Aritmética entera

AMD – Grado en Ingeniería Informática

Objetivos

Al finalizar este tema tendréis que:

- Calcular el máximo común divisor de dos números enteros aplicando el algoritmo de Euclides y expresarlo en función de dichos números aplicando el algoritmo de Euclides extendido.
- Saber si un número es primo y si no lo es, ponerlo como producto de primos
- Calcular todos los divisores de un número

División entera

El **conjunto de los números enteros** denotado por $\mathbb{Z}$ contiene todos los números naturales junto sus negativos:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Suponemos que sabéis sumar, restar, multiplicar y dividir. Aún así, recordemos la división junto sus propiedades:

Teorema de la división

Para $a \in \mathbb{Z}, b \in \mathbb{N}$, existen unos únicos $q, r \in \mathbb{Z}$ tales que:

$$a = q \cdot b + r, 0 \leq r < b$$

A los números a, b, q y r se les llama dividendo, divisor, cociente y resto respectivamente.

Definición

Se dice que b divide a a o que a es múltiplo de b si el resto es 0. Se denota $b|a$

Ejemplo

Si cogemos $a = 13$ y $b = 4$, entonces al tener

$$13 = 3 \cdot 4 + 1,$$

el cociente es 3 y el resto es 1.

Ejemplo

¡Atención! Si cogemos $a = -13$ y $b = 4$, entonces al tener

$$-13 = (-4) \cdot 4 + 3,$$

el cociente es -4 y el resto es 3.

Ejemplo

Si cogemos $a = 36$ y $b = 9$, entonces al tener

$$36 = 4 \cdot 9 + 0,$$

el cociente es 4, el resto es 0, por lo que el 9 divide al 36 o el 36 es múltiplo de 9.

Propiedades de la división

Sean $a, b, c \in \mathbb{Z}$. Entonces:

1. $a|b \Longrightarrow a|bk, \forall\, k \in \mathbb{Z}$.
2. $a|b$ y $b|c \Longrightarrow a|c$.
3. $a|b, a|c \Longrightarrow a|(xb + yc)$ para cualquier par de enteros x e y.
4. $a, b > 0, a|b \Longrightarrow a \leq b$.
5. $a|b, b|a \Longrightarrow a = b$ o $a = -b$.

Máximo común divisor

Supongamos que tenemos dos números enteros, a y b.

Definición

Un número **positivo** d es un común divisor de a y b si divide a ambos.

Definición I de mcd

Un número **positivo** d es el máximo común divisor de a y b si es común divisor y si es divisible por cualquier otro común divisor de a y b. Notación: $\mathrm{mcd}(a, b)$

Otra manera de definir el máximo común divisor es:

Definición II de mcd

El máximo común divisor de a y b es el mayor de los divisores comunes de a y b. Notación: $\mathrm{mcd}(a, b)$

Dos números se dicen coprimos si su mcd es igual a 1.

Recordemos el método "malo" que conocéis la mayoría de vosotros para calcular el mcd. Para ello necesitamos la definición de número primo.

Número primo

Un número enero $p > 1$ es primo si sus únicos divisores positivos son 1 y él mismo.

Ejemplos de números primos: $2, 3, 5, 7, 11, \ldots$ ¿sabríais decir cuántos nº primos hay?

Teorema fundamental de la Aritmética

Todo número entero se puede factorizar en producto de primos. Es decir, sea $n > 1, n \in \mathbb{Z}$, entonces existen números primos $p_1, \ldots, p_k$ tales que

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k} \text{ con } p_1 < p_2 < \ldots < p_k$$

Esta factorización es única.

Ejemplos

$48 = 2^4 \cdot 3, \quad 124 = 2^2 \cdot 31, \quad 234 = 2 \cdot 3^2 \cdot 13, \quad 745 = 5 \cdot 149, \quad 1148 = 2^2 \cdot 7 \cdot 41$

Cálculo poco eficiente del mcd y del mcm

Recordad que el mínimo común múltiplo (mcm) de dos números enteros es el menor de los múltiplos comunes. Entonces, dados dos números enteros junto su factorización en primos,

- su mcd es el producto de los factores comunes con su menor exponente (http://es.wikipedia.org/wiki/Maximo_comun_divisor)
- su mcm es el producto de los factores comunes y no comunes con su mayor exponente, (http://es.wikipedia.org/wiki/Minimo_comun_multiplo)

Ejemplo

El de la Wikipedia:

$$60 = 2^2 \cdot 3 \cdot 5, \quad 48 = 2^4 \cdot 3,$$

$$\mathrm{mcd}(60, 48) = 2^2 \cdot 3 = 12, \quad \mathrm{mcm}(60, 48) = 2^4 \cdot 3 \cdot 5 = 240.$$

PROBLEMA: NO EXISTE UN ALGORITMO EFICAZ PARA LA FACTORIZACIÓN (http://es.wikipedia.org/wiki/Descomposicion_en_factores_primos)

Algoritmo de Euclides

El Algoritmo de Euclides sirve para calcular de forma sencilla el máximo común divisor de dos números a y b. Para enunciar este algoritmo nos serviremos de resultados previos.

Teorema

Sean $b \leq a$ con $b \neq 0$ tal que $a = b \cdot q + r$ con $0 \leq r < b$. Entonces

1. Los divisores comunes de a y b también son divisores de r.
2. Los divisores comunes de b y r también son divisores de a.

Teorema

Si $a = bq + r$, con $a, b, q, r \in \mathbb{Z}, b \neq 0$, se cumple $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$.

Entonces para calcular el mcd tan sólo tenemos que ir dividiendo.

Cálculo eficiente del mcd

Sean a y b dos números enteros. Como $\mathrm{mcd}(a,b) = \mathrm{mcd}(|a|,|b|)$, podemos suponer $a \geq b > 0$. Veamos cómo calculamos su mcd usando el Algoritmo de Euclides.

Algoritmo de Euclides

- Dividimos a por b tal que $a = bq_1 + r_1$, con $0 \leq r_1 < b$.
  1. Si $r_1 = 0$, entonces $b = \mathrm{mcd}(a,b)$ y hemos terminado.
  2. Si $r_1 \neq 0$, sustituimos (a,b) por (b,r_1) y repetimos el proceso hasta llegar al resto igual a 0.

Ejemplo

Seguimos con el de la Wikipedia, $a = 60$, $b = 48$,

1. $60 = 1 \cdot 48 + 12$. Como el resto no es 0, divido ahora 48 entre 12.
2. $48 = 4 \cdot 12 + 0$ Como el resto es 0, el mcd buscado es 12.

Observad que este cálculo es mucho más sencillo que descomponer 60 y 48 en primos.

Teorema de Bezout

El teorema de Bezout nos dice que el mcd de dos números se puede expresar como combinación de dichos números:

Teorema de Bezout

Sean a, b enteros no nulos. El máximo común divisor de a y b es el menor número entero positivo que puede expresarse de la forma $ax + by$, con $x, y \in \mathbb{Z}$.

Puede parecer difícil calcular los valores de x e y de forma que $\mathrm{mcd}(a, b) = ax + by$. Sin embargo existe una modificación del algoritmo de Euclides, el algoritmo de Euclides extendido, que permite calcular a la vez el máximo común divisor y los valores de x e y.

Algoritmo de Euclides extendido

Sirve para hallar el mcd y los términos de la combinación. Veamos un ejemplo:

Ejemplo

Calcula $\mathrm{mcd}(3120, 270)$ y x, y tales que $\mathrm{mcd}(3120, 270) = 3120x + 270y$.

Paso 1.- Cálculo de la sucesión de restos via el algoritmo de Euclides:

1. $3120 = 11 \cdot 270 + 150$.
2. $270 = 1 \cdot 150 + 120$.
3. $150 = 1 \cdot 120 + 30$.
4. $120 = 4 \cdot 30 + 0$, tal que $\boxed{30 = \mathrm{mcd}(3120,270).}$

Paso 2.- Cálculo de x e y: realizamos el camino inverso al algoritmo de Euclides empezando por la expresión donde el máximo común divisor es igual a un resto. Iremos sustituyendo valores hasta llegar a los números 3120 y 270.

3. $150 - 1 \cdot 120 = 30$,
2. $150 - 1 \cdot (270 - 1 \cdot 150) = 30 \implies 2 \cdot 150 - 270 = 30$
1. $2 \cdot (3120 - 11 \cdot 270) - 270 = 30 \implies 2 \cdot 3120 - 23 \cdot 270 = 30$

Así pues, $\mathrm{mcd}(3120, 270) = 30 = 2 \cdot 3120 + (-23) \cdot 270$. Luego, $x = 2, y = -23$.

Descomposición de un nº en primos

El siguiente resultado nos permite ver si un número se factoriza o no, y si se factoriza, encontrar un factor:

Teorema

Un número $a \in \mathbb{Z}, a > 1$ no es primo si y sólo si existe un nº primo $p \leq \sqrt{a}$ tal que p divide a a.

Con lo cual si queremos factorizar un número, tan sólo tenemos que ver si se factoriza por los primos menores o iguales a su raíz cuadrada.

Ejemplos

- $a = 40$. Como $6 < \sqrt{40} < 7$, veamos si se factoriza por el 2,3 o 5. Es facil de ver que $40 = 2^3 \cdot 5$.
- $a = 53$. Como $7 < \sqrt{53} < 8$, veamos si se factoriza por el 2,3, 5 o 7. Observamos que
  - $53 = 2 \cdot 26 + 1$,
  - $53 = 3 \cdot 17 + 2$,
  - $53 = 5 \cdot 10 + 3$,
  - $53 = 7 \cdot 7 + 4$,

  con lo cual 53 es primo.

Divisores de un número

Dado un número factorizado en primos, podemos calcular todos sus divisores. Si

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k} \text{ con } p_1 < p_2 < \ldots < p_k \text{ primos,}$$

entonces todo divisor d de n es de la forma

$$d = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_k^{m_k} \text{ con } 0 \leq m_i \leq e_i,$$

por lo que hay $(e_1 + 1) \cdot \ldots \cdot (e_k + 1)$ divisores.

Ejemplo

Los divisores de $40 = 2^3 \cdot 5$ son:

1. Considerando el primo 2:

$$2, \quad 10 = 2 \cdot 5; \quad 4 = 2^2; \quad 20 = 2^2 \cdot 5; \quad 8 = 2^3; \quad 40 = 2^3 \cdot 5;$$

2. Considerando el primo 5, descartando el 2:

$$5$$

3. No olvidemos el 1

En total: $(3 + 1) \cdot (1 + 1) = 8$ divisores.