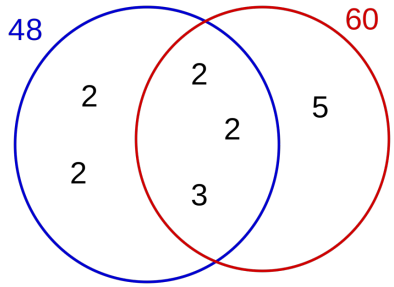
Se realiza la descomposición en factores primos de los números y se toman los factores comunes elevados a la menor potencia y luego se realiza el producto.

48	2
24	2
12	2
6	2
3	3
1	

$48 = 2^4 \cdot 3$

60	2
30	2
15	3
5	5
1	

$60 = 2^2 \cdot 3 \cdot 5$



2^2*3

Este algoritmo sólo es útil para números pequeños.

GCD

MCD

Algoritmo No. 2

Algoritmo de Euclides

Tambien se le llama “método de las divisiones sucesivas”.

Hace uso de las siguientes propiedades:

MCD(A,0) = A.

MCD(0,B) = B.

MCD(A,B) = MCD(B,R) Si A = B·Q + R y B≠0,
donde Q es un entero y R es un entero entre 0 y B-1.

- Las primeras dos propiedades nos permiten encontrar el MCD si cualquiera de los dos números es 0.
- La tercera propiedad nos permite tomar un problema más grande y más difícil de resolver, y reducirlo a un problema más pequeño y más fácil de resolver.

GCD

Ejemplo del Algoritmo de Euclides

Encuentre el MCD de 270 y 192.

- A=270, B=192. Se tiene A ≠0, B ≠ 0
  - División larga para encontrar que 270/192 = 1 con un residuo de 78.
  - Se puede escribir como: 270 = 192 * 1 + 78 equivalente A = B·Q + R
  - Encontrar MCD(192,78), ya que MCD(270,192)=MCD(192,78).
- A=192, B=78. Se tiene A ≠0, B ≠ 0
  - División larga para encontrar que 192/78 = 2 con un residuo de 36.
  - Se puede escribir como :192 = 78 * 2 + 36
  - Encontrar MCD(78,36), ya que MCD(192,78)=MCD(78,36).
- A=78, B=36. Se tiene A ≠0, B ≠ 0
  - División larga para encontrar que 78/36 = 2 con un residuo de 6.
  - Se puede escribir como : 78 = 36 * 2 + 6
  - Encontrar MCD(36,6), ya que MCD(78,36)=MCD(36,6).
- A=36, B=6. Se tiene A ≠0, B ≠ 0
  - División larga para encontrar que 36/6 = 6 con un residuo de 0.
  - Se puede escribir como: 36 = 6 * 6 + 0
  - Encuentra MCD(6,0), ya que MCD(36,6)=MCD(6,0).
- A=6, B=0. Se tiene A ≠0, B =0 => MCD(6,0)=6.
  - En concusión: MCD(270,192) = MCD(192,78) = MCD(78,36) = MCD(36,6) = MCD(6,0) = 6.

LCM

Introducción

MCD (Máximo Común Divisor)
GCD (*Greatest Common Divisor*)
MCM (Mínimo Común Múltiplo)
LCM (*Least Common Multiple*)

Definición

LCM (*Least Common Multiple*)

El LCM es el número más pequeño de los múltiplos comunes de dos o más números.

Ejemplo:

LCM(2,3), los múltiplos de estos dos números son:

2: 2, 4, **6**, 8, 10, 12, 14, 16, 18, ...

3: 3, **6**, 9, 12, 15, 18, 21, …

El más pequeño y común a ambas series es él **6**, así que

LCM(2,3) = 6

GCD

MCD

Algoritmo No. 3

Usando el LCM

Si a y b son distintos de cero se usa la siguiente fórmula:

$$MCD(a,b) = \frac{a * b}{MCM(a,b)}$$

$$\text{MCD}(48,60) = \frac{48 * 60}{MCM(48,60)} = \frac{2880}{240}$$

48: 2,2,2,2,3 = 2^4, 3

60: 2, 2, 3, 5 = 2^2, 3, 5

Los más grandes $2^4 * 3 * 5 = 240$

GCD

MCD

Algoritmo No. 4

Cálculo de más de 2 números

Se calcula de forma recursiva:

GCD(a,b,c) = GCD(a, GCD(b,c))

Prime number

Números primos

De un número
o de un rango

Prime number

Introducción

Un **número primo** es un número natural mayor que 1 que tiene únicamente dos divisores positivos distintos: él mismo y el 1.

Algoritmo ingenuo/inocente (naive)

Para saber si un número P es primo se realizan todas las pruebas, es decir, se analizan todos los números que hay entre 2 y P-1, y se verifica que no tengan división exacta, es decir, sin residuo (definición de módulo).

```
for(i=2; i<=P-1; i++){
   if( P%i == 0 )
      return "No es primo";
   else
      print("Aun no estamos seguros y continuamos");
}
Return "Si es primo";
```

Con el primero que cumpla esta condición, nos paramos, es decir, nos paramos con el 1er múltiplo.

¿Pero qué pasa si queremos conocer los números primos que hay en un intervalo? ¿En necesario hacer todas las pruebas? no es evidente que no.

Prime number

Introducción

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
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Algoritmo mejorado ver 1 (rango)

La criva de eratostenes consiste en eliminar los números que son multiplos de un número inicial N.

Prime number

Introducción

Algoritmo mejorado ver 2

Saber si un número es primo mediante el uso de la raiz cuadrada (cálculo optimizado) lo cual se basa en la siguiente conjetura:

> *Every composite number has a proper factor less than or equal to its square root*.

Un número compuesto es cualquier número natural no primo, a excepción del 1. Es decir, tiene uno o más divisores distintos a 1 y a sí mismo. También se utiliza el término **divisible** para referirse a estos números.

Prime number

Introducción

Ventaja

Reducción del rango

$\sqrt{1x10^6} = 1{,}000 = 1x10^3$

$\sqrt{1x10^{12}} = 1x10^6$

Algoritmo mejorado ver 2

1. Take the Square root of number N.
2. Round the square root to immediately lower integer. Call this no z.
3. Check for divisibility of number N by all prime no below z.
   - If there is no prime no below the value of z which divides N then the number N will be prime.

Example

- Input N= 239.
- Take the square root: $\sqrt{239} = 15.4596$.
- z= 15
- Prime no less than 15: 2,3,7,11 and 13.
- Since 239 is not divisible by any of these: 239 is a prime number.

Prime number

Introducción

Investigar otras Cribas
Euler, Brun, Selberg, etc.

Criba con Raiz

Algoritmo Criba de Eratóstenes (Complejidad $O(n \log\log n)$)

Entrada: Un número natural n

Salida: El conjunto de números primos anteriores a n (incluyendo n)

1. Escriba todos los números naturales desde 2 hasta n
2. **Para** i desde 2 hasta $\lfloor\sqrt{n}\rfloor$ **haga lo siguiente:**
    1. **Si** i no ha sido marcado **entonces:**
        1. **Para** j desde i hasta $n \div i$ **haga lo siguiente:**
            1. Ponga una marca en $i \times j$
3. **El resultado es:** Todos los números sin marca

Acerca de la notación:

- $\lfloor x \rfloor$ es la función parte entera de x
- $a \div b$ es el cociente de dividir a entre b

Función piso (*floor*) vs techo (*ceil*)

Dividendo / Divisor = Cociente + resto/residuo

Prime number

Introducción

Referencias

- Wikipedia
  - Incluye 3 versions: implementación iterative, con raiz, y recursiva.
  - https://www.geeksforgeeks.org/prime-numbers/
- Varias cribas
  - https://matematicas.uam.es/~fernando.chamizo/asignaturas/to2009/semavanz0506/SA2.pdf

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652