

Nombres naturals i enters

Miquel Àngel Perelló

13 de juny de 2026

Índex

Introducció	iv
1 Teoria	1
1.1 Els nombres naturals	1
1.1.1 Axiomes de Peano	2
1.1.2 Recursió	4
1.1.3 Addició de nombres naturals	5
1.1.4 Multiplicació de nombres naturals	8
1.1.5 L'ordre dels nombres naturals	12
1.1.6 Divisibilitat en els nombres naturals	15
1.1.7 Principi d'inducció forta	21
1.2 Els nombres enters	25
1.2.1 Necessitat d'ampliar els nombres naturals	25
1.2.2 Construcció de $\mathbb{Z}$ a partir de $\mathbb{N}$	26
1.2.3 Addició de nombres enters	27
1.2.4 Els naturals com a nombres enters	29
1.2.5 Multiplicació de nombres enters	29
1.2.6 L'ordre als enters	31
1.2.7 Representació gràfica dels nombres enters	39
1.2.8 El teorema de la divisió	40
1.2.9 Divisibilitat en els nombres enters	43
2 Pràctica	47
2.1 Naturals i inducció	47
2.2 Enters i propietats	53
2.2.1 Operacions combinades amb nombres enters	65
2.3 Aplicacions i modelització	69
3 Exercicis proposats	74
3.1 Els nombres naturals	74
3.2 Els nombres enters	76

4	Tests	82
4.1	Test 1: Els nombres naturals	82
4.2	Test 2: Els nombres enters	84
4.3	Test 3: Síntesi: nombres naturals i enters	86
4.4	Test 4: Síntesi avançada i operacions combinades	89

Prefaci

Aquests apunts formen una unitat dedicada als nombres naturals i enters. La intenció no és només aprendre a operar amb aquests nombres, sinó entendre com es poden construir de manera rigorosa i per què les propietats que fem servir habitualment són certes. Per això, els nombres naturals s'introdueixen a partir dels axiomes de Peano, i els nombres enters es construeixen com a classes d'equivalència de parelles de naturals.

Aquesta perspectiva permet veure els nombres com a estructures matemàtiques. En el cas dels naturals, es construeixen la suma, el producte, l'ordre, la divisibilitat i el principi d'inducció. En el cas dels enters, s'estudia com ampliar els naturals per donar sentit a les diferències, als nombres negatius, al valor absolut, a la divisió amb residu i a la divisibilitat dins de $\mathbb{Z}$.

El text està organitzat en quatre blocs. El primer bloc desenvolupa la teoria i presenta les definicions i propietats fonamentals. El segon bloc conté exercicis de pràctica resolta i una secció d'aplicacions i modelització, on es mostra la utilitat dels conceptes en situacions quotidianes. El tercer bloc proposa exercicis amb indicacions breus per orientar-ne la resolució. Finalment, el quart bloc inclou tres tests interactius d'autoavaluació: un sobre nombres naturals, un sobre nombres enters i un de síntesi.

El nivell és adequat per a estudiants de batxillerat que vulguin aprofundir en el fonament dels nombres i també per a professorat que vulgui disposar d'un material estructurat, rigorós i aplicable a l'aula.

Introducció

Els nombres naturals apareixen de manera natural quan volem comptar objectes. Comptem alumnes, llibres, dies, passos o resultats. Aquesta necessitat porta al conjunt

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

Ara bé, les matemàtiques no es limiten a donar noms als nombres que fem servir. També busquen entendre quina estructura tenen i quines propietats se'n poden deduir. Per això, en aquesta unitat els nombres naturals no s'introdueixen només com una llista infinita, sinó a partir dels axiomes de Peano, que formalitzen la idea de començar per 0 i anar comptant d'un en un.

A partir d'aquesta estructura inicial es defineixen les operacions de suma i producte, l'ordre dels naturals, la divisibilitat, el màxim comú divisor, el mínim comú múltiple i el principi d'inducció. Aquestes eines permeten justificar resultats que sovint s'utilitzen de manera mecànica, però que tenen una base matemàtica precisa.

Tanmateix, els nombres naturals no són suficients per descriure totes les situacions. Si volem representar pèrdues, deutes, temperatures sota zero, diferències o desplaçaments en sentits oposats, necessitem ampliar el conjunt dels naturals. Així apareixen els nombres enters:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

En aquesta unitat construirem $\mathbb{Z}$ a partir de $\mathbb{N}$, considerant classes d'equivalència de parelles de naturals. Aquesta construcció permet entendre formalment per què un enter pot interpretar-se com una diferència entre dos naturals.

El pas de $\mathbb{N}$ a $\mathbb{Z}$ es pot resumir en la inclusió

$$\mathbb{N} \subset \mathbb{Z},$$

entesa a través de la identificació de cada natural n amb l'enter $[(n, 0)]$. Aquesta ampliació conserva les operacions dels naturals i, al mateix temps, permet resoldre equacions com

$$x + a = b$$

també quan $b < a$.

Els objectius principals d'aquesta unitat són:

- comprendre el paper dels axiomes de Peano i del principi d'inducció;
- definir recursivament la suma, el producte i les potències en $\mathbb{N}$;
- estudiar l'ordre, la divisibilitat, el màxim comú divisor i el mínim comú múltiple en $\mathbb{N}$;

- construir els nombres enters com a classes d'equivalència de parelles de naturals;
- definir la suma, l'oposat, la resta, el producte i l'ordre en $\mathbb{Z}$;
- treballar el valor absolut, la divisió amb residu i la divisibilitat en els enters;
- aplicar aquests conceptes a situacions quotidianes mitjançant problemes de modelització;
- consolidar els continguts amb exercicis proposats i tests interactius.

D'aquesta manera, la unitat combina tres perspectives: la construcció rigorosa dels nombres, la pràctica tècnica amb les seves propietats i l'aplicació dels conceptes a situacions concretes.

1 Teoria

1.1 Els nombres naturals

Els nombres acompanyen l'ésser humà des dels orígens del pensament. Tot va començar amb la necessitat de comptar. Si simbolitzem amb un palet | la quantitat corresponent a una cosa, amb dos palets || representem dues coses, i així successivament. Cada símbol nou succeeix l'anterior afegint-hi un palet més, i és fàcil pensar que això és així indefinidament. Podríem considerar el conjunt format per la col·lecció d'aquests símbols i anomenar-lo el conjunt per a comptar objectes.

Ara bé, és evident que aquesta manera de fer-ho no és gens eficient; només cal pensar en una quantitat gran d'objectes. Tanmateix, podem millorar la nostra capacitat de recompte si agrupem els palets d'alguna manera. Per exemple, ||| ||| ||| || simbolitza quatre agrupacions de tres palets més dos palets. Expressat aritmèticament, tenim $4 \cdot 3 + 2 = 14$ palets. Si en lloc d'agrupar-los de 3 en 3 ho fem de 10 en 10, ||||| ||||| ||||, tenim $1 \cdot 10 + 4 = 14$. I si la quantitat és molt gran podem agrupar-los també de 100 en 100, de 1000 en 1000, etc.

Aquesta idea és precisament la que dona lloc al sistema de numeració decimal, segons el qual fem ús dels dígit 0, 1, 2, 3, 4, 5, 6, 7, 8 i 9 per representar qualsevol quantitat. Quan escrivim 321 volem expressar la quantitat

$$1 + 2 \cdot 10 + 3 \cdot 100 = 321.$$

Cal observar dos fets importants. En primer lloc, el sistema de numeració és **posicional**: les expressions 123 i 132 simbolitzen dues quantitats diferents ja que

$$3 + 2 \cdot 10 + 1 \cdot 100 \neq 2 + 3 \cdot 10 + 1 \cdot 100.$$

En segon lloc, el dígit 0 és imprescindible per poder distingir 107 i 17:

$$1 \cdot 100 + 0 \cdot 10 + 7 \neq 1 \cdot 10 + 7.$$

Observa en aquest últim cas que en 107 hem fet una agrupació de 100 i cap de 10, mentre que en 17 hem fet 1 agrupació de 10 i cap de 100.

D'aquesta manera intuïtiva hem construït un conjunt de nombres que ens permet comptar quantitats o comptar objectes. Ara bé, des d'un punt de vista matemàtic aquesta forma d'introduir el conjunt no és prou rigorosa. Cal fer-ho mitjançant el llenguatge propi de les matemàtiques, tal com s'ha estudiat a *Lògica, Raonament i Demostració* i *Conjunts, Relacions i Aplicacions*. El que farem serà definir el conjunt dels nombres naturals per la seva **estructura** i no pel que són. Aquesta és precisament la idea que recullen els axiomes de Peano, que tractarem tot seguit.

1.1.1 Axiomes de Peano

Intuïtivament, els axiomes de Peano formalitzen la idea de comptar mitjançant cinc principis senzills:

1. Cal reconèixer que, a vegades, no cal comptar res.
2. Si hem comptat objectes i encara n'hi ha més, sempre podem comptar un objecte més.
3. No podem comptar un objecte més si no hi ha res.
4. Només hi ha una manera de comptar un objecte més.
5. Sempre comptem de la mateixa manera.

Aquests cinc principis, expressats en forma matemàtica, donen lloc als axiomes que caracteritzen el conjunt dels nombres naturals.

Anomenem **conjunt dels nombres naturals**, i el denotem per $\mathbb{N}$, un conjunt dotat d'una aplicació $S : \mathbb{N} \rightarrow \mathbb{N}$, anomenada **successor**, que assigna a cada natural n el seu **següent** o **successor** $S(n)$, i que compleix les propietats següents:

1. $0 \in \mathbb{N}$.
2. Si $n \in \mathbb{N}$, aleshores $S(n) \in \mathbb{N}$.
3. No existeix $n \in \mathbb{N}$ tal que $S(n) = 0$.
4. Si $S(m) = S(n)$, aleshores $m = n$.
5. Si $K \subseteq \mathbb{N}$, $0 \in K$ i $(\forall n)(n \in K \implies S(n) \in K)$, llavors $K = \mathbb{N}$.

El cinquè axioma es coneix com el **principi d'inducció** perquè permet establir propietats per a un nombre infinit de casos sense haver de donar un nombre infinit de proves. Concretament, si $P(n)$ és una propietat sobre $\mathbb{N}$ i comprovem que $P(0)$ és certa (**cas base**), i que per a cada $n \in \mathbb{N}$, si $P(n)$ és certa (**hipòtesi d'inducció**) llavors $P(S(n))$ també ho és (**pas inductiu**), aleshores el principi d'inducció ens permet concloure que $P(n)$ és certa per a tot $n \in \mathbb{N}$. Per això aquest principi és la base de les demostracions per inducció.

Observació 1.1

Una manera equivalent d'introduir els nombres naturals és la següent. $\mathbb{N}$ és el conjunt amb les propietats:

1. $\mathbb{N}$ té un element distingit que simbolitzem per 0. També es podria prendre 1 com a element distingit, però aquí no ho farem perquè volem distingir clarament l'estructura algebraica de $\mathbb{N}$.
2. Hi ha una aplicació $S : \mathbb{N} \rightarrow \mathbb{N}$ anomenada successor.
3. S és injectiva.
4. 0 no pertany al recorregut de S . En particular, S no és exhaustiva.
5. (Principi d'inducció) Si $K \subseteq \mathbb{N}$, $0 \in K$ i $(\forall n)(n \in K \implies S(n) \in K)$, llavors $K = \mathbb{N}$.

La propietat 3 és equivalent a l'axioma 4 original; la propietat 4 és equivalent a l'axioma 3; i la propietat 2 és equivalent a l'axioma 2.

Vegem ara un primer exemple senzill de com es treballa amb els axiomes de Peano.

Exemple 1.1

Provem que $4 \neq 1$.

Solució

Ho farem per reducció a l'absurd. Suposem que $4 = 1$. Aleshores

$$S(S(S(S(0)))) = S(0).$$

Aplicant l'axioma 4 de Peano, deduïm que $S(S(S(0))) = 0$. Ara bé, això és impossible per l'axioma 3 de Peano, ja que $S(S(0)) \in \mathbb{N}$ i el successor de cap natural no pot ser 0. Per tant, queda provat que $4 \neq 1$.

Vegem ara un altre exemple, aquest cop fent ús del principi d'inducció.

Exemple 1.2

Si $n \in \mathbb{N}$ i $n \neq 0$, aleshores existeix $m \in \mathbb{N}$ tal que $S(m) = n$.

Solució

Considerem la propietat

$$P(n) := \text{"Si } n \in \mathbb{N} \text{ i } n \neq 0, \text{ aleshores hi ha } m \in \mathbb{N} \text{ tal que } S(m) = n\text{"}.$$

Volem provar que és certa per a tot $n \in \mathbb{N}$, i ho farem per inducció.

Cas base. $P(0)$ és certa perquè la implicació té antecedent fals (la hipòtesi $n \neq 0$ no es compleix quan $n = 0$).

Pas inductiu. Suposem que $P(n)$ és certa (hipòtesi d'inducció). Volem veure que $P(S(n))$ també ho és. Ara bé, si $S(n) \neq 0$, podem prendre $m = n$ i tenim $S(m) = S(n)$ amb $m \in \mathbb{N}$, i per tant $P(S(n))$ és certa. Pel principi d'inducció, $P(n)$ és certa per a tot $n \in \mathbb{N}$.

Exemple 1.3

Si $n \in \mathbb{N}$, llavors o $n = 0$ o bé n s'obté aplicant S a 0 un nombre finit de vegades.

Solució

Considerem la propietat

$$P(n) := \text{"}n = 0 \text{ o } n \text{ s'obté aplicant } S \text{ a } 0 \text{ un nombre finit de vegades"}.$$

Ho farem per inducció.

Cas base. $P(0)$ és certa de manera trivial.

Pas inductiu. Suposem $P(n)$ certa. Si $n = 0$, llavors $S(n) = S(0)$, i $S(0)$ s'obté aplicant S una vegada a 0. Si $n \neq 0$, per hipòtesi d'inducció n s'obté aplicant S a 0 un cert nombre k de vegades. Aleshores $S(n)$ s'obté aplicant S exactament una vegada més a 0, és a dir, un nombre finit de vegades. Pel principi d'inducció, $P(n)$ és certa per a tot $n \in \mathbb{N}$.

El resultat de l'exemple anterior justifica que puguem escriure els nombres naturals com

$$0, S(0), S(S(0)), S(S(S(0))), \dots$$

i, fent servir la notació tradicional,

$$1 := S(0), \quad 2 := S(S(0)), \quad 3 := S(S(S(0))), \quad \dots$$

de manera que podem expressar el conjunt dels nombres naturals com

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

1.1.2 Recursió

Els nombres naturals permeten introduir el concepte fonamental de **recursió**. Intuïtivament, diem que una definició és recursiva quan per determinar un objecte donem, d'una banda, un valor inicial i, de l'altra, una regla que permet obtenir el cas següent a partir del cas anterior.

Per exemple, podem definir una successió de nombres naturals $(u_n)_{n \in \mathbb{N}}$ de la manera següent:

$$\begin{cases} u_0 = 0, \\ u_{S(n)} = S(u_n). \end{cases}$$

Aquesta definició ens diu que el primer terme és 0 i que cada terme següent s'obté prenent el successor del terme anterior. Així,

$$u_0 = 0, \quad u_1 = S(u_0) = S(0) = 1,$$

$$u_2 = S(u_1) = S(1) = 2, \quad u_3 = S(u_2) = S(2) = 3,$$

i així successivament.

Per tant, aquesta definició recursiva construeix la successió

$$0, 1, 2, 3, \dots$$

sense necessitat d'haver definit encara ni la suma ni la multiplicació.

Un altre exemple senzill de definició recursiva és el següent. Definim una successió de nombres naturals $(v_n)_{n \in \mathbb{N}}$ per

$$\begin{cases} v_0 = 0, \\ v_{S(n)} = S(S(v_n)). \end{cases}$$

Aquesta definició ens diu que el primer terme és 0 i que cada terme següent s'obté aplicant dues vegades el successor al terme anterior. Així,

$$v_0 = 0,$$

$$v_1 = S(S(u_0)) = S(S(0)) = 2,$$

$$v_2 = S(S(v_1)) = S(S(2)) = 4,$$

$$v_3 = S(S(v_2)) = S(S(4)) = 6,$$

i així successivament.

D'aquesta manera obtenim la successió

$$0, 2, 4, 6, \dots$$

Observeu amb aquests exemples com hem definit successions de nombres naturals sense haver definit encara ni l'addició ni la multiplicació. Només hem fet servir el nombre inicial 0 i l'aplicació successor.

1.1.3 Addició de nombres naturals

L'operació d'addició de nombres naturals es defineix per recursió. Tot i que la nostra intuïció ens permet entendre la definició sense dificultat, en un desenvolupament complet caldria justificar que existeix una única operació que compleix les regles següents. Aquesta justificació, però, l'ometrem aquí.

Definició 1.1

Per a tots $a, b \in \mathbb{N}$ definim

$$\begin{cases} a + 0 = a, \\ a + S(b) = S(a + b). \end{cases}$$

El nombre natural $a + b$ s'anomena **suma** dels nombres a i b , i diem que a i b són els **sumands**.

1.1.3.1 Propietats de la suma

Un conjunt dotat d'una operació és una **estructura algebraica**. Aquesta estructura s'anomena **monoide** quan l'operació és associativa i té element neutre. A més, si l'operació és commutativa, el monoide s'anomena **commutatiu**. Provarem tot seguit que els naturals tenen estructura de monoide commutatiu amb l'operació d'addició.

Proposició 1.1

Per a tot $a \in \mathbb{N}$, $a + 0 = a$ i $0 + a = a$. Això vol dir que 0 és l'**element neutre** de la suma.

Demostració

La igualtat $a + 0 = a$ es compleix per definició. Per a la igualtat $0 + a = a$, fem inducció sobre a .

Cas base. Si $a = 0$, llavors $0 + 0 = 0$ per definició.

Pas inductiu. Suposem $0 + a = a$ (hipòtesi d'inducció). Aplicant la definició i la hipòtesi d'inducció:

$$0 + S(a) = S(0 + a) = S(a).$$

Pel principi d'inducció, la propietat val per a tot $a \in \mathbb{N}$.

Observació 1.2

A partir de la proposició anterior i de la definició podem escriure $S(n) = n + 1$ per a tot $n \in \mathbb{N}$. En efecte,

$$S(n) = S(n + 0) = n + S(0) = n + 1,$$

perquè per notació $S(0) := 1$.

Abans de demostrar les propietats associativa i commutativa de la suma, provarem la següent propietat.

Proposició 1.2

Per a tots $a, b \in \mathbb{N}$, es compleix

$$S(a) + b = S(a + b).$$

Demostració

Fixem $a \in \mathbb{N}$ i demostrem la propietat per inducció sobre b .

Per a $b = 0$, tenim

$$S(a) + 0 = S(a),$$

per la definició de la suma. D'altra banda,

$$S(a + 0) = S(a),$$

ja que $a + 0 = a$. Per tant,

$$S(a) + 0 = S(a + 0).$$

Suposem ara que la propietat és certa per a un cert $b \in \mathbb{N}$, és a dir,

$$S(a) + b = S(a + b).$$

Volem demostrar que també és certa per a $S(b)$.

Per la definició de la suma,

$$S(a) + S(b) = S(S(a) + b).$$

Per la hipòtesi d'inducció,

$$S(S(a) + b) = S(S(a + b)).$$

D'altra banda, com que

$$a + S(b) = S(a + b),$$

tenim

$$S(a + S(b)) = S(S(a + b)).$$

Així,

$$S(a) + S(b) = S(a + S(b)).$$

Per tant, la propietat és certa per a $S(b)$. Pel principi d'inducció, queda provat que

$$S(a) + b = S(a + b)$$

per a tots $a, b \in \mathbb{N}$.

Proposició 1.3

Per a tots $a, b, c \in \mathbb{N}$, la suma és **associativa**:

$$a + (b + c) = (a + b) + c,$$

i **commutativa**:

$$a + b = b + a.$$

Demostració

Associativitat. Fem inducció sobre c .

Cas base. Si $c = 0$, llavors $a + (b + 0) = a + b = (a + b) + 0$ per definició.

Pas inductiu. Suposem $a + (b + c) = (a + b) + c$. Aleshores

$$a + (b + S(c)) = a + S(b + c) = S(a + (b + c)) = S((a + b) + c) = (a + b) + S(c).$$

Commutativitat. Fem inducció sobre b .

Cas base. Si $b = 0$, per la proposició anterior $a + 0 = 0 + a = a$.

Pas inductiu. Suposem $a + b = b + a$. Aleshores,

$$\begin{aligned} a + S(b) &= S(a + b) && \text{per definició de suma} \\ &= S(b + a) && \text{per la hipòtesi d'inducció} \\ &= S(b) + a && \text{per la proposició 1.2.} \end{aligned}$$

Exemple 1.4 (Propietat de simplificació)

Per a tots $a, b, c \in \mathbb{N}$, si $c + a = c + b$, aleshores $a = b$.

Solució

Fem inducció sobre c .

Cas base. Si $c = 0$, llavors $0 + a = 0 + b$, així que $a = b$.

Pas inductiu. Suposem que $c + a = c + b$ implica $a = b$. Volem provar que

$S(c) + a = S(c) + b$ també implica $a = b$. En efecte, per la commutativitat de la suma:

$$S(c) + a = S(c) + b \implies a + S(c) = b + S(c) \implies S(a + c) = S(b + c).$$

Per l'axioma 4 de Peano, $a + c = b + c$, i de nou per commutativitat $c + a = c + b$. Per la hipòtesi d'inducció, $a = b$.

1.1.4 Multiplicació de nombres naturals

La multiplicació de nombres naturals també es defineix per recursió. Igual que abans, no justificarem aquí l'existència i la unicitat d'aquesta operació.

Definició 1.2

Per a tots $a, b \in \mathbb{N}$ definim

$$\begin{cases} a \cdot 0 = 0, \\ a \cdot S(b) = a \cdot b + a. \end{cases}$$

El nombre natural $a \cdot b$ s'anomena **producte** dels nombres a i b , i a i b s'anomenen **factors**.

1.1.4.1 Propietats de la multiplicació

Igual que el conjunt dels naturals té estructura de monoide commutatiu amb la suma, també té estructura de monoide commutatiu amb la multiplicació. A més, la multiplicació és distributiva respecte de la suma.

Proposició 1.4

Per a tot $a \in \mathbb{N}$, $a \cdot 0 = 0$ i $0 \cdot a = 0$.

Demostració

La igualtat $a \cdot 0 = 0$ es compleix per definició. Per a la igualtat $0 \cdot a = 0$, fem inducció sobre a .

Cas base. Si $a = 0$, és immediat que $0 \cdot 0 = 0$ per definició.

Pas inductiu. Suposem $0 \cdot a = 0$. Aplicant la definició de multiplicació i la propietat de l'element neutre de la suma:

$$0 \cdot S(a) = 0 \cdot a + 0 = 0 + 0 = 0.$$

Per tant, $0 \cdot a = 0$ per a tot $a \in \mathbb{N}$.

Proposició 1.5

Per a tot $a \in \mathbb{N}$, $a \cdot 1 = a$ i $1 \cdot a = a$. Això vol dir que 1 és l'**element neutre** de la multiplicació.

Demostració

En primer lloc, aplicant que $S(0) = 1$, la definició de multiplicació i la propietat de l'element neutre de la suma:

$$a \cdot 1 = a \cdot S(0) = a \cdot 0 + a = 0 + a = a.$$

Per a la igualtat $1 \cdot a = a$, fem inducció sobre a .

Cas base. Si $a = 0$, $1 \cdot 0 = 0$ per la proposició anterior.

Pas inductiu. Suposem $1 \cdot a = a$. Aleshores

$$1 \cdot S(a) = 1 \cdot a + 1 = a + 1 = a + S(0) = S(a + 0) = S(a).$$

Proposició 1.6

Per a tot $a, b, c \in \mathbb{N}$, la multiplicació és **associativa**,

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

i **distributiva respecte de la suma**,

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Demostració

Distributivitat. Fem inducció sobre c .

Cas base. Si $c = 0$, és immediat que $a \cdot (b + 0) = a \cdot b = a \cdot b + a \cdot 0$.

Pas inductiu. Suposem $a \cdot (b + c) = a \cdot b + a \cdot c$. Aleshores

$$\begin{aligned} a \cdot (b + S(c)) &= a \cdot S(b + c) \\ &= a \cdot (b + c) + a \\ &= (a \cdot b + a \cdot c) + a \\ &= a \cdot b + (a \cdot c + a) \\ &= a \cdot b + a \cdot S(c). \end{aligned}$$

Associativitat. Fem inducció sobre c .

Cas base. Si $c = 0$, $a \cdot (b \cdot 0) = (a \cdot b) \cdot 0 = 0$.

Pas inductiu. Suposem $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. Aplicant la definició de multiplicació i la propietat distributiva:

$$\begin{aligned} a \cdot (b \cdot S(c)) &= a \cdot (b \cdot c + b) \\ &= a \cdot (b \cdot c) + a \cdot b \\ &= (a \cdot b) \cdot c + a \cdot b \\ &= (a \cdot b) \cdot S(c). \end{aligned}$$

Abans de demostrar la propietat commutativa de la multiplicació, provarem la propietat següent.

Proposició 1.7

Per a tots $a, b \in \mathbb{N}$, es compleix

$$S(a) \cdot b = a \cdot b + b.$$

Demostració

Fixem $a \in \mathbb{N}$ i demostrem la propietat per inducció sobre b .

Per a $b = 0$, tenim

$$S(a) \cdot 0 = 0,$$

per la definició del producte. D'altra banda,

$$a \cdot 0 + 0 = 0 + 0 = 0.$$

Per tant,

$$S(a) \cdot 0 = a \cdot 0 + 0.$$

Suposem ara que la propietat és certa per a un cert $b \in \mathbb{N}$, és a dir,

$$S(a) \cdot b = a \cdot b + b.$$

Volem demostrar que també és certa per a $S(b)$.

Per la definició del producte,

$$S(a) \cdot S(b) = S(a) \cdot b + S(a).$$

Per la hipòtesi d'inducció,

$$S(a) \cdot S(b) = (a \cdot b + b) + S(a).$$

Per l'associativitat de la suma,

$$(a \cdot b + b) + S(a) = a \cdot b + (b + S(a)).$$

Ara bé, per la definició de la suma i per la commutativitat de la suma,

$$b + S(a) = S(b + a) = S(a + b) = a + S(b).$$

Així,

$$S(a) \cdot S(b) = a \cdot b + (a + S(b)).$$

Per l'associativitat de la suma,

$$a \cdot b + (a + S(b)) = (a \cdot b + a) + S(b).$$

Finalment, per la definició del producte,

$$a \cdot b + a = a \cdot S(b).$$

Per tant,

$$S(a) \cdot S(b) = a \cdot S(b) + S(b).$$

Això prova la propietat per a $S(b)$. Pel principi d'inducció, queda demostrat que

$$S(a) \cdot b = a \cdot b + b$$

per a tots $a, b \in \mathbb{N}$.

Proposició 1.8

La multiplicació és **commutativa**: $a \cdot b = b \cdot a$ per a tots $a, b \in \mathbb{N}$.

Demostració

Fem inducció sobre b .

Cas base. Si $b = 0$, és clar que $a \cdot 0 = 0 \cdot a = 0$.

Pas inductiu. Suposem $a \cdot b = b \cdot a$. Aleshores,

$$\begin{aligned} a \cdot S(b) &= a \cdot b + a && \text{per definició del producte} \\ &= b \cdot a + a && \text{per la hipòtesi d'inducció} \\ &= S(b) \cdot a && \text{per la proposició 1.7.} \end{aligned}$$

Exemple 1.5

Per a tot $a \in \mathbb{N}$ es compleix $S(a) \neq a$.

Solució

Fem inducció sobre a .

Cas base. Si $a = 0$, $S(0) \neq 0$ per l'axioma 3 de Peano.

Pas inductiu. Suposem $S(a) \neq a$. Pel contrarecíproc de l'axioma 4 de Peano, si $S(a) \neq a$, llavors $S(S(a)) \neq S(a)$. Per tant, la propietat també és certa per a $S(a)$.

Exemple 1.6 (El factorial)

Definim el factorial d'un nombre natural per recursió:

$$\begin{cases} 0! := 1, \\ S(n)! := S(n) \cdot n!. \end{cases}$$

Així,

$$\begin{aligned} 0! &= 1, \\ 1! &= S(0)! = S(0) \cdot 0! = 1 \cdot 1 = 1, \\ 2! &= S(1)! = S(1) \cdot 1! = 2 \cdot 1 = 2, \\ 3! &= S(2)! = S(2) \cdot 2! = 3 \cdot 2 = 6. \end{aligned}$$

Exemple 1.7

Expressa per recursió la successió de Fibonacci

$$f = (0, 1, 1, 2, 3, 5, 8, 13, \dots).$$

Per fer-ho, observa que cada terme a partir del tercer s'obté com a suma dels dos termes anteriors.

Solució

Per a tot $n \in \mathbb{N}$ definim:

$$\begin{cases} f(0) = 0, \\ f(1) = 1, \\ f(n+2) = f(n) + f(n+1). \end{cases}$$

Observa que

$$\begin{aligned} f(2) &= f(0+2) = f(0) + f(1) = 0 + 1 = 1, \\ f(3) &= f(1+2) = f(1) + f(2) = 1 + 1 = 2, \\ f(4) &= f(2+2) = f(2) + f(3) = 1 + 2 = 3, \\ &\vdots \end{aligned}$$

1.1.5 L'ordre dels nombres naturals

A partir de l'addició podem definir en el conjunt $\mathbb{N}$ una relació d'ordre de la manera següent.

Definició 1.3

Per a tots $a, b \in \mathbb{N}$, diem que a és **més gran o igual que** b , i ho escrivim $a \geq b$ o $b \leq a$, si i només si existeix $n \in \mathbb{N}$ tal que $a = b + n$. Diem que a és **més gran estrictament que** b , i ho escrivim $a > b$ o $b < a$, si i només si $a \geq b$ i $a \neq b$. Direm que a és **positiu** si i només si $a > 0$.

Abans de demostrar que $\leq$ és una relació d'ordre total en $\mathbb{N}$, necessitem un resultat tècnic.

Proposició 1.9

- (i) Per a qualsevol $a \in \mathbb{N} \setminus \{0\}$, es compleix $a + b \neq b$ per a tot $b \in \mathbb{N}$.
- (ii) Per a tots $a, b \in \mathbb{N}$, si $a \neq 0$, aleshores $a + b \neq 0$.

Demostració

- (i) Fem inducció sobre b . Si $b = 0$, com $a \neq 0$ tenim $a + 0 = a \neq 0$. Suposem $a + b \neq b$. Per la definició de suma, la hipòtesi d'inducció i el contrarecíproc de l'axioma 4 de Peano,

$$a + S(b) = S(a + b) \neq S(b).$$

Així, $a + b \neq b$ per a tot $b \in \mathbb{N}$.

- (ii) Fixem $a \in \mathbb{N}$ amb $a \neq 0$ i fem inducció sobre b .

Si $b = 0$, aleshores

$$a + 0 = a \neq 0.$$

Suposem $a + b \neq 0$. Per la definició de suma, la hipòtesi d'inducció i el

contrarecíproc de l'axioma 4 de Peano,

$$a + S(b) = S(a + b) \neq 0.$$

Així, $a + b \neq 0$ per a tot $b \in \mathbb{N}$.

Proposició 1.10

La relació $\leq$ és una relació d'ordre parcial sobre $\mathbb{N}$.

Demostració

Reflexivitat. És clar que $a \leq a$ per a tot $a \in \mathbb{N}$, ja que $a = a + 0$.

Antisimetria. Suposem que $a \leq b$ i $b \leq a$. Per la definició de l'ordre, existeixen $m, n \in \mathbb{N}$ tals que

$$b = a + m \quad \text{i} \quad a = b + n.$$

Substituint la primera igualtat en la segona, obtenim

$$a = (a + m) + n.$$

Per l'associativitat de la suma,

$$a = a + (m + n).$$

Per la commutativitat de la suma,

$$a = (m + n) + a.$$

Si $m + n \neq 0$, aleshores, per la Proposició 1.9, aplicada a $m + n$ i a , apartat (i), tindríem

$$(m + n) + a \neq a,$$

cosa que contradiu la igualtat anterior. Per tant, $m + n = 0$. Ara bé, si $m \neq 0$, per la Proposició 1.9, apartat (ii), tindríem $m + n \neq 0$, contradicció. Així, $m = 0$. Finalment, com que $b = a + m$, obtenim $b = a + 0 = a$. Per tant, $a = b$.

Transitivitat. Suposem que $a \leq b$ i $b \leq c$. Si $a = b$, aleshores, com que $b \leq c$, tenim $a \leq c$. Si $b = c$, aleshores, com que $a \leq b$, tenim $a \leq c$. Finalment, suposem que $a < b$ i $b < c$. Aleshores existeixen $n, m \in \mathbb{N}$, amb $n \neq 0$ i $m \neq 0$, tals que

$$b = a + n \quad \text{i} \quad c = b + m.$$

Per tant,

$$c = b + m = (a + n) + m = a + (n + m).$$

Així, existeix $n + m \in \mathbb{N}$ tal que

$$c = a + (n + m),$$

i, per definició, obtenim

$$a \leq c.$$

Teorema 1.11 (Tricotomia de l'ordre)

Per a tots $a, b \in \mathbb{N}$ es compleix exactament una de les tres condicions:

$$(i) \ a < b \quad (ii) \ a = b \quad (iii) \ b < a.$$

Demostració

Si es compleix (ii), llavors $a = b$ i per definició de $<$ s'exclouen (i) i (iii). Si no es compleix (ii) però es complissin (i) i (iii) alhora, la propietat antisimètrica de $\leq$ ens portaria a contradicció. Per tant, com a màxim una de les tres condicions pot ser certa.

Ens queda provar que almenys una de les tres es compleix. Ho farem per inducció sobre a .

Cas base. Si $a = 0$, hem de provar que $0 < b$ o $0 = b$ o $b < 0$. Si $b = 0$, és immediat. Si $b \neq 0$, per l'exemple 1.2 existeix $m \in \mathbb{N}$ tal que $S(m) = b$. Per l'observació 1.2, $m + 1 = 1 + m = b$, i per definició d'ordre $b > 0$. Notem que no és possible que $b < 0$, ja que això voldria dir $0 = b + n$ amb $b \neq 0$ i $n \in \mathbb{N}$, contradint la proposició 1.9, apartat (ii).

Pas inductiu. Suposem que la propietat és certa per a un cert $a \in \mathbb{N}$. És a dir, per a tot $b \in \mathbb{N}$, es compleix exactament una de les tres possibilitats:

$$a < b, \quad a = b, \quad b < a.$$

Volem provar que, per a tot $b \in \mathbb{N}$, es compleix exactament una de les tres possibilitats:

$$S(a) < b, \quad S(a) = b, \quad b < S(a).$$

Fixem $b \in \mathbb{N}$. Per la hipòtesi d'inducció aplicada a a i b , tenim tres casos.

Cas 1: $a = b$.

Aleshores

$$S(a) = S(b).$$

Com que

$$S(b) = b + 1,$$

obtenim

$$b < S(a).$$

Cas 2: $b < a$.

Com que $b < a$ i $a < S(a)$, per la transitivitat de l'ordre obtenim

$$b < S(a).$$

Cas 3: $a < b$.

Com que $a < b$, existeix $n \in \mathbb{N}$, amb $n \neq 0$, tal que

$$b = a + n.$$

Com que $n \neq 0$, existeix $k \in \mathbb{N}$ tal que

$$n = S(k).$$

Per tant,

$$b = a + S(k) = S(a + k).$$

Ara distingim dos subcasos.

Si $k = 0$, aleshores

$$b = S(a + 0) = S(a).$$

Per tant,

$$S(a) = b.$$

Si $k \neq 0$, aleshores

$$b = S(a + k).$$

D'altra banda, com que

$$S(a) + k = S(a + k),$$

tenim

$$b = S(a) + k.$$

Com que $k \neq 0$, per la definició de l'ordre estricta obtenim

$$S(a) < b.$$

Així, en tots els casos obtenim una de les tres possibilitats:

$$S(a) < b, \quad S(a) = b, \quad b < S(a).$$

Corol·lari 1.12

La relació d'ordre sobre $\mathbb{N}$ és total.

Demostració

Recordem que $\leq$ és total si per a qualssevol $a, b \in \mathbb{N}$ es compleix $a \leq b$ o $b \leq a$. Això és immediat del teorema anterior.

Definició 1.4

Sigui $A \subseteq \mathbb{N}$. Diem que $n \in A$ és el **primer element** o **element mínim** de A si $n \leq m$ per a tot $m \in A$.

És immediat comprovar que si hi ha un primer element, aquest és únic. En efecte, si n'hi haguessin dos, diguem n_1 i n_2 , llavors $n_1 \leq n_2$ per ser n_1 primer element, i $n_2 \leq n_1$ per ser n_2 primer element. Per la propietat antisimètrica, $n_1 = n_2$.

1.1.6 Divisibilitat en els nombres naturals

Una de les propietats més importants dels nombres naturals és la possibilitat d'estudiar quan un nombre es pot obtenir multiplicant-ne un altre per un cert factor. Aquesta idea dona lloc a la noció de divisibilitat.

Definició 1.5

Siguin $a, b \in \mathbb{N}$, amb $a \neq 0$. Diem que a **divideix** b , i escrivim

$$a \mid b,$$

si existeix $q \in \mathbb{N}$ tal que

$$b = a \cdot q.$$

En aquest cas, diem que a és un **divisor** de b , que b és un **múltiple** de a , i que q és el **quocient** de la divisió exacta de b per a .

Exemple 1.8

Tenim

$$3 \mid 12,$$

perquè existeix $4 \in \mathbb{N}$ tal que

$$12 = 3 \cdot 4.$$

Per tant, 3 és un divisor de 12 i 12 és un múltiple de 3.

Proposició 1.13 (Propietats bàsiques de la divisibilitat)

Siguin $a, b, c \in \mathbb{N}$, amb $a \neq 0$ i $b \neq 0$. Es compleixen les propietats següents:

- (i) $a \mid a$,
- (ii) $1 \mid a$,
- (iii) $a \mid 0$,
- (iv) si $a \mid b$ i $b \mid c$, aleshores $a \mid c$.

Demostració

(i) Com que

$$a = a \cdot 1,$$

tenim $a \mid a$.

(ii) Com que

$$a = 1 \cdot a,$$

tenim $1 \mid a$.

(iii) Com que

$$0 = a \cdot 0,$$

tenim $a \mid 0$.

(iv) Suposem que $a \mid b$ i $b \mid c$. Aleshores existeixen $q, r \in \mathbb{N}$ tals que

$$b = a \cdot q \quad \text{i} \quad c = b \cdot r.$$

Substituint la primera igualtat en la segona, obtenim

$$c = (a \cdot q) \cdot r.$$

Per l'associativitat del producte,

$$c = a \cdot (q \cdot r).$$

Com que $q \cdot r \in \mathbb{N}$, concloem que

$$a \mid c.$$

Definició 1.6

Siguin $a, b \in \mathbb{N}$, amb $a \neq 0$ i $b \neq 0$. Un nombre natural d és un **divisor comú** de a i b si

$$d \mid a \quad \text{i} \quad d \mid b.$$

El **màxim comú divisor** de a i b , que denotem per

$$\text{mcd}(a, b),$$

és el divisor comú més gran de a i b .

Exemple 1.9

Els divisors positius de 12 són

$$1, 2, 3, 4, 6, 12,$$

i els divisors positius de 18 són

$$1, 2, 3, 6, 9, 18.$$

Els divisors comuns de 12 i 18 són

$$1, 2, 3, 6.$$

Per tant,

$$\text{mcd}(12, 18) = 6.$$

1.1.6.1 L'algorisme d'Euclides

Per calcular el màxim comú divisor de dos nombres naturals positius podem utilitzar l'**algorisme d'Euclides**. Aquest procediment es basa en la divisió amb residu.

Recordem que, si $a, b \in \mathbb{N}$ i $b \neq 0$, podem dividir a entre b i escriure

$$a = b \cdot q + r,$$

on $q, r \in \mathbb{N}$ i

$$0 \leq r < b.$$

El nombre q s'anomena **quocient** i el nombre r s'anomena **residu** de la divisió de a entre b .

La idea fonamental de l'algorisme d'Euclides és la següent: si

$$a = b \cdot q + r,$$

aleshores

$$\text{mcd}(a, b) = \text{mcd}(b, r).$$

En efecte, els divisors comuns de a i b són exactament els divisors comuns de b i r . Per això, el màxim comú divisor no canvia si substituïm el parell (a, b) pel parell (b, r) .

Així, per calcular $\text{mcd}(a, b)$, amb $a \geq b > 0$, procedim de la manera següent. Primer dividim a entre b :

$$a = b \cdot q_1 + r_1, \quad 0 \leq r_1 < b.$$

Si $r_1 = 0$, aleshores

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

Si $r_1 \neq 0$, dividim b entre r_1 :

$$b = r_1 \cdot q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

Si $r_2 = 0$, aleshores

$$\text{mcd}(a, b) = r_1.$$

Si $r_2 \neq 0$, continuem el procés:

$$r_1 = r_2 \cdot q_3 + r_3, \quad 0 \leq r_3 < r_2,$$

i així successivament.

Com que els residus

$$r_1, r_2, r_3, \dots$$

són nombres naturals que van disminuint estrictament, el procés ha d'acabar. L'últim residu no nul és el màxim comú divisor de a i b .

Exemple 1.10

Calculem

$$\text{mcd}(252, 198).$$

Dividim:

$$252 = 198 \cdot 1 + 54.$$

Per tant,

$$\text{mcd}(252, 198) = \text{mcd}(198, 54).$$

Ara dividim 198 entre 54:

$$198 = 54 \cdot 3 + 36.$$

Per tant,

$$\text{mcd}(198, 54) = \text{mcd}(54, 36).$$

Ara dividim 54 entre 36:

$$54 = 36 \cdot 1 + 18.$$

Per tant,

$$\text{mcd}(54, 36) = \text{mcd}(36, 18).$$

Finalment,

$$36 = 18 \cdot 2 + 0.$$

Com que l'últim residu no nul és 18, obtenim

$$\text{mcd}(252, 198) = 18.$$

Definició 1.7

Siguin $a, b \in \mathbb{N}$, amb $a \neq 0$ i $b \neq 0$. Un nombre natural m és un **múltiple comú** de a i b si

$$a \mid m \quad \text{i} \quad b \mid m.$$

El **mínim comú múltiple** de a i b , que denotem per

$$\text{mcm}(a, b),$$

és el múltiple comú positiu més petit de a i b .

Exemple 1.11

Els múltiples positius de 4 són

$$4, 8, 12, 16, 20, 24, \dots,$$

i els múltiples positius de 6 són

$$6, 12, 18, 24, 30, \dots$$

Els primers múltiples comuns positius de 4 i 6 són

$$12, 24, \dots$$

Per tant,

$$\text{mcm}(4, 6) = 12.$$

Observació 1.3

El mínim comú múltiple de dos nombres naturals positius existeix. En efecte, si $a, b \in \mathbb{N}$ són positius, aleshores $a \cdot b$ és un múltiple comú de a i b , ja que

$$a \mid a \cdot b \quad \text{i} \quad b \mid a \cdot b.$$

Per tant, el conjunt dels múltiples comuns positius de a i b no és buit. Pel principi del bon ordre, aquest conjunt té un element mínim.

Observació 1.4

El màxim comú divisor de dos nombres naturals positius també existeix. Els divisors comuns de a i b formen un conjunt no buit, perquè 1 divideix qualsevol nombre natural positiu. A més, cap divisor positiu d'un nombre positiu pot ser més gran que aquest nombre. Per tant, els divisors comuns de a i b estan fitats superiorment, i es pot demostrar que tenen un element màxim.

Definició 1.8

Dos nombres naturals positius a i b s'anomenen **primers entre si** si

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

Exemple 1.12

Els nombres 8 i 15 són primers entre si, perquè l'únic divisor comú positiu que tenen és 1. Per tant,

$$\text{mcd}(8, 15) = 1.$$

Definició 1.9

Un nombre natural p és **primer** si $p > 1$ i els seus únics divisors positius són 1 i p .

Exemple 1.13

El nombre 7 és primer, perquè els seus únics divisors positius són 1 i 7.

Definició 1.10

Un nombre natural $n > 1$ és **compost** si no és primer. Equivalentment, n és compost si existeixen $a, b \in \mathbb{N}$ tals que

$$n = a \cdot b,$$

amb

$$1 < a < n \quad \text{i} \quad 1 < b < n.$$

Exemple 1.14

El nombre 12 és compost, perquè

$$12 = 3 \cdot 4,$$

amb

$$1 < 3 < 12 \quad \text{i} \quad 1 < 4 < 12.$$

Observació 1.5

Els nombres 0 i 1 no són primers. Per definició, un nombre primer ha de ser més gran que 1. Així, els primers nombres primers són

$$2, 3, 5, 7, 11, 13, \dots$$

1.1.7 Principi d'inducció forta

L'axioma 5 dels axiomes de Peano és l'eina principal per provar propietats sobre $\mathbb{N}$. A la pràctica, per demostrar que la propietat $P(n)$ és certa per a tot $n \in \mathbb{N}$, s'ha de provar el cas base $P(0)$ i el pas inductiu $P(n) \implies P(S(n))$.

Tanmateix, hi ha situacions on resulta útil disposar d'una variant més forta d'aquesta tècnica. Es tracta de la **inducció forta**, que es dedueix de l'axioma 5 i resulta especialment útil en moltes demostracions.

El principi d'inducció forta és un mètode per provar que una propietat $P(n)$ és certa a partir d'un determinat nombre natural, és a dir per a tots els nombres naturals $n \geq n_0$, on n_0 és un nombre natural fix. Per fer-ho, se segueixen dos passos:

- **Cas base.** Es demostra que $P(n_0)$ és certa.
- **Pas inductiu.** S'assumeix que $P(k)$ és certa per a tots els naturals k tals que $n_0 \leq k < n$ (**hipòtesi d'inducció forta**) i s'ha de demostrar que $P(n)$ també és certa.

Un cop completats aquests dos passos, es conclou que $P(n)$ és certa per a tot $n \geq n_0$.

Vegem-ne dos exemples ben coneguts.

Exemple 1.15 (Existència de descomposició en factors primers)

Demostrem que tot nombre natural $n \geq 2$ es pot expressar com un producte d'un o més nombres primers.

Solució

Cas base. Per a $n = 2$, el nombre 2 és primer, així que es pot expressar com un producte d'un sol primer (ell mateix).

Pas inductiu. Suposem que tot nombre natural k amb $2 \leq k < n$ es pot escriure com a producte de primers. Volem provar-ho per a n . Distingim dos casos:

- Si n és primer, ja és un producte d'un sol primer (ell mateix).
- Si n és compost, per definició existeixen $a, b \in \mathbb{N}$ amb $2 \leq a < n$ i $2 \leq b < n$ tals que $n = a \cdot b$. Per la hipòtesi d'inducció forta, tant a com b es poden escriure com a productes de primers, diguem $a = p_1 \cdot p_2 \cdots p_r$ i $b = q_1 \cdot q_2 \cdots q_s$. Aleshores

$$n = p_1 \cdot p_2 \cdots p_r \cdot q_1 \cdot q_2 \cdots q_s,$$

que també és un producte de primers.

Pel principi d'inducció forta, tot $n \geq 2$ es pot expressar com a producte de primers.

Exemple 1.16 (El joc de la balança amb monedes)

Suposem que disposem d'una balança i moltes monedes de 3 grams i 5 grams. Volem demostrar que és possible pesar qualsevol quantitat de grams que sigui un nombre natural més gran o igual a 8.

Solució

Casos base. Comprovem directament els primers casos:

- Per a $n = 8$, podem pesar $8 = 3 + 5$.
- Per a $n = 9$, podem pesar $9 = 3 + 3 + 3$.
- Per a $n = 10$, podem pesar $10 = 5 + 5$.
- Per a $n = 11$, podem pesar $11 = 3 + 3 + 5$.

Pas inductiu. Suposem que podem pesar qualsevol quantitat k amb $8 \leq k < n$ i que $n \geq 12$. Aleshores $n - 3 \geq 9 \geq 8$, així que per hipòtesi d'inducció forta podem pesar $n - 3$ grams. Afegint una moneda de 3 grams, podem pesar n grams.

Pel principi d'inducció forta, podem pesar qualsevol quantitat $n \geq 8$.

Una propietat important dels nombres naturals és que estan **ben ordenats**: això significa que qualsevol conjunt no buit de nombres naturals té un primer element.

Teorema 1.14 (Principi del bon ordre)

Tot subconjunt no buit de $\mathbb{N}$ té un element mínim. És a dir, si $A \subseteq \mathbb{N}$ i $A \neq \emptyset$, aleshores existeix $m \in A$ tal que $m \leq a$ per a tot $a \in A$.

Demostració

Suposem, per reducció a l'absurd, que existeix un subconjunt no buit $A \subseteq \mathbb{N}$ que no té element mínim.

Considerem el conjunt

$$K = \{n \in \mathbb{N} : \text{cap element de } A \text{ és menor o igual que } n\}.$$

És a dir,

$$n \in K \iff \text{no existeix } a \in A \text{ tal que } a \leq n.$$

Provarem per inducció que $K = \mathbb{N}$.

En primer lloc, provem que $0 \in K$. Suposem, per contradicció, que $0 \notin K$. Per la definició de K , existiria algun $a \in A$ tal que

$$a \leq 0.$$

Per la definició de l'ordre, això vol dir que existeix $n \in \mathbb{N}$ tal que

$$0 = a + n.$$

Si $a \neq 0$, per la proposició 1.9, apartat (ii), tindríem

$$a + n \neq 0,$$

contradicció. Per tant, necessàriament

$$a = 0.$$

Així, $0 \in A$.

Ara bé, per a tot $m \in \mathbb{N}$ tenim

$$0 \leq m,$$

ja que $m = 0 + m$. En particular, $0 \leq x$ per a tot $x \in A$. Per tant, 0 seria l'element mínim de A , en contradicció amb la hipòtesi que A no té element mínim.

Així doncs,

$$0 \in K.$$

Suposem ara que $n \in K$. Volem provar que $S(n) \in K$.

Per contradicció, suposem que $S(n) \notin K$. Aleshores existeix algun $a \in A$ tal que

$$a \leq S(n).$$

Com que $n \in K$, no hi ha cap element de A que sigui menor o igual que n . Per tant, aquest element a no pot satisfer $a \leq n$.

Ara bé, com que $a \leq S(n)$, per la definició de l'ordre existeix $r \in \mathbb{N}$ tal que

$$S(n) = a + r.$$

Si $r = 0$, aleshores

$$S(n) = a + 0 = a,$$

i per tant

$$a = S(n).$$

Suposem, en canvi, que $r \neq 0$. Aleshores existeix $t \in \mathbb{N}$ tal que

$$r = S(t).$$

Per tant,

$$S(n) = a + r = a + S(t) = S(a + t).$$

Com que el successor és injectiu, obtenim

$$n = a + t.$$

Això vol dir que

$$a \leq n,$$

cosa que contradiu el fet que $n \in K$.

Per tant, no pot ser $r \neq 0$, i necessàriament ha de ser $r = 0$. Així,

$$a = S(n).$$

Per tant,

$$S(n) \in A.$$

A més, com que $n \in K$, cap element de A és menor o igual que n . Això vol dir que no hi ha cap element de A menor que $S(n)$. Per tant, tot element de A és més gran o igual que $S(n)$.

Així, $S(n)$ seria l'element mínim de A , contradient de nou la hipòtesi que A no té element mínim. Aquesta contradicció prova que

$$S(n) \in K.$$

Hem demostrat que $0 \in K$ i que, si $n \in K$, aleshores $S(n) \in K$. Pel principi d'inducció,

$$K = \mathbb{N}.$$

Això significa que no existeix cap element de A menor o igual que algun nombre natural. Però això és impossible, perquè A és no buit: si $a \in A$, aleshores certament

$$a \leq a.$$

Per tant, hem arribat a una contradicció.

Concloem que tot subconjunt no buit de $\mathbb{N}$ té un element mínim.

Proposició 1.15

Siguin a i b nombres naturals. Si $a \cdot b = 0$, aleshores $a = 0$ o $b = 0$. En particular, si a i b són tots dos positius, $a \cdot b$ també és positiu.

Demostració

Demostrem la propietat per inducció sobre b .

Per a $b = 0$, el resultat és immediat, ja que aleshores una de les dues alternatives,

$$a = 0 \quad \text{o} \quad b = 0,$$

ja es compleix.

Suposem ara que la propietat és certa per a un cert $b \in \mathbb{N}$. Volem demostrar-la per a $S(b)$.

Sigui $a \in \mathbb{N}$ i suposem que

$$a \cdot S(b) = 0.$$

Per la definició del producte,

$$a \cdot S(b) = a \cdot b + a.$$

Per tant,

$$a \cdot b + a = 0.$$

Si $a = 0$, ja tenim el resultat. Suposem, doncs, que

$$a \neq 0.$$

Per la commutativitat de la suma,

$$a \cdot b + a = a + (a \cdot b).$$

Com que $a \neq 0$, per la proposició 1.9, apartat (ii), obtenim

$$a + (a \cdot b) \neq 0.$$

Això contradiu que

$$a \cdot b + a = 0.$$

Per tant, necessàriament

$$a = 0.$$

Així, si

$$a \cdot S(b) = 0,$$

aleshores

$$a = 0.$$

En particular,

$$a = 0 \quad \text{o} \quad S(b) = 0.$$

Per tant, la propietat és certa per a $S(b)$. Pel principi d'inducció, queda provat que, per a tots $a, b \in \mathbb{N}$, si

$$a \cdot b = 0,$$

aleshores

$$a = 0 \quad \text{o} \quad b = 0.$$

La segona afirmació s'obté pel contrarecíproc de la primera: si $a \neq 0$ i $b \neq 0$, aleshores $a \cdot b \neq 0$. Per tant, si a i b són positius, el seu producte també és positiu.

1.2 Els nombres enters

1.2.1 Necessitat d'ampliar els nombres naturals

Quan hem après a comptar, a vegades ens trobem amb situacions com aquestes: m'han dit que hi havia 7 pomes i només n'he comptat 5, així que penso que me'n falten dues. O bé: m'han dit que hi havia 8 boles i n'he comptat 9, així que m'ha sobrat una bola. O fins i tot: m'han dit que hi havia 10 gots i n'he comptat exactament 10, així que no ha faltat ni sobrat res.

La raó és que necessitem comptar tant allò que tenim com allò que ens falta, i distingir bé entre les dues coses. Una manera senzilla de fer-ho seria emprar dos colors: per exemple, verd per al que tenim i vermell per al que ens falta. Així, en l'exemple anterior escriuríem 5 en verd i 2 en vermell. Però la convenció habitual ha estat una altra: hem agafat el costum d'escriure $+5$ i -2 , respectivament. Així hem afegit el símbol $+$ per representar les coses que tenim i el símbol $-$ per a les que ens falten. Diem ara que hem introduït la distinció entre nombres **positius** i

nombres **negatius**.

Ambdós tipus de nombres serveixen per comptar, uns en un sentit i els altres en l'oposat. En aquest context, podríem escriure la següent llista de nombres:

$$\dots, -3, -2, -1, 0, +1, +2, +3, \dots$$

i de seguida ens adonem que hem afegit als nombres naturals nous nombres que podríem anomenar negatius. Si agafem el conveni que no cal posar signe als naturals (perquè el + resulta redundant), arribem a la presentació tradicional dels nombres enters.

Una manera més formal de motivar aquesta extensió és pensar en l'equació

$$a + x = b \tag{1.2.1}$$

amb $a, b \in \mathbb{N}$. Aquesta equació no sempre té solució en $\mathbb{N}$. Per exemple, $1 + x = 0$ tindria $x = -1$ com a solució, però $-1 \notin \mathbb{N}$. De fet, (1.2.1) només té solució en $\mathbb{N}$ quan $b \geq a$. Necessitem, doncs, ampliar el conjunt dels naturals.

Hem d'observar un fet important. Considerem parelles ordenades de nombres naturals com $(5, 7)$, $(13, 15)$ o $(19, 21)$, on convenim a escriure primer la quantitat que tenim i, en segon lloc, la quantitat que volem comptar. Totes elles representen la idea de "faltar-ne dos", o -2 . Anàlogament, $(7, 5)$, $(15, 13)$ i $(21, 19)$ representen "sobrar-ne dos", o $+2$. I parelles com $(3, 3)$ i $(10, 10)$ representen "ni faltar ni sobrar".

Observa ara la següent regularitat:

$$\begin{array}{ll} (5, 7) \text{ i } (13, 15) & 5 + 15 = 7 + 13, \\ (5, 7) \text{ i } (19, 21) & 5 + 21 = 7 + 19, \\ (7, 5) \text{ i } (21, 19) & 7 + 19 = 5 + 21, \\ (3, 3) \text{ i } (10, 10) & 3 + 10 = 3 + 10, \\ \vdots & \vdots \end{array}$$

Aquesta regularitat ens suggereix la relació següent entre parelles ordenades de nombres naturals:

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

1.2.2 Construcció de $\mathbb{Z}$ a partir de $\mathbb{N}$

Volem construir un nou conjunt de nombres que ha d'incloure els naturals i també els nombres negatius. Fem-ho amb la següent definició.

Definició 1.11

Considerem el conjunt $\mathbb{N} \times \mathbb{N}$ i definim sobre ell la relació

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

Proposició 1.16

La relació $\sim$ és d'equivalència.

Demostració

Hem de comprovar que és reflexiva, simètrica i transitiva.

Reflexivitat. $(a, b) \sim (a, b)$ perquè $a + b = b + a$ en $\mathbb{N}$ (commutativitat de la suma).

Simetria. Si $(a, b) \sim (c, d)$, llavors $a + d = b + c$, i d'aquí $d + a = a + d = b + c = c + b$, és a dir, $(c, d) \sim (a, b)$.

Transitivitat. Si $(a, b) \sim (c, d)$ i $(c, d) \sim (e, f)$, llavors $a + d = b + c$ i $c + f = d + e$. Aleshores

$$(b + c) + e = (a + d) + e = a + (d + e) = a + (c + f) = (a + f) + c$$

i, d'altra banda,

$$(b + c) + e = b + (c + e) = b + (e + c) = (b + e) + c.$$

Per tant, $(b + e) + c = (a + f) + c$, i per la propietat de simplificació de la suma en $\mathbb{N}$, $b + e = a + f$, és a dir, $(a, b) \sim (e, f)$.

Aquesta relació d'equivalència ens permet definir el conjunt dels **nombres enters**, que denotem per $\mathbb{Z}$, com el conjunt quocient

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N} / \sim.$$

D'aquesta manera, un nombre enter és una classe d'equivalència

$$[(a, b)] = \{(x, y) : x + b = y + a\}.$$

En particular,

$$\begin{aligned} [(0, 0)] &= \{(x, y) : x = y\} = \{(0, 0), (1, 1), (2, 2), \dots\}, \\ [(0, 1)] &= \{(x, y) : x + 1 = y\} = \{(0, 1), (1, 2), (2, 3), \dots\}, \\ [(1, 0)] &= \{(x, y) : x = y + 1\} = \{(1, 0), (2, 1), (3, 2), \dots\}, \\ &\vdots \end{aligned}$$

1.2.3 Addició de nombres enters

Tot seguit definim una operació d'addició que dota $\mathbb{Z}$ d'estructura algebraica de **grup commutatiu**. Això vol dir que la suma compleix les propietats associativa i commutativa, l'element $[(0, 0)]$ actua com a element neutre i tot element $[(a, b)]$ té un element simètric, que és $[(b, a)]$.

Definició 1.12

Per a tots $[(a, b)], [(c, d)] \in \mathbb{Z}$ definim l'addició de nombres enters com

$$[(a, b)] + [(c, d)] = [(a + c, b + d)]. \quad (1.2.2)$$

Cal comprovar que la suma està ben definida, és a dir, que no depèn dels representants escollits. En efecte, suposem

$$[(a, b)] = [(a', b')] \quad \text{i} \quad [(c, d)] = [(c', d')]. \quad (1.2.3)$$

Volem veure que $[(a + c, b + d)] = [(a' + c', b' + d')]$. Aplicant les propietats de la suma en $\mathbb{N}$ i la definició (1.2.3), tenim

$$\begin{aligned}(a + c) + (b' + d') &= (a + b') + (c + d') \\ &= (b + a') + (d + c') \\ &= (b + d) + (a' + c').\end{aligned}$$

1.2.3.1 Propietats de la suma

Veiem ara les propietats algebraiques de la suma en $\mathbb{Z}$.

Proposició 1.17

Per a tots $[(a, b)], [(c, d)], [(e, f)] \in \mathbb{Z}$ es compleixen:

1. **Associativitat:**

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

2. **Commutativitat:**

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

3. **Element neutre.** $[(0, 0)]$ és l'element neutre de la suma i és únic:

$$[(a, b)] + [(0, 0)] = [(0, 0)] + [(a, b)] = [(a, b)].$$

4. **Element simètric.** L'element simètric de $[(a, b)]$ és $[(b, a)]$, i és únic:

$$[(a, b)] + [(b, a)] = [(b, a)] + [(a, b)] = [(0, 0)].$$

Demostració

Totes aquestes propietats es poden demostrar utilitzant les propietats corresponents dels nombres naturals. Com a exemple, demostrem la propietat 4:

$$\begin{aligned}[(a, b)] + [(b, a)] &= [(a + b, b + a)] \\ &= [(a + b, a + b)] \\ &= [(0, 0)],\end{aligned}$$

ja que $(a + b, a + b) \sim (0, 0)$. La unicitat es prova de manera estàndard: si $[(c, d)]$ fos un altre simètric de $[(a, b)]$, llavors

$$\begin{aligned}[(c, d)] &= [(0, 0)] + [(c, d)] \\ &= ([[(b, a)] + [(a, b)]] + [(c, d)] \\ &= [(b, a)] + ([[(a, b)] + [(c, d)]] \\ &= [(b, a)] + [(0, 0)] \\ &= [(b, a)].\end{aligned}$$

1.2.4 Els naturals com a nombres enters

És clar que volem que els nombres naturals formin part del conjunt dels nombres enters, i això ja es pot intuir. La classe $[(0, 0)]$ es correspon amb 0, $[(0, 1)]$ amb -1 , $[(1, 0)]$ amb $+1$, i així successivament. La llista completa dels enters seria

$$\dots, [(0, 3)], [(0, 2)], [(0, 1)], [(0, 0)], [(1, 0)], [(2, 0)], [(3, 0)], \dots$$

Identifiquem els nombres naturals a i b amb els enters $[(a, 0)]$ i $[(b, 0)]$, respectivament. La suma $a + b$ és un nombre natural que es pot identificar amb l'enter $[(a + b, 0)]$. Resulta el mateix enter si sumem $[(a, 0)] + [(b, 0)]$? La resposta és sí, perquè per definició $[(a, 0)] + [(b, 0)] = [(a + b, 0)]$. Així doncs, l'operació definida en (1.2.2) estén l'addició dels nombres naturals.

Estrictament parlant, és incorrecte escriure $\mathbb{N} \subset \mathbb{Z}$, però des d'un punt de vista intuïtiu els nombres naturals són un subconjunt dels enters. Podem fer més rigorosa aquesta identificació definint l'aplicació

$$f : \mathbb{N} \longrightarrow \mathbb{Z}, \quad f(n) = [(n, 0)].$$

És clar que f és injectiva, ja que $[(n, 0)] = [(m, 0)]$ equival a $(n, 0) \sim (m, 0)$, i d'aquí $n = m$. A més, f conserva l'estructura algebraica de $\mathbb{N}$:

$$f(m + n) = [(m + n, 0)] = [(m, 0)] + [(n, 0)] = f(m) + f(n).$$

Diem aleshores que f és una **injecció canònica**, i quan considerem el subconjunt $f(\mathbb{N})$ de $\mathbb{Z}$, escrivim $\mathbb{N} \subset \mathbb{Z}$.

1.2.5 Multiplicació de nombres enters

Tot seguit definirem una operació de multiplicació que compleix les propietats associativa, commutativa i distributiva respecte de la suma, i que té $1 = [(1, 0)] \in \mathbb{Z}$ com a element neutre. Així, l'addició i multiplicació doten $\mathbb{Z}$ d'una estructura algebraica coneguda com **anell commutatiu amb unitat**.

Definició 1.13

Per a tots $[(a, b)], [(c, d)] \in \mathbb{Z}$ definim la multiplicació de nombres enters com

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

Cal comprovar que la multiplicació està ben definida, és a dir, que no depèn dels representants escollits. Suposem

$$[(a, b)] = [(a', b')] \quad \text{i} \quad [(c, d)] = [(c', d')]. \quad (1.2.4)$$

Volem veure que

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

o equivalentment, que

$$(a \cdot c + b \cdot d) + (a' \cdot d' + b' \cdot c') = (a \cdot d + b \cdot c) + (a' \cdot c' + b' \cdot d').$$

Aplicant repetidament les propietats de la suma i del producte en $\mathbb{N}$, junt amb les igualtats de (1.2.4), s'arriba a aquesta igualtat (deixem els detalls al lector com a exercici).

1.2.5.1 Propietats de la multiplicació

Proposició 1.18

Per a tots $[(a, b)], [(c, d)], [(e, f)] \in \mathbb{Z}$ es compleixen:

1. **Associativitat:** $[(a, b)] \cdot ([(c, d)] \cdot [(e, f)]) = (([a, b)] \cdot [(c, d)]) \cdot [(e, f)]$.
2. **Commutativitat:** $[(a, b)] \cdot [(c, d)] = [(c, d)] \cdot [(a, b)]$.
3. **Element neutre.** $[(1, 0)]$ és l'element neutre: $[(a, b)] \cdot [(1, 0)] = [(1, 0)] \cdot [(a, b)] = [(a, b)]$.
4. **Distributivitat:** $[(a, b)] \cdot ([(c, d)] + [(e, f)]) = [(a, b)] \cdot [(c, d)] + [(a, b)] \cdot [(e, f)]$.

Les demostracions són anàlogues a les del cas de l'addició i es deixen al lector.

1.2.5.2 Substracció en $\mathbb{Z}$

A la introducció havíem proposat el problema: "M'han dit que hi ha 7 pomes i n'he comptat 5, quantes pomes em falten?". Havíem dit que en falten 2, però ara estem ja preparats per donar una resposta algebraica rigorosa. De fet, se'ns planteja l'equació $x+2=7$, on x designa el nombre de pomes que falten, i en general $x+b=a$ amb $a, b \in \mathbb{N}$.

Hem vist en cursos anteriors que la solució d'aquesta equació és $a-b$, però aquesta operació encara no la tenim definida. Tal com hem vist a la secció 1.2.4, intuïtivament el nombre enter $[(a, b)]$ s'ha de considerar com a solució de l'equació $x+b=a$.

Per definir-ho amb cura, introduïm una operació unària que anomenem **oposició**, que assigna a cada nombre enter el seu nombre oposat:

$$\mathbb{Z} \longrightarrow \mathbb{Z}, \quad n \longmapsto -n,$$

de tal manera que si $n = [(a, b)]$, llavors $-n = [(b, a)]$, és a dir, el seu simètric. Aquesta operació està ben definida perquè el simètric existeix i és únic.

Ara estem preparats per definir la **substracció** en $\mathbb{Z}$: per a tots $n, m \in \mathbb{Z}$,

$$n - m := n + (-m)$$

Llavors, si $a, b \in \mathbb{N}$,

$$a - b = [(a, b)].$$

Per descomptat, per utilitzar simplement nombres enters en els càlculs no cal entendre el concepte de classes d'equivalència. En lloc d'això, s'escriuen els nombres enters negatius amb el signe menys com $-n$, amb n natural. Com hem identificat anteriorment els nombres naturals n amb els enters $[(n, 0)]$, ara identifiquem els nombres negatius $-n$ amb els enters $[(0, n)]$ (on n és natural). A més,

$$n + [(0, n)] = [(n, 0)] + [(0, n)] = [(n, n)] = [(0, 0)] = 0,$$

i per tant és $-n \stackrel{\text{def}}{=} [(0, n)]$.

Exemple 1.17

Proveu que si $m, n \in \mathbb{Z}$, llavors $m \cdot (-n) = -(m \cdot n)$.

Solució

Siguin $m, n \in \mathbb{Z}$. Aleshores existeixen $a, b, p, q \in \mathbb{N}$ tals que

$$m = [(a, b)] \quad \text{i} \quad n = [(p, q)].$$

Per tant,

$$-n = [(q, p)].$$

Així,

$$m \cdot (-n) = [(a, b)] \cdot [(q, p)].$$

Per la definició del producte en $\mathbb{Z}$,

$$m \cdot (-n) = [(a \cdot q + b \cdot p, a \cdot p + b \cdot q)].$$

D'altra banda,

$$m \cdot n = [(a, b)] \cdot [(p, q)] = [(a \cdot p + b \cdot q, a \cdot q + b \cdot p)].$$

Per tant,

$$-(m \cdot n) = [(a \cdot q + b \cdot p, a \cdot p + b \cdot q)].$$

Així,

$$m \cdot (-n) = -(m \cdot n).$$

Exemple 1.18

Deduïu de la definició que el producte de dos nombres negatius és positiu. Il·lustreu-ho amb $(-2) \cdot (-3) = 6$.

Solució

Si n i m són dos nombres enters negatius, llavors $n = -p$ i $m = -q$, on $p, q \in \mathbb{N} \setminus \{0\}$. Així, $n = [(0, p)]$ i $m = [(0, q)]$, i tenim

$$n \cdot m = [(0, p)] \cdot [(0, q)] = [(p \cdot q, 0)] = p \cdot q.$$

Per tant, $n \cdot m \in \mathbb{N}$ i és positiu.

En particular, $(-2) \cdot (-3) = [(0, 2)] \cdot [(0, 3)] = [(6, 0)] = 6$.

1.2.6 L'ordre als enters

Com hem vist en estudiar els nombres naturals, aquests tenen una relació d'ordre $\leq$. Ara la farem servir per introduir una relació d'ordre en $\mathbb{Z}$.

Si $[(a, b)], [(c, d)] \in \mathbb{Z}$, com podem definir $[(a, b)] \leq [(c, d)]$? Pel que hem vist abans, $[(a, b)] \leq [(c, d)]$ és equivalent a $a - b \leq c - d$. D'aquí, per les propietats de

la suma en $\mathbb{N}$, s'obté

$$a - b \leq c - d \iff a + d \leq b + c.$$

Aquesta equivalència ens permet donar la definició següent.

Definició 1.14

Per a tots $[(a, b)], [(c, d)] \in \mathbb{Z}$ definim

$$[(a, b)] \leq [(c, d)] \iff a + d \leq b + c.$$

Proposició 1.19

La relació d'ordre en $\mathbb{Z}$ està ben definida.

Demostració

Veiem ara que $\leq$ no depèn dels representants escollits. Siguin $[(a, b)] = [(a', b')]$ i $[(c, d)] = [(c', d')]$. Per la definició de la relació d'equivalència en $\mathbb{N} \times \mathbb{N}$, tenim

$$a + b' = b + a'$$

i

$$c + d' = d + c'.$$

Suposem que

$$[(a, b)] \leq [(c, d)].$$

Per la definició de l'ordre, això vol dir que

$$a + d \leq b + c.$$

Volem provar que

$$[(a', b')] \leq [(c', d')],$$

és a dir, que

$$a' + d' \leq b' + c'.$$

Com que

$$a + d \leq b + c,$$

per la compatibilitat de l'ordre amb la suma, podem sumar $b' + c'$ a tots dos costats i obtenim

$$a + d + b' + c' \leq b + c + b' + c'.$$

Reordenant els termes de cada membre, tenim

$$(a + b') + (d + c') \leq (b + c') + (c + b').$$

Ara bé, com que

$$a + b' = b + a'$$

i

$$d + c' = c + d',$$

substituïnt obtenim

$$(b + a') + (c + d') \leq (b + c') + (c + b').$$

Per associativitat i commutativitat de la suma,

$$b + c + a' + d' \leq b + c + b' + c'.$$

Per l'Exercici 2.7, cancel·lant $b + c$ a tots dos costats, obtenim

$$a' + d' \leq b' + c'.$$

Per tant,

$$[(a', b')] \leq [(c', d')].$$

El raonament invers és idèntic, intercanviant els papers de $(a, b), (c, d)$ i $(a', b'), (c', d')$. Per tant,

$$a + d \leq b + c \iff a' + d' \leq b' + c'.$$

Així, la relació d'ordre en $\mathbb{Z}$ està ben definida.

Proposició 1.20

L'ordre definit per $\leq$ sobre $\mathbb{Z}$ és total.

Demostració

Siguin $[(a, b)], [(c, d)], [(e, f)] \in \mathbb{Z}$.

Reflexivitat. $[(a, b)] \leq [(a, b)]$ perquè $a + b \leq b + a = a + b$.

Antisimetria. Si $[(a, b)] \leq [(c, d)]$ i $[(c, d)] \leq [(a, b)]$, llavors $a + d \leq b + c$ i $c + b \leq d + a$. Per la commutativitat de la suma, $a + d \leq b + c$ i $b + c \leq a + d$, i com $\leq$ és antisimètrica a $\mathbb{N}$, $a + d = b + c$, és a dir, $[(a, b)] = [(c, d)]$.

Transitivitat. Suposem que

$$[(a, b)] \leq [(c, d)] \quad \text{i} \quad [(c, d)] \leq [(e, f)].$$

Per la definició de l'ordre en $\mathbb{Z}$, això vol dir que

$$a + d \leq b + c$$

i

$$c + f \leq d + e.$$

Sumant aquestes dues desigualtats membre a membre, obtenim

$$(a + d) + (c + f) \leq (b + c) + (d + e).$$

Per l'associativitat i la commutativitat de la suma en $\mathbb{N}$, podem reordenar els termes:

$$(a + f) + (c + d) \leq (b + e) + (c + d).$$

Ara usem l'Exercici 2.7, que estableix la cancel·lació de l'ordre amb la suma en $\mathbb{N}$. Aplicant-lo amb

$$x = a + f, \quad y = b + e, \quad t = c + d,$$

obtenim

$$a + f \leq b + e.$$

Per tant, per la definició de l'ordre en $\mathbb{Z}$,

$$[(a, b)] \leq [(e, f)].$$

Així, l'ordre en $\mathbb{Z}$ és transitiu.

Total. Com $a + d$ i $b + c$ són naturals i $\leq$ és total a $\mathbb{N}$, es compleix $a + d \leq b + c$ o $b + c \leq a + d$. Per commutativitat, això equival a $[(a, b)] \leq [(c, d)]$ o $[(c, d)] \leq [(a, b)]$.

Si $n, m \in \mathbb{Z}$, escrivim $n < m$ si i només si $n \leq m$ i $n \neq m$. A més, $n \geq m$ és el mateix que $m \leq n$. Diem que $n \in \mathbb{Z}$ és **positiu** si $n > 0$, **no negatiu** si $n \geq 0$, i **negatiu** si $n < 0$. Observa que $[(a, b)]$ és positiu quan $b < a$, ja que $a - b > 0$ equival a $a > b$. També, $n = [(a, b)] > 0$ és equivalent a $a - b > 0$, i això equival a $0 > b - a$, és a dir, $-n = [(b, a)] < 0$. Per tant, n és positiu si i només si $-n$ és negatiu.

1.2.6.1 Compatibilitat de l'ordre amb les operacions

L'ordre dels nombres enters és compatible amb les operacions de suma i producte. Això vol dir que podem sumar un mateix enter als dos membres d'una desigualtat sense alterar-ne el sentit. En canvi, en multiplicar una desigualtat per un enter, cal distingir si aquest enter és positiu, nul o negatiu.

Proposició 1.21 (Compatibilitat de l'ordre amb la suma i el producte)

Siguin $a, b, c \in \mathbb{Z}$. Es compleixen les propietats següents:

- (i) si $a \leq b$, aleshores $a + c \leq b + c$,
- (ii) si $a \leq b$ i $c \geq 0$, aleshores $ac \leq bc$,
- (iii) si $a \leq b$ i $c \leq 0$, aleshores $bc \leq ac$.

Demostració

Recordem primer que, per a dos enters $x, y \in \mathbb{Z}$, tenim

$$x \leq y$$

si, i només si,

$$y - x \geq 0.$$

Aquesta és una manera equivalent d'expressar l'ordre en $\mathbb{Z}$.

(i) Suposem que

$$a \leq b.$$

Aleshores

$$b - a \geq 0.$$

Ara bé,

$$(b + c) - (a + c) = b + c - a - c = b - a.$$

Per tant,

$$(b + c) - (a + c) \geq 0.$$

Això vol dir que

$$a + c \leq b + c.$$

(ii) Suposem ara que

$$a \leq b \quad \text{i} \quad c \geq 0.$$

Com abans,

$$b - a \geq 0.$$

Com que el producte de dos enters no negatius és no negatiu, obtenim

$$(b - a)c \geq 0.$$

Per la propietat distributiva,

$$(b - a)c = bc - ac.$$

Així,

$$bc - ac \geq 0.$$

Per tant,

$$ac \leq bc.$$

(iii) Finalment, suposem que

$$a \leq b \quad \text{i} \quad c \leq 0.$$

Aleshores

$$b - a \geq 0$$

i

$$-c \geq 0.$$

Com que el producte de dos enters no negatius és no negatiu, tenim

$$(b - a)(-c) \geq 0.$$

Ara bé,

$$(b - a)(-c) = ac - bc.$$

Per tant,

$$ac - bc \geq 0.$$

Això vol dir que

$$bc \leq ac.$$

Així queden demostrades les tres propietats.

Observació 1.6

L'apartat (iii) expressa el fet conegut que, quan multipliquem una desigualtat per un enter negatiu, el sentit de la desigualtat s'inverteix.

Definició 1.15 (Valor absolut)

L'aplicació $|\cdot| : \mathbb{Z} \rightarrow \mathbb{N}$ definida com

$$|n| = \begin{cases} n & \text{si } n \geq 0, \\ -n & \text{si } n < 0, \end{cases}$$

s'anomena **valor absolut**.

Proposició 1.22 (Propietats bàsiques del valor absolut)

Per a tot $n \in \mathbb{Z}$ es compleixen les propietats següents:

- (i) $|n| \geq 0$,
- (ii) $|n| = 0 \iff n = 0$,
- (iii) $-|n| \leq n \leq |n|$.

A més, si $k \in \mathbb{Z}$ i $k \geq 0$, aleshores

$$|n| \leq k \iff -k \leq n \leq k.$$

Demostració

Demostrem les propietats a partir de la definició del valor absolut.

(i) Provem que $|n| \geq 0$.

Si $n \geq 0$, aleshores, per definició,

$$|n| = n.$$

Per tant,

$$|n| \geq 0.$$

Si $n < 0$, aleshores

$$|n| = -n.$$

Com que $n < 0$, el seu oposat és positiu. Per tant,

$$-n > 0,$$

i, en particular,

$$|n| \geq 0.$$

Així, en tots els casos,

$$|n| \geq 0.$$

(ii) Provem que

$$|n| = 0 \iff n = 0.$$

En primer lloc, si $n = 0$, aleshores

$$|n| = |0| = 0.$$

Recíprocament, suposem que

$$|n| = 0.$$

Si $n \geq 0$, aleshores $|n| = n$, i per tant

$$n = 0.$$

Si $n < 0$, aleshores $|n| = -n$, i per tant

$$-n = 0.$$

D'aquí es dedueix igualment que

$$n = 0.$$

Per tant,

$$|n| = 0 \iff n = 0.$$

(iii) Provem que

$$-|n| \leq n \leq |n|.$$

Si $n \geq 0$, aleshores $|n| = n$. Per tant,

$$n \leq |n|$$

és una igualtat. A més, com que $|n| = n \geq 0$, tenim

$$-|n| \leq 0 \leq n.$$

Així,

$$-|n| \leq n \leq |n|.$$

Si $n < 0$, aleshores $|n| = -n$. Per tant,

$$-|n| = -(-n) = n,$$

i la desigualtat

$$-|n| \leq n$$

és una igualtat. A més, com que $|n| = -n > 0$ i $n < 0$, tenim

$$n \leq |n|.$$

Per tant, també en aquest cas,

$$-|n| \leq n \leq |n|.$$

Finalment, provem que, si $k \geq 0$, aleshores

$$|n| \leq k \iff -k \leq n \leq k.$$

Suposem primer que

$$|n| \leq k.$$

Per la propietat anterior sabem que

$$-|n| \leq n \leq |n|.$$

Com que $|n| \leq k$, obtenim

$$n \leq k.$$

A més, de $|n| \leq k$ es dedueix

$$-k \leq -|n|.$$

Com que

$$-|n| \leq n,$$

tenim

$$-k \leq n.$$

Per tant,

$$-k \leq n \leq k.$$

Recíprocament, suposem que

$$-k \leq n \leq k.$$

Distingim dos casos.

Si $n \geq 0$, aleshores $|n| = n$. Com que $n \leq k$, obtenim

$$|n| \leq k.$$

Si $n < 0$, aleshores $|n| = -n$. De la desigualtat

$$-k \leq n$$

se'n dedueix, canviant el signe, que

$$-n \leq k.$$

Per tant,

$$|n| \leq k.$$

Així,

$$|n| \leq k \iff -k \leq n \leq k.$$

Observació 1.7

Altres propietats importants del valor absolut, com ara

$$|mn| = |m||n|$$

i

$$|m + n| \leq |m| + |n|,$$

es treballaran com a exercicis resolts a la Pràctica.

Introduïm ara algunes nocions útils. Diem que un subconjunt $S \subset \mathbb{Z}$ està **fitat superiorment** quan existeix $a \in \mathbb{Z}$ tal que $n \leq a$ per a tot $n \in S$, i diem que a és una **fit a superior** de S . Anàlogament, S està **fitat inferiorment** quan existeix $a \in \mathbb{Z}$ tal que $a \leq n$ per a tot $n \in S$, i diem que a és una **fit a inferior** de S . Diem que S està **fitat** quan ho està superiorment i inferiorment.

Anomenem **suprem** d'un subconjunt $S \subset \mathbb{Z}$ a la més petita de les fites superiors, i el denotem per $\sup S$. Anàlogament, l'**ínfim** és la més gran de les fites inferiors, denotat $\inf S$. El **màxim** de S és el suprem quan pertany a S , denotat $\max S$, i el **mínim** de S és l'ínfim quan pertany a S , denotat $\min S$.

Teorema 1.23

Sigui $S \subset \mathbb{Z}$, $S \neq \emptyset$ i fitat inferiorment. Aleshores S té mínim. Anàlogament, si S està fitat superiorment, llavors S té màxim.

Demostració

Provarem la primera part; l'altra es demostra de manera anàloga. Com S està fitat inferiorment, existeix una fita inferior $a \in \mathbb{Z}$ tal que $a \leq n$ per a tot $n \in S$. Així $n - a \geq 0$, i $n - a \in \mathbb{N}$ per a tot $n \in S$. Considerem el conjunt $T = \{n - a : n \in S\}$. Com $S \neq \emptyset$, també $T \neq \emptyset$, i $T \subset \mathbb{N}$. Pel principi de bon ordre a $\mathbb{N}$, T té primer element, diguem $m = p - a$ per a un cert $p \in S$. Llavors p és l'element mínim de S , perquè $m \leq n - a$ per a tot $n \in S$ implica sumant a als dos costats $p \leq n$ per a tot $n \in S$.

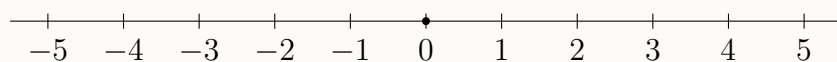
1.2.7 Representació gràfica dels nombres enters

Els nombres enters es poden representar geomètricament com a punts d'una recta, que anomenem *recta numèrica*. Per fer-ho, fixem un punt de la recta i l'identifiquem amb el nombre 0, que anomenarem *origen*. A continuació, triem una unitat de longitud i un sentit positiu sobre la recta.

Amb aquestes convencions:

- el nombre 1 es representa pel punt situat a una unitat de l'origen en el sentit positiu;
- el nombre 2 es representa pel punt situat a dues unitats de l'origen en el mateix sentit;
- en general, cada enter positiu n es representa avançant n unitats des de l'origen en el sentit positiu;
- el nombre -1 es representa pel punt situat a una unitat de l'origen en el sentit contrari;
- en general, cada enter negatiu $-n$ es representa avançant n unitats des de l'origen en el sentit negatiu.

D'aquesta manera, a cada nombre enter li correspon un únic punt de la recta, i recíprocament, els punts obtinguts així representen nombres enters.



Representació d'alguns nombres enters sobre la recta numèrica.

Aquesta representació geomètrica permet visualitzar l'ordre dels nombres enters. Si $a, b \in \mathbb{Z}$, aleshores

$$a < b$$

si, i només si, el punt que representa a queda a l'esquerra del punt que representa b sobre la recta numèrica.

Per exemple,

$$-3 < -1 < 0 < 2 < 5,$$

perquè, en la recta numèrica, el punt corresponent a -3 queda més a l'esquerra que el punt corresponent a -1 , aquest queda a l'esquerra de 0 , i així successivament.

La distància d'un nombre enter a l'origen queda determinada pel seu valor absolut. Així, els nombres 3 i -3 es representen en punts simètrics respecte de l'origen i es troben tots dos a distància 3 del punt 0 .

1.2.8 El teorema de la divisió

Vam aprendre a fer divisions enteres fa anys per resoldre qüestions com la següent: volem repartir 15 pomes entre 7 persones de manera que cadascú rebí el màxim possible i tots la mateixa quantitat. Fent la divisió de 15 (dividend) entre 7 (divisor), obtenim que cadascú rep 2 (quocient) pomes i sobra 1 (residu). Aritmèticament, $15 = 7 \cdot 2 + 1$. El resultat que vindrà ens diu que sempre podem fer això a $\mathbb{Z}$.

Teorema 1.24 (Teorema de la divisió)

Siguin $a, b \in \mathbb{Z}$, amb $b \neq 0$. Aleshores existeixen uns únics $q, r \in \mathbb{Z}$ tals que

$$a = bq + r$$

i

$$0 \leq r < |b|.$$

El nombre q s'anomena **quocient** i el nombre r s'anomena **residu** de la divisió de a per b .

Demostració

Comencem amb un cas concret per il·lustrar la idea. Si $a = 15$ i $b = 7$, hem de trobar $q, r \in \mathbb{Z}$ tals que $15 = 7q + r$ amb $0 \leq r < 7$. Aïllant, $r = 15 - 7q$, i provant valors de q obtenim

$$\dots, 29, 22, 15, 8, 1, -6, \dots$$

La condició $0 \leq r < 7$ ens dona $r = 1$ i $q = 2$.

Aquesta intuïció permet la prova general. Suposem primer $b > 0$ i considerem el conjunt

$$R = \{a - bq : q \in \mathbb{Z} \text{ i } a - bq \geq 0\}.$$

Aquest conjunt és no buit. En efecte, si $a \geq 0$, prenent $q = 0$ obtenim $a - b \cdot 0 = a \geq 0$, i per tant $a \in R$. Si $a < 0$, prenent $q = a$ s'obté

$$a - b \cdot a = (1 - b) \cdot a.$$

Com que $b > 0$, tenim $b \geq 1$, i per tant

$$1 - b \leq 0.$$

Així, com que $a < 0$ i $1 - b \leq 0$, resulta que

$$(1 - b) \cdot a \geq 0.$$

Per tant,

$$a - b \cdot a \in R,$$

i $R \neq \emptyset$. Així doncs, R és un subconjunt no buit dels enters no negatius. Identificant els enters no negatius amb nombres naturals, pel principi del bon ordre, R té un element mínim. Sigui $r = \min R$. Llavors, per definició de R , existeix $q \in \mathbb{Z}$ tal que

$$r = a - bq.$$

Aleshores

$$a = bq + r.$$

A més, com que $r \in R$, tenim $r \geq 0$. Vegem ara que $r < b$. Fem-ho per reducció a l'absurd, suposem que $r \geq b$. Aleshores $r - b \geq 0$, però

$$r - b = (a - bq) - b = a - b(q + 1).$$

Així,

$$r - b \in R.$$

Com que $b > 0$, tenim

$$r - b < r,$$

cosa que contradiu que r era l'element mínim de R . Per tant, $r < b$. Hem provat, doncs, que si $b > 0$, existeixen $q, r \in \mathbb{Z}$ tals que

$$a = bq + r \quad \text{i} \quad 0 \leq r < b.$$

Provem ara la unicitat en el cas $b > 0$. Suposem que tenim dues descomposicions

$$a = bq + r \quad \text{i} \quad a = bq' + r',$$

amb

$$0 \leq r < b \quad \text{i} \quad 0 \leq r' < b.$$

Volem provar que

$$q = q' \quad \text{i} \quad r = r'.$$

Si $q = q'$, aleshores, de

$$bq + r = bq + r',$$

obtenim directament

$$r = r'.$$

Suposem ara que $q \neq q'$. Per la tricotomia de l'ordre en $\mathbb{Z}$, o bé $q < q'$, o bé $q' < q$.

Si $q < q'$, aleshores existeix un enter positiu t tal que

$$q' = q + t.$$

Substituint en la igualtat

$$bq + r = bq' + r',$$

obtenim

$$bq + r = b(q + t) + r' = bq + bt + r'.$$

Cancel·lant bq , resulta

$$r = bt + r'.$$

Com que $b > 0$ i $t > 0$, tenim

$$bt \geq b.$$

Com que $r' \geq 0$, obtenim

$$r = bt + r' \geq b,$$

cosa que contradiu que

$$r < b.$$

Per tant, no pot ser $q < q'$.

De manera anàloga, si $q' < q$, obtindríem

$$r' \geq b,$$

contradient que

$$r' < b.$$

Per tant, tampoc no pot ser $q' < q$.

Així, necessàriament

$$q = q',$$

i aleshores també

$$r = r'.$$

Això prova la unicitat en el cas $b > 0$.

Considerem ara el cas $b < 0$. Aleshores

$$-b > 0.$$

Pel cas ja demostrat, aplicat a a i a $-b$, existeixen uns únics $q', r \in \mathbb{Z}$ tals que

$$a = (-b)q' + r$$

i

$$0 \leq r < -b.$$

Com que

$$(-b)q' = b(-q'),$$

si definim

$$q = -q',$$

obtenim

$$a = bq + r.$$

A més, com que $b < 0$, tenim

$$|b| = -b.$$

Per tant,

$$0 \leq r < |b|.$$

Així queda provada l'existència també en el cas $b < 0$.

Finalment, provem la unicitat en el cas $b < 0$. Suposem que tenim dues descomposicions

$$a = bq + r \quad \text{i} \quad a = bq' + r',$$

amb

$$0 \leq r < |b| \quad \text{i} \quad 0 \leq r' < |b|.$$

Com que $b < 0$, tenim $|b| = -b$. Aleshores podem escriure

$$a = (-b)(-q) + r \quad \text{i} \quad a = (-b)(-q') + r'.$$

Com que $-b > 0$, aquestes són dues descomposicions de a respecte del divisor positiu $-b$, amb residus r i r' que compleixen

$$0 \leq r < -b \quad \text{i} \quad 0 \leq r' < -b.$$

Per la unicitat ja demostrada en el cas del divisor positiu, obtenim

$$-q = -q' \quad \text{i} \quad r = r'.$$

Per tant,

$$q = q' \quad \text{i} \quad r = r'.$$

Així, per a qualsevol $a, b \in \mathbb{Z}$, amb $b \neq 0$, existeixen uns únics $q, r \in \mathbb{Z}$ tals que

$$a = bq + r \quad \text{i} \quad 0 \leq r < |b|.$$

1.2.9 Divisibilitat en els nombres enters

La noció de divisibilitat també es pot estudiar en el conjunt dels nombres enters. La diferència principal respecte dels nombres naturals és que ara els divisors poden ser positius o negatius.

Definició 1.16 (Divisibilitat en $\mathbb{Z}$)

Siguin $a, b \in \mathbb{Z}$, amb $a \neq 0$. Diem que a **divideix** b , i escrivim

$$a \mid b,$$

si existeix $q \in \mathbb{Z}$ tal que

$$b = aq.$$

En aquest cas, diem que a és un **divisor** de b , que b és un **múltiple** de a , i que q és el **quocient** de la divisió exacta de b per a .

Exemple 1.19

Tenim

$$-3 \mid 12,$$

perquè existeix $-4 \in \mathbb{Z}$ tal que

$$12 = (-3) \cdot (-4).$$

Per tant, -3 és un divisor enter de 12.

També tenim

$$3 \mid (-12),$$

perquè

$$-12 = 3 \cdot (-4).$$

Observació 1.8

En $\mathbb{Z}$, els divisors apareixen per parelles de signe. Per exemple, els divisors enters de 12 són

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12.$$

Això vol dir que

$$1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12, -12$$

són tots divisors de 12 en $\mathbb{Z}$.

Proposició 1.25 (Propietats bàsiques de la divisibilitat en $\mathbb{Z}$)

Siguin $a, b, c \in \mathbb{Z}$, amb $a \neq 0$. Es compleixen les propietats següents:

- (i) $a \mid a$,
- (ii) $a \mid 0$,
- (iii) si $a \mid b$, aleshores $a \mid (-b)$ i $(-a) \mid b$,
- (iv) si $a \mid b$ i $a \mid c$, aleshores $a \mid (b + c)$,
- (v) si $a \mid b$ i $b \mid c$, amb $b \neq 0$, aleshores $a \mid c$.

Demostració

Demostrem cada propietat a partir de la definició de divisibilitat.

(i) Com que

$$a = a \cdot 1$$

i $1 \in \mathbb{Z}$, tenim

$$a \mid a.$$

(ii) Com que

$$0 = a \cdot 0$$

i $0 \in \mathbb{Z}$, tenim

$$a \mid 0.$$

(iii) Suposem que

$$a \mid b.$$

Aleshores existeix $q \in \mathbb{Z}$ tal que

$$b = aq.$$

Per tant,

$$-b = -(aq) = a(-q).$$

Com que $-q \in \mathbb{Z}$, obtenim

$$a \mid (-b).$$

D'altra banda,

$$b = aq = (-a)(-q).$$

Com que $-q \in \mathbb{Z}$, obtenim

$$(-a) \mid b.$$

(iv) Suposem que

$$a \mid b \quad \text{i} \quad a \mid c.$$

Aleshores existeixen $q, r \in \mathbb{Z}$ tals que

$$b = aq \quad \text{i} \quad c = ar.$$

Per tant,

$$b + c = aq + ar = a(q + r).$$

Com que $q + r \in \mathbb{Z}$, concloem que

$$a \mid (b + c).$$

(v) Suposem que

$$a \mid b \quad \text{i} \quad b \mid c,$$

amb $b \neq 0$. Aleshores existeixen $q, r \in \mathbb{Z}$ tals que

$$b = aq \quad \text{i} \quad c = br.$$

Substituint la primera igualtat en la segona, obtenim

$$c = (aq)r = a(qr).$$

Com que $qr \in \mathbb{Z}$, concloem que

$$a \mid c.$$

Així queden demostrades les propietats bàsiques.

Observació 1.9

En treballar amb el màxim comú divisor dins de $\mathbb{Z}$, normalment es pren el representant positiu. Per exemple, tot i que 6 i -6 són divisors comuns de 18 i 24, escrivim

$$\text{mcd}(18, 24) = 6,$$

i no -6 .

2 Pràctica

2.1 Naturals i inducció

Exercici 2.1 (Ús directe dels axiomes de Peano)

Prova que $3 \neq 0$ i que $3 \neq 2$, entenent

$$1 = S(0), \quad 2 = S(S(0)), \quad 3 = S(S(S(0))).$$

Solució

Tenim $3 = S(S(S(0)))$. Si $3 = 0$, aleshores $S(S(S(0))) = 0$, contradicció amb l'axioma que diu que 0 no és successor de cap natural.

Si $3 = 2$, aleshores

$$S(S(S(0))) = S(S(0)).$$

Per injectivitat de S , obtenim $S(S(0)) = S(0)$, i aplicant de nou la injectivitat, $S(0) = 0$, contradicció. Per tant, $3 \neq 2$.

Exercici 2.2 (Inducció)

Demostra que per a tot $n \in \mathbb{N}$,

$$1 + 3 + 5 + \cdots + (2n + 1) = (n + 1)^2.$$

Solució

Per $n = 0$, el membre esquerre és 1 i el dret és $(0 + 1)^2 = 1$.

Suposem certa la igualtat per a n :

$$1 + 3 + \cdots + (2n + 1) = (n + 1)^2.$$

Aleshores, per a $n + 1$,

$$\begin{aligned} 1 + 3 + \cdots + (2n + 1) + (2(n + 1) + 1) &= (n + 1)^2 + 2n + 3 \\ &= n^2 + 2n + 1 + 2n + 3 \\ &= n^2 + 4n + 4 \\ &= (n + 2)^2. \end{aligned}$$

Així queda provada la fórmula per inducció.

Exercici 2.3 (Inducció forta)

Prova que tot natural $n \geq 2$ és primer o producte de nombres primers.

Solució

Fem inducció forta sobre n . El cas $n = 2$ és cert perquè 2 és primer.

Suposem que la propietat és certa per a tots els naturals k amb $2 \leq k \leq n$, i provem-la per a $n + 1$. Si $n + 1$ és primer, no cal fer res. Si no és primer, existeixen $a, b \in \mathbb{N}$ amb

$$1 < a < n + 1, \quad 1 < b < n + 1, \quad n + 1 = ab.$$

Per hipòtesi d'inducció, a i b són primers o producte de primers. Per tant, $n + 1 = ab$ és producte de nombres primers.

Exercici 2.4 (Algoritme d'Euclides)

Calcula $\text{mcd}(252, 198)$.

Solució

Fem divisions successives:

$$252 = 198 \cdot 1 + 54,$$

$$198 = 54 \cdot 3 + 36,$$

$$54 = 36 \cdot 1 + 18,$$

$$36 = 18 \cdot 2 + 0.$$

Per tant, $\text{mcd}(252, 198) = 18$.

Exercici 2.5 (Cancel·lació de la suma)

Prova que, per a tots $a, b, c \in \mathbb{N}$, si

$$a + c = b + c,$$

aleshores

$$a = b.$$

Solució

Fem inducció sobre c .

Per a $c = 0$, si

$$a + 0 = b + 0,$$

aleshores, per la definició de la suma,

$$a = b.$$

Suposem ara que la propietat és certa per a un cert $c \in \mathbb{N}$. Volem provar-la per a $S(c)$. Suposem que

$$a + S(c) = b + S(c).$$

Per la definició de la suma,

$$S(a + c) = S(b + c).$$

Com que el successor és injectiu, obtenim

$$a + c = b + c.$$

Per la hipòtesi d'inducció, concloem que

$$a = b.$$

Per tant, per inducció, la propietat queda provada per a tot $c \in \mathbb{N}$.

Exercici 2.6 (Compatibilitat de l'ordre amb la suma)

Prova que, per a tots $a, b, c \in \mathbb{N}$, si

$$a \leq b,$$

aleshores

$$a + c \leq b + c.$$

Solució

Suposem que $a \leq b$. Per definició de l'ordre, existeix $n \in \mathbb{N}$ tal que

$$b = a + n.$$

Aleshores

$$b + c = (a + n) + c.$$

Per l'associativitat i la commutativitat de la suma,

$$(a + n) + c = (a + c) + n.$$

Per tant,

$$b + c = (a + c) + n.$$

Això vol dir, per definició de l'ordre, que

$$a + c \leq b + c.$$

Exercici 2.7 (Cancel·lació de l'ordre amb la suma)

Demostra que, per a tots $a, b, c \in \mathbb{N}$, si

$$a + c \leq b + c,$$

aleshores

$$a \leq b.$$

Solució

Suposem que

$$a + c \leq b + c.$$

Per la definició de l'ordre en $\mathbb{N}$, existeix $n \in \mathbb{N}$ tal que

$$b + c = (a + c) + n.$$

Per l'associativitat de la suma,

$$(a + c) + n = a + (c + n).$$

Per la commutativitat de la suma,

$$c + n = n + c.$$

Per tant,

$$a + (c + n) = a + (n + c) = (a + n) + c.$$

Així,

$$b + c = (a + n) + c.$$

Per la propietat de cancel·lació de la suma, obtenim

$$b = a + n.$$

Com que existeix $n \in \mathbb{N}$ tal que

$$b = a + n,$$

per la definició de l'ordre concloem que

$$a \leq b.$$

Exercici 2.8 (Compatibilitat de l'ordre amb el producte)

Prova que, per a tots $a, b, c \in \mathbb{N}$, si

$$a \leq b,$$

aleshores

$$a \cdot c \leq b \cdot c.$$

Prova també que, si $a < b$ i $c \neq 0$, aleshores

$$a \cdot c < b \cdot c.$$

Solució

Suposem primer que $a \leq b$. Per definició de l'ordre, existeix $n \in \mathbb{N}$ tal que

$$b = a + n.$$

Multiplicant per c , obtenim

$$b \cdot c = (a + n) \cdot c.$$

Per la distributivitat del producte respecte de la suma,

$$(a + n) \cdot c = a \cdot c + n \cdot c.$$

Així,

$$b \cdot c = a \cdot c + n \cdot c.$$

Com que $n \cdot c \in \mathbb{N}$, per definició de l'ordre tenim

$$a \cdot c \leq b \cdot c.$$

Suposem ara que $a < b$ i $c \neq 0$. Aleshores existeix $n \in \mathbb{N}$, amb $n \neq 0$, tal que

$$b = a + n.$$

Com abans,

$$b \cdot c = a \cdot c + n \cdot c.$$

Com que $n \neq 0$ i $c \neq 0$, pel resultat sobre el producte nul tenim

$$n \cdot c \neq 0.$$

Per tant, per definició de l'ordre estricte,

$$a \cdot c < b \cdot c.$$

Exercici 2.9 (Cancel·lació del producte)

Prova que, per a tots $a, b, c \in \mathbb{N}$, si $c \neq 0$ i

$$a \cdot c = b \cdot c,$$

aleshores

$$a = b.$$

Solució

Suposem que $c \neq 0$ i que

$$a \cdot c = b \cdot c.$$

Per la tricotomia de l'ordre en $\mathbb{N}$, es compleix exactament una de les tres possibilitats:

$$a < b, \quad a = b, \quad b < a.$$

Si $a < b$, com que $c \neq 0$, per la compatibilitat estricta de l'ordre amb el producte tenim

$$a \cdot c < b \cdot c,$$

cosa que contradiu la igualtat $a \cdot c = b \cdot c$.

Si $b < a$, de la mateixa manera obtenim

$$b \cdot c < a \cdot c,$$

que també contradiu $a \cdot c = b \cdot c$.

Per tant, l'única possibilitat és

$$a = b.$$

Exercici 2.10 (Potències definides per recursió)

Siguin $a, n \in \mathbb{N}$. Definim les potències de base a per recursió:

$$\begin{cases} a^0 = 1, \\ a^{S(n)} = a^n \cdot a. \end{cases}$$

Prova que, per a tots $m, n \in \mathbb{N}$,

$$a^m \cdot a^n = a^{m+n}.$$

Solució

Fixem $a, m \in \mathbb{N}$ i fem inducció sobre n .

Per a $n = 0$, tenim

$$a^m \cdot a^0 = a^m \cdot 1 = a^m.$$

Com que $m + 0 = m$, obtenim

$$a^m \cdot a^0 = a^{m+0}.$$

Suposem ara que la propietat és certa per a un cert $n \in \mathbb{N}$, és a dir,

$$a^m \cdot a^n = a^{m+n}.$$

Volem provar que també és certa per a $S(n)$. Per la definició de potència,

$$a^m \cdot a^{S(n)} = a^m \cdot (a^n \cdot a).$$

Per l'associativitat del producte,

$$a^m \cdot (a^n \cdot a) = (a^m \cdot a^n) \cdot a.$$

Per la hipòtesi d'inducció,

$$(a^m \cdot a^n) \cdot a = a^{m+n} \cdot a.$$

Per la definició de potència,

$$a^{m+n} \cdot a = a^{S(m+n)}.$$

Finalment, com que

$$m + S(n) = S(m + n),$$

tenim

$$a^{S(m+n)} = a^{m+S(n)}.$$

Per tant,

$$a^m \cdot a^{S(n)} = a^{m+S(n)}.$$

Pel principi d'inducció, queda provat que

$$a^m \cdot a^n = a^{m+n}$$

per a tots $m, n \in \mathbb{N}$.

2.2 Enters i propietats

Exercici 2.11 (Classes d'equivalència en $\mathbb{Z}$)

Decideix si els parells $(4, 9)$, $(7, 12)$, $(10, 15)$ i $(2, 5)$ representen el mateix enter.

Solució

Recordem que $(a, b) \sim (c, d)$ si $a + d = b + c$. Comparem:

$$(4, 9) \sim (7, 12) \iff 4 + 12 = 9 + 7,$$

i això és cert perquè tots dos membres valen 16. També

$$(4, 9) \sim (10, 15) \iff 4 + 15 = 9 + 10,$$

i tots dos membres valen 19. En canvi,

$$(4, 9) \sim (2, 5) \iff 4 + 5 = 9 + 2,$$

que és fals, perquè $9 \neq 11$. Per tant, els tres primers parells representen l'enter -5 , mentre que $(2, 5)$ representa -3 .

Exercici 2.12 (Suma i oposat)

Siguin

$$x = [(3, 8)], \quad y = [(10, 4)].$$

Calcula $x + y$, $-x$ i $x - y$.

Solució

Per definició,

$$x + y = [(3 + 10, 8 + 4)] = [(13, 12)].$$

Aquesta classe representa 1. L'oposat és

$$-x = [(8, 3)].$$

Finalment,

$$x - y = x + (-y) = [(3, 8)] + [(4, 10)] = [(7, 18)],$$

que representa -11 .

Exercici 2.13 (Producte d'enters com a classes)

Calcula

$$[(2, 7)] \cdot [(9, 4)].$$

Interpreta el resultat amb la notació usual d'enters.

Solució

La fórmula del producte és

$$[(a, b)] [(c, d)] = [(ac + bd, ad + bc)].$$

Per tant,

$$[(2, 7)] \cdot [(9, 4)] = [(2 \cdot 9 + 7 \cdot 4, 2 \cdot 4 + 7 \cdot 9)] = [(46, 71)].$$

La classe $[(46, 71)]$ representa $46 - 71 = -25$. Això concorda amb la interpretació usual:

$$(2 - 7)(9 - 4) = (-5) \cdot 5 = -25.$$

Exercici 2.14 (Ordre en $\mathbb{Z}$)

Comprova, usant la definició d'ordre per classes, que

$$[(2, 9)] < [(5, 1)].$$

Solució

Per definició,

$$[(a, b)] \leq [(c, d)] \iff a + d \leq c + b.$$

En aquest cas,

$$2 + 1 \leq 5 + 9,$$

és a dir, $3 \leq 14$, que és cert. A més, les classes no són iguals, perquè

$$2 + 1 \neq 9 + 5.$$

Per tant,

$$[(2, 9)] < [(5, 1)].$$

Exercici 2.15 (Equacions de la forma $x + a = b$)

Resol en $\mathbb{Z}$ l'equació

$$x + 7 = 5.$$

Interpreta la solució utilitzant classes d'equivalència.

Solució

Volem trobar un enter x tal que

$$x + 7 = 5.$$

Això equival a

$$x = 5 - 7.$$

Com que identifiquem 5 i 7 amb els enters $[(5, 0)]$ i $[(7, 0)]$, tenim

$$5 - 7 = [(5, 0)] - [(7, 0)].$$

Per definició de la resta en $\mathbb{Z}$,

$$[(5, 0)] - [(7, 0)] = [(5, 0)] + [-(7, 0)].$$

Com que l'oposat de $[(7, 0)]$ és $[(0, 7)]$, obtenim

$$[(5, 0)] + [(0, 7)] = [(5, 7)].$$

Per tant,

$$x = [(5, 7)].$$

Aquest enter correspon a -2 , ja que representa la diferència $5 - 7$.

Comprovem-ho:

$$[(5, 7)] + [(7, 0)] = [(12, 7)].$$

Ara bé,

$$[(12, 7)] = [(5, 0)],$$

perquè

$$12 + 0 = 7 + 5.$$

Així,

$$x + 7 = 5.$$

Exercici 2.16 (Producte i signe)

Calcula els productes següents i interpreta'n el signe:

$$[(0, 3)] \cdot [(0, 4)], \quad [(5, 0)] \cdot [(0, 2)], \quad [(0, 6)] \cdot [(7, 0)].$$

Solució

Recordem que

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

En primer lloc,

$$[(0, 3)] \cdot [(0, 4)] = [(0 \cdot 0 + 3 \cdot 4, 0 \cdot 4 + 3 \cdot 0)] = [(12, 0)].$$

Per tant,

$$(-3) \cdot (-4) = 12.$$

El producte de dos enters negatius és positiu.

En segon lloc,

$$[(5, 0)] \cdot [(0, 2)] = [(5 \cdot 0 + 0 \cdot 2, 5 \cdot 2 + 0 \cdot 0)] = [(0, 10)].$$

Per tant,

$$5 \cdot (-2) = -10.$$

Finalment,

$$[(0, 6)] \cdot [(7, 0)] = [(0 \cdot 7 + 6 \cdot 0, 0 \cdot 0 + 6 \cdot 7)] = [(0, 42)].$$

Per tant,

$$(-6) \cdot 7 = -42.$$

Exercici 2.17 (Compatibilitat de l'ordre amb la suma)

Siguin $a, b, c \in \mathbb{Z}$. Demostra que, si

$$a \leq b,$$

aleshores

$$a + c \leq b + c.$$

Solució

Suposem que

$$a \leq b.$$

Això vol dir que

$$b - a \geq 0.$$

Ara bé,

$$(b + c) - (a + c) = b + c - a - c = b - a.$$

Com que

$$b - a \geq 0,$$

obtenim

$$(b + c) - (a + c) \geq 0.$$

Per tant,

$$a + c \leq b + c.$$

Així, sumar un mateix enter als dos membres d'una desigualtat no en modifica el sentit.

Exercici 2.18 (Multiplicació d'una desigualtat per un enter positiu o negatiu)

Siguin $a, b, c \in \mathbb{Z}$ amb

$$a \leq b.$$

Demostra que:

- (i) si $c \geq 0$, aleshores $ac \leq bc$,
- (ii) si $c \leq 0$, aleshores $bc \leq ac$.

Solució

Com que

$$a \leq b,$$

tenim

$$b - a \geq 0.$$

(i) Suposem primer que

$$c \geq 0.$$

Aleshores el producte de dos enters no negatius és no negatiu, i per tant

$$(b - a)c \geq 0.$$

Per la propietat distributiva,

$$(b - a)c = bc - ac.$$

Així,

$$bc - ac \geq 0.$$

Per tant,

$$ac \leq bc.$$

(ii) Suposem ara que

$$c \leq 0.$$

Aleshores

$$-c \geq 0.$$

Com que

$$b - a \geq 0$$

i

$$-c \geq 0,$$

tenim

$$(b - a)(-c) \geq 0.$$

Per la propietat distributiva,

$$(b - a)(-c) = ac - bc.$$

Així,

$$ac - bc \geq 0.$$

Per tant,

$$bc \leq ac.$$

Això mostra que, quan multipliquem una desigualtat per un enter positiu, el sentit de la desigualtat es conserva, mentre que, quan la multipliquem per un enter negatiu, el sentit s'inverteix.

Exercici 2.19 (Ús de la compatibilitat de l'ordre amb les operacions)

Resol la desigualtat

$$-3x + 2 \leq 11$$

en el conjunt dels nombres enters.

Solució

Partim de la desigualtat

$$-3x + 2 \leq 11.$$

Restem 2 als dos membres:

$$-3x \leq 9.$$

Ara multipliquem els dos membres per -1 . Com que multipliquem per un enter negatiu, el sentit de la desigualtat s'inverteix:

$$3x \geq -9.$$

Això equival a

$$-9 \leq 3x.$$

Com que $3 > 0$, podem dividir intuïtivament per 3, o bé observar que això equival a

$$x \geq -3.$$

Per tant, les solucions enteres són

$$x \in \mathbb{Z} \quad \text{amb} \quad x \geq -3.$$

És a dir,

$$x \in \{-3, -2, -1, 0, 1, 2, \dots\}.$$

Exercici 2.20 (Oposat i valor absolut)

Demostra que, per a tot $n \in \mathbb{Z}$,

$$|-n| = |n|.$$

Solució

Distingim casos segons el signe de n .

Si $n \geq 0$, aleshores

$$|n| = n.$$

En aquest cas, $-n \leq 0$, i per tant

$$|-n| = -(-n) = n.$$

Així,

$$|-n| = |n|.$$

Si $n < 0$, aleshores

$$|n| = -n.$$

En aquest cas, $-n > 0$, i per tant

$$|-n| = -n.$$

Així,

$$|-n| = |n|.$$

Per tant, en tots els casos,

$$|-n| = |n|.$$

Exercici 2.21 (Distància entre enters)

Demostra que, per a tots $n, m \in \mathbb{Z}$,

$$|n - m| = |m - n|.$$

Solució

Observem que

$$n - m = -(m - n).$$

Per la propietat demostrada a l'exercici anterior,

$$|-(m - n)| = |m - n|.$$

Per tant,

$$|n - m| = |-(m - n)| = |m - n|.$$

Exercici 2.22 (Valor absolut d'un producte)

Demostra que, per a tots $n, m \in \mathbb{Z}$,

$$|n \cdot m| = |n| \cdot |m|.$$

Solució

Distingim casos segons els signes de n i m .

Si $n \geq 0$ i $m \geq 0$, aleshores $n \cdot m \geq 0$ i, per tant,

$$|n \cdot m| = n \cdot m = |n| \cdot |m|.$$

Si $n \geq 0$ i $m < 0$, aleshores $n \cdot m \leq 0$. Per tant,

$$|n \cdot m| = -(n \cdot m) = n \cdot (-m).$$

Com que $|n| = n$ i $|m| = -m$, obtenim

$$|n \cdot m| = |n| \cdot |m|.$$

Si $n < 0$ i $m \geq 0$, el raonament és anàleg:

$$|n \cdot m| = (-n) \cdot m = |n| \cdot |m|.$$

Finalment, si $n < 0$ i $m < 0$, aleshores $n \cdot m > 0$. Per tant,

$$|n \cdot m| = n \cdot m.$$

Ara bé, com que $|n| = -n$ i $|m| = -m$, tenim

$$|n| \cdot |m| = (-n)(-m) = n \cdot m.$$

Així,

$$|n \cdot m| = |n| \cdot |m|.$$

Exercici 2.23 (Desigualtat triangular)

Demostra que, per a tots $n, m \in \mathbb{Z}$,

$$|n + m| \leq |n| + |m|.$$

Solució

Per les propietats bàsiques del valor absolut, sabem que

$$-|n| \leq n \leq |n|$$

i

$$-|m| \leq m \leq |m|.$$

Sumant aquestes desigualtats, obtenim

$$-(|n| + |m|) \leq n + m \leq |n| + |m|.$$

Com que

$$|n| + |m| \geq 0,$$

podem aplicar la propietat

$$|x| \leq k \iff -k \leq x \leq k,$$

amb

$$x = n + m \quad \text{i} \quad k = |n| + |m|.$$

Així,

$$|n + m| \leq |n| + |m|.$$

Exercici 2.24 (Desigualtats amb valor absolut)

Troba tots els enters $n \in \mathbb{Z}$ que compleixen

$$|n - 3| \leq 2.$$

Solució

Utilitzem la propietat

$$|x| \leq k \iff -k \leq x \leq k,$$

amb

$$x = n - 3 \quad \text{i} \quad k = 2.$$

Així,

$$|n - 3| \leq 2$$

equivaleix a

$$-2 \leq n - 3 \leq 2.$$

Sumant 3 a tots els membres, obtenim

$$1 \leq n \leq 5.$$

Per tant, els enters que compleixen la desigualtat són

$$n \in \{1, 2, 3, 4, 5\}.$$

Exercici 2.25 (Teorema de la divisió en $\mathbb{Z}$)

Troba el quocient i el residu de la divisió de -37 entre 5 , i també de la divisió de -37 entre -5 .

Solució

Primer dividim -37 entre 5 . Busquem $q, r \in \mathbb{Z}$ tals que

$$-37 = 5q + r$$

i

$$0 \leq r < 5.$$

Si prenem $q = -8$, obtenim

$$5q = 5 \cdot (-8) = -40.$$

Per tant,

$$-37 = -40 + 3 = 5 \cdot (-8) + 3.$$

Així, en la divisió de -37 entre 5 , el quocient és

$$q = -8$$

i el residu és

$$r = 3.$$

Ara dividim -37 entre -5 . Busquem $q, r \in \mathbb{Z}$ tals que

$$-37 = (-5)q + r$$

i

$$0 \leq r < |-5| = 5.$$

Si prenem $q = 8$, obtenim

$$(-5) \cdot 8 = -40.$$

Per tant,

$$-37 = -40 + 3 = (-5) \cdot 8 + 3.$$

Així, en la divisió de -37 entre -5 , el quocient és

$$q = 8$$

i el residu és

$$r = 3.$$

Exercici 2.26 (Divisibilitat en $\mathbb{Z}$)

Determina si les afirmacions següents són certes o falses:

$$-4 \mid 20, \quad 4 \mid (-20), \quad -5 \mid (-35), \quad 6 \mid 20.$$

Solució

Recordem que, si $a, b \in \mathbb{Z}$ i $a \neq 0$, diem que

$$a \mid b$$

si existeix $q \in \mathbb{Z}$ tal que

$$b = aq.$$

En primer lloc,

$$-4 \mid 20,$$

perquè

$$20 = (-4) \cdot (-5).$$

Per tant, l'afirmació és certa.

En segon lloc,

$$4 \mid (-20),$$

perquè

$$-20 = 4 \cdot (-5).$$

Per tant, l'afirmació és certa.

En tercer lloc,

$$-5 \mid (-35),$$

perquè

$$-35 = (-5) \cdot 7.$$

Per tant, l'afirmació és certa.

Finalment,

$$6 \nmid 20.$$

En efecte, no existeix cap $q \in \mathbb{Z}$ tal que

$$20 = 6q,$$

ja que 20 no és múltiple de 6.

Així,

$$-4 \mid 20, \quad 4 \mid (-20), \quad -5 \mid (-35),$$

però

$$6 \nmid 20.$$

Exercici 2.27 (Divisors enters d'un nombre)

Troba tots els divisors enters de 18.

Solució

Busquem tots els enters $d \in \mathbb{Z}$, amb $d \neq 0$, tals que

$$d \mid 18.$$

És a dir, busquem tots els enters d per als quals existeix $q \in \mathbb{Z}$ tal que

$$18 = dq.$$

Primer trobem els divisors positius de 18:

$$1, 2, 3, 6, 9, 18.$$

Com que treballem en $\mathbb{Z}$, també hem de considerar els divisors negatius corresponents:

$$-1, -2, -3, -6, -9, -18.$$

Per exemple,

$$18 = (-3) \cdot (-6),$$

de manera que -3 també és divisor de 18.

Per tant, els divisors enters de 18 són

$$\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18.$$

És a dir,

$$\{-18, -9, -6, -3, -2, -1, 1, 2, 3, 6, 9, 18\}.$$

Exercici 2.28 (Propietats bàsiques de la divisibilitat en $\mathbb{Z}$)

Siguin $a, b, c \in \mathbb{Z}$, amb $a \neq 0$. Demostra que, si

$$a \mid b \quad \text{i} \quad a \mid c,$$

aleshores

$$a \mid (b - c).$$

Solució

Suposem que

$$a \mid b \quad \text{i} \quad a \mid c.$$

Per la definició de divisibilitat en $\mathbb{Z}$, existeixen $q, r \in \mathbb{Z}$ tals que

$$b = aq \quad \text{i} \quad c = ar.$$

Per tant,

$$b - c = aq - ar.$$

Factoritzant a , obtenim

$$b - c = a(q - r).$$

Com que

$$q - r \in \mathbb{Z},$$

existeix un enter $q - r$ tal que

$$b - c = a(q - r).$$

Així, per definició de divisibilitat,

$$a \mid (b - c).$$

Exercici 2.29 (Transitivitat de la divisibilitat)

Siguin $a, b, c \in \mathbb{Z}$, amb $a \neq 0$ i $b \neq 0$. Demostrea que, si

$$a \mid b \quad \text{i} \quad b \mid c,$$

aleshores

$$a \mid c.$$

Solució

Suposem que

$$a \mid b \quad \text{i} \quad b \mid c.$$

Per la definició de divisibilitat en $\mathbb{Z}$, existeixen $q, r \in \mathbb{Z}$ tals que

$$b = aq \quad \text{i} \quad c = br.$$

Substituint la primera igualtat en la segona, obtenim

$$c = (aq)r.$$

Per associativitat del producte,

$$c = a(qr).$$

Com que

$$qr \in \mathbb{Z},$$

existeix un enter qr tal que

$$c = a(qr).$$

Per tant,

$$a \mid c.$$

2.2.1 Operacions combinades amb nombres enters

En les operacions combinades amb nombres enters cal respectar l'ordre habitual de les operacions:

1. parèntesis;
2. potències i arrels;
3. multiplicacions i divisions;
4. sumes i restes.

També cal tenir una cura especial amb els signes. Recordem que el producte o el quocient de dos nombres enters amb el mateix signe és positiu, mentre que el producte o el quocient de dos nombres enters amb signes diferents és negatiu.

Observació 2.1

La divisió de dos nombres enters no sempre dona un nombre enter. En aquesta subsecció només farem divisions exactes, és a dir, divisions el resultat de les quals és un nombre enter.

Exercici 2.30

Calculeu:

$$-7 + 12 - 5 - 9.$$

Solució

Agrupem els termes positius i els termes negatius:

$$-7 + 12 - 5 - 9 = 12 - (7 + 5 + 9).$$

Com que

$$7 + 5 + 9 = 21,$$

tenim

$$12 - 21 = -9.$$

Per tant,

$$-7 + 12 - 5 - 9 = -9.$$

Exercici 2.31

Calculeu:

$$-3 \cdot (5 - 8) + 4 \cdot (-2).$$

Solució

Primer resollem el parèntesi:

$$5 - 8 = -3.$$

Per tant,

$$-3 \cdot (5 - 8) + 4 \cdot (-2) = -3 \cdot (-3) + 4 \cdot (-2).$$

Ara fem els productes:

$$-3 \cdot (-3) = 9$$

i

$$4 \cdot (-2) = -8.$$

Així,

$$9 + (-8) = 1.$$

Per tant,

$$-3 \cdot (5 - 8) + 4 \cdot (-2) = 1.$$

Exercici 2.32

Calculeu:

$$18 : (-3) - 2 \cdot (4 - 9).$$

Solució

Primer resollem el parèntesi:

$$4 - 9 = -5.$$

Aleshores

$$18 : (-3) - 2 \cdot (4 - 9) = 18 : (-3) - 2 \cdot (-5).$$

Ara fem la divisió i el producte:

$$18 : (-3) = -6$$

i

$$2 \cdot (-5) = -10.$$

Per tant,

$$-6 - (-10) = -6 + 10 = 4.$$

Així,

$$18 : (-3) - 2 \cdot (4 - 9) = 4.$$

Exercici 2.33

Calculeu:

$$(-2)^4 - 3^2 \cdot (-1) + (-5).$$

Solució

Primer calculem les potències:

$$(-2)^4 = 16$$

i

$$3^2 = 9.$$

Per tant,

$$(-2)^4 - 3^2 \cdot (-1) + (-5) = 16 - 9 \cdot (-1) - 5.$$

Ara fem el producte:

$$9 \cdot (-1) = -9.$$

Així,

$$16 - (-9) - 5 = 16 + 9 - 5 = 20.$$

Per tant,

$$(-2)^4 - 3^2 \cdot (-1) + (-5) = 20.$$

Exercici 2.34

Calculeu:

$$-2^4 + (-2)^4.$$

Solució

Aquest exercici és important perquè mostra el paper dels parèntesis.

En primer lloc,

$$-2^4 = -(2^4) = -16.$$

En canvi,

$$(-2)^4 = 16.$$

Per tant,

$$-2^4 + (-2)^4 = -16 + 16 = 0.$$

Exercici 2.35

Calculeu:

$$\sqrt{49} - \sqrt[3]{-27} + (-3)^2.$$

Solució

Calculem cada terme:

$$\sqrt{49} = 7,$$

perquè l'arrel quadrada principal és no negativa.

També tenim

$$\sqrt[3]{-27} = -3,$$

perquè

$$(-3)^3 = -27.$$

Finalment,

$$(-3)^2 = 9.$$

Per tant,

$$\sqrt{49} - \sqrt[3]{-27} + (-3)^2 = 7 - (-3) + 9.$$

Així,

$$7 - (-3) + 9 = 7 + 3 + 9 = 19.$$

Exercici 2.36

Calculeu:

$$\left[(-4)^2 - 3 \cdot (6 - 10)\right] : (-7).$$

Solució

Primer resollem el parèntesi interior:

$$6 - 10 = -4.$$

Aleshores

$$3 \cdot (6 - 10) = 3 \cdot (-4) = -12.$$

També tenim

$$(-4)^2 = 16.$$

Per tant,

$$(-4)^2 - 3 \cdot (6 - 10) = 16 - (-12) = 28.$$

Ara fem la divisió:

$$28 : (-7) = -4.$$

Així,

$$\left[(-4)^2 - 3 \cdot (6 - 10) \right] : (-7) = -4.$$

Exercici 2.37

Calculeu:

$$-5 + 2 \left[3^2 - \sqrt{16} - (-2)^3 \right].$$

Solució

Primer calculem les potències i l'arrel:

$$3^2 = 9, \quad \sqrt{16} = 4, \quad (-2)^3 = -8.$$

Per tant,

$$3^2 - \sqrt{16} - (-2)^3 = 9 - 4 - (-8).$$

Ara simplifiquem:

$$9 - 4 - (-8) = 9 - 4 + 8 = 13.$$

Així,

$$-5 + 2 \left[3^2 - \sqrt{16} - (-2)^3 \right] = -5 + 2 \cdot 13.$$

Finalment,

$$-5 + 26 = 21.$$

Per tant,

$$-5 + 2 \left[3^2 - \sqrt{16} - (-2)^3 \right] = 21.$$

2.3 Aplicacions i modelització

Els nombres naturals i enters no serveixen només per fer càlculs abstractes. També permeten descriure i resoldre situacions molt habituals: organitzar grups, repartir objectes, estudiar cicles que es repeteixen, interpretar saldos, comparar temperatures, mesurar diferències o saber si una quantitat es pot repartir exactament.

En cada cas, el pas important és identificar quina estructura matemàtica hi ha darrere de la situació. Si volem formar grups iguals tan grans com sigui possible, apareix el màxim comú divisor. Si volem saber quan coincideixen dos processos periòdics, apareix el mínim comú múltiple. Si repartim una quantitat i en sobra una

part, fem servir la divisió amb residu. Si treballem amb guanys, pèrdues, temperatures sota zero o desnivells, necessitem els nombres enters. I si només ens interessa la distància entre dues quantitats, sense importar el signe, fem servir el valor absolut.

Les situacions següents mostren com les idees treballades en aquesta unitat apareixen de manera natural en problemes quotidians.

Exercici 2.38 (Situació 1. Organitzar grups iguals)

En una activitat de centre hi participen 84 alumnes de primer de batxillerat i 60 alumnes de segon. Es volen formar grups de la mateixa mida, sense barrejar nivells i sense que sobri cap alumne. A més, es vol que els grups siguin tan grans com sigui possible.

Quants alumnes ha de tenir cada grup?

Solució

Cal trobar el nombre més gran que divideixi 84 i 60. Per tant, hem de calcular

$$\text{mcd}(84, 60).$$

Fem la descomposició en factors primers:

$$84 = 2^2 \cdot 3 \cdot 7, \quad 60 = 2^2 \cdot 3 \cdot 5.$$

Els factors comuns amb l'exponent més petit són

$$2^2 \cdot 3 = 12.$$

Per tant,

$$\text{mcd}(84, 60) = 12.$$

Així, cada grup ha de tenir 12 alumnes. Es formaran 7 grups de primer, perquè

$$84 = 12 \cdot 7,$$

i 5 grups de segon, perquè

$$60 = 12 \cdot 5.$$

Exercici 2.39 (Situació 2. Cicles que tornen a coincidir)

Dos autobusos passen per una mateixa parada. El primer passa cada 12 minuts i el segon cada 18 minuts. Si ara acaben de coincidir, d'aquí a quants minuts tornaran a coincidir?

Solució

Cal trobar el primer instant que sigui múltiple de 12 i també de 18. Per tant, hem de calcular

$$\text{mcm}(12, 18).$$

Descomponem:

$$12 = 2^2 \cdot 3, \quad 18 = 2 \cdot 3^2.$$

Prenem tots els factors que apareixen amb l'exponent més gran:

$$\text{mcm}(12, 18) = 2^2 \cdot 3^2 = 36.$$

Així, els dos autobusos tornaran a coincidir d'aquí a 36 minuts.

Exercici 2.40 (Situació 3. Repartiments amb residu)

Una biblioteca ha rebut 157 llibres nous i els vol col·locar en capsas de 12 llibres. Quantes capsas completes es poden omplir? Quants llibres sobraran?

Solució

Hem de fer una divisió amb residu:

$$157 = 12q + r, \quad 0 \leq r < 12.$$

Com que

$$12 \cdot 13 = 156,$$

obtenim

$$157 = 12 \cdot 13 + 1.$$

Per tant, es poden omplir 13 capsas completes i sobrarà 1 llibre.

Aquesta és una aplicació directa del teorema de la divisió: el quocient indica el nombre de capsas completes i el residu indica allò que sobra.

Exercici 2.41 (Situació 4. Saldos positius i negatius)

Una persona té 25 euros al compte. Després paga una factura de 40 euros i, més tard, rep un ingrés de 18 euros. Quin és el saldo final?

Solució

Representem els ingressos amb enters positius i les despeses amb enters negatius. El saldo final és

$$25 - 40 + 18.$$

Primer,

$$25 - 40 = -15.$$

Després,

$$-15 + 18 = 3.$$

Per tant, el saldo final és de 3 euros.

Els nombres enters permeten expressar en un mateix càlcul quantitats a favor i quantitats en contra.

Exercici 2.42 (Situació 5. Comparar temperatures sota zero)

En dues poblacions de muntanya, la temperatura mínima ha estat de -7°C en una i de -3°C en l'altra. En quina població ha fet més fred?

Solució

Cal comparar els enters

$$-7 \quad \text{i} \quad -3.$$

En l'ordre dels enters es compleix

$$-7 < -3.$$

Per tant, ha fet més fred a la població on la temperatura ha estat de

$$-7^{\circ}\text{C}.$$

Aquest exemple mostra que, quan treballem amb nombres negatius, un nombre amb valor numèric aparentment més gran pot representar una quantitat menor. En particular, -7 és menor que -3 .

Exercici 2.43 (Situació 6. Mesurar errors amb valor absolut)

Un termòmetre havia previst una temperatura de 18°C , però la temperatura real ha estat de 15°C . Un altre dia havia previst 11°C , però la temperatura real ha estat de 14°C . En quin dels dos dies l'error ha estat més gran?

Solució

L'error no ha de dependre del signe, sinó de la distància entre la previsió i el valor real. Per això fem servir el valor absolut.

En el primer cas, l'error és

$$|15 - 18| = |-3| = 3.$$

En el segon cas, l'error és

$$|14 - 11| = |3| = 3.$$

Per tant, en tots dos dies l'error ha estat el mateix:

$$3^{\circ}\text{C}.$$

El valor absolut permet mesurar una diferència sense importar si ens hem quedat per sobre o per sota del valor real.

Exercici 2.44 (Situació 7. Repartir un deute exactament)

Un grup de 7 persones ha acumulat un deute conjunt de 84 euros. Volen repartir-lo exactament a parts iguals. Es pot fer? Quin enter representa la part que correspon a cada persona?

Solució

El deute total es pot representar amb l'enter

$$-84.$$

Volem saber si aquest nombre és divisible per 7. Com que

$$-84 = 7 \cdot (-12),$$

tenim

$$7 \mid (-84).$$

Per tant, el deute es pot repartir exactament.

A cada persona li correspon

$$-12$$

euros, és a dir, un deute de 12 euros.

Aquest exemple mostra que la divisibilitat també té sentit en $\mathbb{Z}$: no només podem dividir quantitats positives, sinó també saldos negatius, pèrdues o deutes.

3 Exercicis proposats

3.1 Els nombres naturals

Exercici 3.1 (Ús dels axiomes de Peano)

Usant només els axiomes de Peano, prova que

$$2 \neq 0, \quad 2 \neq 1, \quad 5 \neq 3.$$

Indicació: Escriu $1 = S(0)$, $2 = S(1)$, $3 = S(2)$, etc. Usa que 0 no és successor de cap natural i que el successor és injectiu.

Exercici 3.2 (Suma dels primers naturals)

Demostra per inducció que, per a tot $n \in \mathbb{N}$,

$$2(0 + 1 + 2 + \cdots + n) = n(n + 1).$$

Indicació: Fes inducció sobre n . En el pas inductiu, escriu la suma fins a $n + 1$ com la suma fins a n més $n + 1$, i factoritza $n + 1$.

Exercici 3.3 (Suma dels quadrats)

Demostra per inducció que, per a tot $n \in \mathbb{N}$, amb $n \geq 1$,

$$6(1^2 + 2^2 + \cdots + n^2) = n(n + 1)(2n + 1).$$

Indicació: Fes inducció sobre n . En el pas inductiu, afegeix $6(n + 1)^2$ als dos membres i comprova que el resultat es pot factoritzar com $(n + 1)(n + 2)(2n + 3)$.

Exercici 3.4 (Cancel·lació de la suma)

Demostra que si $a, b, c \in \mathbb{N}$ i

$$a + c = b + c,$$

aleshores

$$a = b.$$

Indicació: Fes inducció sobre c . En el pas inductiu, transforma $a + S(c) = b + S(c)$ en $S(a + c) = S(b + c)$ i usa la injectivitat del successor.

Exercici 3.5 (Cancel·lació de l'ordre amb la suma)

Demostra que, per a tots $a, b, t \in \mathbb{N}$, si

$$a + t \leq b + t,$$

aleshores

$$a \leq b.$$

Indicació: Usa la definició d'ordre: de $a + t \leq b + t$ obtens $b + t = (a + t) + n$ per a algun $n \in \mathbb{N}$. Reordena els termes i aplica la cancel·lació de la suma.

Exercici 3.6 (Compatibilitat de l'ordre amb la suma)

Demostra que si $a, b, c \in \mathbb{N}$ i

$$a \leq b,$$

aleshores

$$a + c \leq b + c.$$

Indicació: Escribeu $b = a + n$ per a algun $n \in \mathbb{N}$. Després suma c i reordena:

$$b + c = (a + c) + n.$$

Exercici 3.7 (Compatibilitat de l'ordre amb el producte)

Demostra que si $a, b, c \in \mathbb{N}$ i

$$a \leq b,$$

aleshores

$$a \cdot c \leq b \cdot c.$$

A més, si $a < b$ i $c \neq 0$, demostra que

$$a \cdot c < b \cdot c.$$

Indicació: Escribeu $b = a + n$. En multiplicar per c , obtens

$$b \cdot c = a \cdot c + n \cdot c.$$

Per a la desigualtat estricta, usa que si $n \neq 0$ i $c \neq 0$, aleshores $n \cdot c \neq 0$.

Exercici 3.8 (Cancel·lació del producte)

Demostra que si $a, b, c \in \mathbb{N}$, $c \neq 0$, i

$$a \cdot c = b \cdot c,$$

aleshores

$$a = b.$$

Indicació: Usa la tricotomia de l'ordre. Si $a < b$, aleshores $a \cdot c < b \cdot c$; si $b < a$, aleshores $b \cdot c < a \cdot c$. Tots dos casos contradiuen la igualtat.

Exercici 3.9 (Potències)

Definim les potències d'un natural a per recursió:

$$a^0 = 1, \quad a^{S(n)} = a^n \cdot a.$$

Demostra que, per a tots $m, n \in \mathbb{N}$,

$$a^m \cdot a^n = a^{m+n}.$$

Indicació: Fixa m i fes inducció sobre n . En el pas inductiu, usa

$$a^{S(n)} = a^n \cdot a$$

i l'associativitat del producte.

Exercici 3.10 (Algorisme d'Euclides)

Calcula

$$\text{mcd}(924, 396)$$

amb l'algorisme d'Euclides i expressa'l com a combinació lineal amb coeficients enters de 924 i 396.

Indicació: Comença dividint 924 entre 396:

$$924 = 396 \cdot 2 + 132.$$

Després divideix 396 entre 132. Per a la combinació lineal, aïlla el residu 132 de la primera igualtat.

Exercici 3.11 (Descomposició en factors primers)

Descompon en factors primers els nombres 840, 1155 i 2025. Calcula després el mcd i el mcm de 840 i 1155.

Indicació: Descompon cada nombre en potències de primers. Per al mcd, pren els factors comuns amb l'exponent més petit. Per al mcm, pren tots els factors amb l'exponent més gran.

3.2 Els nombres enters

Exercici 3.12 (Classes d'equivalència)

Comprova si els parells següents són equivalents en la construcció de $\mathbb{Z}$:

$$(8, 13), \quad (2, 7), \quad (10, 14), \quad (15, 20).$$

Agrupa'ls per classes d'equivalència.

Indicació: Recorda que

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

Compara cada parell amb $(8, 13)$. Tres dels parells representen el mateix enter.

Exercici 3.13 (Representants d'una mateixa classe)

Demostra que, per a tots $a, b, k \in \mathbb{N}$,

$$[(a, b)] = [(a + k, b + k)].$$

Indicació: Cal provar que

$$(a, b) \sim (a + k, b + k).$$

És a dir, comprova que

$$a + (b + k) = b + (a + k)$$

usant l'associativitat i la commutativitat de la suma en $\mathbb{N}$.

Exercici 3.14 (Suma, resta i producte)

Calcula, com a classes d'equivalència:

$$[(6, 11)] + [(9, 2)], \quad [(6, 11)] - [(9, 2)], \quad [(6, 11)] \cdot [(9, 2)].$$

Interpreta cada resultat en la notació usual dels enters.

Indicació: Per a la suma, suma component a component. Per a la resta, primer pren l'oposat de $[(9, 2)]$. Per al producte, usa

$$[(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)].$$

Exercici 3.15 (L'oposat d'un enter)

Prova que l'oposat de

$$[(a, b)]$$

és

$$[(b, a)].$$

Indicació: Suma les dues classes:

$$[(a, b)] + [(b, a)].$$

Has d'obtenir una classe equivalent a $[(0, 0)]$.

Exercici 3.16 (Equacions de la forma $x + a = b$)

Resol en $\mathbb{Z}$ l'equació

$$x + 7 = 5.$$

Dona la solució com a classe d'equivalència i en la notació usual dels enters.

Indicació: Aïlla formalment:

$$x = 5 - 7.$$

Després escriu $5 = [(5, 0)]$, $7 = [(7, 0)]$ i usa la definició de resta.

Exercici 3.17 (Producte d'enters i signe)

Calcula els productes següents i interpreta'n el signe:

$$[(0, 3)] \cdot [(0, 4)], \quad [(5, 0)] \cdot [(0, 2)], \quad [(0, 6)] \cdot [(7, 0)].$$

Indicació: Interpreta primer les classes com enters usuals:

$$[(0, 3)] = -3, \quad [(0, 4)] = -4, \quad [(5, 0)] = 5.$$

Després comprova els resultats amb la fórmula del producte de classes.

Exercici 3.18 (Ordre en $\mathbb{Z}$)

Usant la definició d'ordre en $\mathbb{Z}$, ordena de menor a major les classes següents, indicant si n'hi ha dues d'iguals:

$$[(1, 8)], \quad [(5, 5)], \quad [(9, 2)], \quad [(3, 10)].$$

Indicació: Pots interpretar cada classe com la diferència entre els seus components. Observa especialment que $[(1, 8)]$ i $[(3, 10)]$ representen el mateix enter.

Exercici 3.19 (Compatibilitat de l'ordre amb la suma)

Demostra que, si $x \leq y$ en $\mathbb{Z}$, aleshores

$$x + z \leq y + z$$

per a tot $z \in \mathbb{Z}$.

Indicació: Usa la caracterització

$$x \leq y \iff y - x \geq 0.$$

Després observa que

$$(y + z) - (x + z) = y - x.$$

Exercici 3.20 (Multiplicació d'una desigualtat)

Siguin $a, b, c \in \mathbb{Z}$, amb

$$a \leq b.$$

Demostra que:

- (i) si $c \geq 0$, aleshores $ac \leq bc$,
- (ii) si $c \leq 0$, aleshores $bc \leq ac$.

Indicació: De $a \leq b$ dedueix $b - a \geq 0$. Si $c \geq 0$, estudia $(b - a)c$. Si $c \leq 0$, estudia $(b - a)(-c)$.

Exercici 3.21 (Resolució d'una desigualtat)

Resol en $\mathbb{Z}$ la desigualtat

$$-3x + 2 \leq 11.$$

Indicació: Resta 2 als dos membres. Després multiplica per -1 i recorda que el sentit de la desigualtat s'inverteix.

Exercici 3.22 (Càlculs amb valor absolut)

Calcula:

$$|-8|, \quad |5-12|, \quad |-4 \cdot 6|.$$

Indicació: Calcula primer l'enter que hi ha dins del valor absolut i després pren-ne la distància a 0.

Exercici 3.23 (Oposat i valor absolut)

Demostra que, per a tot $n \in \mathbb{Z}$,

$$|-n| = |n|.$$

Indicació: Distingueix els casos $n \geq 0$ i $n < 0$. En cada cas, aplica directament la definició de valor absolut.

Exercici 3.24 (Distància entre enters)

Demostra que, per a tots $n, m \in \mathbb{Z}$,

$$|n-m| = |m-n|.$$

Indicació: Observa que

$$n-m = -(m-n).$$

Després aplica la propietat $|-x| = |x|$.

Exercici 3.25 (Valor absolut d'un producte)

Demostra que, per a tots $n, m \in \mathbb{Z}$,

$$|nm| = |n||m|.$$

Indicació: Distingueix quatre casos segons els signes de n i m : tots dos no negatius, un no negatiu i l'altre negatiu, o tots dos negatius.

Exercici 3.26 (Desigualtat triangular)

Demostra que, per a tots $n, m \in \mathbb{Z}$,

$$|n+m| \leq |n| + |m|.$$

Indicació: Parteix de

$$-|n| \leq n \leq |n| \quad \text{i} \quad -|m| \leq m \leq |m|.$$

Suma les dues desigualtats i aplica la caracterització de $|x| \leq k$.

Exercici 3.27 (Desigualtats amb valor absolut)

Troba tots els enters $n \in \mathbb{Z}$ que compleixen

$$|n - 3| \leq 2.$$

Indicació: Transforma la desigualtat en

$$-2 \leq n - 3 \leq 2.$$

Després suma 3 als tres membres.

Exercici 3.28 (Teorema de la divisió en $\mathbb{Z}$)

Troba el quocient i el residu de la divisió de -37 entre 5 , i també de la divisió de -37 entre -5 .

Indicació: El residu ha de ser sempre no negatiu i menor que el valor absolut del divisor. Busca q de manera que

$$-37 = bq + r, \quad 0 \leq r < |b|.$$

Exercici 3.29 (Divisibilitat en $\mathbb{Z}$)

Determina si les afirmacions següents són certes o falses:

$$-4 \mid 20, \quad 4 \mid (-20), \quad -5 \mid (-35), \quad 6 \mid 20.$$

Indicació: Usa la definició: $a \mid b$ si existeix $q \in \mathbb{Z}$ tal que $b = aq$. En cada cas, intenta trobar aquest enter q .

Exercici 3.30 (Divisors enters)

Troba tots els divisors enters de 18 .

Indicació: Comença trobant els divisors positius de 18 . Després afegeix els oposats corresponents, perquè en $\mathbb{Z}$ els divisors apareixen per parelles de signe.

Exercici 3.31 (Diferència de múltiples)

Siguin $a, b, c \in \mathbb{Z}$, amb $a \neq 0$. Demostra que, si

$$a \mid b \quad \text{i} \quad a \mid c,$$

aleshores

$$a \mid (b - c).$$

Indicació: Escribeu $b = aq$ i $c = ar$, amb $q, r \in \mathbb{Z}$. Després factoritza:

$$b - c = aq - ar = a(q - r).$$

Exercici 3.32 (Transitivitat de la divisibilitat)

Siguin $a, b, c \in \mathbb{Z}$, amb $a \neq 0$ i $b \neq 0$. Demostra que, si

$$a \mid b \quad \text{i} \quad b \mid c,$$

aleshores

$$a \mid c.$$

Indicació: Escribeu $b = aq$ i $c = br$, amb $q, r \in \mathbb{Z}$. Substitueix b dins de l'expressió de c .

4 Tests

4.1 Test 1: Els nombres naturals

Instruccions. Marca una sola resposta per pregunta. En acabar, prem el botó **Corregir**. El camp **Nota** mostrarà el resultat.

Corregir Netejar **Nota:**

1. Quin axioma garanteix que 0 no és successor de cap nombre natural?
 - (a) La injectivitat de S .
 - (b) L'axioma que afirma que no existeix cap $n \in \mathbb{N}$ tal que $S(n) = 0$.
 - (c) La commutativitat de la suma.
 - (d) La definició del producte.

Correcció:

2. La suma $a + b$ es defineix recursivament per:
 - (a) $a + 0 = a$ i $a + S(b) = S(a + b)$.
 - (b) $a + 0 = 0$ i $a + S(b) = a + b$.
 - (c) $a + b = b + a$, que és una definició.
 - (d) $a + b = a \cdot b$.

Correcció:

3. El producte $a \cdot b$ es defineix recursivament per:
 - (a) $a \cdot 0 = a$ i $a \cdot S(b) = a \cdot b$.
 - (b) $a \cdot 0 = 1$ i $a \cdot S(b) = S(a \cdot b)$.
 - (c) $a \cdot b = b \cdot a$, que és una definició.
 - (d) $a \cdot 0 = 0$ i $a \cdot S(b) = a \cdot b + a$.

Correcció:

4. Segons la definició d'ordre en $\mathbb{N}$, $a \leq b$ vol dir:

- (a) Existeix $n \in \mathbb{N}$ tal que $a = b + n$.
- (b) Existeix $n \in \mathbb{N}$ tal que $b = a + n$.
- (c) a divideix b .
- (d) a i b són primers entre si.

Correcció:

5. La tricotomia de l'ordre afirma que, per a tots $a, b \in \mathbb{N}$:

- (a) Sempre es compleixen alhora $a < b$, $a = b$ i $b < a$.
- (b) Sempre es compleix $a < b$.
- (c) Es compleix exactament una de les tres possibilitats: $a < b$, $a = b$ o $b < a$.
- (d) Cap nombre natural pot ser comparat amb un altre.

Correcció:

6. Si $a \mid b$, amb $a, b \in \mathbb{N}$ i $a \neq 0$, això vol dir que:

- (a) $a = b$.
- (b) $b \mid a$.
- (c) a és primer.
- (d) Existeix $q \in \mathbb{N}$ tal que $b = a \cdot q$.

Correcció:

7. Quin és $\text{mcd}(84, 90)$?

- (a) 6.
- (b) 12.
- (c) 18.
- (d) 1260.

Correcció:

8. Quin és $\text{mcm}(4, 6)$?

- (a) 4.
- (b) 6.
- (c) 12.

(d) 24.

Correcció:

9. Quin dels nombres següents és primer?

(a) 21.

(b) 23.

(c) 25.

(d) 27.

Correcció:

10. Quan és especialment útil el principi d'inducció forta?

(a) Quan per demostrar el cas n convé usar tots els casos anteriors.

(b) Quan no es vol usar cap hipòtesi d'inducció.

(c) Quan es treballa només amb nombres enters negatius.

(d) Quan es vol evitar definir l'ordre en $\mathbb{N}$.

Correcció:

4.2 Test 2: Els nombres enters

Instruccions. Marca una sola resposta per pregunta. En acabar, prem el botó **Corregir**. El camp **Nota** mostrarà el resultat.

Corregir Netejar **Nota:**

1. En la construcció de $\mathbb{Z}$, la relació d'equivalència sobre $\mathbb{N} \times \mathbb{N}$ és:

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

(b) $(a, b) \sim (c, d) \iff ab = cd.$

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

(d) $(a, b) \sim (c, d) \iff a = c.$

Correcció:

2. La classe $[(0, 3)]$ representa habitualment:

(a) 3.

(b) $-3.$

- (c) 0.
- (d) $1/3$.

Correcció:

3. La suma d'enters es defineix per:

- (a) $[(a, b)] + [(c, d)] = [(ac, bd)]$.
- (b) $[(a, b)] + [(c, d)] = [(a + d, b + c)]$.
- (c) $[(a, b)] + [(c, d)] = [(a - c, b - d)]$.
- (d) $[(a, b)] + [(c, d)] = [(a + c, b + d)]$.

Correcció:

4. El producte $[(a, b)] [(c, d)]$ és:

- (a) $[(ac, bd)]$.
- (b) $[(a + c, b + d)]$.
- (c) $[(ac + bd, ad + bc)]$.
- (d) $[(ad, bc)]$.

Correcció:

5. L'oposat de $[(a, b)]$ és:

- (a) $[(b, a)]$.
- (b) $[(a, b)]$.
- (c) $[(0, 0)]$.
- (d) $[(a + 1, b + 1)]$.

Correcció:

6. Segons l'ordre definit en $\mathbb{Z}$, $[(a, b)] \leq [(c, d)]$ si:

- (a) $a + b \leq c + d$.
- (b) $a + c \leq b + d$.
- (c) $ab \leq cd$.
- (d) $a + d \leq b + c$.

Correcció:

7. En $\mathbb{Z}$, la solució de l'equació

$$x + 7 = 5$$

és:

- (a) $[(7, 5)]$.
- (b) $[(5, 7)]$.
- (c) $[(12, 0)]$.
- (d) $[(0, 12)]$.

Correcció:

8. Si $a \leq b$ i $c \leq 0$, aleshores:

- (a) $ac \leq bc$.
- (b) $a + c \geq b + c$.
- (c) $ac = bc$.
- (d) $bc \leq ac$.

Correcció:

9. En la divisió euclidiana de -37 entre 5 , el quocient i el residu són:

- (a) $q = -7, r = -2$.
- (b) $q = -7, r = 2$.
- (c) $q = 8, r = 3$.
- (d) $q = -8, r = 3$.

Correcció:

10. Quina afirmació de divisibilitat en $\mathbb{Z}$ és certa?

- (a) $-4 \mid 20$.
- (b) $6 \mid 20$.
- (c) $5 \mid 23$.
- (d) $0 \mid 12$.

Correcció:

4.3 Test 3: Síntesi: nombres naturals i enters

Instruccions. Marca una sola resposta per pregunta. En acabar, prem el botó **Corregir**. El camp **Nota** mostrarà el resultat.

Corregir Netejar **Nota:**

1. Quina és la manera canònica d'identificar un nombre natural n amb un enter?

- (a) Mitjançant la classe $[(0, n)]$.
- (b) Mitjançant la classe $[(n, 0)]$.
- (c) Mitjançant la classe $[(n, n)]$.
- (d) Mitjançant la classe $[(0, 0)]$.

Correcció:

2. Quina de les equacions següents té solució en $\mathbb{Z}$, però no en $\mathbb{N}$?

- (a) $x + 2 = 5$.
- (b) $x + 5 = 2$.
- (c) $x + 0 = 7$.
- (d) $x + 3 = 3$.

Correcció:

3. Si $a, b \in \mathbb{N}$ i $a \leq b$, què podem dir de l'enter $[(a, b)]$?

- (a) És sempre positiu.
- (b) És sempre nul.
- (c) És no positiu, és a dir, $[(a, b)] \leq 0$.
- (d) No es pot comparar amb 0.

Correcció:

4. Quina igualtat expressa correctament la resta en $\mathbb{Z}$?

- (a) $a - b = a + (-b)$.
- (b) $a - b = a + b$.
- (c) $a - b = b - a$.
- (d) $a - b = -(a + b)$.

Correcció:

5. Si $p, q \in \mathbb{N} \setminus \{0\}$, quin és el resultat de

$$[(0, p)] \cdot [(0, q)]?$$

- (a) Un enter negatiu.
- (b) La classe $[(0, pq)]$.
- (c) La classe $[(p, q)]$.

- (d) La classe $[(pq, 0)]$, que representa un enter positiu.

Correcció:

6. Quina diferència hi ha entre els divisors de 12 en $\mathbb{N}$ i en $\mathbb{Z}$?

- (a) En $\mathbb{Z}$, 12 no té divisors.
(b) En $\mathbb{N}$, 12 té divisors negatius.
(c) En $\mathbb{Z}$, també apareixen els oposats dels divisors positius.
(d) En $\mathbb{N}$ i en $\mathbb{Z}$ els divisors són exactament els mateixos.

Correcció:

7. En el teorema de la divisió en $\mathbb{Z}$, si $a = bq + r$, amb $b \neq 0$, quina condició ha de complir el residu?

- (a) $-|b| < r < |b|$.
(b) $0 \leq r < |b|$.
(c) $0 < r \leq |b|$.
(d) $r < 0$.

Correcció:

8. Quina afirmació és correcta sobre el màxim comú divisor en el context dels enters?

- (a) Es pren habitualment el representant positiu; per exemple, $\text{mcd}(18, 24) = 6$.
(b) Sempre es pren el representant negatiu; per exemple, $\text{mcd}(18, 24) = -6$.
(c) No té sentit parlar de màxim comú divisor en $\mathbb{Z}$.
(d) El màxim comú divisor de dos enters sempre és 0.

Correcció:

9. Si $n \in \mathbb{N} \setminus \{0\}$, què representa l'enter $[(0, n)]$?

- (a) El natural n .
(b) L'enter 0.
(c) L'enter negatiu $-n$.
(d) Un nombre que no pertany a $\mathbb{Z}$.

Correcció:

10. Quin mètode és natural per demostrar que tot nombre natural $n \geq 2$ és primer o producte de primers?

- (a) La inducció forta.
- (b) La definició de l'oposat en $\mathbb{Z}$.
- (c) La divisió euclidiana amb divisor negatiu.
- (d) La definició de valor absolut.

Correcció:

4.4 Test 4: Síntesi avançada i operacions combinades

Instruccions. Marca una sola resposta per pregunta. En acabar, prem el botó **Corregir**. El camp **Nota** mostrarà el resultat.

Corregir Netejar **Nota:**

1. Quin és el valor de l'expressió

$$-3^2 + (-3)^2?$$

- (a) 18.
- (b) -18.
- (c) 0.
- (d) -9.

Correcció:

2. Calculeu:

$$-7 + 4 \cdot (3 - 8) - 18 : (-3).$$

- (a) -33.
- (b) -21.
- (c) -9.
- (d) 19.

Correcció:

3. Calculeu:

$$(-2)^3 - 5 \cdot (-4) + 36 : (-6).$$

- (a) -34 .
- (b) -18 .
- (c) 6 .
- (d) 18 .

Correcció:

4. Quin és el resultat de

$$-2^4 + (-2)^4 - (-3)^2?$$

- (a) -9 .
- (b) 9 .
- (c) -41 .
- (d) 0 .

Correcció:

5. Calculeu:

$$\left[(-4)^2 - 5 \cdot (3 - 7)\right] : (-12).$$

- (a) 3 .
- (b) -1 .
- (c) 12 .
- (d) -3 .

Correcció:

6. Calculeu:

$$\sqrt{64} - \sqrt[3]{-125} + (-2)^5.$$

- (a) -29 .
- (b) -19 .
- (c) -9 .
- (d) 45 .

Correcció:

7. Quin és el valor de

$$\left|-3^2 + (-3)^2 - 5\right|?$$

- (a) 23 .
- (b) 13 .

(c) -5 .

(d) 5 .

Correcció:

8. Quin enter representa l'expressió següent?

$$[(0, 4)] \cdot [(3, 0)] + [(5, 2)].$$

(a) $[(0, 9)]$.

(b) $[(9, 0)]$.

(c) $[(0, 15)]$.

(d) $[(15, 0)]$.

Correcció:

9. Sigui

$$a = (-3)^3 + 2 \cdot 8 - 5.$$

En la divisió euclidiana de a entre 5, quin és el quocient i quin és el residu?

(a) $q = -3, r = -1$.

(b) $q = -3, r = 1$.

(c) $q = -4, r = 4$.

(d) $q = 4, r = -36$.

Correcció:

10. En la recta numèrica, quin enter està a distància 7 de -2 i és més petit que -2 ?

(a) 5 .

(b) 9 .

(c) -9 .

(d) -5 .

Correcció:

11. Calculeu:

$$\text{mcd}(-84, 60) - \text{mcm}(12, 18).$$

(a) 24 .

(b) -24 .

(c) 48 .

(d) $-48.$

Correcció:

12. Quina de les expressions següents no representa un nombre enter?

(a) $14 : 5.$

(b) $\sqrt{81} - \sqrt[3]{-27}.$

(c) $(-2)^5 + 3 \cdot 7.$

(d) $(-18) : 3 + 4.$

Correcció: