Bloc 2. ELS ENTERS

Lliçó 1.
ELS NOMBRES ENTERS

1. ELS ENTERS. PRINCIPI DE LA BONA ORDENACIÓ.

DEFINICIÓ: El conjunt Z verifica els axiomes següents:

A1. Hi ha definides dos operacions binàries + i ·

A2. Són commutatives.

A3. Són associatives.

A4. Hi ha element neutre per a cada una d'elles.

A5. · és distributiva respecte de+

A6. $\forall a \in \mathbb{Z}\ \exists!(-a) \in \mathbb{Z}\ /\ a + (-a) = 0$

A7. Si $a \neq 0$ i $a \cdot b = a \cdot c$, aleshores $b = c$

Existeix en Z una relació ≤ que verifica:

A8. És reflexiva.

A9. És antisimètrica.

A10. És transitiva.

A11. Si $a \leq b$, aleshores $a+c \leq b+c$.

A12. Si $a \leq b$ i $0 \leq c$, aleshores $a \cdot c \leq b \cdot c$

A13. Si X és un subconjunt no buit i tancat inferiorment, aleshores X posseeix mínim.

2. DIVISIBILITAT

TEOREMA (Algoritme de la divisió)

Siguen a, b dos enters. Si b no és nul, hi ha dos únics enters q, r verificant $a = b \cdot q + r$, amb $0 \leq r < |b|$.

DEFINICIÓ:

El càlcul de q i r en el teorema anterior s'anomena divisió euclídea de a per b; el nombre q és el **quocient** de la divisió, i r és la **resta**.

EXEMPLE:

La divisió euclídea de a=27 per b=4, produeix com a quocient q=6 i com a resta r=3.

$$27 = 4 \cdot 6 + 3$$

La divisió euclídea de a=27 per b=-4, produeix com a quocient q=-6 i com a resta r=3.

$$27 = (-4) \cdot (-6) + 3$$

2. DIVISIBILITAT

APLICACIÓ: REPRESENTACIÓ EN BASE t D'UN ENTER

Siga t ≥ 2 un enter (base per al càlcul).
Per a qualsevol enter x, per aplicació reiterada de l'algoritme de la divisió, tenim:

$$\begin{cases} x &= t \cdot q_0 + r_0 \\ q_0 &= t \cdot q_1 + r_1 \\ q_1 &= t \cdot q_2 + r_2 \\ & \cdots \\ & \cdots \\ q_{n-2} &= t \cdot q_{n-1} + r_{n-1} \\ q_{n-1} &= t \cdot q_n + r_n \end{cases}$$

Amb:

$$r_i \in \mathbb{Z} \;/\; 0 \le r_i \le t-1, \;\; i = 0, 1, 2, \ldots, n.$$

Si parem quan q_n=0, obtenim, eliminant els quocients q_i:

$$x = r_n \cdot t^n + r_{n-1} \cdot t^{n-1} + \cdots + r_1 \cdot t + r_0.$$

Hem representat x en base t:

$$x = (r_n r_{n-1} \cdots r_1 r_0)_t.$$

2. DIVISIBILITAT

EXEMPLE:

Convencionalment $t = 10$ és la base usual i generalment s'omet d'aquesta representació el subíndex $t = 10$. Per exemple,

$$1432 = 1 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10^1 + 2 \cdot 10^0.$$

Vegem quina és la representació en base 2 de $(109)_{10}$:

$$109 = 2{\cdot}54+1$$
$$54 = 2{\cdot}27+0$$
$$27 = 2{\cdot}13+1$$
$$13 = 2{\cdot}6+1$$
$$6 = 2{\cdot}3+0$$
$$3 = 2{\cdot}1+1$$
$$1 = 2{\cdot}0+1$$

Així: $109 = 1{\cdot}2^6 + 1{\cdot}2^5 + 0{\cdot}2^4 + 1{\cdot}2^3 + 1{\cdot}2^2 + 0{\cdot}2^1 + 1{\cdot}2^0.$

I la seua representació en base 2 és: $(1101101)_2$

2. DIVISIBILITAT

Lliçó 1. ELS NOMBRES ENTERS.

DEFINICIÓ:

Siguen a, $b \in \mathbb{Z}$, amb b no nul. Es diu que:

- b **divideix** al enter a,
- b és un **divisor** de a,
- o que a és un **múltiple** de b

y ho representem per $b|a$, si hi ha un enter q tal que

$$a = b \cdot q.$$

EXEMPLE:

7 és un divisor de 63, ja que 63=7·9. Direm també que 7 divideix a 63, o que 63 és un múltiple de 7.

Al contrari, 8 no és divisor de 63 ja que:

$$\nexists q \in \mathbb{Z} \;/\; 63 = 8 \cdot q$$

Índex

2. DIVISIBILITAT

PROPOSICIÓ:
Siguen a, b, c $\in \mathbb{Z}$.

1. $1|a$, $a|0$, $a|a$
2. Si $a|b$ i $b|a$, aleshores $a=\pm b$
3. Si $a|b$ i $b|c$, aleshores $a|c$.
4. Si $a|b$, aleshores $a|bx$, $\forall x \in \mathbb{Z}$.
5. Si $a|b$ i $a|c$, aleshores $a|(bx+cy)$, $\forall x,y \in \mathbb{Z}$.

3. MÀXIM COMÚ DIVISOR. MÍNIM COMÚ MÚLTIPLE

DEFINICIÓ:

Siguen a,b $\in \mathbb{Z}$, on almenys un d'ells és no nul. Aleshores, c $\in \mathbb{Z}$ es denomina màxim comú divisor (mcd) de a,b si:

1. c|a i c|b.
2. Si existeix un enter d, tal que d|a i d|b, aleshores d|c.

EXEMPLE:

El màxim comú divisor de a=60 i b=84 és d=12, ja que:

1. 12 és un divisor comú de 60 i de 84 (60=12·5 i 84=12·7)
2. Els divisors comuns de 60 i 84 són els elements del conjunt:

$$D=\{-12,-6,-4,-3,-2,-1,1,2,3,4,6,12\}$$

Qualsevol element d'aquest conjunt és un divisor de 12.

3. MÀXIM COMÚ DIVISOR. MÍNIM COMÚ MÚLTIPLE

TEOREMA

Per a qualssevol $a,b \in Z^+$, existeix un $c \in Z^+$, únic, que és el màxim comú divisor de a i b.

OBSERVACIÓ

$$\mathrm{mcd}(a,b) = \mathrm{mcd}(-a,b) = \mathrm{mcd}(a,-b) = \mathrm{mcd}(-a,-b)$$

EXEMPLE:

$$\mathrm{mcd}(8,24) = \mathrm{mcd}(-8,24) = \mathrm{mcd}(8,-24) = \mathrm{mcd}(-8,-24)=4$$

3. MÀXIM COMÚ DIVISOR. MÍNIM COMÚ MÚLTIPLE

DEFINICIÓ:

Els enters a,b es denominen **primers entre si**, quan mcd(a,b)=1.

EXEMPLE:

15 i 8 són primers entre si perquè mcd(15,8)=1.

COROL·LARI (Identidad de Bezout)

Siguen $a,b \in \mathbb{Z}$ i $d=\text{mcd}(a, b)$. Aleshores $\exists\ s,t \in \mathbb{Z}$ / $d=as + bt$.

EXEMPLE:

Siguen a=21 i b=35. El mcd(21,35)=7.

Podem prendre s=2 i t =-1 i tenim que $7=21\cdot2+35\cdot(-1)$.

3. MÀXIM COMÚ DIVISOR. MÍNIM COMÚ MÚLTIPLE

TEOREMA (Algoritme d'Euclides)

Si a,b $\in Z$ i s'aplica l'algoritme de la divisió:

$$
\begin{aligned}
a &= q_1 b + r_1 \quad 0 < r_1 < b \\
b &= q_2 r_1 + r_2 \quad 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 \quad 0 < r_3 < r_2 \\
&\dots \\
r_i &= q_{i+2} r_{i+1} + r_{i+2} \quad 0 < r_{i+2} < r_{i+1} \\
&\dots \\
r_{k-2} &= q_k r_{k-1} + r_k \quad 0 < r_k < r_{k-1} \\
r_{k-1} &= q_{k+1} r_k
\end{aligned}
$$

Aleshores, r_k l'última resta diferent de zero és igual al mcd(a,b).

3. MÀXIM COMÚ DIVISOR. MÍNIM COMÚ MÚLTIPLE

EXEMPLE:

Aplicarem l'algoritme d'Euclides per a calcular el màxim comú divisor de 791 i 336. Aplicarem l'algoritme de la divisió als enters inicials i després anirem dividint divisor entre resta fins a obtindre un resta nul·la.

$$
\begin{aligned}
791&=2\cdot336+119, && 0<119<336\\
336&=2\cdot119+98, && 0<98<119\\
119&=1\cdot98+21, && 0<21<98\\
98&=4\cdot21+14, && 0<14<21,\\
21&=1\cdot14+7, && 0<7<14,\\
14&=2\cdot7
\end{aligned}
$$

Per tant, el mcd(791,336)=7.

3. MÀXIM COMÚ DIVISOR. MÍNIM COMÚ MÚLTIPLE

EXEMPLE: A més, podem utilitzar les equacions anteriors per a expressar 7 com a combinació lineal de 791 i 336, és a dir, per a trobar una solució de la identitat de Bezout

$$791s+336t=7.$$

$$\begin{array}{ll}
791=2\cdot 336+119, & 7 = 21 - 1\cdot 14 \\
336=2\cdot 119+98, & \quad = 21 - (98 - 4\cdot 21) = 5\cdot 21 - 98 \\
119=1\cdot 98+21, & \quad = 5(119 - 1\cdot 98) - 98 = 5\cdot 119 - 6\cdot 98 \\
98=4\cdot 21+14, & \quad = 5\cdot 119 - 6(336 - 2\cdot 119) = 17\cdot 119 - 6\cdot 336 \\
21=1\cdot 14+7, & \quad = 17(791-2\cdot 336) - 6\cdot 336 = 791\cdot 17+336\cdot(-40) \\
14=2\cdot 7 &
\end{array}$$

Així la solució de la identitat de Bezout és s=17 i t=−40.

3. MÀXIM COMÚ DIVISOR. MÍNIM COMÚ MÚLTIPLE

DEFINICIÓ:

Siguen $a,b \in Z$ i $c \in Z^+$. Es denomina equació diofántica a l'equació $ax+by = c$, on $x,y \in Z$ són incògnites.

TEOREMA

Siguen $a,b \in Z$, $c \in Z^+$ i $d=mcd(a,b)$. L'equació diofántica $ax+by = c$ té solució en Z si, i només si, $d|c$, és a dir, si $c=k\cdot d$, $k \in Z$.

EXEMPLE:

El $mcd(791,336)=7$. Podem assegurar que l'equació diofántica $791x+336y=7$ té solució sencera perquè 7 és divisor de si mateix (Sol.: $x=17$, $y=-40$).

No obstant això $791x+336y=22$ no té solució sencera perquè 22 no és múltiple de 7.

OBSERVACIÓ

És obvi que obtinguda una solució sencera que verifique la identitat de Bezout,

$$ax+by=d,\ d=mcd(a,b)\ (x=x_0,\ y=y_0),$$

tindrem també una solució sencera de l'equació

$$ax+by=c,\ c=k\cdot d,$$

sense més que considerar $x=k\cdot x_0$, $y=k\cdot y_0$.

EXEMPLE:

Tenint en compte que es compleix

$$791x+336y=7 \text{ amb } x=17 \text{ i } y=-40$$

tindrem que l'equació diofántica

$$791x+336y=28$$

tindrà com a solucions ($28=4\cdot 7$):

$$x=4\cdot 17=68 \text{ i } y=4\cdot(-40)=-160.$$

3. MÀXIM COMÚ DIVISOR. MÍNIM COMÚ MÚLTIPLE

TEOREMA

Siguen a,b $\in Z^+$ i d=mcd(a,b).

Siguen $\alpha,\beta \in Z^+$ / a = α·d, b = β·d, y $x_0,y_0 \in Z$ una solució de l'equació diofántica:

$$ax+by = d\cdot n$$

Aleshores, x,y $\in Z$ és solució de l'anterior equació si, i només si,

$$\left.\begin{aligned} x &= x_0 + k\beta \\ y &= y_0 - k\alpha \end{aligned}\right\} \; k \in \mathbb{Z}.$$

3. MÀXIM COMÚ DIVISOR. MÍNIM COMÚ MÚLTIPLE

EXEMPLE:

Estudiem les solucions de $791x+336y=28$.

1. Té solució?

Com $\mathrm{mcd}(791,336)=7$, i $7|28$, aleshores hi ha una solució.

2. Càlcul d'una solució particular de $791x+336y=7$: Una solució és $(17,-40)$.

3. Càlcul d'una soluciò particular de $791x+336y=28$:

Com $28=4\cdot 7$, aleshores $x_0=4\cdot 17=68$, $y_0=4\cdot(-40)=-160$.

4. Càlcul de la solució general:

Com $791=113\cdot 7$ y $336=48\cdot 7$, aleshores $\alpha=113$ i $\beta=48$.

Per tant, qualsevol solució d'aquesta equació és de la forma

$$\left.\begin{aligned} x &= 68 + 48\cdot k \\ y &= -160 - 113\cdot k \end{aligned}\right\} \quad k \in \mathbb{Z}$$

3. MÀXIM COMÚ DIVISOR. MÍNIM COMÚ MÚLTIPLE

DEFINICIÓ:

Siguen $a,b \in Z^+$. Direm que $c \in Z^+$. és el mínim comú múltiple de a i b i escriurem c=mcm(a, b), si c és el menor dels enters positius que són múltiples comuns de a i b.

EXEMPLE: Siguen a=550, b=84. Calculem el seu mcm:

Múltiples positius de a=550: $550 \cdot x$, $x \in Z^+$.

Múltiples positius de b=84: $84 \cdot y$, $y \in Z^+$.

Per a trobar múltiples comuns: $550x = 84y$, $x,y \in Z^+$.

La solució del qual és: $x=42k$, $y=275k$, $k \in Z^+$.

Per tant, el conjunt d'enters positius múltiples comuns de 550 i 84 és:

$$S = \{550(42k) \;/\; k \in \mathbb{Z}^+\} = \{84(275k) \;/\; k \in \mathbb{Z}^+\}.$$

El seu element mínim serà el mcm: aquest s'aconsegueix per a k=1, i és

mcm(550,84)=550·42=84·75=23100.

3. MÀXIM COMÚ DIVISOR. MÍNIM COMÚ MÚLTIPLE

TEOREMA

Siguen a,b $\in \mathbb{Z}^+$, i c=mcm(a,b).
Si $\exists$ d $\in \mathbb{Z}^+$. tal que a|d i b|d, aleshores c|d.

EXEMPLE:

Siga **a**=550 i **b**=84. El mcm(550,84)=23100.
Prenguem qualsevol enter positiu **d** que siga múltiple de 550 i 84. Aquest conjunt és

$$S = \{550(42k) \ / \ k \in \mathbb{Z}^+\} = \{84(275k) \ / \ k \in \mathbb{Z}^+\}.$$

I per tant **d** serà de la forma **d**=23100·k, és a dir, **d** és també un múltiple del mcm(550,84).

4. NOMBRES PRIMERS. FACTORITZACIÓ

DEFINICIÓ:

Direm que $p \in Z^+$ és **primer** si té exactament dos divisors positius distints.

EXEMPLE: Els divisors positius de 13 són 1 i 13. Per tant 13 és primer.

TEOREMA

Si a és un enter estrictament major que 1, el seu menor divisor estrictament major que 1 és un nombre primer.

EXEMPLE: Siga a=25. El seu menor divisor estrictament major que 1 és 5. 5 és un nombre primer.

4. NOMBRES PRIMERS. FACTORITZACIÓ

TEOREMA

Tot element de $\mathbb{Z}^+$ major o igual que 2, és un nombre primer o és un producte de nombres primers. Esta descomposició és única excepte l'orde.

DEFINICIÓ:

El càlcul dels nombres primers el producte del qual coincideix amb un nombre enter donat n, s'anomena descomposició en factors primers de n.

EXEMPLE: Siga n=2200. 2200 no és primer

La seua descomposició en factors primers és $2200=2^3 \cdot 5^2 \cdot 11$.

Enter / quocients	2200	1100	550	275	55	11	1
Menor divisor > 1	2	2	2	5	5	11	

4. NOMBRES PRIMERS. FACTORITZACIÓ

TEOREMA

Siguen a,b $\in \mathbb{Z}^+$ i

$$a = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}, \; b = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t},$$

amb cada p_i primer i e_i, $r_i \geq 0$, $1 \leq i \leq t$.

Aleshores, si

$$a_i = \min\{e_i, r_i\}, \quad b_i = \max\{e_i, r_i\}, \quad 1 \leq i \leq t,$$

s'obté que

$$\mathrm{mcd}(a,b) = \prod_{i=1}^{t} p_i^{a_i}, \quad \mathrm{mcm}(a,b) = \prod_{i=1}^{t} p_i^{b_i}$$

4. NOMBRES PRIMERS. FACTORITZACIÓ

EXEMPLE:

Siguen a=2200 i b=3388. Les seues descomposicions en factors primers són:

$$2200=2^3\cdot5^2\cdot11$$

$$3388=2^2\cdot7\cdot11^2$$

que reescrites queden:

$$2200=2^3\cdot5^2\cdot7^0\cdot11^1$$

$$3388=2^2\cdot5^0\cdot7^1\cdot11^2$$

Per tant:

$$\text{mcd}(2200,3388)=2^2\cdot5^0\cdot7^0\cdot11^1=2^2\cdot11=44,$$

$$\text{mcm}(2200,3388)=2^3\cdot5^2\cdot7^1\cdot11^2=169400.$$

4. NOMBRES PRIMERS. FACTORITZACIÓ

TEOREMA

Siguen $a,b \in \mathbb{Z}^+$, aleshores

$$a \cdot b = \mathrm{mcd}(a,b) \cdot \mathrm{mcm}(a,b).$$

EXEMPLE:

Siguen $a=2200=2^3 \cdot 5^2 \cdot 11$ i $b=3388=2^2 \cdot 7 \cdot 11^2$.

$\mathrm{mcd}(2200,3388)=2^2 \cdot 11=44$,

$\mathrm{mcm}(2200,3388)=2^3 \cdot 5^2 \cdot 7 \cdot 11^2=169400$.

Podem comprovar que:

$$\begin{aligned} 2200 \cdot 3388 &= (2^3 \cdot 5^2 \cdot 11) \cdot (2^2 \cdot 7 \cdot 11^2) \\ &= (2^2 \cdot 11) \cdot (2^3 \cdot 5^2 \cdot 7^1 \cdot 11^2) \\ &= \mathrm{mcd}(2200,3388) \cdot \mathrm{mcm}(2200,3388) \end{aligned}$$