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 26/11/2020

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:

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

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

$r_2 = r_3 \cdot q_3 + r_4$

$r_3 = r_4 \cdot q_4 + r_5$

$\ldots$

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.

EX.: (16) Calculeu $mcd(a^2-1, a^3-1)$.

Utilitzem el teorema d'Euclides:

$$mcd(a^2-1, a^3-1) = mcd(a^2-1, a^3-1-a(a^2-1)) = mcd(a^2-1, a^3-1-a^3+a) =$$
$$= mcd(a^2-1, a-1) = mcd(a^2-1-a(a-1), a-1) = mcd(a^2-1-a^2+a, a-1) =$$
$$= mcd(a-1, a-1) = a-1$$

Vigileu perquè si penseu en fer un raonament com si fossin polinomis el raonament no seria correcte (malgrat que s'arribaria al mateix resultat). Per exemple, amb $mcd(a(a-1), (a-2)(a-3))$ podríem pensar que el màxim comú divisor és 1 perquè mirat com a polinomis no tenen cap factor en comú. Però mirat com a nombres enters sí que tenen factors en comú. Si utilitzeu per exemple $a = 5$ surt $mcd(20, 6) = 2$ i per $a = 6$ surt $mcd(30, 12) = 6$.

EX.: (17) Trobeu tots els enters a tals que $(a-1)|a$. Pista: Qui és $mcd(a, a-1)$?

Calculem el màxim comú divisor que ens suggereixen:

$d = mcd(a, a-1) = mcd(a-(a-1), a-1) = mcd(1, a-1) = 1$. Ara observem que $a-1$ és un divisor comú de a i de $a-1$, per tant ha de passar $a-1|1$ per tant $a-1 = 1$ o bé -1 per tant $a = 2$ (que satisfà $1|2$) o bé $a = 0$ (que satisfà $-1|0$).