# QUÈ HEM FET FINS ARA?

El darrer que hem treballat és el final del tema de funcions i la primera part del tema de divisibilitat.

# CLASSE D'AVUI 27/11/2020

Avui treballarem part del que ens queda del tema de divisibilitat.

Amb els exemples anteriors hem vist una manera de calcular el màxim comú divisor molt eficient. Mirem el darrer exemple i sistematitzem els càlculs:

Per calcular el $mcd(122, 54)$ vam fer l'esquema:

| | | | | |
|---|---|---|---|---|
| | 2 | 3 | 1 | 6 |
| 122 | 54 | 14 | 12 | 2 |
| 14 | 12 | 2 | 0 | |

$\rightarrow mcd(122, 54) = 2$

i pel raonament que vam fer el màim comú divisor és el darrer residu diferent de zero.

En general es pot fer el mateix? Sí: suposem que hem de calcular $mcd(a, b)$. Podem suposar per les propietats del màxim comú divisor que els dos nombres són positius i que $a \geq b$. Seguim com en els exemples la mateixa idea que surt del teorema d'Euclides (anar treient $b$ unitats al nombre $a$):

| | |
|---|---|
| $a$ | $b$ |
| $r_2$ | $q_1$ |

$$\rightarrow \left.\begin{array}{c} mcd(a,b) = mcd(a - bq_1, b) = mcd(r_2, b) = mcd(b, r_2) \\ a = bq_1 + r_2 \\ 0 \leq r_2 < b \end{array}\right\} \rightarrow$$

| | |
|---|---|
| $b$ | $r_2$ |
| $r_3$ | $q_2$ |

$$\rightarrow \left.\begin{array}{c} mcd(b,r_2) = mcd(b - r_2q_2, r_2) = mcd(r_3, r_2) = mcd(r_2, r_3) \\ b = r_2q_2 + r_3 \\ 0 \leq r_3 < r_2 \end{array}\right\} \rightarrow$$

| | |
|---|---|
| $r_2$ | $r_3$ |
| $r_4$ | $q_3$ |

$$\rightarrow \left.\begin{array}{c} mcd(r_2,r_3) = mcd(r_2 - r_3q_3, r_3) = mcd(r_4, r_3) = mcd(r_3, r_4) = \\ r_2 = r_3q_3 + r_4 \\ 0 \leq r_4 < r_3 \end{array}\right\} \rightarrow \ldots$$

S'observa que els residus van decreixent $r_2 > r_3 > r_4 > \ldots$ i són nombres naturals més grans que o iguals que $0$. Per tant, tard o d'hora, arribarem a un residu nul: diem-li

$r_{n+1} = 0$ i $r_n \neq 0$ el darrer residu no nul. Per la construcció que estem fent tenim:

$$r_2 > r_3 > r_4 > \ldots > r_n > r_{n+1} = 0$$

$$mcd(a,b) = mcd(b,r_2) = mcd(r_2,r_3) = mcd(r_3,r_4) = \ldots = mcd(r_{n-1},r_n) = mcd(r_n,0) = r_n$$

Així els càlculs els podem escriure en una taula com la següent:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | $q_1$ | $q_2$ | $q_3$ | $q_4$ | ... | $q_{n-1}$ | $q_n$ | |
| $a$ | $b$ | $r_2$ | $r_3$ | $r_4$ | ... | $r_{n-1}$ | $r_n$ | 0 |
| $r_2$ | $r_3$ | $r_4$ | $r_5$ | ... | ... | $r_{n+1} = 0$ | | |

Per escriure les fórmules en forma recurrent va bé anomenar $r_1 = b,\ r_0 = a$ i observant les igualtats:

$r_0 = r_1 \bullet q_1 + r_2$ (o sigui $a = b \bullet q_1 + r_2$)

$r_1 = r_2 \bullet q_2 + r_3$ (o sigui $b = r_2 \bullet q_2 + r_3$)

$r_2 = r_3 \bullet q_3 + r_4$

$r_3 = r_4 \bullet q_4 + r_5$

$\ldots$

s'obtenen les fórmules: $r_0 = a,\ r_1 = b,\ r_i = r_{i+1}q_{i+1} + r_{i+2},\ 0 \leq r_{i+2} < r_{i+1},$ $i = 0,1,2,\ldots,n-1$. Aquesta sistematització del càlcul es diu algorisme d'Euclides.

**EX.**: Calculeu $mcd(125,35)$.

| | | | | | |
|---|---|---|---|---|---|
| | 3 | 1 | 1 | 3 | |
| 125 | 35 | 20 | 15 | 5 | 0 |
| 20 | 15 | 5 | 0 | | |

$\rightarrow mcd(125,35) = 5$

De vegades s'escriu sense la darrera fila:

| | | | | | |
|---|---|---|---|---|---|
| | 3 | 1 | 1 | 3 | |
| 125 | 35 | 20 | 15 | 5 | 0 |

$\rightarrow mcd(125,35) = 5$

**EX.**: (15) Demostreu que $mcd(n,n+2) = 2$ si $2|n$ i $1$ altrament.
Utilitzem el teorema d'Euclides:

$$mcd(n,n+2) = mcd(n,n+2-n) = mcd(n,2) = \begin{cases} 2 \text{ si } 2|n \\ 1 \text{ si } no(2|n) \end{cases}$$

tal com es demanava de raonar.

I què podem dir de la divisió entera que hem estat utilitzant? La divisió entera o euclidiana que vau aprendre a l'escola es basa en el resultat següent:

**PROP**.: Donats $a, b$ enters amb $b \neq 0$, existeixen uns únics enters $q, r$ tals que:

$$a = bq + r, \quad 0 \leq r < |b|$$

**DEM**.: Anomenem $[x] \in \mathbb{Z}$ part entera del nombre $x \in \mathbb{R}$, que consisteix en donar el nombre enter més gran d'entre els que són menors o iguals que $x$ ($[5,1] = 5$, $[7] = 7$, $[-2,1] = -3$) que satisfà: $[x] \leq x < [x] + 1$. De vegades s'escriu també $\lfloor x \rfloor$ o bé $E(x)$.

Primer veiem que sí que existeixen $q$ i $r$: només cal calcular $q = sig(b)\left[\frac{a}{|b|}\right]$, $r = a - bq$ amb $sig(b) = \frac{b}{|b|}$, és a dir, $sig(b) = 1$ si $b > 0$ i $sig(b) = -1$ si $b < 0$. Per construcció $a = bq + r$ perquè $r = a - bq$. Ara ens falta veure que $0 \leq r < |b|$:

$$\left[\frac{a}{|b|}\right] \leq \frac{a}{|b|} < \left[\frac{a}{|b|}\right] + 1 \Rightarrow bsig(b)\left[\frac{a}{|b|}\right] \leq bsig(b)\frac{a}{|b|} < bsig(b)\left[\frac{a}{|b|}\right] + bsig(b) \Rightarrow$$

$$\Rightarrow bq \leq (sig(b))^2 a < bq + bsig(b) \Rightarrow bq \leq a < bq + |b| \Rightarrow 0 \leq a - bq < |b| \Rightarrow$$
$$\Rightarrow 0 \leq r < |b|$$

I són únics: suposem que en tenim uns altres $q', r'$:

$$\left.\begin{array}{r} a = bq + r,\ 0 \leq r < |b| \\ a = bq' + r',\ 0 \leq r' < |b| \end{array}\right\}$$

d'aquí obtenim que $bq + r = bq' + r' \Rightarrow b(q - q') = r - r' \Rightarrow b|r - r'$ però com que $r, r'$ són dos nombres positius menors que $|b|$ llavors $r - r' = 0 \Rightarrow r = r'$. Per demostrar la unicitat del quocient tenim que: $bq + r = bq' + r \Rightarrow bq = bq' \Rightarrow q = q'$.