TEMA 1 : ARITMÈTICA MODULAR i XIFRATS.

1.1. ALGORITME DE EUCLIDES i IDENTITAT DE BÉZOUT.

Començarem recordant un resultat molt conegut i recordant conceptes també coneguts com el màxim comú divisor i el mínim comú múltiple.

TEOREMA (De la divisió entera)

Siguin a i b enters $a \geq b$. Aleshores, existeixen enters q (quocient) i r (resta) tals que

$$a = q \cdot b + r \quad \text{on} \quad 0 \leq r < b$$

I aquesta expressió és única.

DEFINICIÓ: Siguin $m, n \in \mathbb{N}$

ⓐ Diem que n divideix a m $\left(n \mid m\right)$ si existeix $l \in \mathbb{N}$ tal que

$$m = l \cdot n$$

(en altres paraules en fer la divisió entera el $r=0$) De vegades es denota $m = \dot{n}$

ⓑ Siguin $a, b \in \mathbb{N}$

El nombre més gran n que verifica que $n \mid a$ i $n \mid b$ és el que anomenem MÀXIM COMÚ DIVISOR i es denota per

$$n = mcd\,(a,b) = MCD(a,b)$$

ⓒ Siguin $a, b \in \mathbb{N}$

El nombre més petit $m \in \mathbb{N}$ que verifica que $a \mid m$ i $b \mid m$ l'anomenem el MÍNIM COMÚ MÚLTIPLE de a i b i es denota per

$$m = mcm\,(a,b) = MCM(a,b)$$

PROPOSICIÓ:

Siguin $a, b \in \mathbb{N}$. Suposem que

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

Alashores,

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

NOTE BOOK

EXEMPLE

Volem calcular el mcd (2406, 654)

Si fem la divisió, $2406 = 3\cdot 654 + 444$

Per tant, $mcd(2406,654) = mcd(654,444)$. Tornant a fer la divisió:

$$654 = 1\cdot 444 + 210$$

Per tant, $mcd(654,444) = mcd(444,210)$. Com que $444 = 2\cdot 210 + 24$

tenim $mcd(444,210) = mcd(210,24)$. Finalment com

$$210 = 8\cdot 24 + 18 \quad ; \quad 24 = 1\cdot 18 + 6 \quad , \quad 18 = 6\cdot 3$$

Tenim $mcd(2406,654) = mcd(18,6) = 6$

Aquest resultat ens dóna una forma pràctica de calcular el mcd entre dos nombres. Això és el que anomenem ALGORITME D'EUCLIDES.

ALGORITME D'EUCLIDES

Donats $a, b \in \mathbb{N}$ definim de manera recursiva els enters q_i, r_i mitjançant les equacions que obtenim de fer les divisions de forma recursiva:

$$a = q_1\cdot b + r_1 \qquad (0 \le r_1 < b)$$
$$b = q_2\cdot r_1 + r_2 \qquad (0 \le r_2 < r_1)$$
$$r_1 = q_3\cdot r_2 + r_3 \qquad (0 \le r_3 < r_2)$$
$$\vdots$$
$$r_{k-3} = q_{k-1}\cdot r_{k-2} + r_{k-1}$$
$$r_{k-2} = q_k\cdot r_{k-1} + \underset{\overset{\|}{0}}{r_k}$$

Els restes cada cop són més petits per tant sempre arribarem a resta 0.

Aleshores el MCD que busquem és:

$$mcd(a,b) = mcd(b,r_1) = mcd(r_1,r_2) = mcd(r_2,r_3) = \cdots =$$
$$= mcd(r_{k-2}, r_{k-1}) = r_{k-1}$$

En altres paraules el mcd és el últim resta no nul de l'algoritme de Euclides.

EXEMPLE mcd (2450, 510)

$$2450 = 4\cdot 510 + 410$$
$$510 = 1\cdot 410 + 100$$
$$410 = 4\cdot 100 + 10 \longrightarrow \text{darrer resta no nul}$$
$$100 = 10\cdot 10$$

Per tant mcd $(2450, 510) = 10$.
$\llcorner$

OBS : Quan parlem de la factorització en nombres primers parlarem d'una altra forma de calcular el mcd i el mcm però no pràctica quan tenim nombres grans.
$\llcorner$

Com a segona aplicació de l'algoritme tenim la identitat de Bézout.

TEOREMA (IDENTITAT DE BÉZOUT)

Siguin $a, b \in \mathbb{N}$ i sigui $d = \text{mcd}(a,b)$. Aleshores existeixen p i $q \in \mathbb{Z}$ tals que

$$\boxed{d = p\cdot a + q\cdot b}$$

$\llcorner$.

Observem que l'algoritme de euclides ens dóna de forma explícita la manera de calcular p i q.

En efecte, segons l'algoritme de euclides (seguint la notació anterior)

$$d = \text{mcd}(a,b) = r_{k-1} \underset{\text{substituïm en la anterior}}{=} r_{k-3} - r_{k-2}\cdot q_{k-1}$$

Sabem que $r_{k-2} = r_{k-4} - r_{k-3}\cdot q_{k-2}$ per tant, substituint

$$d = r_{k-3} - q_{k-1}(r_{k-4} - r_{k-3}\cdot q_{k-2}) \underset{\text{operem}}{=} (q_{k-1}\cdot q_{k-2} + 1)\cdot r_{k-3} - q_{k-1}\cdot r_{k-4}$$

Ara sabem que $r_{k-3} = r_{k-5} - r_{k-4}\cdot q_{k-3}$ i podríem anar substituint i operant fins arribar a una expressió en a i b.
$\llcorner$.

EXEMPLE Hem vist que $6 = mcd(2406, 654)$.

Per calcular-lo hem fet servir l'algoritme de euclides i hem vist que:

$$
\begin{aligned}
2406 &= 3\cdot 654 + 444 \quad (5)\\
654 &= 1\cdot 444 + 210 \quad (4)\\
444 &= 2\cdot 210 + 24 \quad (3)\\
210 &= 8\cdot 24 + 18 \quad (2)\\
24 &= 1\cdot 18 + 6\\
18 &= 3\cdot 6
\end{aligned}
$$

Per tant ara per determinar la identitat de Bézout anirem substituint enrera i operant:

$$6 = 24 - 1\cdot 18 \underset{(2)}{=} 24 - 1\cdot(210 - 8\cdot 24) \underset{\text{opero}}{=} 9\cdot 24 - 1\cdot 210 \underset{(3)}{=} 9(444 - 2\cdot 210) - 1\cdot 210$$

$$\underset{\text{opero}}{=} 9\cdot 444 - 19\cdot 210 \underset{(4)}{=} 9\cdot 444 - 19(654 - 1\cdot 444) = 28\cdot 444 - 19\cdot 654 \underset{(5)}{=}$$

$$= 28(2406 - 3\cdot 654) - 19\cdot 654 = 28\cdot 2406 - 103\cdot 654$$

És a dir, $\boxed{6 = 28\cdot 2406 - 103\cdot 654}$

OBSERVACIÓ:

$$mcm(a,b) = \frac{|ab|}{mcd(a,b)}$$

Per tant l'algoritme de euclides indirectament permet calcular el mcm(a,b).

DEFINICIÓ

Diem que a i b són primers entre ells o COPRIMERS si

$$mcd(a,b) = 1.$$

Per tant si a i b són coprimers, existeixen p i q tals que

$$1 = p\cdot a + q\cdot b.$$

└.

DEFINICIÓ:

Diem que p és PRIMER, $p \geq 2$, si els únics nombres naturals que divideixen a p són 1 i p.

└.

PROPOSICIÓ:

Sigui $p \in \mathbb{N}$ primer i $a_1 — a_m \in \mathbb{N}$

Si $p | a_1 \cdots a_m \Rightarrow \exists i$ tal que $p | a_i$

L.

Aquest resultat ens permet demostrar:

TEOREMA

Sigui $n \in \mathbb{N}$, $n \geq 2$. Aleshores existeixen nombres primers diferents $p_1 — p_k$ tals que

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots \cdots p_k^{a_k} \quad , a_i \in \mathbb{N}$$

A més aquesta descomposició és única llevat l'ordre dels factors.

L.

Aquest resultat sovint es coneix com el Teorema de descomposició en factors primers.

OBS:

Si coneixem la factorització en primers de dos enters a i b aleshores es fàcil determinar mcd(a,b) i mcm(a,b).

L.

La relació de divisibilitat i sobretot la primalitat d'un nombre són conceptes molt lligats a la SEGURETAT INFORMÀTICA en el que denominem CRIPTOGRAFIA

Aquest dos conceptes són la clau per poder enviar un missatge i que una persona aliena al sistema no el pugui desxifrar.

La idea fonamental és que els algoritmes que es coneixen per saber si un nombre és primer o no requereixen molt de temps. Fins el punt de que si multipliquem dos nombres primers "prou grans" i donem aquest valor a una tercera persona, no tindrà forma ni eines de descobrir quins són aquest dos primers. Amb computació "usual" la factorització en nombres primers és un problema sense solució. La cosa canviaria possiblement si tinguéssim la computació quàntica. En parlarem al final del tema.

Un altre problema obert i que ha portat a molta gent a investigar-lo però que segueix sent un misteri és la distribució de nombres primers al llarg dels enters.