QUÈ HEM FET FINS ARA?

El darrer que hem treballat és formalment el tema de la divisió entera, l'algorisme d'Euclides extés, les identitats de Bézout i aplicacions d'aquestes identitats.

CLASSE D'AVUI 03/12/2020

Avui continuem amb el maxim comú divisor amb exercicis i propietats utilitzant la descomposició factorial.

EX.: (48) Demostreu que els coeficients d'una identitat de Bézout són primers entre sí. (Pista: useu linealitat.)

Suposem que tenim una identitat de Bézout $ax+by=d$ amb $d=mcd(a,b)$:

$$ax+by=d \Rightarrow \frac{a}{d}x+\frac{b}{d}y=1$$

És molt important fixar-se que $\frac{a}{d},\frac{b}{d}$ són nombres enters (d divideix a a i b). Hem de calcular el $mcd(x,y)=D$ per veure si són primers entre si, per tant:

$$D|x, D|y \Rightarrow D|\frac{a}{d}x+\frac{b}{d}y=1 \Rightarrow D|1.$$

Aleshores podem afirmar que $D=1$ o sigui $mcd(x,y)=1$. Per tant són primers entre si perquè $mcd(x,y)=1$.

EX.: (66) Escrivim $n=p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$ amb cada p_i primer i cada $e_i\geq 0$. Demostreu que $\sqrt{n}$ és un nombre natural $\Leftrightarrow$ tots els e_i són parells.

Justifiquem la doble implicació:

$\Rightarrow$: Si $\sqrt{n}=p_1^{f_1}p_2^{f_2}\dots p_k^{f_k} \Rightarrow n=p_1^{2f_1}p_2^{2f_2}\dots p_k^{2f_k}$ i ja estarà;

$\Leftarrow$: Si els exponents de n són tots parells llavors $n=p_1^{2g_1}p_2^{2g_2}\dots p_k^{2g_k} \Rightarrow \sqrt{n}=\left(p_1^{2g_1}p_2^{2g_2}\dots p_k^{2g_k}\right)^{1/2} \Rightarrow \sqrt{n}=p_1^{g_1}p_2^{g_2}\dots p_k^{g_k}$ que és un nombre natural.

EX.: (67)

a) Demostreu que tot nombre racional $r\neq 0$ es pot escriure de la forma $r=\varepsilon p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$ amb $\varepsilon=\pm 1$, cada p_i primer i cada e_i enter.

b) Demostreu que tant ε com els e_i són únics.

c) Demostreu que el criteri de l'exercici anterior també és cert per als racionals.

a)Suposem que $r=\varepsilon\frac{a}{b}$, amb ε igual a 1 o -1, a, b enters i $b\neq 0$. Per exemple si $r=-\frac{6}{99}$ el podem escriure com a $r=-\frac{2^1 3^1}{3^2 11^1}$ o també utilitzant tots els nombres primers que apareixen en el numerador i el denominador (segona versió de la factorització admetent exponents nuls), $r=-\frac{2^1 3^1 11^0}{2^0 3^2 11^1}$ i que, fixem-nos, es pot simplificar posant $r=-2^1 3^{-1} 11^{-1}$. Ara, després de l'exemple, fem-ho en general: suposem que els primers que surten a les descomposicions factorials de tots dos nombres són $p_1,p_2,\dots,p_k$ $\Rightarrow a=p_1^{f_1}p_2^{f_2}\dots p_k^{f_k}, b=p_1^{g_1}p_2^{g_2}\dots p_k^{g_k}$ amb $f_i\geq 0, g_i\geq 0$ llavors:

$$r=\varepsilon\frac{p_1^{f_1}p_2^{f_2}\dots p_k^{f_k}}{p_1^{g_1}p_2^{g_2}\dots p_k^{g_k}}=\varepsilon p_1^{f_1-g_1}p_2^{f_2-g_2}\dots p_k^{f_k-g_k},$$

amb cada $e_i = f_i - g_i$ serà positiu o negatiu, però serà enter i ε igual a 1 o -1.

b) Supposem que tenim dues expressions per un nombre racional:

$r = \varepsilon_1 p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}, r = \varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$

amb cada e_i, f_i enter i $\varepsilon_1, \varepsilon_2$ igual a 1 o -1. Com que els dos nombres són iguals, el signe ha de ser igual i per tant $\varepsilon_1 = \varepsilon_2$. Aleshores $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} = p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$. Per a cada primer p_i si $e_i \geq f_i$ llavors dividim els dos cantons de la igualtat per $p_i^{f_i}$ i així en un cantó ens quedarà $p_i^{e_i - f_i}$ amb l'exponent $e_i - f_i \geq 0$ i a l'altre cantó ens quedarà p_i^0; si $e_i < f_i$ llavors dividim la igualtat per $p_i^{e_i}$ i en un cantó ens quedarà $p_i^{f_i - e_i}$ amb l'exponent $f_i - e_i > 0$ i a l'altre cantó ens quedarà p_i^0. D'aquesta manera tenim una descomposició de nombres enters en dos formes diferents i per la unicitat dels exponents ens quedarà que $e_i - f_i = 0$ o bé que $f_i - e_i = 0$. En ambdós casos arribem a la conclusió que $e_i = f_i$, és a dir que els exponents són únics.

c)Simplement cal mirar cadascun dels passos del raonament a l'exercici anterior i es veu que és completament correcte amb exponents enters i només canviant "natural" per "enter".

EX.: (68) Demostreu que:

a) $mcd(a^n, b^n) = (mcd(a,b))^n$ per $n \geq 0$ (pista: useu la descomposició en factors primers).

b) Si $m \leq n$ llavors $(mcd(a,b))^m | mcd(a^n, b^m) | (mcd(a,b))^n$ (pista: useu l'apartat anterior).

c) Si $m \leq n$ llavors $(mcd(a,b))^m \leq mcd(a^n, b^m) \leq (mcd(a,b))^n$.

a)Utilitzem la descomposició factorial dels nombres, fent sortir els mateixos primers (i per tant possiblement algun exponent nul): $a = \varepsilon_1 p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}, b = \varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$ llavors:

- $mcd(a^n, b^n) = mcd(\varepsilon_1^n p_1^{ne_1} p_2^{ne_2} \dots p_k^{ne_k}, \varepsilon_2^n p_1^{nf_1} p_2^{nf_2} \dots p_k^{nf_k}) = p_1^{\min(ne_1, nf_1)} p_2^{\min(ne_2, nf_2)} \dots p_k^{\min(ne_k, nf_k)}$
- $(mcd(a,b))^n = \left(p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \dots p_k^{\min(e_k,f_k)}\right)^n = p_1^{n\min(e_1,f_1)} p_2^{n\min(e_2,f_2)} \dots p_k^{n\min(e_k,f_k)}$

i com es veu són iguals ja que fer el mínim abans o després de multiplicar per $n \geq 0$ dona el mateix resultat.

b)Utilitzant l'apartat anterior tenim que: $(mcd(a,b))^m = mcd(a^m, b^m)$, $(mcd(a,b))^n = mcd(a^n, b^n)$. A més sabem que si $m \leq n$ llavors $mcd(a^n, b^m) | mcd(a^n, b^n)$, $mcd(a^m, b^m) | mcd(a^n, b^m)$ simplement per la manera de calcular el mpaxim comú divisor a partir de la factorització. Per tant tindrem justificat el que es demana perquè:

$(mcd(a,b))^m = mcd(a^m, b^m) | mcd(a^n, b^m) | mcd(a^n, b^n) = (mcd(a,b))^n$

c)Aquest apartat és conseqüència de que per $A, B > 0$ tenim que si $A | B \Rightarrow A \leq B$.

Veiem més propietats del màxim comú divisor:

PROP.:

1) Tot divisor comú de a, b divideix $mcd(a,b)$. De fet: $d|a$ i $d|b \Leftrightarrow d | mcd(a,b)$.

2) Associativitat del màxim comú divisor:

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

3) $mcd(ca, cb) = |c| mcd(a,b)$.

4) Si $d = mcd(a,b)$ no és nul llavors $mcd(a/d, b/d) = 1$.

5) Totes les propietats anteriors valen també amb 3 o més enters.

DEM.: només un comentari i una de les demostracions.

1)És una propietat important;

4)Sabem que existeixen x, y tals que $ax + by = d \Rightarrow \frac{a}{d}x + \frac{b}{d}y = 1$. Si $D = mcd(\frac{a}{d}, \frac{b}{d})$ llavors $D|\frac{a}{d}, D|\frac{b}{d} \Rightarrow D|\frac{a}{d}x + \frac{b}{d}y = 1$

$\Rightarrow D|1 \Rightarrow D = 1 \Rightarrow mcd(\frac{a}{d}, \frac{b}{d}) = 1$

EX.: (77) Demostreu que si $a|c$ i $b|d$ llavors $mcd(a,b)|mcd(c,d)$.

Si anomenem $D = mcd(a,b)$ llavors $D|a, D|b$ i a més sabem que $a|c$ i $b|d$ llavors $D|c, D|d$ per tant $D|mcd(c,d)$ o sigui $mcd(a,b)|mcd(c,d)$.