5. DIVISIBILITATI

(5) Demostrar

(IV) $a|0$

(V) $a|b,\ b|c \Rightarrow a|c$

(VIII) $a|b \Rightarrow a|b\cdot c$

(IX) $a|b \Leftrightarrow a|-b \Leftrightarrow -a|b \Leftrightarrow -a|-b \Leftrightarrow |a||b|$

Dem (IV) $0 = k\cdot a \Rightarrow k=0$, $\forall a$ ✓

(V) $\left.\begin{array}{l} b = k\cdot a \\ c = t\cdot b \end{array}\right\} \Rightarrow c = t\cdot b = t\cdot k\cdot a \Rightarrow a|c$

(VIII) $a|b \Rightarrow b = a\cdot k \Rightarrow \forall c,\ b\cdot c = a\cdot k\cdot b \Rightarrow$ ✓

(IX) $a|b \Rightarrow b = k\cdot a \Rightarrow -b = -k\cdot a \Rightarrow a|-b \Rightarrow -b = t\cdot a$

$\Rightarrow -b = (-t)(-a) \Rightarrow -a|-b \Rightarrow a|b$

i dibuixant $|a||b|$ pels casos $a<0,\ b\leq 0$, $a\leq 0,\ b>0$..

(6) $a|a' \wedge b|b' \Rightarrow ab \mid a'b'$

Dem

$\left.\begin{array}{l} a' = ka \\ b' = tb \end{array}\right\} \Rightarrow a'b' = k.t\,ab \Rightarrow ab \mid a'b'$ ✓

(7) ~~$a|b-1$~~ ~~$\Rightarrow$~~

$\left.\begin{array}{l} a|c-1 \end{array}\right\}$

$\left.\begin{array}{l} x|y \\ y|2x \end{array}\right\} \Rightarrow |x| = |y| \text{ ó } |x| = 2|y|$

Dem

$\left.\begin{array}{l} y = x.k \\ 2x = y.t \end{array}\right\} \Rightarrow 2x = x.k.t \Rightarrow k.t = 2$

$\Rightarrow k = 1 \wedge t = 2$ (a)

ó $k = -1 \wedge t = -2$ (b)

ó $k = 2 \wedge t = 1$ (c)

ó $k = 2 \wedge t = -1$ (d)

(a) $y = x$
(b) $y = -x$ $\Big\}$ $|x| = |y|$

(c) $y = 2x$
(d) $y = -2x$ $\Big\}$ $|y| = 2|x|$

$\Rightarrow$ l'énoncé est malvenu !

(8) $a \mid b-1$, $a \mid c-1$ $\Rightarrow$ $a \mid bc-1$

Pour

$b-1 = k \cdot a$

$c-1 = t \cdot a$

$\Rightarrow (b-1)(c-1) = kta^2$

~~$bc - b - c + 1 = kta^2$~~

$\Downarrow$

~~$bc - c = kca$~~

~~$bc - b = tba$~~

$bc - c = kac$ $\Rightarrow$ $bc - ta - 1 = kac$

$\uparrow$

$ta+1$

$\Downarrow$

$bc - 1 - ta = kca$

$\Leftarrow$ $(x \mid xt+\alpha \Rightarrow x \mid \alpha)$

$bc - 1 = wa$

(8) $\left.\begin{array}{l} a \mid b-1 \\ a \mid c-1 \end{array}\right\} \Rightarrow a \mid bc-1$

Dem

$\left.\begin{array}{l} b-1 = k \cdot a \\ c-1 = t \cdot a \end{array}\right\} \Rightarrow bc - c = k \cdot c \cdot a \Rightarrow$ (con $c = t \cdot a + 1$)

$\Rightarrow bc - ta - 1 = kca \Rightarrow bc - 1 = (kc + t)a$ /

(9) $\left.\begin{array}{l} x \mid 2y \\ y \mid 2x \end{array}\right\} \Rightarrow x = \pm y$ (12) ó $x = \pm 2y$ (1) ó $y = \pm 2x$ (3)

Dem

$\left.\begin{array}{l} 2y = k \cdot x \\ 2x = t \cdot y \end{array}\right\} \Rightarrow 2y = k \cdot \frac{ty}{2} \Rightarrow$

$\Rightarrow$ (a) $2 \mid t \Rightarrow 2y = wy \Rightarrow k\left(\frac{t}{2}\right) = 2 \Rightarrow$ ($w = k \cdot \frac{t}{2}$)

$\Rightarrow \begin{cases} k = \pm 1 \; ; \; \frac{t}{2} = \pm 2 \Rightarrow 2y = \pm x \; (1) \\ \text{ó} \\ k = \pm 2 \; ; \; \frac{t}{2} = \pm 1 \Rightarrow 2y = \pm 2x \; (2) \end{cases}$

(b) $2 \nmid t \Rightarrow 2y = k \cdot t \cdot \left(\frac{y}{2}\right) \Rightarrow 4 = k \cdot t \Rightarrow$

$\Rightarrow$ • $k = \pm 1$, $t = \pm 4$ — (NO) $\Rightarrow 2 \mid t$

• $k = \pm 2$, $t = \pm 2$ — (NO)

$K = \pm 4, \quad t = \pm 1$

$2y = Kx \Rightarrow 2y = \pm 4x \Rightarrow y = \pm 2x$ (3)

(10) $aRb \overset{(dj)}{\iff} a \mid b^n, \; b \mid a^n$ per algun $n \geq 1$

R és d'equivalència

- reflexiva: aRa, ja que $a \mid a^n$ i $a \mid a^n$ $\forall n$
- simètrica $aRb \overset{?}{\Rightarrow} bRa$

$a \mid b^n, \; b \mid a^n$ per algun n

$\nwarrow \quad \nearrow$

és la pròpia definició ✓

- transitiva $\left.\begin{matrix} aRb \\ bRc \end{matrix}\right\} \overset{?}{\Rightarrow} aRc$

$\left.\begin{matrix} a \mid b^n \text{ i } b \mid a^n \\ \text{i} \\ b \mid c^m \text{ i } c \mid b^m \end{matrix}\right\} \Rightarrow a \mid c^{m+n} \text{ i } c \mid a^{n+m}$ ✓

(11) $a, b \neq 0$

Son equivalents:

a) $\forall n \geq 0 \quad e \mid ca^n + db^n$

b) $e \mid c+d$, $e \mid ca + db$

c) $e \mid c+d$, $e \mid c(a-b)$

~~a $\Rightarrow$ b~~ Pent $n=1$, $e \mid ca + db$

~~Veiem que $e \mid c+d$~~

Pent $n=0$, $e \mid c+d$

~~b $\Rightarrow$ c~~ Veiem que $e \mid c(a-b)$

Tenim $\left.\begin{array}{l} c+d = Ke \\ ca+db = t \cdot e \end{array}\right\} \Rightarrow \begin{array}{l} d = Ke - c \\ ca + (Ke-c)b = te \end{array}$

$\Rightarrow ca + kbe - cb = te \Rightarrow$

$\Rightarrow ca - cb = we \Rightarrow e \mid c(a-b)$

~~c $\Rightarrow$ b~~ (~~No em surt c $\Rightarrow$ a~~)

$\left.\begin{array}{l} ca - cb = ek \\ c+d = et \end{array}\right\} \Rightarrow \begin{array}{l} ca - cb = ck \\ cb + db = etb \end{array}$

$ca + db = cw \Rightarrow \begin{array}{l} e \mid c+d \\ e \mid ca+db \end{array}$ ✓

Només falta per $b \Rightarrow a$

Fem-ho per inducció

$n=0$, $n=1$ és b)

Suposem $e \mid ca^{n-1} + db^{n-1}$

Vegem que $e \mid ca^n + db^n$

$$ca^{n-1} + db^{n-1} = \dot{e}$$

$\times a \rightarrow$

$$ca^n + adb^{n-1} = \dot{e}$$

$\times b \rightarrow$

$$bca^{n-1} + adb^n = \dot{e}$$

$$ca^n + db^n + bca^{n-1} + adb^{n-1} = \dot{e}$$

$$ca^n + db^n = \dot{e} - bca^{n-1} - adb^{n-1} =$$

$$= \dot{e} - ba\left[ca^{n-2} - db^{n-2}\right]$$

Com que hem fet $n=0$, $n=1$, per hipòtesi d'inducció podem suposar $n-1$ i $n-2$

$$ca^n + db^n = \dot{e} - ba\dot{e} \Longrightarrow e \mid ca^n + db^n \quad \checkmark$$

(12) $a+b+c \mid abc \Rightarrow a+b+c \mid a^3+b^3+c^3$

Fem

$$(a+b+c)(a^2+b^2+c^2-ab-ac-bc) =$$

$$= a^3 + ab^2 + ac^2 - a^2b - a^2c - abc + a^2b + b^3 + bc^2 - ab^2 - abc - b^2c +$$

$$+ a^2c + b^2c + c^3 - abc - ac^2 - bc^2 =$$

$$= a^3 + b^3 + c^3 - 3abc$$

Sa $a+b+c \mid abc \Rightarrow abc = (a+b+c)k$

$$a^3+b^3+c^3 = (a+b+c)\underbrace{(a^2+b^2+c^2-ab-ac-bc)}_{\alpha} + 3abc =$$

$$= (a+b+c)\alpha + (a+b+c)\beta = (a+b+c)\lambda$$

$$\Rightarrow a+b+c \mid a^3+b^3+c^3 \quad \checkmark$$

$|a+b| \mid a+b$; $|a+b| \mid a^2-b^2$, poi $d \mid a+b \Rightarrow |d| \leq |a+b|$

per tali $d = |a+b|$

21 $\gcd(a+b, a^2-b^2) = ?$

Sapp: $d = \gcd(a+b, a^2-b^2) = \gcd(|a+b|, |a^2-b^2|) = \gcd(|a+b|, |a+b||a-b|) =$
$= |a+b| \gcd(1, |a-b|) = |a+b|$ ✓

Tesi: $d \mid a+b$; $d \mid a^2-b^2 = (a+b)(a-b)$

Osservo $d \mid dk(a-b)$

$\Rightarrow d w(a-b) = d \Rightarrow w(a-b) = 1 \Rightarrow$ $w = \pm 1$, $a-b = \pm 1$
($w \in \mathbb{Z}$, $a-b \in \mathbb{Z}$)

~~Senza perdita di generalità posso dire $a \geq b$~~

Per tali, $a = b+1$ (I) o $a = b-1$ (II)

(II) $d \mid 2b+1$; $d = \gcd(2b+1, 2b+1) \Rightarrow$

$\Rightarrow d = |2b+1|$ ~~$\neq 0$~~

(II) $d \mid 2b-1$; $d = \gcd(2b-1, 1-2b) \Rightarrow$

$\Rightarrow d = |2b-1|$ ~~$\neq 0$~~

Sopra come sopra, $\gcd(a+b, a^2-b^2) = |a+b|$

(22) $d = mcd(a,b)$

a) $b = ca$

$d = mcd(a, ca) \Rightarrow d = |a|$

b) $b = a^n \quad (n>1)$

$d = mcd(a, a^n) \Rightarrow d = |a|$

c) $b = p$ primo

$d = mcd(a,p) \Rightarrow \begin{cases} d = |p| \text{ se } p|a \\ d = 1 \text{ se } p \nmid a \end{cases}$

d) $b = 2a - 1$

$d = mcd(a, 2a-1) \Rightarrow d | 2a-1 \Rightarrow d | 1 \Rightarrow d = 1$

(23) $mcd(4k+14, 6k+20) \overset{?}{=} 2 \quad \forall k$

Sejam $d = mcd(4k+14, 6k+20) = mcd(2(2k+7), 2(3k+20))$

Pode ser, $d|2$ ou $d \nmid 2$

Se $d|2 \Rightarrow d = 2$ isto está

Vamos ver se $d \nmid 2$ pode acontecer

$d \nmid 2 \Rightarrow \begin{cases} d \mid 2k+7 \\ d \mid 3k+6 \end{cases} \Rightarrow \begin{cases} 2k+7 = d \cdot r \\ 3k+6 = d \cdot s \end{cases}$

$k+3 = d w$

Per tant, $2k+7 = d \cdot r$

$k+3 = d w$

$k+4 = d t$

i també $k+4 = d t$

$k+3 = d w$

$1 = d w$

$\Rightarrow d = 1$

Però si $d=1$, llavors $d = mcd(4k+14, 6k+20) = 1$

La qual cosa és un absurd, ja que $d \geq 2$, ja que $2 \mid 4k+14 \; i \; 2 \mid 6k+20$!!!

Per tant, $d \nmid 2 \Rightarrow$ absurd.

ped

* Una altra manera més "tècnica" de fer el mateix és:

Euclides

$$\text{mcd}(4k+14, 6k+20) \overset{\text{Euclides}}{=} \text{mcd}(4k+14, 6k+20-4k-14) =$$

$$= \text{mcd}(4k+14, 2k+6) \overset{\text{Euclides}}{=} \text{mcd}(2k+8, 2k+6) \overset{\text{Euclides}}{=}$$

$$= \text{mcd}(2, 2k+6) = \text{mcd}(2, 2(k+3)) = 2$$

↑ hem pot fer això.

pel

(24) $\text{mcd}(a^2-1, a^3+1) = ?$

$$\text{mcd}(a^2-1, a^3+1) \overset{\text{Euclides}}{=} \text{mcd}(a^2-1, a^3+a^2+1-1) =$$

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

$$= \text{mcd}((a+1)\cdot(a-1), a\cdot(a+1)) = d$$

on $d \mid a+1$, és a dir $d = k\cdot|a+1|$

Però $d \mid (a+1)(a-1) \Rightarrow (a+1)(a-1) = d\cdot r = |k\cdot r\cdot|a+1| \Rightarrow$

$$\Rightarrow a-1 = |k\cdot r'$$

i $d \mid (a+1)a \Rightarrow (a+1)\cdot a = k\cdot s\cdot|a+1| \Rightarrow a = k\cdot s'$

Però $k \mid a$ i $k \mid a-1 \Rightarrow k = \pm 1 \Rightarrow \boxed{d = |k+1|}$ ✓

(25) $ab+c=1 \Rightarrow mcd(a,c) = mcd(b,c) = 1$

Dem

$mcd(a,c) = mcd(a, 1-ab) =$ Euclides

$= mcd($ Euclides

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

$= mcd(a,1) = 1$

$mcd(b,c) = mcd(b, 1-ab) = mcd(b,1) = 1$

qed

(26) $mcd(2k+9, 3k+15) = 3$ si $3 \mid k$ y 1 si $3 \nmid k$

Dem

$mcd(2k+9, 3k+15) = mcd(2k+9, k+6) = mcd(k+3, k+6) =$

$= mcd(k+3, 3) =$ $\begin{cases} 3 & \text{si } 3 \mid k+3, \text{ o sea si } 3 \mid k \\ 1 & \text{si } 3 \nmid k+3, \text{ o sea si } 3 \nmid k \end{cases}$

(2) $a \in \mathbb{Z}$ $\quad a+2 \mid a$?

$$\text{mcd}(a+2, a) = \text{mcd}(2, a) = \begin{cases} 2 & \text{si } 2 \mid a \\ 1 & \text{si } 2 \nmid a \end{cases}$$

Cas $a = \dot{2}$ $\Rightarrow$ $2 \mid a+2$ i $2 \mid a$ i 2 és el divisor més gran

~~$\Rightarrow$ si $a > 0 \Rightarrow 2 \geq a+2 \geq 2 \Rightarrow a = 0$~~

~~si $a < 0 \Rightarrow 2 > a+2$~~

$\Rightarrow |a+2| \leq 2 \Rightarrow -2 \leq a+2 \leq 2 \Rightarrow$

$\Rightarrow -4 \leq a \leq 0$

Per tant, $a = 0, -2, -4$

Cas $a = \dot{2}+1$

$\Rightarrow |a+2| \leq 1 \Rightarrow -1 \leq a+2 \leq 1 \Rightarrow$

$\Rightarrow -3 \leq a \leq -1 \Rightarrow a = -1, -3$

Per tant, els únics enters que compleixen $a+2 \mid a$

són

$$a \in \{0, -1, -2, -3, -4\}$$

(28) $\text{mcd}(32k+12, 12k+4) =$

$= \text{mcd}(20k+8, 12k+4) = \text{mcd}(8k+4, 12k+4) =$

~~$= \text{mcd}(6k+4, 2k+4) = \text{mcd}(2\cdot 3k, 2(k+2))$~~

$= \text{mcd}(8k+4, 4k) = \text{mcd}(4k+4, 4k) = \text{mcd}(4, 4k) = 4$

(29) $\forall i\ \exists j \mid a_i \mid b_j \Rightarrow \text{mcd}(a_1 \dots a_n) \leq \text{mcd}(b_1 \dots b_m)$

⚠ L'EXERCICI ÉS FALS !!

Ex.

$\text{mcd}(24) > \text{mcd}(4,5)$

$\quad\ \|\qquad\qquad\ \|$

$\quad\ 2\qquad\qquad\ 1$

I en conu, $\forall a \in \{2,4\}\ \exists b \in \{4,5\} \mid a \mid b$!!!

(30) $\text{mcd}(\pm 1, b, c, \dots) = 1$

Dem

$d = \text{mcd}(\pm 1, b, c, \dots)$

$d \mid \pm 1 \Rightarrow d = \pm 1$ (pq $d > 0$),

per tant, $d = 1$

(31) $\text{mcd}(a) = |a|$

Dem $\text{mcd}(a) = d$

$d \mid a$ i $d \geq e \ \forall e \mid a$.

Llavors, $\pm a \mid a$ i $|a| \geq d$

Per tant, $d = |a|$

(33) $\text{mcd}(0, b, c, \dots) = \text{mcd}(b, c, \dots)$

Sigui $d = \text{mcd}(b, c, \dots)$, $D = \text{mcd}(0, b, c, \dots)$

$d \mid b, c, \dots$ pqd també $d \mid 0$ Per tant,

$d \mid \text{mcd}(0, b, \dots)$

Llavors, $d \mid D$

però $D \mid d$, ja que $D \mid b, c, d \dots$

(34) $\mcd(a,b,c,\dots) = \mcd(a+ub, b, c, \dots)$

Seria obvi si abans hagéssim vist que

$\mcd(a,b,c) = \mcd(\mcd(a,b), c)$ ←

Dem $\mcd(a,b) = d$

$\mcd(d,c) = e$ i $e \mid d \Rightarrow e \mid a, b$ ∴ $e \leq d$

$e \mid a,b,c$ i si $\exists\, t \geq e \mid t \mid a,b,c$

tindrien $t \mid |a|, |b|$ i $t \geq e$, ~~contradicció~~ ∴ $d \geq t$

~~(absurd $\mcd(a,b)$)~~

Per tant $d \geq t \geq e$

Però $t \mid |a|, |b| \Rightarrow t \mid d$ i com que $t \mid |c|$

llavors $t \mid d, |c|$ però $e \geq t$ ja que $e = \mcd(d,c)$

Per tant, $e \geq t$ i $t \geq e$, o sigui $t = e$

Per què ho hi ha un exercici així ??

35

El professor ens diu:

$$mcd(a_1, \dots, a_n) = mcd(0, 0, \dots, b_1, \dots, b_m) =$$

(reordenant) ; $b_1 \leq \dots \leq b_m$, $b_i \geq 0$ ben fet $|a_i|$

ex. 33

$$= mcd(b_1, \dots, b_m) =$$

$$= mcd(b_1 \dots, b_m \bmod b_1) =$$

(r) ; ↑ tornem a reordenar

on: $b_m = b_1 \cdot k + r$

Correcte per l'exercici 32, ja que ben fet $b_m - b_1 k$

$$= mcd(c_1, \dots c_m)$$

(podem fer $c_1 = 0$)

→ El procés acaba, ja que $b_1 \mid b_m \Rightarrow r = 0$

i llavors tenim un "0" i ben fet per m-1

Però si $r \neq 0$,

$b_m > b_1 \cdot k + r$

$b_m > 0$, $b_1 > 0$, $k > 0$, $r \geq 0$

(estricte per construcció) és > 0 per l'operació $b_m \bmod b_1$

Per tant, $0 \leq r < b_m$

A cada pas,

$(\alpha_1 \dots \alpha_k) \rightarrow (\beta_1 \dots \beta_k)$

amb $\max(\beta_1 \dots \beta_k) < \alpha_1 \dots \alpha_k \quad \forall k$

i tota successió estrictament decreixent de valors enters positius acaba a 0.

(41) Res a demostrar → Fer-ho o classe.

(42) $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

$(x, y) \longmapsto 5548x + 1727y$ és exhaustiva

$\alpha \qquad \beta$

Pem

Volem pr $\forall z \in \mathbb{Z} \quad \exists x, y \in \mathbb{Z} \mid z = \alpha x + \beta y$

La id. de Bézout ens diu pr

$\mathrm{mcd}(\alpha, \beta) = A\alpha + B\beta$ per certs $A, B \in \mathbb{Z}$

$\mathrm{mcd}(\alpha, \beta) = 1$

← fer-ho

q		3	4	1	2	2	1	1	
r	5548	1727	367	259	108	43	22	21	(1)

mcd

Per tant $1 = A\alpha + B\beta$

$\forall z \in \mathbb{Z}, \quad z = z \cdot 1 = z \cdot A\alpha + z \cdot B\beta$

Per tant, $\forall z, \exists x = z \cdot A : \exists y = z \cdot B$ tals que $z = \alpha x + \beta y$ ✓

(45) $n \geq 0$, $m > 0$ a^n, $a^m - 1$ primers entre sí

Rem

Si no ho fessin,

$\exists\, d > 1 \mid d \mid a^n$ i $d \mid a^m - 1$

Aquest d podem pensar que és primer

O sigui, $p \mid a^n$ i $p \mid a^m - 1$

Però llavors $p \mid a^n \Rightarrow p \mid a$ ($\forall n > 0$)

però $p \mid a \Rightarrow p \mid 1 \Rightarrow p = 1$
$p \mid a^m - 1$

(Si $n = 0 \Rightarrow p \mid 1$)

(46) $\text{mcd}(a, b) = 1 \Rightarrow \text{mcd}(a, bc) = \text{mcd}(a, c)$

Rem $d = \text{mcd}(a, b \cdot c) \Rightarrow d \mid a$ i $d \mid b \cdot c$

$\forall$ primer $\alpha \mid \alpha \mid d$, $\alpha \mid b \cdot c$ però $\alpha \nmid b$ (ja que si no, $\text{mcd}(a, b) \neq 1$)

Per tant, $\alpha \mid c$ $\forall \alpha$ divisor de d.

Per tant $\alpha = d$ també que $d \mid a$ i $d \mid c$, però $d \geq \text{mcd}(a, c)$

Per tant, $\text{mcd}(a, c)$: ... $d = \text{mcd}(a, bc)$

(47) $a \in \mathbb{Z} \mid (a+1) \mid a$

$\mcd(a+1, a) = \mcd(1, a) = 1$

(Euclides)

$\forall d \mid d \mid a$ i $d \mid a+1$, $|d| \leq 1$

Però $a+1 \mid a$, per tant, $|a+1| \leq 1$

$\Rightarrow \quad -1 \leq a+1 \leq 1 \Rightarrow \quad -2 \leq a \leq 0$

$\Rightarrow a \in \{0, -1, -2\}$

(48) Els coeficients de la identitat de Bézout són primers entre sí.

$\mcd(a, b) = d \Rightarrow \quad d = \alpha a + \beta b$

Volem veure que $\mcd(\alpha, \beta) = 1$

~~$\mcd(\alpha, \beta) = \mcd($~~ Sigui $e = \mcd(\alpha, \beta)$

$e \mid \alpha$ i $e \mid \beta$

Però $e \cdot d \mid \alpha \cdot a$ i $e d \mid \beta \cdot b \Rightarrow e \cdot d \mid \alpha a + \beta \cdot b = d$ (linealitat)

$\Rightarrow e \cdot d \mid d \Rightarrow e = 1$ ...

(4.9) $M_a = \{ x \in \mathbb{Z} \mid a \mid x \}$

a) p, q primers, $p \neq q \Rightarrow M_p \cap M_q = M_{pq}$

b) $M_a \cap M_b = M_{ab}$ per a valors $a, b \in \mathbb{Z}$??

a) $M_p = \{ kp \mid k \in \mathbb{Z} \}$ $M_q = \{ tq \mid t \in \mathbb{Z} \}$

$\subseteq$) $x \in M_p \cap M_q \Rightarrow x = kp$ i $x = tq \Rightarrow$

(*) ja que primers

$\Rightarrow x = kp = tq \Rightarrow q \mid k$ i $p \mid t \Rightarrow$

$\Rightarrow x = qrp$ per algun $r \in \mathbb{Z} \Rightarrow x \in M_{pq}$

$\supseteq$) $x \in M_{pq} \Rightarrow x = pqk \Rightarrow x = p(qk) \Rightarrow x \in M_p$

$x = q(pk) \Rightarrow x \in M_q$

b) En general, no!

El pas "trompós" és el (*)

No cal però que p, q siguin primers, però sí $\text{mcd}(a,b) = 1$

i.e. ... $\Rightarrow x = ka = t \cdot b \Rightarrow b \mid k$ i $a \mid t \Rightarrow$ ✓

$\uparrow$ $\text{mcd}(a,b) = 1$

(50) $\{x+y \mid x \in M_a, y \in M_b\} = M_{mcd(a,b)}$ $\forall a,b \in \mathbb{Z}$

Dem

$\supseteq$ Trivial:

$t \in M_{mcd(a,b)} \Rightarrow t = k \cdot mcd(a,b) \overset{\text{Bézout}}{=} k(\alpha a + \beta b) = \underbrace{k\alpha a}_{\in M_a} + \underbrace{k\beta b}_{\in M_b}$

$\subseteq$ $t \in \{\dots\} \Rightarrow t = ka + tb$

$d = mcd(a,b) \Rightarrow d \mid a \;;\; d \mid b$

Per linealitat $d \mid t$

O sigui $t = j \cdot d = j[Aa + Bb] = jAa + jBb$

$\overset{\text{Bézout}}{\uparrow}$ que és el que volíem!

(ja que $d \mid t$)

q.e.d

5.1

Són equivalents:

a) $p \mid a$

b) $mcd(p, a) = p$

c) $p \mid a^2$

d) $p^2 \mid a^2$

Dem

a $\Rightarrow$ b] $mcd(p, pk) = p$, ja que $p \mid p, p \cdot k$ i no pot ser que $\exists d > p > 0$, ja que llavors $d \mid p$ i $d > p$ $\Rightarrow$!!

b $\Rightarrow$ c] Tenim $p \mid a$ llavors $p \mid a \cdot k$ $\forall k \neq 0$

Cas $a \neq 0$ $\Rightarrow$ $p \mid a^2$ ✓

Cas $a = 0$ $\Rightarrow$ $mcd(p, 0) = 0 \neq p$ $\Rightarrow$!! no pot ser!

c $\Rightarrow$ d] $p \mid a^2 \Rightarrow$ ~~$p \mid a \cdot k$~~ (propietat...) $\Rightarrow p \mid a$ ó $p \mid a \Rightarrow$

$\Rightarrow p \mid a \Rightarrow a = k \cdot p \Rightarrow a^2 = k^2 \cdot p^2 \Rightarrow p^2 \mid a^2$

d $\Rightarrow$ a] $a^2 = k p^2 = k \cdot p \cdot p \Rightarrow p \mid a^2 \Rightarrow p \mid a$ ✓ (propietat...)

(52) $p \mid b_1 \cdots b_n$ i p primer $\Rightarrow$ $p \mid b_1$ ó $p \mid b_2$ ó ...

Dem

$n=1$ $\quad p \mid b_1$ ✓

Suposem $p \mid b_1 \cdots b_{n-1} \Rightarrow p \mid b_1$ ó ... ó $b \mid b_{n-1}$

Vegem què passa quan $p \mid b_1 \cdots b_n$

$p \mid (b_1 \cdots b_{n-1}) b_n \Rightarrow p \mid (b_1 \cdots b_{n-1})$ ó $p \mid b_n \Rightarrow$

(hipòtesi inducció)

(Lema Euclides)

$\Rightarrow p \mid b_1$ ó ... ó $p \mid b_{n-1}$ ó $p \mid b_n$ qed

(53) $a+b+c \mid a^3+b^3+c^3$

$a+b+3 \not\vdots 3$

$\Rightarrow \quad a+b+c \mid abc$

Rem

$(a+b+c)(a^2+b^2+c^2-ac-ab-bc) =$

$= a^3+b^3+c^3+a^2b+ac^2-a^2c-a^2b-abc-abc+a^2b+bc^2-ab^2-b^2c$

$+a^2c+b^2c-ac^2-abc-bc^2 =$

$= a^3+b^3+c^3-3abc$

$a^3+b^3+c^3 = k(a+b+c)$

k is pr. $a+b+c \mid a^3+b^3+c^3$

$(a+b+c)(\sim) + 3abc$

$\Downarrow$

$(a+b+c) \mid 3abc$

$3 \nmid a+b+c \Rightarrow a+b+c \mid abc$ qed

54) $n, r \geq 0 \quad m \geq 0$

$\text{mcd}(a,b)=1 \Rightarrow \text{mcd}(a^n, ua^m+b^r) = 1$

$\forall u \in \mathbb{Z}$

Dem

p primer

Si $p \mid a^n$ i $p \mid ua^m+b^r$, llavors

$p \mid a^n \Rightarrow p \mid a \Rightarrow p \mid b \Rightarrow p \mid a,b \rightarrow$

$p \mid ua^m+b^r$

$\Rightarrow p = 1 \Rightarrow !!!$

Hem vist que $\forall p$ divisor de a^n i ua^m+b^r,

llavors $p=1$.

(55)

$a_1, \dots a_n$, $\exists\, x_1 \dots x_n \mid \gcd(a_1 \dots a_n) = a_1x_1 + \dots + a_nx_n$

Dem

Fem inducció

$n=2 \quad \gcd(a_1, a_2) = a_1x_1 + a_2x_2$

Suposem que $\gcd(a_1 \dots a_{n-1}) = a_1x_1 + \dots + a_{n-1}x_{n-1}$

$$\gcd(a_1 \dots a_{n-1}, a_n) = \gcd(\underbrace{\gcd(a_1 \dots a_{n-1})}_{d}, a_n) =$$

$$= y \cdot d + z\, a_n = y a_1x_1 + \dots + y a_{n-1}x_{n-1} + z\, a_n$$

Per tant, $\exists\ yx_1, yx_2, \dots yx_{n-1}, z$

(*) Lema: $\gcd(a,b,c) = \gcd(\gcd(a,b), c)$

e = $\gcd(a,b,c)$; $d = \gcd(a,b)$; $f = \gcd(d,c)$

→ $e \mid a,b,c \overset{?}{\Rightarrow} e \mid d, c \Rightarrow e \le f$

→ $e \mid a,b,c \Rightarrow e \ge f$ (és el mcd)

$\Rightarrow e = f$

Ol veure que $\gcd(a,b,c) \mid \gcd(a,b)$ i $\gcd(a,b,c) \mid c$

~~$x \mid a,b,c \Rightarrow x \mid a,b$~~ (*)

dous

56 $a_1 \sim a_n \in \mathbb{Z}$

$\text{mcd}(a_i, a_j) = 1 \quad \forall i,j$

$\Rightarrow \exists x_1 \sim x_n \mid 1 = \sum_{i=1}^{n} x_i \prod_{j \neq i} a_j$

Dem

Podem traduir el consegüent a:

~~$\forall i \; \forall j \neq i \; | \; \text{mcd}\left(\prod_{j \neq i} a_j\right)$~~

$\text{mcd}\left(\prod_{j \neq 1} a_j, \prod_{j \neq 2} a_j, \ldots \prod_{j \neq n} a_j\right) = 1$

Si val això, llavors també el p primer

Però llavors,

$p \mid a_2 \cdots a_n \Rightarrow \exists i \mid p \mid a_i$

Però també $p \mid \frac{a_1 \sim a_n}{a_i}$

Cosa que provoca que $\exists j \neq i \mid p \mid a_j$

$\therefore$ llavors $(a_i, a_j) \geq p > 1$!!!

És cert el recíproc?

$$1 = \gcd(a_2 \cdots a_n,\ a_1 a_3 \cdots a_n,\ \ldots) \overset{??}{\Rightarrow} \gcd(a_i, a_j) = 1 \ \forall i,j$$

Rem

Si $\exists\, i,j \mid \gcd(a_i, a_j) = d = p \cdot \alpha$ (p primer)

llavors $p \mid \frac{a_1 \cdots a_n}{a_i}$ i $p \mid \frac{a_1 \cdots a_n}{a_j}$

ja que $p \mid a_j$ ja que $p \mid a_i$

Pintat, $\forall k$ $p \mid \left(\frac{a_1 \cdots a_n}{a_k}\right)$ ← ja que a_i està al producte i, fins, a_j hi és

Pintat, el recíproc és cert.

qed

(57) $a_1 - a_n \in \mathbb{Z}$, $a_i \neq 0$ $\forall i$

$$A = \{ a_1 x_1 + \dots + a_n x_n \mid x_i \in \mathbb{Z} : a_1 x_1 + \dots + a_n x_n > 0 \}$$

Provar

a) $A \neq \emptyset$

b) $d \mid a_i \ \forall i \Rightarrow d \mid \alpha \ \forall \alpha \in A$ (usar linealitat)

c) ~~$\min A = \text{mcd}(a_1 \dots a_n)$~~

$\min A \mid a_i \ \forall i$ (per divisió Euclidea)

d) $\min A = \text{mcd}(a_1 - a_n)$ (usar b, c)

e) $d \mid a_i \ \forall i \Rightarrow d \mid \text{mcd}(a_1 - a_n)$ (usar b, e)

Pw a) $\text{mcd}(a_1 - a_n) \in A$,

Si pe $\text{mcd}(\alpha_1 - \alpha_k)$ existeix sempre

Aixi $\text{mcd}(\alpha_1 - \alpha_k) \geq 1$ si $\alpha_1 - \alpha_k \neq 0$

b) $d \mid a_i \ \forall i \Rightarrow d \mid a_1 x_1 + \dots + a_n x_n$ per linealitat ✓

c) $\alpha \in A$, $\alpha \leq \beta \ \forall \beta \in A$

Vull $\alpha \mid a_i \ \forall i$

Fan divisió euclidiana:

$a_i \mid \alpha$ $\qquad a_i = q_i \cdot \alpha + r_i$

r_i q_i

$r_i < \alpha$ o bé $0 \leq r_i$

Si $r_i = 0 \ \forall i$, llavors $\alpha \mid a_i \ \forall i$ ✓

Suposem que $\exists i \mid r_i \neq 0$,

$$r_i = a_i - q_i \alpha = a_i - \sum_{j=1}^{n} x_j q_i a_j \in A$$

(doncs !!)

però això és absurd, ja que $r_i < \alpha \Rightarrow r_i < \min A$!!!

d) $\min A = \text{mcd}(a_1 \dots a_n)$

per c) $\min A \mid a_i \ \forall i$

Si $\exists d \mid d \mid a_i \ \forall i$ i $d \not\mid \min A$, per b) $d \mid \min A$

O sigui $d = \min A$

e) $d \mid a_i \ \forall i \overset{?}{\Rightarrow} d \mid \text{mcd}(a_1 - a_n)$

Como que $\text{mcd}(\cdot) \in A$,

pra b) temos que $d \mid \text{mcd}(a_1 - a_n)$

(58) $a_n - a_n \in \mathbb{Z}$

$\{ \sum x_i a_i \mid x_i \in \mathbb{Z} \} = \{ x \mid \text{mcd}(a_1 - a_n) \mid x \}$

$\subseteq$

$z \in \{ \sum x_i a_i \mid x_i \in \mathbb{Z} \} \Rightarrow z = \sum_{i=1}^{n} x_i a_i$

Vale que $\text{mcd}(a_1 - a_n) \mid z$

Por #57, sabemos que $d \mid a_i \ \forall i \Rightarrow d \mid \text{mcd}(a_1 - a_n)$

Porém $d \mid a_i \Rightarrow d \mid \sum x_i a_i = z$

Portanto $d := \text{mcd}(a_1 - a_n)$ então $d \mid a_i \ \forall i$

$\therefore$ em consequência, $d \mid z$

$\supseteq$

Sigui $\mathbb{Z} \mid \mathrm{mcd}(a_1 \dots a_n) \mid \mathbb{Z}$

Per Euclides, $\exists\, x_1 \dots x_n \mid \sum_{i=1}^{n} x_i a_i = \mathrm{mcd}(a_1 \dots a_n) \mid \mathbb{Z}$

$\Rightarrow \exists\, k \mid \mathbb{Z} = k \cdot \sum_{i=1}^{n} x_i a_i = \sum_{i=1}^{n} k x_i a_i \in \{\Sigma x_i a_i \mid x_i \in \mathbb{Z}\}$

Com volíem ✓

$b_1 - b_n \in \mathbb{Z}$, $a \in \mathbb{Z}$

(59) $\mathrm{mcd}(a, b_i) = 1 \ \forall i \Rightarrow \mathrm{mcd}(a, \prod_{i=1}^{n} b_i) = 1$

Dem per R.A. $\exists\, d \mid d \mid a$ i $d \mid b_1 - b_n$

$d \neq 1 \Rightarrow d = p \cdot \alpha$, p primer

$\Rightarrow p \mid b_1 \dots b_n \Rightarrow \exists\, j \mid p \mid b_j$

Llavors, $\mathrm{mcd}(a, b_j) = p$!!!

Ref

Es cert el recíproc?

$$\gcd\left(a, \prod_i b_i\right) = 1 \overset{??}{\Longrightarrow} \gcd(a, b_i) = 1 \quad \forall i$$

Ren

Si fos que $\exists i \mid \gcd(a, b_i) = d \neq 1$

Llavors, $d \mid a$ i $d \mid b_i$

Per llavors $\gcd\left(a, \prod_{j=1}^{n} b_j\right) \geq d$

Sed

(69) $c \neq 0$

$a^n \mid b^n c \ \forall n \geq 0 \Rightarrow a \mid b$

Rem

Tenim $a \mid bc \Rightarrow a \mid b$ o $a \mid c$

Sí pbs $a \nmid b$ llavors $a \mid c$

Però $a^2 \mid b^2 c \Rightarrow a^2 \mid c$

i així successivament, $a^n \mid c \ \forall n$ cosa que és contradictòria

(ja que $c \in \mathbb{Z} \Rightarrow c = \varepsilon \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$a \mid c \Rightarrow a = p_1^{\beta_1} \cdots p_r^{\beta_r}$ amb $\beta_i \leq \alpha_i$

Però $a^n = p_1^{\beta_1 n} \cdots p_r^{\beta_r n}$

No pot ser que $n\beta_i \leq \alpha_i \ \forall n$)

És cert el recíproc??

↳ Sí!

$a \mid b \Rightarrow a^n \mid b^n \ \forall n \geq 0 \Rightarrow a^n \mid b^n \cdot c$

↑ ja que $b^n \mid b^n \cdot c$

(70) p, q, r premiers distincts

Quels sont les diviseurs de $n = pq^2r^3$?

→ Exposants possibles :

$p \to \{0,1\} = P$

$q \to \{0,1,2\} = Q$

$r \to \{0,1,2,3\} = R$

$D = \{p^x q^y r^s \mid x \in P, y \in Q, s \in R\}$

↑

$2 \times 3 \times 4$ diviseurs

↳ Calculer-les à classe ←

(71) p premier, $n \geq 2$, $r, s \in \mathbb{Z} \mid n-1 < r/s \leq n$

Sont équivalents :

a) $p^n \mid a$

b) $p^n \mid a^s$

c) $\text{pgcd}(p^n, a) = p^n$

d) $p^n \mid \text{pgcd}(p^n, a)$

e) $p^n \mid \text{pgcd}(p^{n+m}, a) \quad (m \geq 0)$

Dem

a ⇒ b) ~~abst~~

$s(n-1) \leq r \leq n \cdot s$ (si $s \geq 0$)

$s(n-1) \geq r \geq n \cdot s$ (si $s \leq 0$)

⇐ $s \neq 0$ si no, no tindria sentit r/s !!

Cas $s \geq 0$

$r \geq 0$ $\quad p^n | a \Rightarrow a = p^n \cdot k$

$\Rightarrow a^s = p^{n \cdot s} \cdot k^s$

$\Rightarrow p^{r} | p^{ns} \Rightarrow p^r | a^s$ ✓

↑ ja que $r \leq ns$

Cas $s < 0$

$r < 0$ $\quad a^s = \frac{1}{a^{-s}} = \frac{1}{p^{-ns} \cdot k^{-s}} \Rightarrow a^{-s} = p^{-ns} \cdot k^{-s}$

continuar igual ✓

$(n-1 < r/s \leq n \quad n \geq 2)$

b ⇒ c) $p^r \mid a^s \overset{?}{\Rightarrow} \operatorname{mcd}(p^n, a) = p^n$

$a = p^{\alpha} \cdot q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ descomposició en primers $q_i \neq p \ \forall i$

α pot ser 0 a priori

$p^r \mid a^s \Rightarrow a^s = p^{\alpha \cdot s} \cdot q_1^{m} \cdots = p^r \cdot k$

$\Downarrow$

$|r| \leq |\alpha \cdot s|$

$r, s > 0$ (sino, es fa similarment)

$(n-1)\, s \leq r \leq n \cdot s \quad$ i $\quad r \leq \alpha \cdot s$

Compte vol $\forall r, s$ tals que $\ldots$, pel cas $s = 1$ també:

~~$(n-1) \leq r \leq n$ i $r \in \mathbb{Z} \Rightarrow r = n-1$ o $r = n$~~

Pel cas $n-1 < r \leq n$ i $r \in \mathbb{Z} \Rightarrow r = n$

i llavors la hipòtesi és $p^n \mid a^1$

Per tant directament $p^n \mid \operatorname{mcd}(p^n, a)$

però $\operatorname{mcd}(p^n, a) \leq p^n$, ja que p^n no té cap divisor més gran a p^n!

Per tant, $\operatorname{mcd}(p^n, a) = p^n$ ✓

c ⇒ d) $\mathrm{mcd}(p^n, a) = p^n \Rightarrow p^n \mid \mathrm{mcd}(p^n, a)$

Obvi ✓

d ⇒ e) $p^n \mid \mathrm{mcd}(p^n, a) \Rightarrow p^n \mid \mathrm{mcd}(p^{n+m}, a)$ $\forall m \geq 0$

$p^n \mid \mathrm{mcd}(p^n, a) \Rightarrow p^n = \mathrm{mcd}(p^n, a)$

↑

No sé perquè l'exercici està fet així

$\mathrm{mcd}(p^{n+m}, a) = p^{\lambda}$ amb $\lambda \leq n+m$

$n \leq \lambda$ ↑ $\mathrm{mcd}(p^n, a) = p^n$

per tant $p^n \mid p^\lambda$

e ⇒ a) $p^n \mid \mathrm{mcd}(p^{n+m}, a)$ $m \geq 0 \Rightarrow p^n \mid a$

Sempre $\underbrace{\mathrm{mcd}(p^{n+m}, a)}_{d} \mid a \Rightarrow a = k \cdot d$

Però $p^n \mid d \Rightarrow d = k' \cdot p^n$

$a = k \cdot k' p^n \Rightarrow p^n \mid a$

pel

(72) $a, b \in \mathbb{Z}$

$aRb \Leftrightarrow a \mid b^n,\ b \mid a^n$ per un $n \geq 1$

a) $a \neq 0$, $a \mid b^n$ per un $n \geq 1$ $\Leftrightarrow$ $[\forall p \,(p \mid a,\ p \text{ primer}) \Rightarrow p \mid b]$

$\Rightarrow$]

$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ amb $\alpha_i \neq 0\ \forall i$, p_i primers

Sabem que $a \mid b^n$

Llavors, $p_i \mid b^n\ \forall i$

Però $p \mid b^n \Rightarrow p \mid b$, ja que p és primer!

Per tant, $p_i \mid b\ \forall i$

~~Volem veure que $p \mid b, q \mid b \Rightarrow pq \mid b$~~

~~b) $\forall a = \{b \in \mathbb{Z} \mid a \mid b^n \Rightarrow b \mid a^n$ per algun $n\}$~~

$\Leftarrow$] Veiem que $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ $\alpha_i \neq 0$ p_i primers

i $p_i \mid b\ \forall i$

és clar que $p_1 \cdots p_k \mid b$

Sigui $n = \max(\alpha_1 \ldots \alpha_k)$

$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \mid p_1^n \cdots p_k^n$ i $p_1^n \cdots p_k^n \mid b^n$ Per tant $a \mid b^n$

b) $\bar{a} = \{ b \mid \forall p_i \mid b \ \forall p_i \text{ primer de } a \} =$

$= \{ \lambda \cdot p_1 \cdots p_K \mid \lambda \in \mathbb{Z} \}$

c) $\mathbb{Z}\setminus\{0\}/R \approx \{ A_n \mid A_n = \{ p_1 \sim p_n \mid p_i \text{ primer} \}, n \in \mathbb{N} \}$

P''

$\varphi : \mathbb{Z}\setminus\{0\}/R \longrightarrow P$

$\bar{a} \longmapsto \{ p_1 \cdots p_K \}$

↖ ~~el~~ els primers de la descomposició de a

Cal veure:

(I) → ben definida (no depèn del representant)

(II) → injectiva

(III) → ~~bijectiva~~

(I) $b \in \bar{a}$, $b = q_1^{\beta_1} \cdots q_r^{\beta_r}$; $a = p_1^{\alpha_1} \cdots p_K^{\alpha_K}$

Però $p_1 \sim p_K \mid b \iff q_1 \sim q_r \mid a$

~~Si~~ Podem posar $p_1 = q_1, \ldots p_K = q_K$; potser $\exists\, q_{K+1} \cdots q_r$

Però no! ja que $q_1 \sim q_r \mid a = p_1^{\alpha_1} \cdots p_K^{\alpha_K}$!!

(II) Injectivă?

$\varphi(\bar{a}) = \varphi(\bar{b}) = \{p_1, \dots p_k\}$

$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ $\quad$ $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$

Dar atunci avem pt $p_i \mid b$ și $p_i \mid a$ $\forall i$

Prin fapt, $a \mathcal{R} b$ $\quad$ deci $\bar{a} = \bar{b}$

(III) Exhaustivă?

Fie $\{q_1 \dots q_s\} \in \mathcal{P}$

$x := q_1 \cdot \dots \cdot q_s \in \mathbb{Z}$

și evident pt $x \neq 0$ și $\varphi(\bar{x}) = \{q_1 \dots q_s\}$ ✓

(77) $a|c$, $b|d \Rightarrow \mcd(a,b) \mid \mcd(c,d)$

Rem $\mcd(a,b)|a$; $\mcd(a,b)|b$

$\Rightarrow \mcd(a,b)|c$; $\mcd(a,b)|b$

Però $\forall\ \alpha|c,d$, $\alpha|\mcd(c,d)$

$\Rightarrow \mcd(a,b) \mid \mcd(c,d)$ ped

(78) $d|a$ $d|b \Rightarrow \mcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\mcd(a,b)}{|d|}$

Clàrament $\frac{\mcd(a,b)}{|d|} \mid \mcd\left(\frac{a}{d}, \frac{b}{d}\right)$

Si $\exists\ \varepsilon \mid \varepsilon|\mcd\left(\frac{a}{d}, \frac{b}{d}\right)$, llavors també tindríem:

$\varepsilon \mid \frac{a}{d}$; $\exists$ divisor més gran $\Rightarrow \varepsilon \cdot d \mid a$; no hi ha divisor més gran

$\varepsilon \mid \frac{b}{d}$ " " " $\Rightarrow \varepsilon \cdot d \mid b$ " "

⚠ d no és divisor

$\Rightarrow \cancel{\mcd(a,b)} \cancel{\mid d} \Rightarrow \varepsilon \cdot d \mid \mcd(a,b)$

Hem dit que $\frac{mcd(a,b)}{|d|} \mid mcd\left(\frac{a}{d}, \frac{b}{d}\right)$

$\forall \varepsilon$ tal que $\varepsilon \mid \frac{a}{d}$ i $\varepsilon \mid \frac{b}{d}$

Llavors, $\varepsilon \cdot d \mid a$ i $\varepsilon \cdot d \mid b$

Per tant, $\varepsilon \cdot d \mid mcd(a,b)$

però això vol dir que $\varepsilon \mid \frac{mcd(a,b)}{d}$

O sigui $\forall \varepsilon$ divisor de $\frac{a}{d}$ i $\frac{b}{d}$, és divisor de $\frac{mcd(a,b)}{|d|}$: Aquest és el diferència de $mcd\left(\frac{a}{d}, \frac{b}{d}\right)$

gcd

(79)

$\forall i \; \exists j \;\; b_j \mid a_i \Rightarrow \underbrace{mcd(b_1 - b_m)}_{\beta} \mid \underbrace{mcd(a_1 - a_n)}_{\alpha}$

Dem

Tenim $\alpha \mid a_i \;\; \forall i$ (i és el més gran)

$\beta \mid b_i \;\; \forall i$ (i és el més gran)

$\forall i \; \exists j \;\; b_j \mid a_i$

$a_i = \alpha \cdot k = b_j \cdot r$ per algun j

$\Rightarrow b_j \mid \alpha$

Però $\beta \mid b_j$ (ja que $\beta \mid b_i \; \forall i$)

$\Rightarrow \left.\begin{array}{l} \exists j \; \beta \mid b_j \\ b_j \mid \alpha \end{array}\right\} \Rightarrow \beta \mid \alpha$ ped

(80) $a \geq 0$, $a \in \mathbb{Z}$

$\sqrt{a} \in \mathbb{Q} \Rightarrow a = k^2$ ab $k \in \mathbb{Z}$

Pun $\sqrt{a} = \frac{\alpha}{\beta}$ ab $\alpha, \beta \in \mathbb{Z}$, $\beta \neq 0$, $mcd(\alpha, \beta) = 1$

* i fodum dr, $\alpha, \beta \geq 0$

(Ja pe si $\alpha, \beta \leq 0$, fem $-\alpha, -\beta$, ja pe $\sqrt{a} \geq 0$)

$a = \frac{\alpha^2}{\beta^2}$ L'unica manera pe $\beta^2 \mid \alpha^2$ és pe $\beta \mid \alpha$

↑

O sigui pe $\frac{\alpha^3}{\beta^2} \in \mathbb{Z}$

Però $mcd(\alpha, \beta) = 1 \Rightarrow \beta = 1$ o $\alpha = 1$

⇓

$\beta = 1$ ja tot pe $\frac{\alpha^2}{\beta^2} \in \mathbb{Z}$

Per tal, $a = \alpha^2$ pqcd

(81) x = dia de naixent

y = mes de naixent

Sabem $12x + 31y = 500$

És clar que $\begin{cases} 1 \le x \le 31 \\ 1 \le y \le 12 \end{cases}$ ← clarament, potser

$1 \le x \le 30$ i $y \in \{4, 5, 9, 11\}$

i $1 \le x \le 28$ i $y = 2$

Fem algorisme d'Euclides cap Bézout:

x	1	0	1	−1	2	−5
y	0	1	−2	3	−5	13
q		2	1	1	2	2
r	31	12	7	5	2	1 | 0

Així, $\text{mcd}(31, 12) = 1 = 31(-5) + 12(13)$

Per tant, $500 = 31 \cdot \underbrace{[500 \cdot (-5)]}_{x} + 12 \cdot \underbrace{[500(13)]}_{y}$ és una solució

Però ens interessa $\begin{cases} x = 13 - 5t \\ y = -5 + 13t \end{cases}$ són totes les solucions, ja que $(13, 5) = 1$

Si $1 \le y \le 12$, cal que $t = 1$

$y = -5 + 13 \cdot t = -5 + 13 = 8$

Llavors, $x = 13 - 5 = 8$

Per tal, la sola és 8 d'hores ✓

(82) $x = x_0 + \lambda t$ $\forall t \in \mathbb{Z}$ Sols totes les solucions de $ax + by = c$
$y = y_0 + \mu t$

⇙

a) $x = x_0 + \lambda t$ és solució
$y = y_0 + \mu t$

b) $\text{mcd}(\lambda, \mu) = 1$

Per

⇒ a) és cert ✓

b) Si fos $\text{mcd}(\lambda, \mu) = d \neq 1$, llavors

$x = x_0 + \frac{\lambda}{d} t$
$y = y_0 + \frac{\mu}{d} t$ ⇒ seria també solució

↑

Però $a x_0 + a \frac{\lambda}{d} t + b y_0 + b \frac{\mu}{d} t = c$

$= c$

$a \frac{\lambda}{d} t + b \frac{\mu}{d} t = 0$ per tot t

Tindrem que $\tilde{x} = x_0 + \frac{\lambda}{d} t$

$\tilde{y} = y_0 + \frac{\mu}{d} t$

Això diu que $\tilde{x}, \tilde{y}$ són solucions de la hipòtesis

Però,

$$a\tilde{x} + b\tilde{y} = \underbrace{ax_0 + by_0}_{c} + \left(a\frac{\lambda}{d} + b\frac{\mu}{d}\right)t$$

Així x, y solucions $\Leftrightarrow$ $c = ax + by = \underbrace{ax_0 + by_0}_{c} + (a\lambda + b\mu)t$

$\Downarrow$

$a\lambda + b\mu = 0$

Llavors, $\left(a\frac{\lambda}{d} + b\frac{\mu}{d}\right) = \frac{1}{d}(a\lambda + b\mu) = 0$

O sigui, tenim infinit $\tilde{x}, \tilde{y}$ solucions diferents !!!!

$\Leftarrow$ Sigui $\tilde{x}, \tilde{y}$ solucions

$a\tilde{x} + b\tilde{y} = \frac{c}{\uparrow \mathrm{mcd}(a,b)} \cdot \mathrm{mcd}(a,b) = \frac{b}{\mathrm{mcd}()} \cdot \lambda \cdot a + \frac{a}{\mathrm{mcd}()} \mu b$

$\uparrow$ Bé, ja que divideix a a i b

$\uparrow$ Bé, fet.

Per tant, $x = x_0 + \frac{\lambda b}{\mathrm{mcd}()} t$ és solució ✓

(83) Trobar solucions, si n'hi ha de:

a) $512x + 88y = 20$

$\text{mcd}(512, 88, 20) = 2^2$

$2^9 \quad 2^3 \cdot 11 \quad 2^2 \cdot 5$

Per tant a) és equivalent a:

$2^7 x + 2 \cdot 11 y = 5$

$\text{mcd}(2^7, 2 \cdot 11) = 2$

$\Rightarrow \nexists \lambda, \mu \mid 2^7 \lambda + 2 \cdot 11 \mu = 2$

$\times 10 \rightsquigarrow 2^8 \cdot 5 \lambda + 2^2 11 \cdot \mu = 20$

No té solució !!

$\text{mcd}(512, 88) = 8 \Rightarrow 8 \cdot (2^6 x + 11y) = 20$ impossible!!

ja que $8 \nmid 20$!

a2) $512x + 88y = 40$

Ara sí té solució!

$8\cdot(2^6 x + 11y) = 8\cdot 5$

($a = 2^6$, $b = 11$, $c = 5$)

$\text{mcd}(2^6, 11) = 1 \Rightarrow \exists\, \lambda, \mu \mid \lambda\cdot 2^6 + \mu\, 11 = 1$ (Bézout)

Llavors, $5\cdot\lambda$ i 5μ seran solucions.

Fem-ho:

x	1	0	1	-1	(5)	
y	0	1	-5	6	(-29)	
q		5	1	4	2	
r	64	11	9	2	(1)	0

(1 ↑ mcd)

$\Rightarrow 5\cdot 64 + (-29)\,11 = 1$ ✓ ($\lambda = 5$, $\mu = -29$)

$x_0 = 25$, $y_0 = -5\cdot 29 = -145$

i totes les solucions són:

$$x = x_0 + \alpha t$$
$$y = y_0 + \beta t$$

on ~~$\alpha = \frac{5\cdot 40}{5} = 40$~~

~~$\beta = \frac{-29\cdot 40}{5} = -29\cdot 8 = -232$~~

$\Rightarrow$ ~~$x = 25 + 40t$~~ ~~$y = -145 - 232t$~~

~~$x = 25 + 40t$~~
~~$y = -145 - 232t$~~

$$\left.\begin{aligned} x &= x_0 + \frac{b}{d}t \\ y &= y_0 + \frac{a}{d}t \end{aligned}\right\} \quad \text{où } d = \text{pgcd}(a,b) = 1$$

Par tout, $\left.\begin{aligned} x &= 25 + 11t \\ y &= -145 - 64t \end{aligned}\right\}$

a3) $-512x - 88y = 40$

Oùaut, $\begin{aligned} x &= -25 - 11t \\ y &= 145 + 64t \end{aligned}$

a4) $-512x + 88y = 40$

Solumpre ho de ser $\left.\begin{aligned} x &= -25 - 11t \\ y &= -145 - 64t \end{aligned}\right\}$

a5) $512x - 88y = 40$

$\left.\begin{aligned} x &= 25 + 11t \\ y &= 145 + 64t \end{aligned}\right\}$

6.1) $1234x + 221y = 20$

$\text{mcd}(1234, 221) = 1$

$\Rightarrow \exists \lambda, \mu \mid \lambda 1234 + 221\mu = 1$

x	1	0	1	-1	+2	-5	+12
y	0	1	-5	6	-11	28	-67
q		5	1	1	2	2	18
r	1234	221	129	92	37	18	(1) 0

$1234 \cdot \underbrace{12 \cdot 20}_{x_0} + 221 \underbrace{(-67) \cdot 20}_{y_0} = 20$

$$\left.\begin{aligned} x &= x_0 + \frac{b}{d}t = x_0 + 221t \\ y &= y_0 - \frac{a}{d}t = y_0 - 1234t \end{aligned}\right\}$$

Ogni $\left.\begin{aligned} x &= 240 + 221t \\ y &= -1340 - 1234t \end{aligned}\right\}$

Rosen equation variable

b2) $-1234t + 221w = 40$

$1234 \cdot (-t) + 221w = 2 \cdot 20$

$1234 \cdot \left(\frac{-t}{2}\right) + 221 \cdot \left(\frac{w}{2}\right) = 20$

↑ al posto di t ↗

$\frac{-t}{2} = x \Rightarrow \quad t = -2x = -480 - 442t$

$\frac{w}{2} = y \Rightarrow \quad w = 2y = -2680 - 2468t$

b3) $-1234t - 221r = 40$

$+221(-r)$

$t = t$

$r = -w$

(84) (x,y) | y maxima për $y \le -3$

Fen-ne $512x + 88y = 40$

Sdoma që $\begin{cases} x = 25 + 11t \\ y = -145 - 64t \end{cases}$

$y \le 3 \Rightarrow -145 - 64t \le -3 \Rightarrow -64t \le 142$

$t \ge \frac{142}{-64} = -2\frac{14}{32}$

$t \ge -2$

$\begin{cases} y = -145 + 64 \cdot 2 = -17 \\ x = 25 - 11 \cdot 2 = 3 \end{cases}$

(85) $F = \frac{9}{5}C + 32$

Busquem $5F - 9C = 160$, $C \geq -273'15$

$\text{mcd}(5, -9) = 1$

$\Rightarrow \exists \lambda, \mu \quad 5\lambda - 9\mu = 1$

x	1	0	1	(-1)
y	0	1	-1	(2)
q		1	1	4
r	9	5	4	1	0

↑

Compte no hay equivocarse amb el signe!!!

~~$8C(29)$~~ $5 \cdot (2) - 9 \cdot (1) = 1$

$5 \cdot (2 \cdot 160) - 9(160) = 160$

$F_0 = 320$, $C_0 = 160$

$$\left.\begin{aligned} F &= F_0 - 9t = 320 - 9t \\ C &= C_0 - 5t = 160 - 5t \end{aligned}\right\}$$

Cal $C \geq -273'15$

a sgw, $C \geq -273$

$-273 \leq C = 160 - 5t \Rightarrow 5t \leq 433 \Rightarrow$

$\Rightarrow t \leq 86'6$

Per tant, les solucions són $t \in (-\infty, 86] \cap \mathbb{Z}$

(86) Volem $6x + 11y = 45$

on x = vegades que usem el rellotge de 5 units

y = " " 11 units

Caldrà que $x, y \in \mathbb{Z}$, $x, y \geq 0$

$\text{mcd}(6, 11) = 1 \Rightarrow \exists \lambda, \mu \mid 6\lambda + 11\mu = 1$

$\Rightarrow \lambda = 2$ i $\mu = -1$ serveix

$6 \cdot (2 \cdot 45) + 11(-45) = 45$

x_0 y_0

$$\begin{cases} x = x_0 + 11t = 90 + 11t \\ y = y_0 - 6t = -45 - 6t \end{cases}$$

$x, y \geq 0 \Rightarrow \begin{cases} 90 + 11t \geq 0 \\ -45 - 6t \geq 0 \end{cases} \Rightarrow \begin{cases} t \geq \frac{-90}{11} = -8'\ldots \\ t \leq \frac{-45}{6} = -7'5 \end{cases}$

O sigui, $-8 \leq t \leq -8$

L'única solució possible és $t = -8$

$x = 90 - 8 \cdot 11 = 2$

$y = -45 + 6 \cdot 8 = 3$

O sigui, l'única forma de fer-ho és usant

$2 \cdot 6 + 3 \cdot 11 = 45$

↑ 2 vegades ↑ 3 vegades

(91) $a_1 \sim a_n \in \mathbb{Z}$

$\text{mcd}(a_i, a_j) = 1 \ \forall i \neq j \Rightarrow \text{mcm}(a_1 \sim a_n) = |a_1 \sim a_n|$

Per inducció NOTA $a_i \neq 0 \ \forall i$ ⚠ $\exists a_i = 0$ el fem a part !!

$n = 2$ $\text{mcd}(a_1, a_2) = 1$, $\text{mcm}(a_1, a_2) = \frac{|a_1 a_2|}{\text{mcd}} = |a_1 a_2|$ ✓

Suposem $n-1$, és a dir, $a_1 \sim a_{n-1}$

$\text{mcd}(a_i, a_j) = 1 \ \forall i, j \in \{1, \dots n-1\}, \ i \neq j \Rightarrow \text{mcm}(a_1 \sim a_{n-1}) = (\sim 1)$

Vegem n

Per associativitat,

$$\text{mcm}(a_1 \sim a_{n-1}, a_n) = \text{mcm}(\text{mcm}(a_1 \sim a_{n-1}), a_n) =$$

$$= \text{mcm}(|a_1 \sim a_{n-1}|, a_n)$$

Com pe $\text{mcd}(a_i, a_j) = 1 \ \forall i, j, \ i \neq j$

llavors, $\text{mcd}(a_i, a_n) = 1 \ \forall i \in \{1, \dots n-1\}$

Això vol dir pe $\text{mcd}(a_1 \dots a_{n-1}, a_n) = 1$

ja pe si no, $\exists p$ tal pe $p | a_n$ i $p | a_1 \dots a_{n-1} \Rightarrow p | a_j$ per algun j

Por tanto,

$$mcm\left(|a_1 \cdots a_{n-1}|, a_n\right) = \frac{|a_1 \cdots a_{n-1}| \cdot |a_n|}{mcd\left(|a_1 \cdots a_{n-1}|, a_n\right)} =$$

$$= |a_1 \cdots a_n| \quad \text{qed}$$

(92) $mcm(c\cdot a, c\cdot b) = |c| \cdot mcm(a,b)$

Dem Supongamos $\neq 0$ (si no, es trivial ✓)

$$mcm(ca, c\cdot b) = \frac{|cacb|}{mcd(ca, cb)} = \frac{|c||c||ab|}{|c|\, mcd(a,b)} =$$

$|ab| = mcd(\cdot) \cdot mcm(\cdot)$

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

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

qed

(93) $a, b \quad a+b=57$

$mcm(a,b) = 680$

$a+b=57 \Rightarrow 1\cdot a + 1\cdot b = 57$

$mcd(1,1) = 1 \Rightarrow 1\cdot 1 + 0\cdot 1 = 1$

$\lambda \quad \mu$

$a_0 = 57\cdot 1 = 57$

$b_0 = 57\cdot \mu = 0$

$$\left.\begin{aligned} a &= a_0 + \frac{1}{1}t = 57 + t \\ b &= b_0 - \frac{1}{1}t = -t \end{aligned}\right\}$$

cel pe $mcm(a,b) = 680 = mcm(|a|,|b|)$

~~$mcm(a,b) = mcm(|a|,|b|) = mcm(57+t, t) = 680$~~

~~$680 = mcm(57+t, t) = \frac{|57+t|\,|t|}{mcd(57+t, t)}$~~

~~$57 = 19\cdot 3$~~

Observ pe $mcm(57+t, t) = 680$

Fie $mcd(57+t, t) = d \Rightarrow d \mid t$ și $d \mid 57+t \Rightarrow d \mid 57$

Pois $d \mid 57 \Rightarrow d \in \{1, 3, 19, 57\}$

$$680 = mcm(57+t, t) = \frac{|57+t|\,|t|}{mcd(57+t, t)} = \frac{|57+t|\,|t|}{d}$$

Fem-ho per casos:

$d = 1$

$$680 = |57+t|\,|t| \neq$$

$$\Rightarrow t^2 + 57t - 680 = 0 \Rightarrow t = \frac{-57 \pm \sqrt{57^2 + 4 \cdot 680}}{2} = \frac{-57 \pm 23}{2} =$$

(ja vencem el $|t|$ després)

$$= \begin{cases} -17 \\ -80 \end{cases}$$

$t = \pm 17$, $t = \pm 80$

Pois $t = +17$ no val
$t = +80$ no val
← No compleixen $|57+t|\,|t| = 680$

$t = -17$ sí, $t = -80$ no val ← No compleix $|57+t|\,|t| = 680$

$mcm(40, +17) = 680$

$mcd(40, +17) = 1$

$a = 40$
$b = 17$ ✓

$\underline{d=3}$ $$680 = \frac{|57+t||t|}{3}$$

$$2040 = 57t + t^2 \Rightarrow t^2 + 57t - 2040 = 0$$

$$t = \frac{-57 \pm \sqrt{57^2 + 4\cdot 2040}}{2} = \frac{-57 \pm \sqrt{n}}{2} \notin \mathbb{Z} \;!!$$

~~De fet, això dar, ja que $680 = \frac{|57+t||t|}{3} \Rightarrow \nexists$~~

~~com que $3 \nmid 57$ llavors $3 \nmid t$~~

Per tant, $d=3 \Rightarrow \nexists\, t \in \mathbb{Z}$

$\underline{d=19}$ $$680 = \frac{|57+t||t|}{19} \Rightarrow t^2 + 57t - 12.920 = 0$$

$$t = \frac{-57 \pm \sqrt{57^2 + 4\cdot 12920}}{2} \notin \mathbb{Z}$$

$\underline{d=57}$ $$680 = \frac{|57+t||t|}{57} \Rightarrow t = n \notin \mathbb{Z}$$

~~(*) Per tant només pot ser $a=40$, $b=17$ (*)~~

(9) $M_a = \{x \in \mathbb{Z} \mid a \mid x\}$

a) $M_a \cap M_b = M_{mcm(a,b)}$

b) Val per a més enters? (i.e. $M_a \cap M_b \cap M_c = M_{mcm(a,b,c)}$??)

c) Quin a, b satisfan $M_a \cap M_b = M_{a \cdot b}$?

a)

$\subseteq$] $t \in M_{mcm(a,b)} \Rightarrow mcm(a,b) \mid t$

$\Rightarrow a \mid mcm(a,b)$ per tant, $a \mid t$ i $b \mid t$
$b \mid mcm(a,b)$

$\Rightarrow t \in M_a \cap M_b$

$\supseteq$] $t \in M_a \cap M_b \Rightarrow a \mid t$ i $b \mid t \Rightarrow mcm(a,b) \mid t$ ✓

(propietat mcm)

b) Està clar que $M_{mcm(a,b,c)} \subseteq M_a \cap M_b \cap M_c$

Per la propietat $a \mid c$ i $b \mid c \Leftrightarrow mcm(a,b) \mid c$, que val per n enters

c) Dins a, b | $M_a \cap M_b = M_{ab}$?

Sabem que $M_a \cap M_b = M_{mcm(a,b)}$

Per tant la pregunta és

$$a \cdot b = mcm(a,b)$$

Però $mcd(a,b) \cdot mcm(a,b) = |ab|$

Per tant, cal que $mcd(a,b) = 1$ (primers entre ells)

(95) p primer

Són equivalents

a) $p^2 \mid a$

b) $p^4 \mid a^2$

c) $p^3 \mid a^2$

d) $\operatorname{mcm}(p^2, a) = |a|$

e) $p^2 \mid \operatorname{mcm}(p, a)$

Dem

a $\Rightarrow$ b) trivial : $a = kp^2 \Rightarrow a^2 = k^2 p^4$

b $\Rightarrow$ c) trivial : $a^2 = k^2 p^4 = (k^2 p) p^3$

c $\Rightarrow$ d) $\operatorname{mcm}(p^2, a) = \dfrac{|a| \cdot p^2}{\operatorname{mcd}(p^2, a)}$

Com que $p^3 \mid a^2$, $\operatorname{mcd}(p^2, a) = p^2$, ja que és clar $p^2 \mid a$

I ja que $p^3 \mid a^2$ ~~$\Leftrightarrow p \mid$~~ i si $p^2 \mid a$ llavors $a = p \cdot R$ amb $p \nmid R$

però $p^3 \mid a^2 = p^2 \cdot R \Rightarrow p \mid R$!!!

Llavors, $\operatorname{mcm}(p^2, a) = \dfrac{|a| \, p^2}{p^2} = |a|$

d $\Rightarrow$ e) $p^2 \mid \operatorname{mcm}(p, a) = \dfrac{|p||a|}{\operatorname{mcd}(p, a)}$

Cal veure que $p \mid \dfrac{a}{\operatorname{mcd}(p, a)}$

p primer $\Rightarrow \mathrm{mcd}(p,a) = \begin{cases} 1 & (\text{si } p \nmid a) \\ p & (\text{si } a = p^{\alpha_1} \cdot R) \end{cases}$

si $p \nmid a \Rightarrow \mathrm{mcm}(p^2, a) \geq |a|$

↑

ja que $\mathrm{mcm}(p^2, a) = |a| \Rightarrow a = kp^2$ i

portat $p \mid a$!!

Per tant, $\mathrm{mcd}(p, a) = p$

Cal veure que $p \mid \frac{a}{p}$

Però ja hem raonat que $\mathrm{mcm}(p^2, a) = |a| \Rightarrow a = kp^2$

per tant, $p^2 \mid a$ i $p \mid \frac{a}{p}$ com volíem

$c \Rightarrow a$) $p^2 \mid \mathrm{mcm}(p^2, a) \Rightarrow p^2 \mid a$

p primer $\Rightarrow \mathrm{mcm}(p, a) = p \cdot R$

$p^2 \mid \mathrm{mcm}(p, a) = p \cdot R \Rightarrow p \mid R$, o sigui $p \mid a$

però $a = p^{\alpha_1} \cdot q$ je hem mirat $\alpha_1 \geq 1$

$\mathrm{mcm}(p, a) = p^{2+\beta} \cdot \tilde{R}$, on $\beta \geq 0$

$2 + \beta = \max(1, \alpha_1) \Rightarrow \alpha_1 = 2 + \beta \geq 0 \Rightarrow a = p^2 \cdot S$

$\Rightarrow p^2 \mid a$ ped.....

(96) $\forall i \; \exists j \quad a_i \mid b_j \Rightarrow mcm(a_1 - a_n) \mid mcm(b_{1,m} b_{j_n})$

Dem $mcm(a_1 - a_n) \mid \prod_{i=1}^{n} a_i$ Fem $\forall$:

Fem $a_i \neq 0$ ja pe

si $\exists\, a_i = 0$, llavors no

té sentit $0 \mid \infty$

Però $\forall i \; \exists_{j(i)} \; a_i \mid b_{j(i)}$

Per tant $\prod_{i=1}^{n} a_i \mid \prod_{i=1}^{n} b_{j(i)}$

i $b_i \neq 0 \; \forall i$, ja pe $\exists\, b_i = 0$

vol dir $mcm(a_1 - a_n) \mid 0$ sempre

Fem $mcm(\{b_j \mid a_i \mid b_i\}) = m$

↖ els pe surten de $\forall i \; \exists j \; a_i \mid b_j$

$m \mid mcm(b_1, \dots b_m)$, ja pe $mcm(A) \mid mcm(B)$

si $A \subseteq B$ [*]

Però $a_i \mid m$ (per construcció de m, ja pe són els b_j tals pe $a_i \mid b_j$

i $b_k \mid mcm(\{b_j\}) \quad \forall b_k \in \{b_j \mid a_i \mid b_i\}$

i $a_i \mid b_k \quad \forall i \in \{1, \dots n\}$

Per tant, $mcm(a_1 - a_n) \mid m$ i $m \mid mcm(b_1 - b_{mc})$

[*]

Vrem să $A \subseteq B \Rightarrow \text{mcm}(A) \mid \text{mcm}(B)$

~~Știm că $\alpha \mid a$ pt $a \mid \alpha$ $\forall a \in A$~~

~~Deci avem $\text{mcm}(A) \mid \alpha$~~

$\text{mcm}(B) = \text{mcm}(\text{mcm}(A), \text{mcm}(B \setminus A))$

$\alpha \neq 0$ $\quad \beta$

Știm deja că $\alpha \mid \text{mcm}(\alpha, \dots)$

(97) $d \mid a, b \Rightarrow \operatorname{mcm}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\operatorname{mcm}(a,b)}{|d|}$

$\operatorname{mcm}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\left|\frac{a}{d}\right|\left|\frac{b}{d}\right|}{\operatorname{mcd}\left(\frac{a}{d}, \frac{b}{d}\right)}$

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

$\operatorname{mcm}(a,b) = \operatorname{mcm}(\lambda d, \mu d) = |d| \cdot \operatorname{mcm}(\lambda, \mu)$

($d \mid a, b$; Propietat)

ja ho tenim, ja que $\lambda = \frac{a}{b}$, $\mu = \frac{b}{d}$ pel

(98) p primer $n \geq 2$ $r, s \in \mathbb{Z}$ $1 \leq n-1 \leq \frac{r}{s} \leq n$

Són equivalents:

a) $p^n \mid a$

b) $p^r \mid a^s$

c) $\operatorname{mcm}(p^n, a) = |a|$

d) $p^n \mid \operatorname{mcm}(p, a)$

e) $p^n \mid \operatorname{mcm}(p^{n-1}, a)$

a) $\Rightarrow$ b): $r, s \geq 0 \Rightarrow p^r \mid p^{n \cdot s} \mid a^s$ ($\exists$ $r, s \leq 0$ llavors (-1)) i.e. $s(n-1) \geq r \geq sn$

$s(n-1) \leq r \leq ns$

a) $\Rightarrow$ c): $p^n \mid a \Rightarrow p^{n-1} \mid a$

$p \mid a^s \Rightarrow p \mid a$ (p primer)

$a^s = \frac{1}{a^{-s}} = \frac{1}{p^n \cdot k} \Rightarrow a^{-s} = p^n k$

$\therefore p^{-r} \mid a^{-s}$

b ⇒ c

$a = p^{\alpha} \cdot q_1 \cdots$ (no p) $\quad \alpha \neq 0$

$p^r \mid a^s \Rightarrow |r| \leq |\alpha \cdot s|$

$r, s \neq 0$ (si no, es fa servir)

$p^r \mid a^s \quad \forall n s \quad (n-1)s < r \leq ns$

pel cas $s=1$ tenim $n-1 < r \leq n$

$\Rightarrow r = n$ i llavors $p^n \mid a$

$\mathrm{mcm}(p^n, a) = |a|$ ✓

c ⇒ d $\quad \mathrm{mcm}(p^n, a) = |a| \overset{?}{\Rightarrow} p^n \mid \mathrm{mcm}(p, a)$

$\mathrm{mcm}(p^n, a) = |a| \Rightarrow a = p^n \cdot p^{\beta} \cdot q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ amb $\beta \neq 0$

Per tal, $p^n \mid a$

d ⇒ e $\quad p^n \mid \mathrm{mcm}(p, a) \overset{?}{\Rightarrow} p^n \mid \mathrm{mcm}(p^{n-1}, a)$

$p^n \mid \mathrm{mcm}(p, a) \Rightarrow a = p^n \cdot K \Rightarrow p^n \mid \mathrm{mcm}(p^{n-1}, a)$

e ⇒ a $\quad p^n \mid \mathrm{mcm}(p^{n-1}, a) \overset{?}{\Rightarrow} p^n \mid a$

$\mathrm{mcm}(p^{n-1}, a) = p^n \cdot K$ on $a = p^h \cdot p^{\alpha} q_1^{\beta_1} \cdots \Rightarrow p^h \mid a$

ref

(99) $a_1 \dots a_n \in \mathbb{Z}$ i $n \geq 3$

Són equivalents:

a) $\text{mcd}(a_1 \dots a_n) \cdot \text{mcm}(a_1 \dots a_n) = |a_1 \dots a_n|$

b) $a_1 \dots a_n$ són primers entre sí: $(\text{mcd}(a_i, a_j) = 1 \ \forall i,j)$

Dem

b $\Rightarrow$ a

$n=2$) ✓ (ja el sabem: $\text{mcd}(a_1, a_2) = 1$)

$n-1$) $a_1 \dots a_{n-1}$ primers entre sí $\Rightarrow \text{mcd}(a_1 \dots a_{n-1}) \text{mcm}(a_1 \dots a_{n-1}) = |a_1 \dots a_{n-1}|$

Hagem n:

$$\text{mcd}(a_1 \dots a_{n-1}, a_n) = \text{mcd}(\underbrace{\text{mcd}(a_1 \dots a_{n-1})}_{d}, a_n)$$

$$\text{mcm}(a_1 \dots a_n) = \text{mcm}(\underbrace{\text{mcm}(a_1 \dots a_{n-1})}_{m}, a_n)$$

Sabem:

~~$\text{mcd}(d, a_n) \cdot \text{mcm}(m, a_n) =$~~

Per hipòtesi inducció, $m \cdot d = |a_1 \dots a_{n-1}|$

Però a_i, a_j primers entre sí $\Rightarrow d = 1$

(ja pe $d \mid a_i \ \forall i$ i si $d \neq 1$, llavors $d \mid a_\ell$ i $d \mid a_t \Rightarrow \text{mcd}(a_\ell, a_t) = d > 1$!!)

Soln

$\mathrm{mcd}(d, a_n) = \mathrm{mcd}(1, a_n) = 1$

$\mathrm{mcm}(m, a_n) = \mathrm{mcm}(|a_1 \cdots a_{n-1}|, a_n)$

~~$|a_1 \cdots a_{n-1}| \cdot |a_n| = \mathrm{mcd}(|a_1 \cdots a_{n-1}|, a_n) \cdot \mathrm{mcm}(|a_1 \cdots a_{n-1}|, a_n)$~~

$$\mathrm{mcd}(a_1 \cdots a_n) \cdot \mathrm{mcm}(a_1 \cdots a_n) = 1 \cdot \mathrm{mcm}(|a_1 \cdots a_{n-1}|, a_n) =$$

$$= \frac{|a_1 \cdots a_{n-1}| \cdot |a_n|}{\mathrm{mcd}(|a_1 \cdots a_{n-1}|, a_n)} = |a_1 \cdots a_n| \quad \checkmark$$

és 1, ja que $\mathrm{mcd}(|a_1 \cdots a_{n-1}|, a_n) = \varepsilon_{>1} \Rightarrow$

$\Rightarrow \varepsilon \mid a_1 \cdots a_{n-1}$ i $\varepsilon \mid a_n$

$\Downarrow$

$\varepsilon \mid a_j$ per algun j $\Rightarrow \mathrm{mcd}(a_j, a_n) = \varepsilon$!!

$a=7b$ $\mid \gcd(a_1 \dots a_n) \cdot \operatorname{mcm}(a_1 \dots a_n) = \mid a_1 \dots a_n \mid$

$\Leftarrow$?

$\gcd(a_i, a_j) > 1 \quad \forall i, j \quad i \neq j$

Si existeix $i, j \mid \gcd(a_i, a_j) = \varepsilon > 1$,

reordenant podem ser a_1, a_2

O bé: $\gcd(a_1, a_2) = \varepsilon > 1$

$$\gcd(a_1 \dots a_n) = \gcd(a_1, \underbrace{\gcd(a_2 \dots a_n)}_{d})$$

$$\operatorname{mcm}(a_1 \dots a_n) = \operatorname{mcm}(a_1, \underbrace{\operatorname{mcm}(a_2 \dots a_n)}_{m})$$

Tenim $\gcd(a_1, d) \cdot \operatorname{mcm}(a_1, m) = \mid a_1 \dots a_n \mid$

però, a més, com que vol $\forall n$,

$$d \cdot m = \mid a_2 \dots a_n \mid$$

$$\gcd(a_1, d) \cdot \frac{|a_1| \cdot m}{\gcd(a_1, m)} = \mid a_1 \dots a_n \mid$$

$=$ ↓

$$\gcd(a_1 \dots a_n) \cdot \frac{\frac{|a_1| \, |a_2 \dots a_n|}{\gcd(a_2 \dots a_n)}}{\gcd(a_1, m)} = \mid a_1 \dots a_n \mid$$

$$\Rightarrow \gcd(a_1 \dots a_n) \cdot \cancel{|a_1 \dots a_n|} = \cancel{|a_1 \dots a_n|} \gcd(a_1, m) \gcd(a_2 \dots a_n)$$

$\Rightarrow \mcd(a_1 \dots a_n) = \mcd(a_1, \mcm(a_2 \dots a_n)) \cdot \mcd(a_2, \dots a_n)$

a_1 hipòtesi a_2

$\varepsilon \mid a_1$ $\varepsilon \mid a_2$

$\Downarrow$

$\varepsilon \mid \mcd(a_1, \mcm(a_2 \dots a_n))$

$\Downarrow$

$\mcd(a_1 \dots a_n) = \varepsilon \cdot$ ☺

$\Rightarrow \varepsilon \mid a_i \quad \forall i$

Però això és contradicció (ho hagués sabut d'eliminar el principi de la hipòtesi!)

EXO/21 CAP-1 TO

Ja pre: $\varepsilon \mid a_i \Rightarrow$ podem fer $b_j = \frac{a_j}{\varepsilon}$

i tindríem: $\mcd(a_1 \dots a_n) \cdot \mcm(a_1 \dots a_n) = \varepsilon^n |b_1 \dots b_n|$

$\varepsilon \mcd(b_1 \dots b_n) \cdot \varepsilon \mcm(b_1 \dots b_n)$

(ja pre $\mcd(ac, bc) = |c| \mcd(a,b)$ i el mateix pel mcm)

$\Rightarrow \mcd(b_1 \dots b_n) \cdot \mcm(b_1 \dots b_n) = \varepsilon^{n-2} |b_1 \dots b_n|$

$\Downarrow$ hipòtesi

$|b_1 \dots b_n| \Rightarrow \varepsilon^{n-2} = 1$!!!