División de los enteros

Luis Eduardo Amaya B.
Sede Guanacaste, Universidad de Costa Rica.

MA-0320 - Matemáticas Discretas
Agosto 2020

Contents

Teorema Fundamental de la aritmética

Teorema

Cualquier entero n mayor que 1, se puede expresar como un productos de números primos.
Más aún, si los primos se escriben en orden no decreciente, la factorización es única.

$$n = p_1 \cdot p_2 \cdots p_k$$

donde los números p_k son primos.
Notar que la cantidad de números primos que pueden cumplir este teorema es infinita.

Ejemplo 4: realizar la descomposición en números primos de:

a. 42 $= 6 \cdot 7 = 2 \cdot 3 \cdot 7$
b. 100 $= 4 \cdot 25 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
c. 17 $= 1 \cdot 17$

Máximo común divisor

Definición

Sean m y n enteros diferentes de cero. Un divisor común de m y n es un entero que divide tanto a m como a n, a partir de lo anterior podemos definir al ***máximo común divisor****, denotado como* $mcd(m,n)$ *como el divisor común mas grande de m y n*

Ejemplo 5:

- Los divisores positivos del 30 son: 1, 2, 3, 5, 6, 10, 15, 30.
- Los divisores positivos del 105 son: 1, 3, 5, 7, 15, 21, 35, 105.
- Los divisores positivos comunes de 30 y 105 son 1, 3, 5, 15.
- De lo anterior tenemos

$$mcd(30,105) = 15$$

$$\begin{array}{l|l} 30, 105 & 3 \\ 10, 35 & 5 \\ 2, 7 & 15 \end{array}$$

$mcd(a,b) = mcd(b,a)$

Máximo común divisor

Existe otra forma de encontrar el máximo común divisor de dos enteros *m* y *n* observando con cuidado sus factorizaciones primas.

Ejemplo 6:

- La descomposición en números primos de 30 es, $30 = 2^1 \cdot 3^1 \cdot 5^1$.
- La descomposición en números primos de 105 es, $105 = 3^1 \cdot 5^1 \cdot 7^1$.
- En la descomposición en primos de 30 y 105 son comunes 3 y 5.
- De lo anterior tenemos

$$mcd(30, 105) = 3 \cdot 5 = 15$$

$$30 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0 \quad 1$$

$$105 = 1 \; 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^1$$

Máximo común divisor

Lo anterior es un caso del siguiente teorema

Teorema

Sean m y n enteros, $m > 1$, $n > 1$ con factorizaciones primas

$$m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

$$n = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

Si el primo p_i no es un factor de m, se hace $a_i = 0$. De manera similar, si el primo p_i no es un factor de n, se hace $b_i = 0$, entonces

$$\boxed{mcd(m, n) = p_1^{min(a_1, b_1)} p_2^{min(a_2, b_2)} \cdots p_n^{min(a_n, b_n)}}$$

Máximo común divisor

Ejemplo 7

Haciendo uso del teorema anterior determinar $mcd(30, 105)$.

Tenemos

i) $30 = 2^1 \cdot 3^1 \cdot 5^1 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0$

ii) $105 = 3^1 \cdot 5^1 \cdot 7^1 = 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^1$

$mcd(30, 105) = 2^{\min(0,1)} \cdot 3^{\min(1,1)} \cdot 5^{\min(1,1)} \cdot 7^{\min(0,1)}$

$= 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^0 = 15$

$1 \quad 1$

$0^0 = ???$

0

Máximo común divisor

Ejemplo 8

$a^0 = 1, \; a \in \mathbb{R} - \{0\}$

Haciendo uso del teorema anterior determinar $mcd(82320, 950796)$.

Tenemos

i) $82320 = 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^3 = 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^3 \cdot 11^0$

ii) $950796 = 2^2 \cdot 3^2 \cdot 7^4 \cdot 11^1 = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^4 \cdot 11^1$

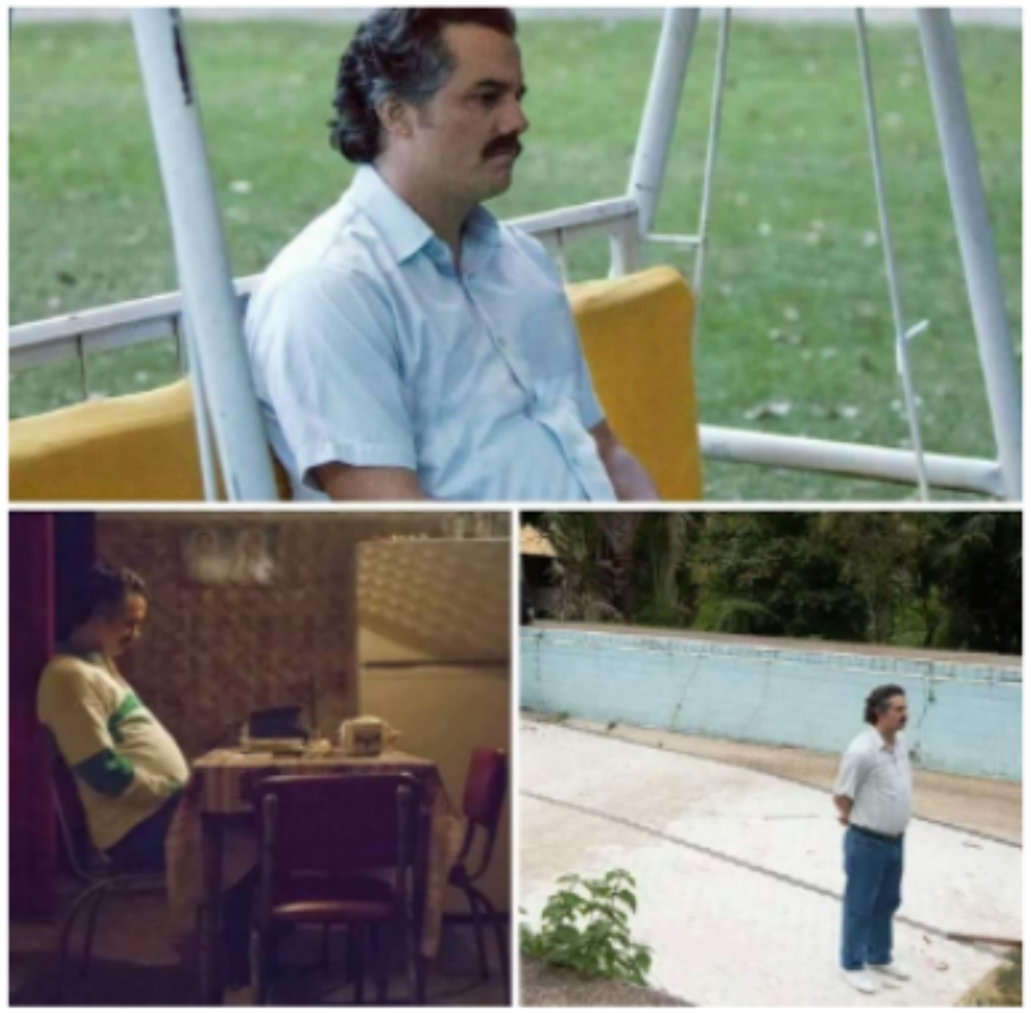
$m.c.d(82320, 950796) = 2^{\min(2,4)} \cdot 3^{\min(1,2)} \cdot 5^{\min(1,0)} \cdot 7^{\min(3,4)} \cdot 11^{\min(0,1)}$

$= 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^3 \cdot 11^0 = \boxed{4116}$

Máximo común divisor

¿Cómo te encuentro de forma eficiente?

Ni el método de la "lista de todos los divisores" del ejemplo 5 ni el de los factores primos del ejemplo 7 es eficiente para encontrar el máximo común divisor.
El problema es que ambos métodos requieren encontrar los factores primos de los números implicados y no se conoce un algoritmo eficiente.



Existe una solución, la cual no esta en **photomath**...

El algoritmo euclidiano

Introducción

El algoritmo euclidiano es un algoritmo antiguo, conocido y eficiente para encontrar el máximo común divisor de dos enteros.
El algoritmo euclidiano se basa en el hecho de si

$$r = mod(a, b) = a \bmod b$$

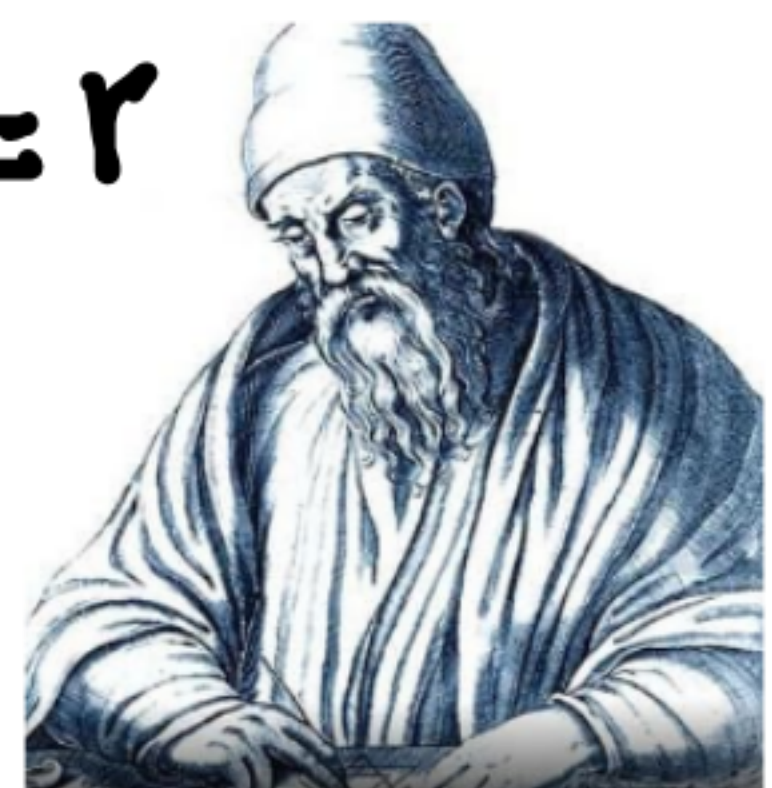
entonces

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

30, 105

$105 \bmod 30 = 15 = r$

$m.c.d(105,30) = m.c.d(30,15)$



Euclides
(330 a.C. - 275 a.C.)

$$\boxed{m.c.d(a,0) = a}$$

$m.c.d(20,0) = 20$

El algoritmo euclidiano

Algoritmo

Teorema

Si a es un entero no negativo, b es un entero positivo y $r = mod(a, b)$ entonces

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

Algoritmo euclidiano

Este algoritmo encuentra el máximo común divisor de los enteros no negativos a y b, donde no son cero a y b.

Entrada: a y b (enteros no negativos, ambos diferentes de cero)
Salida: máximo común divisor de a y b

```
mcd(a, b) {
    // sea a el mayor
    if (a < b)
        intercambia(a, b)
    while (b ¬=0) {
        r = a mod b
        a = b
        b = r
    }
    return a
}
```

El algoritmo euclidiano

Implementación en Mathematica

```
MaxComDiv[a_, b_] := Module[{x = a, y = b, r = 0},
                     módulo
  temp1 = x;
  temp2 = y;
  If [x < y,
  si
   temp1 = y;
   temp2 = x;
  ];
  (*Lo anterior es para garantizarnos siempre el mayor*)

  While[temp2 != 0,
  mientras
   r = Mod[temp1, temp2];
       operación módulo
   temp1 = temp2;
   temp2 = r;

  ];
  Print[temp1];
  escribe
 ];
```

El algoritmo euclidiano

Ejemplo 9

Haciendo uso del algoritmo euclidiano determinar $mcd(30, 105)$.

$a = 30$, $b = 105$ // cambiar

$mcd(30, 105) = mcd(105, 30)$

i) $a = 105$, $b = 30$, $b \neq 0$, entonces

$r = mod(105, 30) \Rightarrow r = 15$

ahora $\boxed{a = b = 30,\ b = r = 15}$

$mcd(105, 30) = mcd(30, 15)$

ii) $a = 30$, $b = 15$, $b \neq 0$, entonces

$r = \mathrm{mod}(30, 15) = 0$

ahora $a = b = 15$, $b = r = 0$

Como $b = 0$, Fin, Salida $= a = 15$

$\underbrace{\mathrm{mcd}(105, 30)}_{15} = \underbrace{\mathrm{mcd}(30, 15)}_{15} = \underbrace{\mathrm{mcd}(15, 0)}_{15}$