TEMA 4. NOMBRES ENTERS. DIVISIBILITAT. PRIMERS. CONGRUÈNCIES.

1. INTRODUCCIÓ

1.1. JUSTIFICACIÓ DELS CONTINGUTS

Els continguts d'aquest tema s'estructuren en tres parts. Una primera part en que construirem, ampliant el conjunt dels nombres naturals, l'anell commutatiu unitari dels nombres enters amb les operacions suma i producte.

A la segona part desenvoluparem la relació de divisibilitat i introduïrem els nombres primers. Per acabar, a la tercera part tractarem el concepte de congruència, relacionant-lo amb la divisibilitat.

La construcció d'aquest tema es basa en la legislació vigent, en especial en el decret 175/2022 i l'actual convocatòria d'oposicions.

Falta coneixements sobre els nombres naturals (1) i sobre els conjunts numèrics i classes d'equiv (1.1)

2. CONSTRUCCIÓ DE $\mathbb{Z}$

El conjunt dels nombres enters ($\mathbb{Z}$) sorgeix de la necessitat d'ampliar els nombres naturals ($\mathbb{N}$) per a que l'equació $a+x=b$ amb $a>b$ tingués solució.

L'operació que definim a continuació té com a objectiu estendre els naturals de forma natural i verificar que $\mathbb{N} \subseteq \mathbb{Z}$ de forma canònica.

2.1. RELACIÓ D'EQUIVALÈNCIA ALS ENTERS

Definim a $\mathbb{N}\times\mathbb{N}$ una relació $\sim$ de forma que

$$(a,b)\sim(c,d) \Longleftrightarrow a+d=b+c$$

On (+) és la llei de composició interna definida a $(\mathbb{N},+,\cdot)$

Aquesta relació és d'equivalència ja que verifica les propietats:

- Reflexiva: $a+b=b+a \Rightarrow (a,b)\sim(b,a)$

- Simètrica:

$a+d=b+c \Leftrightarrow c+b=d+a \rightarrow (a,b)\sim(c,d) \Leftrightarrow (c,d)\sim(a,b)$.

- Transitiva:

$$\left.\begin{array}{l} a+d=b+c \\ c+f=d+e \end{array}\right\} \Rightarrow a+d+c+f=b+c+d+e \Rightarrow a+f=b+e$$

Aleshores si $(a,b)\sim(c,d)$ i $(c,d)\sim(e,f) \Rightarrow (a,b)\sim(e,f)$.

2.2. CONJUNT QUOCIENT I REPRESENTANT CANÒNIC.

Definim $\mathbb{Z}$ com el conjunt quocient $\mathbb{N}\times\mathbb{N}/\sim$ i l'anomenem conjunt de nombres enters, els elements del qual són les classes d'equivalència que representem per:

$$[(a,b)]=\{(x,y)\in\mathbb{N}\times\mathbb{N} \ / \ (a,b)\sim(x,y)\}$$

Podem escollir un representant més senzill per cada classe d'equivalència, distingim tres casos:

- Si $a>b \Rightarrow a=b+n,\ n\in\mathbb{N} \Rightarrow (a,b)\sim(n,0) \Rightarrow [(a,b)]=[(n,0)]$

Escrivim $[(n,0)]=+n$, o simplement n, i el conjunt $\mathbb{N}^+=\{[(n,0)] \ / \ n\in\mathbb{N}\setminus\{0\}\}$ s'anomena conjunt d'enters positius.

- Si $a<b \Rightarrow b=a+n,\ n\in\mathbb{N} \Rightarrow (a,b)\sim(0,n) \Rightarrow [(a,b)]=[(0,n)]$.

Escrivim $[(0,n)]=-n$ i $\mathbb{N}^-=\{[(0,n)] \ / \ n\in\mathbb{N}\setminus\{0\}\}$ s'anomena conjunt d'enters negatius.

- Si $a=b \Rightarrow (a,b)\sim(0,0) \Rightarrow [(a,b)]=[(0,0)]=0$

Amb això tenim $\mathbb{Z}=\mathbb{Z}^-\cup\{0\}\cup\mathbb{Z}^+$

3. OPERACIONS

3.1. SUMA

Definim la suma de dos elements de $\mathbb{Z}$ com:

$$[(a,b)]+[(c,d)] = [(a+c, b+d)]$$

És veu fàcilment que l'operació suma està ben definida, és a dir, no depenen dels representants canònics.

Les seves propietats elementals són

- Associativa
- Commutativa
- Existència i unicitat d'element neutre (el $[(0,0)]$)
- Existència i unicitat de l'oposat de tot element de $\mathbb{Z}$.
  L'oposat de $[(a,b)]$ és $[(b,a)]$.

No les demostrem per ser trivials.

3.2. PRODUCTE

Definim el producte de dos elements de $\mathbb{Z}$ com:

$$[(a,b)]\cdot[(c,d)] = [(a\cdot c+b\cdot d, a d+b\cdot c)]$$

On $(\cdot)$ és l'operació producte definida a $(\mathbb{N},+,\cdot)$.

Al igual que al cas anterior, aquesta operació tampoc depèn dels representants escollits.

Les seves propietats elementals són:

- Associativa
- Commutativa
- Existència i unicitat de l'element neutre (el $[(1,0)]$).
- Distributiva respecte la suma.

Obviem en aquest cas les proves.

A més, existeixen altres propietats del producte que se'n deriven directament de la seva definició:

i) Llei de simplificació: $m \cdot n = m \cdot p \Rightarrow n = p \quad \forall m \in \mathbb{Z}, m \neq 0$.

ii) Existència d'element absorvent $m \cdot 0 = 0 \quad \forall m \in \mathbb{Z}$.

iii) Absència de divisors de 0 no trivials: $\forall m, n \in \mathbb{Z} \; m \cdot n = 0 \Longleftrightarrow$
$\Longleftrightarrow m = 0 \vee n = 0$

(Aquesta propietat també s'enuncia dient que $\mathbb{Z}$ és Domini d'Integritat.)

iv) Regla dels signes:

$(+m) \cdot (+n) = [(m,0)] \cdot [(n,0)] = [(mn,0)] = +(mn)$

$(+m) \cdot (-n) = [(m,0)] \cdot [(0,n)] = [(0,m \cdot n)] = -(mn)$

$(-m) \cdot (+n) = [(0,m)] \cdot [(n,0)] = [(0,m \cdot n)] = -(mn)$

$(-m) \cdot (-n) = [(0,m)] \cdot [(0,n)] = [(m \cdot n,0)] = +(mn)$.

Amb totes les propietats vistes $(\mathbb{Z},+)$ és un grup abelià, $(\mathbb{Z},\cdot)$ és un semigrup abelià i unitari amb propietat distributiva i, per tant, $(\mathbb{Z},+,\cdot)$ té estructura d'anell commutatiu i unitari.

4. ORDRE A $\mathbb{Z}$

Donats $a, b \in \mathbb{Z}$ diem que a és menor o igual que b, i ho escrivim $a \leq b$, si i només si $b - a \in \mathbb{N}^+ \cup \{0\}$.

(La definició de a menor estricte que b, $a < b$, és anàloga però amb $b - a \in \mathbb{N}^+$)

La relació $\leq$ és d'ordre total en $\mathbb{Z}$ donat que verifica les prop.:

- Reflexiva: $a \leq a \quad \forall a \in \mathbb{Z}$
- Antisimètrica: si $a \leq b$ i $b \leq a \Rightarrow a = b \quad \forall a, b \in \mathbb{Z}$
- Transitiva: si $a \leq b$ i $b \leq c \Rightarrow a \leq c \quad \forall a, b, c \in \mathbb{Z}$
- Tots els elements són comparables: $\forall a, b \in \mathbb{Z} \quad a \leq b$ o $b \leq a$.

Per tant, el conjunt $(\mathbb{Z}, \leq)$ és totalment ordenat.

Notem que, com a conseqüències, tenim que $0 \in \mathbb{Z}$ és menor que qualsevol enter positiu i major que qualsevol enter negatiu i que qualsevol enter negatiu és menor que qualsevol enter positiu.

5. DIVISIBLITAT A $\mathbb{Z}$

Per parlar de divisibilitat a $\mathbb{Z}$ necessitem enunciar prèviament el següent teorema.

TEOREMA:- DE LA DIVISIÓ ENTERA

Donats $a, b \in \mathbb{Z}$, $b \neq 0$, existeixen $q, r \in \mathbb{Z}$ únics tals que $a = bq + r$ amb $0 \leq r \leq b$. s'anomenen, respectivament, quocient i residu de la divisió entera d'a per b.

5.1. MÚLTIPLES I DIVISORS

Siguin $a, b \in \mathbb{Z}$ diem que b divideix a, o que b és un divisor d'a, si el residu de la divisió entera d'a per b és zero, és a dir si $\exists!\, q \in \mathbb{Z} / a = bq$, ho denotem per $b|a$.

També ho podem expressar dient que a és divisible per b o que a és un múltiple de b.

Escrivim el conjunt dels múltiples de b com (b), de manera que aquest conjunt verifica:

Si $m, n \in (b)$ i $c \in \mathbb{Z} \Rightarrow m + n \in (b)$ i $mc, nc \in (b)$

Algunes propietats bàsiques que es dedueixen immediatament de la definició de divisibilitat són:

- Reflexivitat: $a|a$ $\forall a \in \mathbb{Z}$ ja que $a = 1 \cdot a$.

- transitivitat: Si $a|b$ i $b|c \Rightarrow a|c$ ja que $b = k \cdot a$ i $c = l \cdot b \Rightarrow$
$\Rightarrow c = a \cdot l \cdot k \Rightarrow a|c$.
- $\forall a \in \mathbb{Z}$ $0|a$, $1|a$ i $-1|a$
- Si $a|b$ i $b|a \Rightarrow a = \pm b$ ja que $a = k \cdot b$, $b = l \cdot a \Rightarrow a = k \cdot l a$
  - Si $a = 0 \Rightarrow b = 0$
  - Si $a \neq 0 \Rightarrow k \cdot l = 1 \Rightarrow k = l = 1$ o $k = l = -1$
- Si $a|b$ i $a|c \Rightarrow a|b+c$ ja que $b = k \cdot a$ i $c = l \cdot a \Rightarrow b + c = (k+l) \cdot a$
- Si $a|b \Rightarrow a|b \cdot c$ $\forall c \in \mathbb{Z}$ ja que $b = k \cdot a \Rightarrow b \cdot c = k \cdot a \cdot c$.

A partir de la definició de divisor/múltiple podem introduir dos nous conceptes:

5.2 MÀXIM COMÚ DIVISOR

Donats $a, b \in \mathbb{Z}$ anomenem màxim comú divisor d'a i b, i ho denotem per $d = mcd(a,b)$, el nombre de $\mathbb{Z}$ que verifica:

i) $d|a$ i $d|b$

ii) Si $\exists c \in \mathbb{Z} \,/\, c|a$ i $c|b \Rightarrow c|d$.

És a dir, es tracta del major divisor comú d'a i b.

L'mcd és únic, excepte pel signe, que per conveni es pren positiu.

Diem que dos enters a i b són primers entre ells o coprimers si $mcd(a,b) = 1$.

De la definició d'mcd se'n deriven els següents resultats:

TEOREMA.- IDENTITAT DE BEZOUT

Si $d = mcd(a_1, \dots, a_n)$ llavors $\exists c_1, c_2, \dots, c_n \,/\, d = a_1c_1 + \dots + a_nc_n$

COROL·LARI.-

Si $a = bq + r$ és la divisió entera d'a per b, llavors $mcd(a,b) = mcd(b,r)$.

Aplicant reiteradament el resultat anterior obtenim un mètode pràctic per calcular l'mcd entre dos nombres, es coneix com l'algoritme d'Euclides.

TEOREMA.- D'EUCLIDES

Si $a|bc$ i $mcd(a,b) = 1 \Rightarrow a|c$.

5.3. MÍNIM COMÚ MÚLTIPLE.

Donats $a, b \in \mathbb{Z}$ anomenem mínim comú múltiple d'a i b, i ho denotem per $m = mcm(a,b)$, el nombre $m \in \mathbb{Z}$ que verifica:

i) $a|m$ i $b|m$

ii) Si $\exists c \in \mathbb{Z}$ / $a|c$ i $b|c \Rightarrow m|c$

És a dir, es tracta del menor múltiple comú d'a i b.

La següent propietat relaciona els conceptes d'mcd i mcm:

PROPIETAT.- Siguin $a, b \in \mathbb{Z}$:

- $a \cdot b = mcd(a,b) \cdot mcm(a,b)$
- Si $mcd(a,b) = 1 \Rightarrow mcm(a,b) = a \cdot b$

6. NOMBRES PRIMERS

Un nombre enter $p \in \mathbb{Z} \setminus \{\pm 1\}$ es diu primer si els seus únics divisors són ± 1 i $\pm p$.

PROPIETAT.- El conjunt de nombres primers és infinit.

dem.- Donat $S = \{p_1, p_2, \dots, p_n\}$ conjunt finit de nombres primers, podem trobar un nou primer $p \notin S$.

En efecte, sigui $a = p_1 \cdot p_2 \cdots p_n + 1$ i p el menor divisor positiu d'a distint d'1. Notem que p és primer i no és cap dels p_i doncs, en cas contrari, p dividiria $a - p_1 \cdots p_n = 1$, fet que no és possible en ser $p \neq 1 \Rightarrow p$ primer, $p \notin S$.

Aquesta és la idea que va fer servir Euclides per demostrar aquest mateix resultat al segle III a.C.

Un dels resultats més importants, que relaciona els nombres primers amb la teoria de nombres és:

TEOREMA FONAMENTAL DE L'ARITMÈTICA:

Tot nombre enter $a \neq 0, \pm 1$ es pot escriure com a producte de nombres primers. Aquesta factorització és única tret de l'ordre dels factors i del signe.

dem.- Donat $a \neq 0, \pm 1$ sabem que a sempre tindrà un divisor primer $p_1 \neq \pm 1$ de manera que $a = p_1 \cdot a_1$ amb $|a| > |a_1|$. D'igual manera si $a_1 \neq \pm 1$, a_1 tindrà un divisor primer $p_2 \neq \pm 1$ i $a = p_1 \cdot a_1 = p_1 \cdot p_2 \cdot a_2$ amb $|a| > |a_1| > |a_2|$.

Repetint aquest procés reiteradament obtenim la successió decreixent $|a| > |a_1| > |a_2| > \cdots$ i sabem que aquest procés acabarà arribant a: $a = p_1 p_2 \cdots a_n$ amb $|a_n| = 1$.

Per introduir els nombres primers a secundària podem fer ús del Garbell d'Eratostenes. Aquest mecanisme ens permet trobar tots els nombres primers anteriors a un n (nombre natural) donat.

La idea per portar-ho a terme és escriure un llistat amb tots els naturals fins n. Llavors, es ratllen tots els múltiples de 2, començant pel 4. El següent nombre que queda sense ratllar és el 3, pel que ratllem tots els seus múltiples fins a n, i així successivament.

En acabar, els nombres que queden per ratllar són els primers menors que n.

7. CONGRUÈNCIES

7.1 ENTERS CONGRUENTS

Sigui $m \in \mathbb{N}$, $m \neq 0$, direm que dos enters a i b són congruents mòdul m, i ho escriurem $a \equiv b \pmod m$, si $a-b \in (m)$.

PROPIETAT.- $a \equiv b \pmod m \Leftrightarrow$ Les divisions enteres d'a i de b tenen el mateix residu.

dem.- Sigui $a = m \cdot q_1 + r_1$ i $b = m \cdot q_2 + r_2 \Rightarrow a-b = (q_1-q_2)\cdot m + (r_1 - r_2)$, amb $|r_1 - r_2| < |m|$. Per tant $a-b \in (m) \Leftrightarrow r_1 = r_2$.

7.2. CONSTRUCCIÓ DEL CONJUNT QUOCIENT $\mathbb{Z}/(m)$

Notem que la relació de congruència mòdul m és una relació d'equivalència ja que és

- Reflexiva $a \equiv a \pmod m$ $0 \in (m)$
- Simètrica $a \equiv b \pmod m \Leftrightarrow b \equiv a \pmod m$
- Transitiva: $a \equiv b \pmod m, b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$

Podem construir, llavors, el conjunt quocient $\mathbb{Z}/(m)$ que té m classes d'equivalència, anomenades classes de residu mòdul m.

$[0] = \{n \in \mathbb{Z} \mid$ El residu de la divisió d'n per m és $0\} = \{\dots, -m, 0, m, \dots\}$

$[1] = \{n \in \mathbb{Z} \mid$ El residu de la divisió d'n per m és $1\} = \{\dots, -m-1, 1, m+1, \dots\}$

$\vdots$

$[m-1] = \{n \in \mathbb{Z} \mid$ El residu de la divisió d'n per m és $m-1\} = \{\dots, -1, m-1, \dots\}$

PROPIETAT.- Si $a \equiv a' \pmod m$ i $b \equiv b' \pmod m$, llavors:

- $a+b \equiv a'+b' \pmod m$
- $a-b \equiv a'-b' \pmod m$
- $a \cdot b \equiv a' \cdot b' \pmod m$

Tanmateix, si $a \cdot b \equiv 0 \pmod m \not\Rightarrow a \equiv 0 \pmod m$ o $b \equiv 0 \pmod m$, per exemple $6 \cdot 5 \equiv 0 \pmod{15}$ però $6 \equiv 6 \pmod{15}$ i $5 \equiv 5 \pmod{15}$

Aquesta propietat ens garanteix poder trobar unes operacions suma i producte a $\mathbb{Z}/(m)$ que són consistents, és a dir, que no depenen del representant escollit per a cada classe.

Així, si $[a],[b] \in \mathbb{Z}/(m)$ definim $[a]+[b]=[a+b]$ i $[a]\cdot[b]=[a\cdot b]$. Aquestes operacions hereten les propietats de les equivalents a $\mathbb{Z}$ dotant a $\mathbb{Z}/(m)$ d'estructura d'anell commutatiu unitari.

OBS.- A diferència de a $\mathbb{Z}$, $\mathbb{Z}/(m)$ té altres propietats com ara l'existència de divisors de 0 i elements que tenen invers respecte del producte, per exemple:

A $\mathbb{Z}/(6)$, $[2]\cdot[3]=0$ i $[5]\cdot[5]=1$

També hi ha propietats que no són certes a $\mathbb{Z}/(m)$, com la cancel·lació del producte, per exemple:

A $\mathbb{Z}/(6)$, $[2]\cdot[3]=[4]\cdot[3]$ i, en canvi, $[2]\neq[4]$.

6.3. CRITERIS DE DIVISIBILITAT

Una de les aplicacions de l'aritmètica modular més vinculades amb la secundària és l'obtenció immediata dels criteris de divisibilitat en base 10 més coneguts.

Veiem-ne alguns exemples:

Si escrivim un nombre $a=a_0+a_1\cdot 10+\dots+a_k 10^k$, tenim:

- $10\equiv 0 \pmod 2 \Rightarrow 10^n\equiv 0 \pmod 2 \;\forall n\in\mathbb{N}$

Així, $a\equiv 0 \pmod 2 \Leftrightarrow a_0\equiv 0 \pmod 2$, és a dir, a és parell sii la xifra de les unitats també ho és.

El criteri del mòdul 5 és idèntic en ser també $10\equiv 0 \pmod 5$.

• $10 \equiv 1 \pmod 3 \Rightarrow 10^n \equiv 1^n \equiv 1 \pmod 3$.

Així, $a \equiv 0 \pmod 3 \Leftrightarrow a_0 + a_1 + \dots + a_k \equiv 0 \pmod 3$.

és a dir, a és múltiple de 3 si la suma de les seves xifres també ho és.

El criteri del mòdul 9 és idèntic en ser també $10 \equiv 1 \pmod 9$.

• $10 \equiv -1 \pmod{11} \Leftrightarrow 10^n \equiv (-1)^n \pmod{11} \;\forall n \in \mathbb{N}$

Així, $a \equiv 0 \pmod{11} \Leftrightarrow a_0 - a_1 + a_2 - \dots + (-1)^k a_k \equiv 0 \pmod{11}$

a és múltiple d'11 sii la suma de les xifres que ocupen un lloc parell menys la suma de les que ocupen un lloc senar també és múltiple d'11.