

## QUÈ HEM FET FINS ARA?

El darrer que hem treballat és formalment el tema del càlcul del màxim comú divisor amb l'algorisme d'Euclides (no experimentalment com el dia anterior) dintre del tema de divisibilitat i alguns problemes de caire més teòric sobre el màxim comú divisor.

## CLASSE D'AVUI 30/11/2020

Avui continuarem amb el tema de la divisió entera, l'algorisme d'Euclides extès, les identitats de Bézout i aplicacions d'aquestes identitats. Comencem amb un exemple

sobre divisió entera.

**EX.:** Trobeu quocient i residu per 1)  $a = 17, b = 7$ ; 2)  $a = 17, b = -7$ ; 3)  $a = -17, b = 7$ ;

4)  $a = -17, b = -7$ ;

1) Per les fórmules de la demostració:  $q = \text{sig}(7) \left[ \frac{17}{7} \right] = 1 \cdot [2, 42 \dots] = 2$ ,  
 $r = 17 - 7 \cdot 2 = 3$ . Pel algorisme que vam aprendre a l'escola:

$$\begin{array}{|c|c|} \hline 17 & 7 \\ \hline 3 & 2 \\ \hline \end{array} \rightarrow q = 2, r = 3$$

2) Per les fórmules:  $q = \text{sig}(-7) \left[ \frac{17}{|-7|} \right] = -1 \cdot [2, 42 \dots] = -2$ ,  $r = 17 - (-7) \cdot (-2) = 3$ .

Amb l'algorisme de la divisió podem fer-la amb els valors absoluts dels nombres i escriure:  $17 = 7 \cdot 2 + 3 \Rightarrow 17 = (-7) \cdot (-2) + 3$ , és a dir, canviem el 7 per  $-7$  i ens veiem obligats a canviar el signe al 2 per mantenir la igualtat, o sigui,  $q = -2, r = 3$ .

3) Igual que abans:  $q = \text{sig}(7) \left[ \frac{-17}{7} \right] = 1 \cdot [-2, 42 \dots] = -3$ ,  $r = -17 - 7 \cdot (-3) = 4$ . La segona versió és fer l'algorisme amb els valors absoluts dels nombres i:  
 $17 = 7 \cdot 2 + 3 \Rightarrow -17 = 7 \cdot (-2) - 3 = 7 \cdot (-2) - 7 + 7 - 3 = 7 \cdot (-3) + 4$ , és a dir, hem multiplicat per  $-1$  tota la igualtat i hem sumat i restat 7 perquè el que sembla que hauria de ser el residu ha sortit negatiu, o sigui,  $q = -3, r = 4$ .

4) I el darrer:  $q = \text{sig}(-7) \left[ \frac{-17}{|-7|} \right] = -1 \cdot [-2, 42 \dots] = (-1)(-3) = 3$ ,  $r = -17 - (-7) \cdot 3 = 4$ . La segona versió és com en els anteriors fer l'algorisme de l'escola amb els valors absoluts i després fer la manipulació:  
 $17 = 7 \cdot 2 + 3 \Rightarrow -17 = (-7) \cdot 2 - 3 = (-7) \cdot 2 - 7 + 7 - 3 = (-7) \cdot 3 + 4$ , és a dir, hem multiplicat per  $-1$  tota la igualtat i hem sumat i restat 7 perquè el que sembla que hauria de ser el residu ha sortit negatiu, o sigui,  $q = 3, r = 4$ .

**EX.:** (16) Calculeu  $\text{mcd}(a^2 - 1, a^3 - 1)$ .

Utilitzem el teorema d'Euclides:

$$\begin{aligned} \text{mcd}(a^2 - 1, a^3 - 1) &= \text{mcd}(a^2 - 1, a^3 - 1 - a(a^2 - 1)) = \text{mcd}(a^2 - 1, a^3 - 1 - a^3 + a) = \\ &= \text{mcd}(a^2 - 1, a - 1) = \text{mcd}(a^2 - 1 - a(a - 1), a - 1) = \text{mcd}(a^2 - 1 - a^2 + a, a - 1) = \\ &= \text{mcd}(a - 1, a - 1) = a - 1 \end{aligned}$$

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.:** (18) Demostreu que si  $a + c = 1$  llavors  $mcd(a, c) = 1$ .

Utilitzem el teorema d'Euclides:

$$mcd(a, c) = mcd(a, 1 - a) = mcd(a, 1 - a + a) = mcd(a, 1) = 1$$

**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  $a-1|1$  i aleshores  $a-1 = 1$  o bé  $-1$ , o sigui  $a = 2$  (que satisfà  $1|2$ ) o bé  $a = 0$  (que satisfà  $-1|0$ ).

**EX.:** (19) Demostreu que si  $a + b \mid a$  llavors  $a = -b \pm mcd(a, b)$ . Pista: Qui és

$mcd(a, a+b)$ ?

Utilitzem una altra vegada el teorema d'Euclides:

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

Com que  $a+b|a$  i  $a+b|a+b$  llavors  $mcd(a, a+b) = \pm(a+b)$ . Aleshores:

$$mcd(a, b) = \pm(a+b) \Rightarrow a+b = \pm mcd(a, b) \Rightarrow a = -b \pm mcd(a, b)$$

**EX.:** (20) Demostreu que si  $a \mid c$  i  $b \mid d$  llavors  $mcd(a, b) \leq mcd(c, d)$ .

Diem  $D = mcd(a, b) \Rightarrow D|a, D|b \Rightarrow D|c, D|d \Rightarrow D \leq mcd(c, d) \Rightarrow mcd(a, b) \leq mcd(c, d)$  (també podríem dir que  $D|mcd(c, d)$ ).

Un concepte que es fa servir sovint és el de nombres primers entre sí o relativament primers o coprimers:

**DEF.:**  $a$  i  $b$  són primers entre si  $\Leftrightarrow mcd(a, b) = 1$ .

Una altra manera d'entendre aquest concepte és pensant que no tenen cap factor en comú primer.

**PROP.:**  $a$  i  $b$  són primers entre si  $\Leftrightarrow$  no tenen cap divisor primer comú

**DEM.:** Anomenem  $d = mcd(a, b)$

$\Rightarrow$  Raonem per contrarecíproc: si tenen un divisor primer comú  $p$  llavors

$$p \leq d \Rightarrow d \neq 1$$

$\Leftarrow$  També raonem per contrarecíproc: si  $d \neq 1$  llavors en el cas que  $d = 0$  hauran de ser  $a = b = 0$  i qualsevol primer és divisor de 0; i en el cas que  $d \neq 0$  tindrem un primer  $p|d$  i com  $d|a, d|b$  aleshores  $p|a, p|b$ .

Un concepte que s'utilitza sobretot per nombres primers entre si és el de la identitat de Bézout. Veiem primer un exemple:

**EX.:** Són primers entre si els nombres 561 i 182? Intenteu posar el màxim comú divisor dels dos nombres com a combinació lineal de 561 i 182.

Calculem el  $mcd(561, 182)$ :

	3	12	7	2	
561	182	15	2	1	0
15	2	1	0		

Per tant són primers entre si perquè  $\text{mcd}(561, 182) = 1$ . Ara mirem si podem trobar el nombre 1 com a combinació lineal de  $a = 561$  i  $b = 182$ :

$$\left. \begin{array}{l} a = b \cdot 3 + 15 \\ b = 15 \cdot 12 + 2 \\ 15 = 2 \cdot 7 + 1 \end{array} \right\} \Rightarrow \left. \begin{array}{l} 15 = a - b \cdot 3 \\ 2 = b - 15 \cdot 12 \\ 1 = 15 - 2 \cdot 7 \end{array} \right\} \Rightarrow$$

$$15 = a - b \cdot 3 \Rightarrow 2 = b - 15 \cdot 12 = b - (a - b \cdot 3) \cdot 12 = -12a + 37b \Rightarrow$$

$$\Rightarrow 1 = 15 - 2 \cdot 7 = (a - b \cdot 3) - (-12a + 37b) \cdot 7 = 85a - 262b$$

Sí que es pot:  $1 = 85a - 262b$ .

I en general sempre es podrà fer? Sí:

**PROP.:** (identitats de Bézout) Si  $d = \text{mcd}(a, b)$  aleshores existeixen enters  $x, y$  tals que  $d = ax + by$ .

**DEM.:** Si utilitzem l'algorisme d'Euclides per trobar el màxim comú divisor obtenim un quadre com el següent:

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

Posant les igualtat de les divisions i procedint com a l'exemple anterior obtindrem la combinació lineal. Per calcular la combinació lineal de forma sistemàtica es fa:

$$\left. \begin{array}{l} a = bq_1 + r_2 \\ b = r_2q_2 + r_3 \\ r_2 = r_3q_3 + r_4 \\ \dots \\ r_{i-4} = r_{i-3}q_{i-3} + r_{i-2} \\ r_{i-3} = r_{i-2}q_{i-2} + r_{i-1} \\ r_{i-2} = r_{i-1}q_{i-1} + r_i \\ \dots \\ r_{n-2} = r_{n-1}q_{n-1} + r_n \end{array} \right\} \Rightarrow \left. \begin{array}{l} r_2 = a - bq_1 \\ r_3 = b - r_2q_2 \\ r_4 = r_2 - r_3q_3 \\ \dots \\ r_{i-2} = r_{i-4} - r_{i-3}q_{i-3} = x_{i-2}a + y_{i-2}b \\ r_{i-1} = r_{i-3} - r_{i-2}q_{i-2} = x_{i-1}a + y_{i-1}b \\ r_i = r_{i-2} - r_{i-1}q_{i-1} = x_ia + y_ib \\ \dots \\ r_n = r_{n-2} - r_{n-1}q_{n-1} \end{array} \right\} \Rightarrow$$

$$r_i = (x_{i-2}a + y_{i-2}b) - (x_{i-1}a + y_{i-1}b)q_{i-1} = (x_{i-2} - x_{i-1}q_{i-1})a + (y_{i-2} - y_{i-1}q_{i-1})b \Rightarrow$$

$$\left. \begin{array}{l} x_i = x_{i-2} - x_{i-1}q_{i-1} \\ y_i = y_{i-2} - y_{i-1}q_{i-1} \end{array} \right\}, \left. \begin{array}{l} x_0 = 1, x_1 = 0 \\ y_0 = 0, y_1 = 1 \end{array} \right\}$$

perquè  $r_0 = a, r_1 = b \Rightarrow x_0 = 1, y_0 = 0, x_1 = 0, y_1 = 1$ . Aquests càlculs se sistematitzen a l'algorisme d'Euclides extès:

1	0	$x_2$	$x_3$	$x_4$	...	$x_{n-1}$	$x_n$	
0	1	$y_2$	$y_3$	$y_4$	...	$y_{n-1}$	$y_n$	
	$q_1$	$q_2$	$q_3$	$q_4$	...	$q_{n-1}$	$q_n$	
$a$	$b$	$r_2$	$r_3$	$r_4$	...	$r_{n-1}$	$r_n$	0
$r_2$	$r_3$	$r_4$	$r_5$	...	...	$r_{n+1} = 0$		

**EX.:** Trobeu la identitat de Bézout per  $a = 122, b = 62$ .

1	0	1	-1
0	1	-1	2
	1	1	30
122	62	60	2
60	2	0	$r_5$

La identitat de Bezout que ens dona l'algorisme queda:  $-1 \cdot 122 + 2 \cdot 62 = 2$ .

Malgrat que molt sovint diem LA identitat de Bézout, aquesta identitat no és única ja que sempre es poden sumar i restar múltiples del nombre  $\frac{ab}{\text{mcd}(a,b)}$  ja que:

$$ax + by = d \Rightarrow ax + t \frac{ab}{\text{mcd}(a,b)} + by - t \frac{ab}{\text{mcd}(a,b)} = d \Rightarrow a \left( x + t \frac{b}{\text{mcd}(a,b)} \right) + b \left( y - t \frac{a}{\text{mcd}(a,b)} \right) = d$$

**EX.:** Trobeu més identitats de Bézout per  $a = 122, b = 62$ .

Apliquem el comentari anterior:

$$-1 \cdot 122 + 2 \cdot 62 = 2 \Rightarrow (-1 + 31t) \cdot 122 + (2 - 61t) \cdot 62 = 2$$

$$\text{Per exemple per } t = 1: 30 \cdot 122 - 59 \cdot 62 = 2$$

$$\text{Per exemple per } t = -1: -32 \cdot 122 + 63 \cdot 62 = 2$$

Aquestes identitats són molt útils entre d'altres coses (codificació, criptografia, teoria de nombres, etc.) per demostrar els dos lemes següents:

**LEMA:** (Lema de Gauss) Si  $a|bc$  i  $\text{mcd}(a,b) = 1$  llavors  $a|c$ .

**DEM.:** Sabem que  $bc = ka$  (per certa  $k$ ) i que existeixen enters  $x, y$  tals que  $ax + by = 1$  llavors:

$$acx + bcy = c \Rightarrow acx + kay = c \Rightarrow a(cx + ky) = c \Rightarrow a|c$$

**LEMA:** (Lema d'Euclides) Si  $p$  és primer i  $p|bc$  llavors  $p|b$  o  $p|c$ .

**DEM.:** Si  $p|b$  ja estarà demostrat. Si  $p$  no divideix  $b$  llavors  $\text{mcd}(p,b) = 1$  i aplicant el lema de Gauss tenim que  $p|c$ .

**EX.:** (45) Demostreu que si  $n \geq 0, m > 0$  llavors  $a^n$  i  $a^m - 1$  són primers entre si.

Calculem  $\text{mcd}(a^n, a^m - 1)$  :

$$\text{Si } n \leq m \Rightarrow \text{mcd}(a^n, a^m - 1) = \text{mcd}(a^n, a^m - 1 - a^n a^{m-n}) = \text{mcd}(a^n, -1) = 1$$

$$\text{Si } n > m \Rightarrow \text{mcd}(a^n, a^m - 1) = \text{mcd}(a^n - (a^m - 1)a^{n-m}, a^m - 1) = \text{mcd}(a^{n-m}, a^m - 1).$$

S'observa que hem tret  $m$  unitats de l'exponent però potser encara  $n - m > m$ . Es

repeteix la mateixa idea les vegades que calgui i ens quedarà en el primer cas i per tant serà 1 el màxim comú divisor.

**EX.:** (46) Demostreu que si  $a, b$  son primers entre si, llavors  $\text{mcd}(a, bc) = \text{mcd}(a, c)$ .

Pista: Useu el Lema de Gauss.

Tenen els mateixos divisors:

- si  $d|a, d|bc \Rightarrow_{\text{mcd}(d,b)=1} d|a, d|c$
- si  $d|a, d|c \Rightarrow d|a, d|bc$

Per tant si tenen els mateixos divisors, tindran el mateix màxim comú divisor.

**EX.:** (47) Trobeu tots els enters  $a$  tals que  $a + 1|a$ . Pista: Qui és  $\text{mcd}(a, a + 1)$ ? Igual que el (17).

Una altra qüestió que hem de repassar és la descomposició en factors primers i com s'utilitza per calcular el màxim comú divisor.

**PROP.:** Tot nombre enter  $n \geq 2$  té una descomposició única de la forma següent:

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

on cada  $p_i$  és primer i cada  $e_i > 0$ . Això vol dir que si demanem que  $p_1 < p_2 < \dots < p_k$ , llavors el  $k$ , els  $p_1, p_2, \dots, p_k$  i els  $e_1, e_2, \dots, e_k$  són únics.

**DEM.:** Ø

També es podria enunciar un resultat de factorització per nombres enters no nuls dient que tot nombre enter  $n \neq 0$  té una descomposició de la forma  $n = \varepsilon p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$  a on  $\varepsilon = \pm 1$ , cada  $p_i$  és primer i cada  $e_i \geq 0$ . En aquest cas es pot assegurar la unicitat de  $\varepsilon$  i dels  $e_i \geq 0$ .

Amb la descomposició factorial podem calcular el màxim comú divisor com vam aprendre a l'escola:

**PROP.:** Si expressem  $a = \varepsilon_1 p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$  i  $b = \varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$  amb  $\varepsilon_i = \pm 1$ , cada  $p_i$  primer i cada  $e_i, f_i \geq 0$  llavors tenim:

1.  $a \mid b \Leftrightarrow e_i \leq f_i$  per a cada  $i$ .

2.  $\text{mcd}(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_k^{\min(e_k, f_k)}$

3. La fórmula del màxim comú divisor val amb més nombres agafant el mínim dels exponents.

4. Els divisors positius de  $a$  són tots els nombres de la forma  $p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}$  amb  $0 \leq g_i \leq e_i$  per a tot  $i$ . El nombre d'aquests divisors és  $(e_1 + 1)(e_2 + 1) \dots (e_k + 1)$ .

**DEM.:** OK.