Divisibilitat

$\boxed{a \mid b \Leftrightarrow \exists q \in \mathbb{Z} : b = aq}$ "b és divisible entre a"

"a divideix b" o "a és un divisor de b" o "b és múltiple de a"

$6 \mid 6 \to 6 = 6 \cdot 1$ $1 \mid 0 \to 0 = 1 \cdot 0$ $1 \mid 33 \to 33 = 1 \cdot 33$

$\boxed{a \mid a}$ $\boxed{a \mid 0}$ $\boxed{1 \mid a}$

Obs: $0 \mid b$ NO es pot fer, nomes $0 \mid 0$, que això si és complex.

$\boxed{a \mid ab}$ $\boxed{a \mid b,\ b \mid c \Rightarrow a \mid c}$

$\exists q \in \mathbb{Z} : b = a \cdot q \to b \cdot s = aq \cdot s \to c = a \cdot q \cdot s$

$\exists s \in \mathbb{Z} : c = b \cdot s$ Llavors tenim $\overset{q \cdot s}{v}$ t.q. $c = a \cdot v$

$\boxed{a \mid b \Rightarrow ac \mid bc}$ $\boxed{\text{Si } c \neq 0\ \ ac \mid bc \Rightarrow a \mid b}$

$\boxed{a \mid b \Rightarrow a \mid bc}$ $\boxed{\text{No depén signe}}$

$\boxed{\text{Si } \neq 0,\ a \mid b \Rightarrow |a| \leq |b|}$ $\boxed{a \mid b,\ b \mid a \Rightarrow |a| = |b|}$

$\boxed{a \mid b,\ a \mid c \Rightarrow a \mid (ub + vc)}$ ← IMPORTANT

Demo: $a \mid b,\ a \mid c \Rightarrow a \mid ub + vc$

$a \mid b \wedge a \mid c \Rightarrow \exists q_1 : b = aq_1 \wedge \exists q_2 : c = aq_2 \Rightarrow \exists q_1 : bu = aq_1 u \wedge \exists q_2 : cv = aq_2 v \Rightarrow$

$\Rightarrow bu + cv = aq_1 v + aq_2 v \Rightarrow bu + cv = a(q_1 v + q_2 v) \Rightarrow [q_1 v + q_2 v \in \mathbb{Z}] \Rightarrow$

Per tant, $\exists$ un enter t.q. $bu + cv = a \cdot$ enter $\Rightarrow a \mid bv + cv$ com volíem :)

Demo: Si $b \neq 0,\ a \mid b \Rightarrow |a| \leq |b|$

Cas 1; $a = 0$: Impossible pq no hi ha cap nombre que $0 \cdot c = b$ i $b \neq 0$

Cas 2; $a \neq 0$: En aquest cas $a \mid b$ si és complex. $\exists c \in \mathbb{Z} : b = ac$

- $c = 0$: Impossible pq hem dit que $b \neq 0$ i no hi ha cap 'a' t.q. $b = a \cdot 0$ i $b \neq 0$.
- $c \neq 0$: Fins ara sabem que $b \neq 0$, $a \neq 0$ i $c \neq 0$.

  Agafem el valor absolut t.q. $|b| = |ac| \overset{\text{prop. v.l. absolut}}{\Rightarrow} |b| = |a| \cdot |c|$

  Com hem discutit $c \neq 0$ llavors $|c| \geq 1$.

  Donat que hem de mantindre que $|b| = |a| \cdot |c|$ no hi ha cap $|c|$ que faci que $|ac| \geq |b|$. llavors Sabem que $|a| \leq |b|$ Com volíem :)

$3 \mid 12 \Rightarrow 12 = 3 \cdot 4$ $(|a| = 3 \leq |b| = 12)$ $-3 \mid -9 \Rightarrow -9 = -3 \cdot 3$ $(|a| = 3 \leq |b| = 9)$

$-2 \mid 8 \Rightarrow 8 = -2 \cdot (-4)$ $(|a| = 2 \leq |b| = 8)$

Nombres Primers

$\boxed{p \text{ primer} \Leftrightarrow p \geq 2 \text{ i únics divisors positius de } p \text{ són } 1 \text{ i } p}$

1. Tot enter $n \geq 2$ és primer o producte de nombres primers. sqrt() # Busca for en C++
2. Tot enter $n \geq 2$ té algún divisor primer. Si $\underline{n}$ no primer, trobarem divisor abans $\sqrt{n}$
3. Hi ha infinits nombres primers.

Demo 2:

Si n no primer. $n = r \cdot s$ i $1 < r \leq s < n$

R.A: Suposem que r i s $> \sqrt{n}$ t.q $r > \sqrt{n}$ i $s \sqrt{n}$. Si multipliquem les dues preposicions $rs > n$ cosa falsa. Llavors $r \cdot s \leq \sqrt{n}$.

Podem continuar la demostració suposant que $r \leq \sqrt{n}$. Si r és prim doncs ja està.

Si r no és prim significa que $\underline{r}$ es pot descomposar en prims.

Sigui $\underline{p}$ el menor prim en la factorització de $\underline{r}$.

Tenim que p/r i $r/n \Rightarrow p/n$ i $p \leq r \leq \sqrt{n} \Rightarrow p \leq \sqrt{n}$:)

Demo 3:

Farem la demo mitjançant R.A:

Partim de que els núm. primers són finits fins arribar contradicció.

Anomenarem P a l'últim nombre primer (Donat que suposem finits).

Anomenarem N a la multiplicació de tots els nombres primers t.q $N = 2 \cdot 3 \cdot \ldots \cdot P$

Anomenarem M a $N+1$. # $M > P$

Ara em preguntem qui divideix M

Llavors tenim: $2|N$, $3|N$, $5|N$, ...

Però significa que pròxim N divisible per 2 serà $N+2$, divisible entre 3 serà $N+3$, ...

Llavors veiem que cap primer divideix a $\overset{\to N+1}{M}$, això implica (per def de primer) que M és primer. Això és contradicció pq suposàvem que eren finits i P era l'últim.

Com que fèiem R.A. Demostro cert l'enunciat. :)

Màxim Comú Divisor

El mcd dels nombres $\overbrace{a_1, a_2, \dots, a_n}^{\in \mathbb{Z}}$ és el divisor més gran dels divisors comuns.

⚠ Això passa si algun d'aquests no és 0.

Llavors tenim que $\exists d \in \mathbb{Z} : d | a_1, d | a_2, \dots, d | a_n$

Nota 1: Si algun $a_i \neq 0$ aleshores $d | a_i \Rightarrow |d| \leq |a_i|$ en particular $d \leq |a_i|$

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

Si algun $a_i \neq 0$ el $\text{mcd}(a_1, a_2, \dots, a_n)$ és l'únic enter d que verifica les dues prop.:

- $d | a_i$ per cada i # Comú divisor
- Si $d' | d$ per cada $i \Rightarrow d' \leq d$

Formalitza la idea del "màxim".

Obs: $\text{mcd}(a_1, a_2, \dots, a_n) \geq 0$. Pq si tenim $\overset{\in \mathbb{Z}}{\text{divisor}} < 0$ aleshores $|q|$ també és divisor i tenim que $q \leq |q|$.

Per divisibilitat NO importa el signe.

Obs: $\text{mcd}(a_1, a_2, \dots, a_n) = 0 \Leftrightarrow a_1 = a_2 = \dots = a_n = 0$. Pq si hi ha algun $a_i \neq 0$ llavors tenim que $1 | a_i \; \forall i$ llavors el $\text{mcd}(a_1, a_2, \dots, a_n) \geq 1$.

Si $a | b \Rightarrow \text{mcd}(a, b) = |a|$ $\quad$ $\text{mcd}(a, 0) = |a|$ $\quad$ mcd no depèn signe

Si p primer i no divideix $b \Rightarrow \text{mcd}(p, b) = 1$ $\quad$ $\text{mcd}(a, b) = \text{mcd}(a + ub, b)$

Demo: Si $a | b \Rightarrow \text{mcd}(a, b) = |a|$

- Si $a = 0$ aleshores si sabem (per hipòtesi) que $a | b \Rightarrow b = 0 \cdot c \Rightarrow b = 0$

Llavors $\text{mcd}(0, 0) = 0$

- Si $a \neq 0$ sabem que $a | b$ (per hipò.) i $a | a$ (per propietat) $\Rightarrow |a|$ és un divisor comú $\Rightarrow |a| \leq d = \text{mcd}(a, b)$

Però també sabem que $\overset{d = \text{mcd} \,;\, a \neq 0}{d | a} \Rightarrow |d| \leq |a|$

Llavors tenim que $|a| \leq d$ i $|d| \leq |a| \Rightarrow d = a$

$\boxed{\text{mcd}(a, b) = \text{mcd}(b, a - b) = \text{mcd}(b, a - 2b)}$

Demo: $mcd(a,b) = mcd(a+ub, b)$

Partim de que $d_1 = mcd(a,b)$ t.q $d_1 | a \Leftrightarrow \exists p : a = d_1 \cdot p$
$d_1 | b \Leftrightarrow \exists q : b = d_1 \cdot q$

$d_2 = mcd(a+ub, b)$ t.q $d_2 | a+ub \Leftrightarrow \exists r : a+ub = d_2 \cdot r$
$d_2 | b \Leftrightarrow \exists s : b = d_2 \cdot s$

Llavors podem fer sub de a i b en $a+ub$ t.q $\overset{a}{(d_1 p)} \overset{+}{+} \overset{u}{u} \overset{b}{(d_1 q)} = d_1(p+uq)$
donat que "$p+uq$" són $\mathbb{Z}$, d_1 divideix $a+ub$ i també a b t.q
$d_1 \leq mcd(a+ub, b)$.

Ara fem la segona part on $d_2 = mcd(a+ub, b)$. Llavors faig sub de $b \to a+ub$ t.q.
$a + ub = a + u(d_2 s) = d_2 \cdot r \Rightarrow a = d_2 \cdot r - ud_2 s \Rightarrow a = d_2(r-us)$.
Donat que $r-us$ és enter, d_2 divideix a i també a b t.q $d_2 \leq mcd(a,b)$.

Per acabar tenim $d_1 = mcd(a,b)$ i $d_1 \leq mcd(a+ub, b)$
$d_2 = mcd(a+ub, b)$ i $d_2 \leq mcd(a,b)$

Fem un sandwich i tenim que $mcd(a,b) = mcd(a+ub, b)$ Com volíem ◡̈

$\boxed{a \text{ i } b \text{ són primers entre si} \Leftrightarrow mcd(a,b) = 1}$ # No tenen factors en comú.

Obs: a i b són primers entre si $\Leftrightarrow$ No tenen cap divisor primer comú.

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

$\Rightarrow$| Demo per contrarecíproc: Suposem que a i b tenen divisor primer comú $\Rightarrow mcd(a,b) \neq 1$.
Si a i b són divisibles per primer comú $\Rightarrow \exists p \geq 2 : p | a$ i $p | b \Rightarrow mcd(a,b) \geq p \geq 2$
$\Rightarrow mcd(a,b) \geq 2$ ☑

$\Leftarrow$| Demo per contrarecíproc: Suposem $mcd(a,b) \neq 1 \Rightarrow$ Trobem divisor primer comú.
Cas 1: $mcd(a,b) = 0 \Rightarrow a = b = 0 \Rightarrow$ qualsevol primer $| 0 \Rightarrow$ Tenim div. primer comú.
Cas 2: $mcd(a,b) = d \Rightarrow \exists$ primer $(p \geq 2)$ t.q. $p | d$. (Donat que d té descomp. en nombres primers, llavors "p" és un d'aquest)
Ara tenim que $p | d$ i $d | a \Rightarrow p | a$
$p | d$ i $d | b \Rightarrow p | b$
p és primer i divisor comú

Per tant ja hem arribat on volíem ◡̈

Divisió Euclidiana

Donats $a, b \in \mathbb{Z}$ amb $b \neq 0$ $\exists$ únics q, r t.q. $\boxed{\begin{matrix} a = bq + r \\ 0 \leq r < |b| \end{matrix}}$

q: Quocient ; r: Residu.

Demo: $a = bq + r \wedge 0 \leq r < |b|$

Considerem el conjunt $S = \{a - bx \mid x \in \mathbb{Z},\ a - bx \geq 0\}$

Però abans de continuar hem de veure que aquest S no és buit.

Cas 1; $b > 0$:

En aquest cas direm que $x = 0$. t.q $a - b \cdot (0) \geq 0$. Podem veure que és complex llavors $a \in S$. # En aquest cas no és buit.

Cas 2; $b < 0$: Busquem un x negatiu donat que b és negatiu per complir $a - bx \geq 0$

En aquest cas volem trobar un $-bx \geq a$ per demostrar que $S \neq \emptyset$.

$$-bx \geq a \overset{\text{div } \frac{1}{-b}}{\Longrightarrow} \frac{1}{-b} \cdot (-b)x \leq \frac{a}{-b} \overset{\text{opera}}{\Longrightarrow} x \leq \frac{a}{-b}$$

Quan divideixes entre negatiu has de canviar desigualtat.

Ara tenim que $\frac{a}{-b} \in \mathbb{R}$ podem agafar la part entera d'aquest i convertir-lo a $\mathbb{Z}$.

Si diem que $x = \lfloor \frac{a}{-b} \rfloor$ estem assegurant que $-bx \geq a$ i S té com a mínim un element. $S \neq \emptyset$ ☑

Donat que S no està buit, direm que $r = \overbrace{\min(S)}^{\text{Element més petit}}$ i direm que $q = x$.

Llavors tenim que $r = a - bq \Rightarrow a = bq + r$. Però hem de demo que $0 \leq r < |b|$

Farem demo per Contradicció: $r \geq b$.

$r = a - bq \geq b \Rightarrow r - b = a - bq - b \geq b - b \Rightarrow r - b = a - b(q+1) \geq 0$

Però això sig. que $r - b$ és un element de S (donat que $= a - b(q+1)$) i $r - b < r$, però havíem dit que $r = \min(S)$ generant contradicció. $0 \leq r < |b|$ ☑

Per acabar, hem de demostrar la unicitat de q i r.

Suposem que q, q' i r, r' t.q. $a = bq + r = bq' + r' \Rightarrow bq - bq' = r' - r \Rightarrow$

$\Rightarrow \underbrace{b(q - q')}_{LHS} = \underbrace{r' - r}_{RHS}$. LHS = Multiple de b.

$RHS = 0 \leq r' - r < |b|$ (Donat que $\begin{matrix} 0 \leq r < |b| \\ 0 \leq r' < |b| \end{matrix}$

Llavors tenim que $\begin{matrix} r' - r \text{ mai arriba a } |b| \\ b(q - q') \text{ serà } \underline{b} \text{ o més gran.} \end{matrix}$ $\Big\{$ L'única forma de fer $LHS = RHS$ és si $0 = 0$. $\Rightarrow$

$\Rightarrow r' - r = 0 \Rightarrow r' = r$

$\Rightarrow b(q - q') = 0 \Rightarrow q = q'$

Identitat de Bézout.

Donats $a, b \in \mathbb{Z}$ qualsevols, $\exists\, x, y \in \mathbb{Z}$ t.q. $\boxed{mcd(a,b) = ax + by}$

Obs: Aquest parell x, y no és únic.

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

Lema de Gauss

$$\boxed{\text{Si } a \mid bc \text{ i } mcd(a,b) = 1 \Rightarrow a \mid c}$$

Lema d'Euclides

$\boxed{\text{Si } p \text{ primer i } p \mid bc \Rightarrow p \mid b \text{ o } p \mid c}$ # Si p no primer, no té pq passar.

Si p primer i $p \mid b_1 b_2 \cdots b_n \Rightarrow p \mid b_1$ o $p \mid b_2 \cdots p \mid b_n$.

Dem: Lema de Gauss

Com que $mcd(a,b) = 1$, per Bézout sabem $ax + by = mcd(a,b) = 1$.

$\exists s: bc = as$

$ax + by = 1 \xRightarrow{\text{Multi} \times c} axc + byc = c \xRightarrow{\text{Resum}} c = a(xc) + \overbrace{bc}(y) \Rightarrow c = a(xc) + as(y) \Rightarrow$

$\Rightarrow c = a(\overbrace{xc + y}^{\in \mathbb{Z}}) \Rightarrow a \mid c$ ☺

Dem: Lema d'Euclides

Cas 1; $p \mid b$: Ja ho tenim per tant suposem que $p \nmid b$ i veiem que $\Rightarrow p \mid c$.

Cas 2; $p \nmid b$: Com que $p \nmid b$ (Per hipòt.) llavors $mcd(p, b) = 1$.

Llavors apliquem el lema de Gauss.

Tenim que $p \mid bc$ i $mcd(p, b) = 1 \Rightarrow p \mid c$ ☺

Demo: Unicitat descomposició en factors primers.

"Tot enter $n \geq 2$ té descomposició única t.q. $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$ on p_i primer i $e_k > 0$"

Ja hem fet prèviament la demostració de que n té descomposició en primers.

Ara volem veure que aquesta és única i ho farem per contradicció.

Suposem que hi ha 2 descomposicions $\Rightarrow$??.

$$\left.\begin{array}{l} n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \\ n = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r} \end{array}\right\} \Rightarrow \text{Volem veure que } k = r \text{ i } p_1 = q_1,\ p_2 = q_2, \ldots, p_k = q_r$$

Tenim que $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}$. p primer i $p \mid bc \Rightarrow p \mid b$ o $p \mid c$.

Podem veure que $\overbrace{p_i \mid q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}}^{p_i(p_2 \cdots p_k) = q_1 q_2 \cdots q_r}$ per tot i. Llavors pel $\overbrace{\text{Lema d'Euclides}}$ $p_i \mid q_j^{b_j}$ per algún j.

Donat que p i q són primers si $p_i \mid q_j \Rightarrow p_i = q_j$

Això també passa al revés $q_i \mid p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \Rightarrow q_i \mid p_j \Rightarrow q_i = p_j$

Llavors podem veure que $k = r$ i $p_i = q_j$ per algun j.

Ara podem reescriure l'anterior t.q. $p_i = q_i \Rightarrow p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = p_1^{b_1} \cdot p_2^{b_2} \cdots p_k^{b_k}$ i ens falta demostrar que $\forall i\ a_i = b_i$:

Cas 1; $a_i = b_i$: Ja està hem acabat donat que si són el mateix dons fin.

Cas 2; $a_i \neq b_i$: Sense perdre rigor podem dir que $a_i > b_i$ (Hi ha més dels a RHS)

Llavors podem dividir les dues bandes de la igualtat entre p^{b_1} t.q:

$p_1^{a_1 - b_1} \cdot p_2^{a_2} \cdots p_k^{a_k} = p_2^{b_2} \cdots p_k^{b_k}$.

En RHS en sent $p_1^{a_1 - b_1}$ (on $a_1 - b_1 > 0$) i segueix sent divisible entre p_1.

En LHS ja no tenim p_1 fent que no sigui divisible entre p_1.

Això és una contradicció pq si són iguals, tots dos haurien de ser divisibles per els mateixos elements.

Això implica que $a_i = b_i$ pq no passi.

Ja hem demostrat que la descomposició en factors primers és única. ☺

Càlcul del mcd a partir de la factorització i conseqüències

Suposem $a = \varepsilon_1 \cdot p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$ i $b = \varepsilon_4 \cdot p_1^{f_1} \cdot p_2^{f_2} \cdots p_k^{f_k}$, $e_i, f_i \geq 0$ i $\varepsilon_i = \pm 1$.

I. $a | b \Leftrightarrow e_i \leq f_i$ per cada i.

Podem dir que en tots dos casos és 'k' pq podem afegir $p^0 = 1$ fins que siguin iguals.

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

III. Fórmula del mcd només val agafant el mínim dels exponents.

IV. Els divisors positius de a són tots de la forma $p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k}$ amb $0 \leq g_i \leq e_i$.

El nombre de divisors és $(e_1+1)(e_2+1)\cdots(e_k+1)$.

Demo: $a|b \Leftrightarrow e_i \leq f_i$ per cada i

$\Rightarrow$|

Si $a|b \overset{def}{\Leftrightarrow} b = a d$. Donat que tots els nombres tenen descomposició única en factors primers, podem reescriure t.q. $\varepsilon_2 \cdot p_1^{f_1} \cdot p_2^{f_2} \cdots p_k^{f_k} = (\varepsilon_1 p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k})(\varepsilon_3 p_1^{g_1} \cdot p_2^{g_2} \cdots p_k^{g_k})$.

Simplifiquem expressió com $\varepsilon_2 p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} = \varepsilon_1 \varepsilon_3 \, p_1^{e_1+g_1} \cdot p_2^{e_2+g_2} \cdots p_k^{e_k+g_k}$

Donat que b es pot reputar com a multiplicat per algun altre factor, implica que els exponents de la factorització ~~no~~ poden ser superiors als de b: $\forall i\ f_i = e_i + g_i$.

Donat que $g_i \geq 0$ (Si $g_i = 0$ seria el mateix d pq $x^0 = 1$) tenim que $f_i \geq e_i$. ☑

$\Leftarrow$| Suposem: Per cada p_i de la factorització de a i b $f_i \geq e_i$.

$a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$; f_i es pot reescriure com $f_i = e_i + (f_i - e_i)$

$b = p_1^{f_1} \cdot p_2^{f_2} \cdots p_k^{f_k}$; Llavors definim $d = p_1^{f_1 - e_1} \cdot p_2^{f_2 - e_2} \cdots p_k^{f_k - e_k}$

Ara podem veure que $b = a d$ donat que ens queda així:

$$\underbrace{(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k})}_{a} \cdot \underbrace{(p_1^{f_1-e_1} \cdot p_2^{f_2-e_2} \cdots p_k^{f_k-e_k})}_{d} = \underbrace{p_1^{e_1+f_1-e_1} \cdot p_2^{e_2+f_2-e_2} \cdots p_k^{e_k+f_k-e_k}}_{b}$$

Per definició de divisibilitat $b = ad \Leftrightarrow a | b$ ☑

Queda demostrat cert que $a|b \Leftrightarrow f_i \geq e_i$:)

Demo: $\text{mcd}(a,b) = p_1^{\min(e_1,f_1)} \cdot p_2^{\min(e_2,f_2)} \cdots p_k^{\min(e_k,f_k)}$

Això és així pq el mcd és el nombre més gran que divideix a tots dos nombres.

Si agafessim l'exponent més gran, el mcd dividiria al que té l'exponent gran, però no al petit. $d = p_1^{g_1} \cdot p_2^{g_2} \cdots p_k^{g_k}$ on $g_i \leq e_i$ i $g_i \leq f_i$ Com hem vist en I.

Demo: Divisors positius de a son tots de la forma $p_1^{g_1} \cdot p_2^{g_2} \cdots p_k^{g_k}$ amb $0 \leq g_i \leq e_i$

El nombre de divisors és $(e_1+1)(e_2+1)\cdots(e_k+1)$

Aquí estem dient que si $p_i^{e_i}$ està en la descomposició de $\underline{a}$, aquest exponent e_i és el nombre màxim, fent que el mateix primer elevat a un nombre inferior $i \geq 0$ continuarà sent divisor de $\underline{a}$.

Donat que comencem a comptar a partir de 1, fem '+1' i sumem el $e_i = 0$ donat que '1' és divisor de tots els nombres.

Altres propietats del mcd

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

II. Associativa del mcd: # Surt de l'associativa del min(). $min(a,b,c) = min(a, min(b,c))$

$$\boxed{mcd(mcd(a,b), c) = mcd(a, mcd(b,c)) = mcd(a,b,c)}$$

III. $mcd(ac, bc) = |c|\, mcd(a,b)$

IV. Si $d = mcd(a,b) \neq 0 \Rightarrow mcd(a/d, b/d) = 1$.

V. Propietats anteriors valen per 3 o més enters.

Demo: Tot divisor comú de a, b divideix mcd(a,b).

$a = \varepsilon_1 p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ | Hem demostrat prèviament que: $mcd(a,b) = p_1^{min(e_1,f_1)} \cdots p_k^{min(e_k,f_k)}$

$b = \varepsilon_2 p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ | $g_i \leq e_i$ i $g_i \leq f_i$ pertot i

$d = \varepsilon_3 p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k}$ | Llavors podem fer la demostració t.q:

$d|a$ i $d|b \Leftrightarrow g_i \leq e_i$ i $g_i \leq f_i \Leftrightarrow g_i \leq min(e_i, f_i) \Leftrightarrow d \mid mcd(a,b)$.

Demo: $d = mcd(a,b) \neq 0 \Rightarrow mcd(a/d, b/d) = 1$

Partim de que la prop. III és certa ($min(g_i+e_i, g_i+f_i) = g_i + min(e_i + f_i)$).

Suposem que $c = mcd(a,b)$ i apliquem prop. III. # Donat que $c \neq 0$.

$c = mcd(a,b) = mcd(c \cdot \frac{a}{c}, c \cdot \frac{b}{c}) = |c| \cdot mcd(\frac{a}{c}, \frac{b}{c}) = c \Rightarrow \frac{c}{|c|} = mcd(\frac{a}{c}, \frac{b}{c}) = 1$.

Nota: Es pot calcular el $mcd(a_1, a_2, \ldots, a_n)$ fent ús de l'associativa i fent algoritme d'euclides en cada cas.

Equacions diofantiques

Equacions amb coeficients enters de les quals busquem solucions enteres.

Ens centrarem amb $ax+by=c$ | $d=\text{mcd}(a,b)$ i $d\neq 0$. (a o b no son 0)

1. Determinar que ∃ una solució

té sol.

$\boxed{ax+by=c \Leftrightarrow d \mid c}$ Això és així pq. $d \mid a \wedge d \mid b \Rightarrow d \mid (ax+by) \Rightarrow d \mid c$

2. Utilitzar Algoritme d'Euclides Estès

Donat que ∃ una sol. fem ús de l'algoritme per trobar $\text{mcd}(a,b)$, x_0 i y_0 t.q.

$ax_0+by_0=\text{mcd}(a,b)$.

3. Solucions generals

Suposem que ja hem trobat una solució (x_0,y_0). Hem de veure si ∃ (x,y) que també sigui sol.

$ax+by=ax_0+by_0$ [Punt inicial]

$a(x-x_0)=b(y_0-y)$ [Reescriure]

$\frac{a}{d}(x-x_0)=\frac{b}{d}(y_0-y)$ [Dividir entre d]

$\underbrace{\frac{a}{d}}_{a}\underbrace{(x-x_0)}_{x}$

Fem ús de la propietat IV i Lema de Gauss t.q. si $\text{mcd}(a,b)=d \Rightarrow \underline{\text{mcd}(\frac{a}{d},\frac{b}{d})=1}$ Prop IV

Llavors podem veure que $\frac{a}{d}$ divideix $\frac{b}{d}(y_0-y)$. Però pel Lema de Gauss tenim que:

Si $a \mid bc$ i $\text{mcd}(a,b)=1 \Rightarrow a \mid c$. Així que podem veure-ho com $\underbrace{\frac{a}{d}}_{a}\underbrace{(x-x_0)}_{x}=\underbrace{\frac{b}{d}}_{b}\underbrace{(y_0-y)}_{c}$

Podem dir que $\frac{a}{d}$ divideix (y_0-y) és a dir $\overbrace{y_0-y}^{b}=\overbrace{\frac{a}{d}}^{a}\cdot\overbrace{t}^{k}$

Fem substitució a l'equació t.q. $\frac{a}{d}(x-x_0)=\frac{b}{d}(\frac{a}{d}\cdot t)$

Podem simplificar-ho. $x-x_0=\frac{b}{d}\cdot t \Rightarrow x=\frac{b}{d}t+x_0$

Després faríem el recíproc per trobar y.

Si x_0, y_0 és solució de $ax+by=c$, totes les solucions són de forma:

$$\boxed{x=x_0+\frac{b}{d}t \quad , \quad y=y_0-\frac{a}{d}t \quad \text{per cert } t\in\mathbb{Z}}$$

4. Verificació de Solucions

x_0, y_0 son sol. particulars.

• Totes les solucions de l'equació han de poder ser expressades t.q. $\boxed{\begin{array}{l} x=x_0+\lambda t \\ y=y_0+\mu t \end{array}}$

• λ i μ han de ser primers entre si. Això assegura no trobar solucions repetides per dif. valors de K

λ i μ es troben solucionant l'equació. λ i μ no han de per què

K paràmetre variable per generar totes les solucions. ser $\frac{a}{d}$ i $\frac{b}{d}$ respectivament. Pot variar.

Mínim Comú Múltiple

Nombre més petit dels múltiples positius comuns. Si algun $a_i = 0 \Rightarrow mcm = 0$.

- Si algun $a_i = 0$, $mcm(a_1, a_2, \dots, a_n) = 0$
- Si tots els $a_i \neq 0$, el $mcm(a_1, a_2, \dots, a_n)$ és l'únic enter m que verifica:
  - $m > 0$ i $a_i | m$ per cada i
  - Si $m' > 0$ i $a_i | m'$ per cada $i \Rightarrow m \leq m'$

I. Si $a|b \Rightarrow mcm(a,b) = |b|$

II. No depen de signe: $mcm(a,b) = mcm(a,-b) = mcm(-a,b) = mcm(-a,-b)$

Demo: $a|b \Rightarrow mcm(a,b) = |b|$

Hipòtesi: $a|b \Leftrightarrow \exists k \in \mathbb{Z}: b = ak$

Demo per Contradicció: Suposem: $m = mcm(a,b)$ i $m < b$.

Si $m = mcm(a,b) \overset{def}{\Leftrightarrow} a|m$ i $b|m \overset{Hip}{\Rightarrow} a|m$ i $a|b$ i $b|m \overset{\text{trans.}\ T_1 T \Rightarrow T}{\Rightarrow} a|m$

Llavors tenim que $a|m \Leftrightarrow \exists t \in \mathbb{Z}: m = at$

$a|b \Leftrightarrow \exists k \in \mathbb{Z}: b = ak$

Donat que $m < b \Rightarrow at < ak \Rightarrow t < k$.

Però veiem que això no és possible donat que k és el valor que fa que a sigui igual a b ($b = ak$). Si $t < k \Rightarrow at < b$ i això faria que $b \nmid m$ donat que un nombre no pot dividir a un altre més petit. Es per això que no compliria la def. de $mcm(a,b) \Leftrightarrow a | mcm(a,b)$ i $b | mcm(a,b)$.

Arribem a la conclusió que m no pot ser més petit, llavors el "següent" valor és b i compliria la def donat que $b|b$.

Hem demostrat que si $a|b \Rightarrow mcm(a,b) = b$:)

Càlcul del mcm a partir de factorització

Si expressem $a = \varepsilon_1 p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$ i $b = \varepsilon_2\, p_1^{f_1} \cdot p_2^{f_2} \cdots p_k^{f_k}$ amb $e_i, f_i \geq 0$ $\quad \varepsilon_i = \pm 1$, p_i primer

$$\boxed{mcm(a,b) = p_1^{\max(e_1,f_1)} \cdot p_2^{\max(e_2,f_2)} \cdots p_k^{\max(e_k,f_k)}}$$

Demo:

Aquesta demo és similar al del mcd, però aquest cas ha de ser el màxim donat que un nombre no pot dividir a un altre més petit, llavors si agafem el max, pot passar que un nombre divideixi a ell mateix o a un més gran.

No és demostració rigurosa però es podria fer a partir de Prop. II del mcd amb fact i demo del mcm.

Propietats del mcm

I. $\boxed{mcd(a,b) * mcm(a,b) = |ab|}$ Càlcul eficient del mcm.

II. Tot múltiple comú de a, b és múltiple de mcm(a,b). De fet:

$$\boxed{a|c \text{ i } b|c \Leftrightarrow mcm(a,b)|c}$$

III. $mcm(mcm(a,b),c) = mcm(a, mcm(b,c)) = mcm(a,b,c)$

IV. Prop II i III valen amb més enters, però I NO $\begin{cases} mcm(2,2,1) = 2; \\ mcd(2,2,1) = 1; \\ mcd * mcm = 2 \\ 2 \times 2 \times 1 = 4 \quad \times \end{cases}$

Demo: $mcd(a,b) * mcm(a,b) = |ab|$

Partim de que $a \neq 0$ i $b \neq 0$ i $a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$ i $b = p_1^{f_1} \cdot p_2^{f_2} \cdots p_k^{f_k}$

Sabem per demostracions anteriors que:

$mcm(a,b) = p_1^{\max(e_1,f_1)} \cdot p_2^{\max(e_2,f_2)} \cdots p_k^{\max(e_k,f_k)}$

$mcd(a,b) = p_1^{\min(e_1,f_1)} \cdot p_2^{\min(e_2,f_2)} \cdots p_k^{\min(e_k,f_k)}$

Llavors $mcd(a,b) * mcm(a,b) = p_1^{\max(e_1,f_1)+\min(e_1,f_1)} \cdots p_k^{\max(e_k,f_k)+\min(e_k,f_k)} =$

$$= p_1^{e_1+f_1} \cdots p_k^{e_k+f_k} = \left[p_1^{e_1} \cdots p_k^{e_k}\right] * \left[p_1^{f_1} \cdots p_k^{f_k}\right] =$$
$$= |ab|$$

Queda demostrat que $mcm(a,b) * mcd(a,b) = |ab|$.

Demo: $a|c$ i $b|c \Leftrightarrow mcm(a,b)|c$

$\Rightarrow$) $\left.\begin{array}{l} a|c \text{ i } b|c \Leftrightarrow c = mcm(a,b) \\ c|c \text{ [Cosa certa]} \end{array}\right\} \Rightarrow mcm(a,b)|c$ ☑

$\Leftarrow$) $\left.\begin{array}{l} mcm(a,b) = m \Rightarrow a|m \text{ i } b|m \\ mcm(a,b)|c \end{array}\right\} \begin{array}{l} m|c \text{ i } a|m \text{ i } a|b \text{ i } m|c \text{ // Transitivitat } [T = T \wedge T] \\ a|c \text{ i } a|b \text{ ☑} \end{array}$

(2). $a|a+b$ volem veure que $a|b$

Tenim:

$a|a$ per la prop. reflexiva

$a|\underset{c}{a+b}$ per hipòtesi

Volem: $a|b$

$\Rightarrow a|$ qualsevol comb. lineal ⊛ Mètode Alternatiu

en particular $a|(a+b)-a \Leftrightarrow a|b$.

$a|(-1\cdot a)+(1\cdot(a+b))$

⊛ $a|a+b \Leftrightarrow \exists k: a+b=ak \Rightarrow \exists k: b=ak-a \Rightarrow \exists k: \overset{v\cdot b}{b}=\overset{+ u\cdot c}{a(-1+k)} \Rightarrow a|b$

(5). Demo. que úniques sol. $xy=x+y$ son $x=y=0$ i $x=y=2$.

Pista: Proveu que x, y es divideixen mutuament i feu $\underline{XI}$

Tenim:

$x|x \Rightarrow x|x$

$x|xy \Rightarrow$ Com que $xy=x+y \Rightarrow x|x+y$

$x|$ qualsevol com. lineal entera, en particular $x|x+y-x \Rightarrow x|y$.

El mateix q. amb y.

Tenim:

$y|y \Rightarrow y|y$

$y|xy \Rightarrow y|x+y$

$y|x+y-y \Rightarrow y|x$

Llavors tenim que $x|y$ i $y|x$ llavors per la prop $\underline{XI}$ tenim que $|x|=|y|$

Cas 1; $x=y$:

$xy=x+y \Rightarrow y^2=y+y \Rightarrow y^2=2y \Rightarrow y=2=x$ Pq per hipòtesi $x=y$.

Cas 2; $x=-y$:

$xy=x+y \Rightarrow -y\cdot y=-y+y \Rightarrow -y^2=0 \Rightarrow y=0=x$

(10). $a|(b-1)$ i $a|(c-1) \Rightarrow a|bc-1$

Suposem:

$a|(b-1) \Leftrightarrow \exists \overset{\in\mathbb{Z}}{k}: b-1=ak \Rightarrow \exists k: b=ak+1$

$a|(c-1) \Leftrightarrow \exists \overset{\in\mathbb{Z}}{p}: c-1=ap \Rightarrow \exists p: c=ap+1$

$bc=(ak+1)\cdot(ap+1)$ [Multi]

$bc=a^2kp+ak+ap+1$ [Distrib]

$bc=a(akp+k+p)+1$ [Factor comú]

Donat que a, k, p són enters, el resultat de "$akp+k+p$" continuarà sent un enter,

és per això que $\exists r \div \overset{\in\mathbb{Z}}{r}=akp+k+p$ t.q. $bc=ar+1 \Rightarrow bc-1=ar \Leftrightarrow a|(bc-1)$

Llavors tenim que "$bc-1$" és una combinació lineal de $a\,(akp+k+p)$. ✓

⑥. (Difícil). Si $b^2=ac \Rightarrow (a+b+c) \mid (a^2+b^2+c^2)$

Suposem: $b^2=ac$

Volem demo: $\exists k \in \mathbb{Z}: a^2+b^2+c^2=(a+b+c)\cdot k$

Partim de veure que significa $a^2+b^2+c^2$, primerament veiem que podria ser $(a+b+c)^2$ però no és així pq. $(a+b+c)^2=a^2+b^2+c^2+2ab+2ac+2bc$.

Però el resultat el podem reescriure t.q. $a^2+b^2+c^2=(a+b+c)^2-2ac-2bc-2ba$

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

$\Downarrow$ Aplica Hipòtesi.

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

Ara veiem que podem fer factor comú de b t.q. $a^2+b^2+c^2=(a+b+c)^2-2b(b+a+c)$

I ens resulta a una altre possible factor comú t.q. $a^2+b^2+c^2=(a+b+c)((a+b+c)-2b)$

Donat que $a+b+c$ enters, el resultat continua sent un enter t.q $\exists k: a^2+b^2+c^2=(a+b+c)\cdot k$

Això és el que buscàvem així que queda demo. ☺.

㉙. Calc $mcd(a,b)$ en següents cassos.

a) $b=ac$ $\quad mcd(a,ac)$

Tenim $d=mcd(a,ac) \Leftrightarrow d \mid a$ i $d \mid ac$.

Per la propietat de divisibilitat que diu si $a \mid b \Rightarrow a \mid bc$.

Com que $a \mid a \Rightarrow a \mid ac$ i a serà el màxim comú divisor fent que $\boxed{mcd(a,ac)=|a|}$ ✓

b) $b=a^n$ $(n \geq 1)$

Tenim $d=mcd(a,a^n) \Rightarrow d \mid a$ i $d \mid a^n$

Sabem que $a \mid a$ i que a^n esta format per alguns una a, llavors un divisor de a segur serà divisor de a^n (pq esta format per a's). Llavors tenim que $\boxed{mcd(a,a^n)=|a|}$ ✓

c) b és primer.

Tots els nombres són $\begin{cases} \to \text{primers} \\ \to \text{Descomp. en primers} \end{cases}$ • Per def, els nombres primers només tenen de divisor $\begin{cases} \to \text{ell} \\ \to 1 \end{cases}$. Per saber el mcd de a, b podem passar dues coses:

$b|a$:

Si $b|a \Leftrightarrow \exists k: a = b \cdot k$. Pq. això es compleixi ($k = 1$ i b = primer)

Llavors donat que 1 no és primer, el divisor més gran serà b.

Això seg. que $b|b$ i $b|a \Rightarrow \boxed{mcd(a,b) = b}$

$b \nmid a$:

Ara $\nexists k: a = b \cdot k$. Llavors, l'únic nombre que divideix a a i b és el 1.

$\boxed{mcd(a,b) = 1}$ ✓

d) $b = 2a - 1$.

El $mcd(a, 2a-1)$ significa que d divideix a a i a $2a-1$.

$d|a \Leftrightarrow \exists k: a = d \cdot k$ [def de |]

prop. divis. 2. l.l.c.f.
$d|a \Rightarrow d|2a$

Llavors substituïm en $2a-1$ t.q. $2a-1 = 2dk-1$.

Sabem que $d|a$ i $d|2a-1$, llavors d tmb divideix a $2a-(2a-1)$ t.q.

→ si $d|a$ i $d|b$ llavors $d|a-b$

$2dk - (2dk-1) = 2dk - 2dk + 1 = +1$

Llavors veiem que $d|1$ (on 1 és el resultat de fer "a-b")

Els únics nombres que divideixen 1 són ± 1. i el més gran d'aquest és el 1

Concloïm que $\boxed{mcd(a, 2a-1) = 1}$ ✓

(33). Demo que $mcd(2k+9, 3k+15) = 3$ si $3|k$, 1 altrament.

Cas 1: $3|k$:

$\exists q: k = 3q \Rightarrow mcd(2 \cdot 3 \cdot q + 9, 3 \cdot 3 \cdot q + 15)$.

Podem veure que 9 i 15 tmb múltiples de 3 t.q. $mcd(2 \cdot 3 \cdot q + 3 \cdot 3, 3 \cdot 3 \cdot q + 3 \cdot 5)$

Considerem $a = 2 \cdot 3 \cdot q + 3 \cdot 3$, $b = 3 \cdot 3 \cdot q + 3 \cdot 5$ i podem reescriure $a = 3(2 \cdot q + 3)$, $b = 3(3q + 5)$

Ara veiem que $3|a$ i $3|b$, llavors podem dir que $mcd(a,b) = 3$

Confirmant que si $3|k \Rightarrow \boxed{mcd(2k+9, 3k+15) = 3}$ ☑.

Cas 2 ; $3 \nmid k$:

d'aquesta expressions lineals

Ara que $3 \nmid k$, fem ús de l'algoritme d'Euclides per trobar mcd. (*)

$(3k+15)-(2k+9) = k+6$

$(2k+9)-(k+6) = k+3$

$(k+6)-(k+3) = 3$

Veiem que el mcd és 3, però ja hem dit que, en aquest cas 3 no pot ser. Per tant, el mcd haurà de ser 1. (Expressions mai valdran '0').

$\boxed{mcd(2k+9, 3k+15) = 1}$

Queda demostrat enunciat :).

(18). Calc $mcd(a^2-1, a^3-1)$.

~~Fem divisió euclidiana.~~

$$a^3+0+0-1 \;\big\lfloor\; a^2-1$$
$$\underline{-a^3 \quad +a} \qquad a$$
$$+a-1$$

~~Llavors $a^3-1 = a(a^2-1)+a-1$.~~

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

~~$= mcd(a^2-1, a-1)$.~~

~~Tornem a fer div:~~

$$a^2+0-1 \;\big\lfloor\; a-1$$
$$\underline{-a^2+a} \qquad a+1$$
$$a-1$$
$$\underline{-a+1}$$
$$0$$

~~Llavors $a^2-1 = (a-1)(a+1)$~~

~~$mcd((a-1)(a+1), a-1) = |a-1|$~~

~~$\square$ [illegible]~~

(18). Calc $mcd(a^2-1, a^3-1)$

Per resoldre aquest problema farem algoritme d'euclides.

$$a^3+0+0-1 \;\big\lfloor\; a^2-1$$
$$\underline{-a \quad +a} \qquad a$$
$$/ \quad +a-1$$

$a^3-1 = a(a^2-1)+a-1$ però no hem acabat donat que el residu no és 0.

$$a^2+0-1 \;\big\lfloor\; a-1$$
$$\underline{-a^2+a} \qquad a+1$$
$$a-1$$
$$\underline{-a+1}$$
$$0$$

$a^2-1 = (a-1)(a+1)$ Ara si que hem obtingut residu '0' així que podem determinar que el mcd serà l'últim divisor no nul. En aquest cas "$a-1$".

$\boxed{mcd(a^2-1, a^3-1) = |a-1|}$

(16). Demo que el nombre que s'escriu <u>1331</u> en base <u>b</u> no és primer (sigui quina sigui <u>b</u>).

Volem demo que el núm. 1331 en qualsevol base <u>no</u> és primer.

Això sig. que 1331 és producte d'alguns nombres (no importa que siguin primers).

30 no és primer pq 30 = 6·5 i 6 no és primer. És veu que però això bàsicament.

Expressar el nombre 1331 en qualsevol base sig. que $1\cdot b^3 + 3b^2 + 3b + 1b^0$.

Simplificat expressió equival a $b^3 + 3b^2 + 3b + 1$.

Hem de veure que aquesta expressió es pot reescriure com a producte d'alguns coses.

Per aconseguir-ho farem factorització.

$$b^3 + 3b^2 + 3b + 1 = b^3 + 1 + 3b^2 + 3b = b^3 + 1^3 + 3b^2 + 3b \Rightarrow$$

$$\boxed{a^3 + b^3 = (a+b)(a^2 - ab + b^2)} \quad (b+1)(b^2 - b + 1) + 3b^2 + b \Rightarrow$$

$$(b+1)(b^2 - b + 1) + 3b(b+1) \Rightarrow$$

$$\Rightarrow (b+1)(b^2 - b + 1 + 3b) \Rightarrow (b+1)(b^2 + 2b + 1) \Rightarrow (b+1)((b+1)^2) \Rightarrow (b+1)^3$$

Ara aquí poden passar dues coses. Donat que enunciat diu <u>qualsevol</u> base, també significa base = 1. Aquesta no és posicional com les altres, sinó que representa la quantitat de termes (digits) que té un nombre. En aquest cas $1331_1 = 4_{10}$.

4 no és primer. i si $b > 1$ tampoc ho serà pq el nombre resultant es podrà reescriure com a producte de termes més petits (el que va en contra de def de primer).

Onde demo que $\boxed{\text{1331 no serà primer en cap base}}$:)

(47). Executa algoritme Euclides. mcd (5548, 1727) = ? x = ? y = ?

r	q	x	y
5548	—	1	0
1727	3	0	1
367	4	1	
259	1	−4	
108	2	+9	
43	2	−67	
22	1	+76	
21	1	46	
mcd ← 1	21		
0			

① 5548 − 1727 = 3821 − 1727 = 2094 − 1727 = 367 ✓ 3 = q

② 1 − 3·0 = 1 − 0 = 1
0 − 4·1 = 0 − 4 = −4

Refer.

53. $mcd(2k+9, 3k+15) = \begin{cases} 3 & \text{si } 3 \mid k \\ 1 & \text{altrament} \end{cases}$. Demo.

$mcd(2k+9, 3k+15) \overset{\text{T. Euc.}}{=} mcd(2k+9, k+6) \overset{\text{T. Euc}}{=} mcd(k+6, k+3) \overset{\text{T. Euc.}}{=} mcd(k+3, \overset{\text{3 primer}}{3})$

$mcd(k+3, 3) = \begin{cases} 3 & \text{si } 3 \mid k+3 \\ 1 & \text{si } 3 \nmid k+3 \end{cases}$ Però busquem que compleixi $3 \mid k$ i tenim $3 \mid k+3$.

$3 \mid (k+3) \Leftrightarrow 3 \mid k$

$\Rightarrow)$ $3 \mid (k+3) \Leftrightarrow \exists m \in \mathbb{Z} : k+3 = 3m \Rightarrow \exists m \in \mathbb{Z} : k = 3m-3 = 3(m-1) \Rightarrow \exists r \in \mathbb{Z} : k = 3r$

$\Rightarrow 3 \mid k$

Aquí hem vist que $3 \mid k+3 \Leftrightarrow 3 \mid k$ llavors queda demo. enunciat :).

47. Aplica Algoritme d'Euclides.

$mcd(7084, -3563)$. Per comoditat, tractem tot positiu, PERÒ haurem de vigilar amb X, Y.

X	1	0	$1-0*1$ 1	$0-1*2$ -1	$1-(-1)*83$ 84	$-1-84*1$ $\boxed{-85}$	–
Y	0	1	$0-1*1$ -1	$1-(-1)*1$ 2	$-1-2*83$ -167	$2-(-167)*1$ $\boxed{169}$	–
Q	–	1	1	83	1	5	–
R	7084	3563	3521	42	35	$\boxed{7}$	0

Donat que mcd no importa símbol, $\boxed{mcd(7084, -3563) = \lvert 7 \rvert}$

Ara hem de veure que passa amb X, Y.

$-85 * 7084 + 169 * (-3563) = -1204287 \neq 7$

llavors haurem de modificar pq sigui 7

t.q $X = -85$, $Y = -169 \rightarrow -85 * 7084 + (-169) * (-3563) = 7$. $\boxed{X = -85}$ $\boxed{Y = -169}$

51. Demo si $n \geq 0$, $m > 0 \Rightarrow a^n$ i $a^m - 1$ són primers entre si.

Són primers entre si sii $mcd(a^n, a^m - 1) = 1$.

Cas 1; $n > m$:

Suposem que $mcd(a^n, a^m - 1) > 1$ t.q $\exists p$ (primer) : $p \mid a^n$ i $p \mid a^m - 1$.

Donat que $n > m$, si $p \mid a^n$ tmb ho farà a a^m. Però tenim $a^m - 1$.

Llavors suposem que $p \mid a^m - 1 \Leftrightarrow \exists l \in \mathbb{Z} : a^m - 1 = pl$.

Sabem que $p \mid a$ (pq $p \mid a^n$) llavors $\exists k \in \mathbb{Z} : a = pk$.

Podem fer sub. t.q.

(51). Demo que si $n \geq 0$ i $m > 0 \Rightarrow a^n$ i $a^m - 1$ primers entre si.

Primers entre si significa que $mcd(a^n, a^m - 1) = 1$.

Cas 1; $n \leq m$:

Volem demo: $mcd(a^n, a^m - 1) = 1$

Ho farem per contradicció t.q. $mcd(a^n, a^m - 1) > 1. \rightarrow ⚡$

Si $mcd(a^n, a^m - 1) > 1$ significa que $\exists p \xrightarrow{\text{primer}}$: $p | a^n$ i $p | a^m - 1$.

Si $p | a^n$ significa que $p | a^m$ (donat que $n < m$).

Ara tenim que $p | a^m$ llavors $p | a$ (Lema d'Euclides). $\exists k \in \mathbb{Z}: a = pk$

Donat que $p | a^m$ i $p | a^m - 1$ (per prop del mcd) $p |$ diferència t.q.

$p | a^m - (a^m - 1) \Rightarrow p | 1$ i això és una ⚡. Donat que 1 només el divideix $\langle_{-1}^{1}$.

Cas 2; $n > m$:

Ho farem per contradicció. t.q $mcd(a^n, a^m - 1) > 1. \rightarrow ⚡$

Si $mcd(a^n, a^m - 1) > 1$ sig. que $\exists p \xrightarrow{\text{primer}}$: $p | a^n$ i $p | a^m - 1$.

Donat que $p | a^n$ i $n > m \Rightarrow p | a^m$ (i per Lema euclides $p | a$).

Llavors tenim mateixa situació que anterior que, donat que sabem que

$mcd(a, b) \Rightarrow mcd(a, a - b)$ podem fer $mcd(a^m, a^m - 1 - a^m)$ t.q.

$p | a^m$ i $p | -1$ però $p | -1$ és ⚡.

Demostrat que pq. no passin les contradiccions $\boxed{mcd(a^n, a^m - 1) = 1}$:)

(56). $M_a = \{x \in \mathbb{Z} \mid a|x\}$

mcm de 2 nombres primers és el producte

a) Siguin p i q primers dif. $M_p \cap M_q = M_{pq}$.

$$x \in M_p \cap M_q \overset{\text{def } \cap}{\Leftrightarrow} x \in M_p \wedge x \in M_q \overset{\text{def conjunt}}{\Leftrightarrow} p|x \wedge q|x \overset{\text{Caract. del mcm}}{\Leftrightarrow} mcm(p,q)|x \Leftrightarrow pq|x \overset{\text{def del Conjunt.}}{\Leftrightarrow} x \in M_{pq}$$

b) Val $M_p \cap M_q = M_{pq}$ per p i q qualsevol?

Fals; Contraexemple: $4|12$ i $6|12$ però $6 \cdot 4 \nmid 12$ llavors $M_4 \cap M_6 \neq M_{24}$

(58). Suposem que p primer. Demo equiv.

a) ⇒ b) | Suposem: $p|a$ Volem Demo: $mcd(p,a) = p$

Si $p|a$ el mcd de p i a serà p donat que és el divisor més petit.

$p|a$ i $p|p \Leftrightarrow mcd(a,p) = p$ ☑.

c) ⇒ d) | Suposem: $p|a^2$ Volem Demo: $p^2|a^3$

$$\text{Partim } p|a^2 \Leftrightarrow \exists k \in \mathbb{Z} : a^2 = pk \overset{()^2}{\Rightarrow} \exists k \in \mathbb{Z} : a^4 = (pk)^2 \overset{k^2 = g}{\Rightarrow} \exists g \in \mathbb{Z} : a^4 = p^2 g$$

Llavor tenim que $p^2|a^4$ i pel Lema d'Euclides tenim que $p^2|a^4 \Rightarrow p^2|a^3$ o $p|a$

En concret tenim que $p^2|a^3$ ☑.

$$p|a^2 \underset{\text{Lema Euclides}}{\Rightarrow} p|a \overset{()^2}{\Rightarrow} \begin{matrix} p^2|a^2 \\ a^2|a^2 \end{matrix} \Rightarrow \begin{matrix} p^2|a^2 \\ a^2|a^3 \end{matrix} \overset{\text{Transitivitat}}{\Rightarrow} p^2|a^3$$ # Una altra forma més fàcil.

d) ⇒ a) | Suposem: $p^2|a^3$ Volem Demo: $p|a$

$$\begin{matrix} p^2|a^3 \\ p|p^2 \end{matrix} \overset{\text{Trans}}{\Longrightarrow} p|a^3 \overset{\text{Lema Euclides}}{\Longrightarrow} p|a \text{ ☑.}$$

(62). a, b primers entre si ⇒ a^4 i $5a^2 + 3b^3$ tmb primers entre si.

Farem Demo per R.A. $mcd(a,b) = 1$ i $mcd(a^4, 5a^2+3b^3) \neq 1 \longrightarrow$ ↯

$a|x \wedge a|y \Rightarrow a|ux+vy$ ⇒ $v=1$, $u=5a$

$p|a \wedge p|5a^2+3b^3$ linealitat $p|5a^2+3b^3 + a(-5a)$

Si $mcd(a^4, 5a^2+3b^3) \neq 1$ sig que $\exists p$ prime: $p|a^4$ i $p|5a^2+3b^3$.

Pel Lema d'Euclides $p|a^4 \Rightarrow p|a$. Si $p|a$ i $p|5a^2+3b^3 \Rightarrow p|5a^2+3b^3 - a(5a)$ i $p|a$

$$\Rightarrow p|3b^3 \text{ i } p|a \underset{\text{Lema Euclides}}{\Rightarrow} p|b \text{ i } p|a \underset{\text{Def de mcd}}{\Rightarrow} mcd(a,b) = p \neq 1 \rightarrow ↯$$ Cosa falsa pq suposàvem que $mcd(a,b) = 1$.

Això sig que $mcd(a,b) = 1 \Rightarrow mcd(a^4, 5a^2+3b^3) = 1$. ☑.

(93). Digeu si eq. diof. tenen sol. Si tenen, trobeu solució.

• $512x + 88y = 40$.

Pas 0: Mirem si eq. diof. té sol. Mirem si $mcd(512,88) \mid 40$

Q		5	1	4	8	
R	512	88	72	16	$\boxed{8}$	0

$mcd(512,88) = 8$ i $8 \mid 40$

Així que eq. sí que té solucions.

Pas 1: Simplifiquem eq:

$512x + 88y = 40 \to 64x + 11y = 5$ i donat que 11 primer i $11 \nmid 64 \Rightarrow mcd(64,11) = 1$.

Pas 2: Busquem solució particular de l'eq. diof via id. de Bezout, que es calcula amb algoritme Euclides estès.

X	1	0	1	-1	5
Y	0	1	-5	6	-29
Q		5	1	4	
R	64	11	9	2	1

$5 \cdot 64 - 29 \cdot 11 = 1 = mcd(64,11)$

$\Downarrow *5$

$(5*5) \cdot 64 - (29*5) \cdot 11 = 5$

$\Downarrow$

$$\boxed{\begin{matrix} 25*64 - 145*11 = 5 \\ x*64 + y*11 = 5 \end{matrix}}$$

$$\boxed{\begin{cases} x_0 = 25 \\ y_0 = -145 \end{cases} \text{sol. particular}}$$

Pas 3: Escriure la solució general:

$$\boxed{\begin{cases} x = 25 - 11t \\ y = -145 + 64t \end{cases} \text{per } t \in \mathbb{Z} \quad \text{sol. general}}$$

(103). Calc tots $\mathbb{Z} > 0$ de a, b t.q $a + b = 57$ i $mcm(a,b) = 680$.

$\begin{cases} a + b = 57 \\ mcm(a,b) = 680 \end{cases}$ és el mateix que dir "$mcm * mcd = ab$" $\begin{cases} a + b = 57 \\ \dfrac{ab}{mcd(a,b)} = 680 \end{cases}$

Direm que $d := mcd(a,b)$

$d \mid a \wedge d \mid b \xRightarrow{\text{linealitat}} d \mid (a+b) \Rightarrow$

$\Rightarrow \underline{d \mid 57}$

Pel $mcm(a,b) = 680$ sig. que $a \mid 680$ i $b \mid 680$.

Llavors tenim que $d \mid a$ i $a \mid 680 \xRightarrow{\text{linealitat}} \underline{d \mid 680}$

Q		11	1	13	
R	680	57	53	4	1 → mcd

Veiem que $d \mid 680$ i $d \mid 57 \Rightarrow d \mid mcd(680, 57)$

Això sig. que $d \mid 1$ i això serà cert quan $d = 1$.

Llavors $\dfrac{ab}{d} = 680 \Rightarrow ab = 680$. Ara tenim $\begin{cases} a + b = 57 \\ a \cdot b = 680 \to a = \dfrac{680}{b} \end{cases}$

$\dfrac{680}{b} + b = 57 \Rightarrow 680 + b^2 = 57b \Rightarrow b^2 - 57b + 680 = 0$ $\begin{cases} \to b = 40 \\ \to b = 17 \end{cases}$

$b = 40 \Rightarrow a = 17$

$b = 17 \Rightarrow a = 40$

$\boxed{\text{Les solucions són } (a,b) = (17,40) \text{ i } (a,b) = (40,17).}$

(105). Demo que són equivalents (p primer)

c) $\Rightarrow$ a)|| Suposem: $p^3 | a^2$ Volem Demo: $p^2 | a$

Pel teorema de factorització $a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}$ p primer dif 2 a 2.

Tenim que $\left.\begin{array}{l} p^3 | a^2 \Rightarrow p^3 | p_1^{2e_1} \cdot p_2^{2e_2} \cdots p_n^{2e_n} \\ p | p^3 \end{array}\right\} \Rightarrow p | p_1^{2e_1} \cdot p_2^{2e_2} \cdots p_n^{2e_n} \Rightarrow$ L. Euclides.

$p | p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n} \Rightarrow \exists i : p | p_i \Rightarrow \exists i : p = p_i$

☐ Revisar

Tenim que $p^3 | p_i^{2e_i}$ llavors $\left.\begin{array}{l} 2e_i \geq 3 \Rightarrow e_i \geq 1'5 \\ e_i \text{ enter} \end{array}\right\} \Rightarrow e_i \geq 2 \Rightarrow p^2 | a$.