Alef$_0$

Algebră

Numere întregi

ALEF₀/ALGEBRĂ

ALEF$_0$/ALGÈBRE

Terminale C nombres entiers

C. GAUTIER
G. GIRARD
D. GERLL
C. THIERCÉ
A. WARUSFEL

L'ensemble N des nombres entiers a été étendu à des „nombres" cardinaux transfinis, traditionnellement désignés par la lettre hébraïque aleph diversement indexée. Aleph-zéro représente ainsi le cardinal de N lui-même. Aleph-un est le plus petit cardinal supérieur a Aleph-zéro et ainsi de suite.

Classiques Hachette, 79 Boulevard Saint-Germain, Paris

ALEF₀/ALGEBRĂ

Numere întregi

C. GAUTIER
G. GIRARD
D. GERLL
C. THIERCÉ
A. WARUSFEL

Editura didactică și pedagogică — București, 1974

Traducerea din limba franceză:

ELISABETA IORGULESCU
ANGELICĂ IORGULESCU
AFRODITA GÎRLEANU
ECATERINA VASILESCU
NATALIA PETRIN

Confruntarea traducerii: prof. univ. dr. CONSTANTIN POPOVICI
Redactor: prof. EUGENIA PANTELIMON
Tehnoredactor: VIORICA CONDOPOL

Prefață

Acest fascicul este consacrat studiului numerelor întregi. În zilele noastre, un curs de aritmetică este compus din două părți distincte.

Prima parte studiază construcțiile, mai mult sau mai puțin axiomatice, ale mulțimilor **N** *și* **Z**. *Mulțimea* **N** *poate fi introdusă în multe feluri. Matematicienii o obțin ca un derivat al teoriei cardinalilor. Rațiuni tehnice evidente ne interzic o astfel de metodă; dacă ar fi fost simplu să definim întregii plecînd de la mulțimi finite, am fi ales această cale; dar o anexă, care conține organigrama unui astfel de studiu, dovedește că aceasta depășește cu mult nivelul unei clase terminale normale.*

Rămîneau deci două axiomatizări clasice: aceea a lui Peano-Dedekind, pe care am ales-o, și axiomatica bazată pe proprietățile ordinale ale submulțimilor lui **N**. *Dealtfel am demonstrat cu grijă echivalența dintre cele două puncte de vedere, la fel de importante.*

Axiomatica lui Peano se generalizează foarte ușor la mulțimea **Z** *pe care am definit-o, intuitiv, plecînd de la mulțimi de întregi pozitivi și negativi, izomorfe amîndouă cu* **N**. *Noțiunea de inducție dublă ne permite demonstrații foarte apropiate de cele care figurează în primul capitol. Definirea lui* **Z** *ca mulțime cît, mai uzuală poate, este prezentată într-un șir de probleme foarte detaliat: profesorul va putea s-o adapteze, dacă dorește, la cursul său personal.*

În orice caz, structura de inel a mulțimii $\mathbf{Z}/n\mathbf{Z}$ *a fost stabilită cu ajutorul unei treceri la cît. Ni s-a părut interesant din punct de vedere pedagogic să variem la maximum procedeele de construcție, ca să nu lăsăm să se creadă că orice structură algebrică se definește automat printr-o relație de echivalență bine aleasă. (De aceea, într-un alt fascicul:* **C** *este studiat ca mulțime de matrice și nu ca mulțime cît a unui inel de polinoame,* Q *este intersecția tuturor subcorpurilor lui* **R** *— existența căruia este presupusă — care conțin unitatea multiplicativă).*

A doua parte este mai tradițională și cuprinde studiul divizibilității.

Acest studiu l-am plasat în **Z** *de cele mai multe ori și nu în* **N**, *în ciuda unor complicații care apar pe parcurs.*

Nedorind „să modernizăm" cu orice preț, n-am căutat generalizarea cea mai mare. Astfel, cu toate că este vorba de proprietățile idealelor lui **Z**, *am vorbit aproape exclusiv de cele ale subgrupurilor lui* **Z**, *deoarece, din fericire, aceste două noțiuni coincid în acest caz, iar noțiunea de subgrup este mai simplă.*

Din contră, n-am ezitat să introducem de la început noțiunile de c.m.M.d.c. și c.m.m.m.c. pentru o familie de întregi — și nu pentru o mulțime — în loc să începem cu două numere, iar apoi să le extindem la familii mai bogate.

Sfîrșitul capitolului, consacrat numerelor prime, se inspiră dintr-o lucrare remarcabilă a lui Georges Papy. Fără să insistăm ca dînsul asupra faptului că aplicația, care asociază unui întreg pozitiv divizorii săi primi, este un caz particular al celebrei teoreme a lui Stone asupra laticilor booleene, ni s-a părut necesar să studiem mai de aproape această injecție remarcabilă de la **N** *în mulțimea părților sale: aceasta clarifică într-adevăr toate proprietățile*

(și anumite algoritme deja binecunoscute de elevi) ale celui mai mare divizor comun și celui mai mic multiplu comun.

Sînt propuse elevilor numeroase exerciții; orice eroare din text care ne va fi semnalată va fi corectată imediat în ediția următoare. La fel, a fortiori, pentru erorile care s-ar putea strecura în textul propriu-zis sau în tabelul de numere prime, colaționat deja după cel al lui Ferrier și al lui Laborde.

Conștienți de deosebirea dintre un curs scris și unul vorbit, am fost totuși constrînși de exigențele programei să acordăm mai mult loc părților abstracte, formale, constructive, în defavoarea poate, a aplicațiilor care constituie aritmetica propriu-zisă și în același timp formatoare.

Credem că totuși colegii noștri vor fi mulțumiți de faptul că vor putea recomanda celor mai buni elevi această carte, pentru cutare sau cutare punct delicat al axiomaticii, și vor dezvolta, conform experienței lor, părțile mai clasice și mai inteligibile pentru majoritatea clasei lor. În tot cazul, sperăm că vor găsi un sprijin apreciabil în acest fascicul. Toate observațiile care ne vor fi trimise vor fi binevenite.

AUTORII

MATEMATICĂ / CLASE TERMINALE

PROGRAME NOI

Decretul din 14 Mai 1971

SECȚIUNEA A

Parte obligatorie

Funcții exponențiale și logaritmice

I. Recapitularea noțiunilor relative la continuitate, la limite, la derivata unei funcții reale de o variabilă reală. Derivata unei funcții compuse.
Se va admite fără demonstrație că dacă o funcție numerică este derivabilă pe un interval și dacă derivata ei este pozitivă sau nulă pe acest interval, atunci ea este crescătoare în sens larg pe acest interval și că imaginea unui interval este tot un interval.
Interpretarea geometrică a derivatei.
Aplicație la studiul și la reprezentarea grafică a cîtorva funcții simple (numai pe exemple numerice).
Funcția $x \longmapsto x^n (n \in \mathbf{Z})$.
(Nu se va cere candidaților la bacalaureat să demonstreze direct continuitatea unei funcții sau să caute direct o limită; se va mărgini să se folosească teoremele generale, enunțate fără demonstrație, cu privire la limitele sumelor, produselor, cîturilor de funcții).
II. 1. Exemple, scoase din științele umane și naturale, de funcții a căror creștere pe orice interval $[x, x + \ell]$. pentru orice ℓ dat, este proporțională cu valoarea funcției în punctul x.
2. Studiul șirurilor $n \longmapsto f(n)$ astfel că $f(n+1) - f(n) = kf(n)$, $n \in \mathbf{N}$, calculul lui $f(n)$, monotonia lui f; limita lui f cînd n tinde spre $+\infty$.
3. Se va admite existența, pentru orice a real strict pozitiv, a unei unice funcții continue și derivabile f_a definită pe $\mathbf{R}$ astfel ca pentru orice pereche de numere reale (x, y) să avem $f_a(x+y) = f_a(x) f_a(y)$ și $f_a(1) = a$. Calcul lui $f_a(x)$ pentru $x \in \mathbf{Z}$ și $x \in \mathbf{Q}$.
(Se va putea admite existența unei rădăcini a n-a pentru orice număr real pozitiv și pentru orice întreg pozitiv n).
Calculul lui $f'_a(x)$ în funcție de $f'_a(0)$.
Notația a^x (funcția exponențială de bază a), proprietățile exponenților: $(ab)^c = ab^c\,(ab)^c = a^c b^c$. Semnul și monotonia lui f_a limita lui f_a cînd x tinde spre $\pm\infty$.
4. Numărul e Notațiile $\exp x$ și e^x. Funcția $x \longmapsto \exp x$ va fi caracterizată printre funcțiile exponențiale prin faptul că derivata ei este 1 pentru $x = 0$.
Ecuațiile diferențiale $y' = ky$.
5. Funcția reciprocă a funcției $x \longmapsto a^x$. Notația Log a. Logaritmii zecimali și neperieni, notațiile Log sau ln; funcția $a^x = e^{x \mathrm{Log} a}$.
Folosirea tabelelor și a riglei de calcul.
6. Reprezentarea grafică a funcțiilor exponențiale și logaritmice.
7. Studiul funcțiilor $x \longmapsto \dfrac{a^x}{x^n}$ pentru $n \in \mathbf{N}$, $a > 1$. Se va enunța rezultatul cu privire la limita acestor funcții cînd x tinde spre $+\infty$. (Orice demonstrație este în afara programei.)
Aplicație la funcțiile logaritmice.

PROGRAMA COMPLEMENTARĂ

Calculul probabilităţilor

Spaţii probabilistice finite (Ω, $\mathcal{P}$ (Ω), p). Exemple (plecînd de la măsluirea sau nu a cărţilor, a urnelor, ...).
Variabila aleatoare numerică; evenimente legate de o variabilă aleatoare X (de exemplu părţile lui Ω astfel ca $X(\omega) = a$, sau $X(\omega) < a$ pentru a dat); densitate discretă; funcţia de repartiţie, creştere; speranţa matematică (sau valoarea medie) şi varianţa unei variaţii aleatoare. Probabilitatea condiţională a unui eveniment în raport cu un eveniment de probabilitate nenulă. Produs de spaţii probabilistice finite; exemple.

SECŢIUNEA B

„Rubricele programei au o ordine de enumerare. Această ordine exprimă uneori un exemplu din care profesorii s-ar putea inspira, ci nici de cum ceva obligatoriu; este, de exemplu, la alegere posibilitatea de a schimba I.1 cu 2 (noţiunile de continuitate şi de limită) etc..."

I. — Studiul funcţiilor numerice de o variabilă reală

1. Noţiunea de continuitate (într-un punct, pe un interval)
Definiţii, lămurite prin numeroase exemple şi contra-exemple. Enunţul proprietăţilor funcţiilor continue (se vor admite teoremele cu privire la sumă, produsul, citul acestor funcţii; se va admite că imaginea unui interval printr-o funcţie continuă este un interval).
Funcţia reciprocă a unei funcţii continue strict monotonă pe un interval. Exemple.
2. Noţiunea de limită
Definiţii, lămuriri prin numeroase exemple şi contra-exemple. Se va arăta unicitatea limitei şi se vor admite teoremele cu privire la limita unei sume, produs, cît.
Cazuri particulare de şiruri.
3. Noţiunea de derivată
Revederea programei anului *IB*.
Derivata într-un punct a funcţiei compuse a două funcţii derivabile; a funcţiei reciproce a unei funcţii derivabile strict monotone.
Se va admite că dacă o funcţie numerică admite o derivată pozitivă sau nulă pe un interval, ea este crescătoare (în sens larg) pe acest interval.
Studiul sensului de variaţie al unei funcţii derivabile cu ajutorul semnului derivatei ei.
Exemple de reprezentare grafică de funcţii derivabile pe intervale (se vor evita exemplele care prezintă dificultăţi tehnice).

II. — Calcul integral

1. Suma Riemann a unei funcţii numerice f de o variabilă reală definită pe un interval închis mărginit $[a, b]$. Se va admite că dacă f este continuă sau monotonă pe porţiuni, există un unic număr real $\int_a^b f(t)dt$ de care sumele lui Riemann se apropie arbitrar cînd lungimea celui mai mare interval de subdiviziune este suficient de mică.
2. Proprietăţile de liniaritate ale integralei unei funcţii continue sau monotone pe porţiuni, pe un interval închis mărginit. Media unei asemenea funcţii. Legătura cu derivata dacă funcţia este continuă. Primitiva unei funcţii continue, mulţimea primitivelor; egalitatea $\int_a^b f(t)dt = F(b) - F(a)$, f fiind continuă pe $[a, b]$ şi admiţînd pe F ca primitivă. Calcul de primitive în cazuri simple; integrarea prin părţi.
3. Se vor enunţa, fără demonstraţie, proprietăţile ariilor a căror existenţă este admisă aci (aditivitatea, unitatea de arie).

Aplicarea calculului integral la evaluarea ariei părții $R \times R$ definită prin $a \leqslant x \leqslant b$ $0 \leqslant y \leqslant f(x)$, f fiind o funcție pozitivă, monotonă pe porțiuni, apoi o funcție pozitivă continuă.
Extensie la $b < a$ și la o funcție negativă.

III. — Funcții elementare

Va fi necesar să se repartizeze diferitele rubrici ale acestui capitol în mai multe perioade ale anului, pentru a putea fi studiate în legătură cu titlurile I și II.
1. Funcțiile $x \longmapsto x^n$ $(n \in \mathbf{Z})$; derivate, primitive, reprezentare grafică.
2. Funcțiile $x \longmapsto x^r (x > 0,\ r \in \mathbf{Q})$; derivate, primitive.
3. Șiruri aritmetice și geometrice. Suma primilor n termeni.
4. Funcții circulare (recapitulare); derivatele și primitivele lui $x \longmapsto \cos(ax + b)$ și $x \longmapsto \sin(ax + b)$.
5. Logaritmul neperian (notația Log)

$$\operatorname{Log} x = \int_1^x \frac{dt}{t} \quad (x > 0).$$

Limita, cînd variabila pozitivă x tinde spre infinit, a lui $\operatorname{Log} x$ și a lui $\dfrac{\operatorname{Log} x}{x}$.

Limita, cînd x tinde spre 0, a lui $x \operatorname{Log} x$. Reprezentarea grafică.
6. Funcția exponențială (notația exp).

Proprietăți; derivata; reprezentarea grafică; numărul e; notația e^x; limita lui $\dfrac{e^x}{x}$ cînd x tinde spre $+\infty$.
7. Alte funcții logaritmice și exponențiale. Relații între funcțiile exponențiale și logaritmice de bază a și acelea de bază e.

IV. — Statistică și probabilități

Revederea programei anului I *B*.

SECȚIUNEA D

a) Paragrafele marcate cu o steluță nu pot face obiectul chestiunilor la cursuri, pentru lucrările scrise sau orale, nici nu pot fi folosite, în matematici, cu ocazia unei probleme sau exerciții, la scris sau la oral, la bacalaureat.
b) Rubricele programei au o ordine de enumerare. Această ordine exprimă uneori o idee din care profesorii s-ar putea inspira, nicidecum ceva obligatoriu; de exemplu, este la alegere de a da în I.3 o altă introducere a numerelor complexe, de a permuta pe II.1 și 2 (noțiunea de continuitate și de limită) etc...
c) De cîte ori va fi ocazie, se va pune în evidență, pe exemplele studiate în diferitele capitole, structurile de grup, subgrup, inel, corp, spațiu vectorial.

I. — Numere reale; calcul numeric; numere complexe

1. Însușirea (fără demonstrație) a proprietăților lui **R**: este un corp comutativ total ordonat (recapitulare); orice parte nevidă majorată admite un cel mai mic majorant; orice interval din **R** care conține mai mult de un punct conține un număr rațional.
2. Valorile zecimale apropiate cu aproximație de la 10^{-n}, prin lipsă și prin adaos ale unui număr real.
Reprezentarea unui număr real printr-un șir zecimal nelimitat (studiul periodicității nu este în programă). Valorile apropiate ale unui număr real, încadrare, incertitudine absolută și relativă.

Valorile apropiate ale unei sume, ale unei diferenţe, ale unui produs, ale unui cît de numere reale ale căror valori apropiate se cunosc.
Vor fi făcute numeroase exerciţii de calcul numeric cu ocazia studiului funcţiilor uzuale şi cu ocazia problemelor, pentru a pune în practică noţiunile de valori apropiate, de încadrare, de ordin de mărime ale unui rezultat, de incertitudine (cf. IV.8).
3. Adunarea şi înmulţirea matricilor 2×2 înzestrează mulţimea **C** a matricilor cu coeficienţi reali de forma $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ cu o structură de corp comutativ. Identificarea lui **R** ca un subcorp al lui **C** prin aplicaţia $a \longrightarrow \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$; **C** este un spaţiu vectorial de dimensiune 2 pe **R**.
Notaţia $a + bi$; număr complex; numere complexe conjugate; modulul unui număr complex.
4. Homomorfismul θ al lui **R** pe grupul multiplicativ al numerelor complexe de modul 1 (a se revedea cursul de anul I); forma trigonometrică a unui număr complex nenul: $r(\cos x + i \sin x)$ cu $r > 0$ şi $x \in \mathbf{R}$; argumentul unui asemenea număr (clasa numerelor x sau, prin abuz de limbaj, unul din ele).
Calculul lui $\cos nx$ şi al lui $\sin nx (x \in \mathbf{R}, n = 2, 3, 4)$ şi linearitatea polinoamelor trigonometrice.
Existenţa şi reprezentarea geometrică a rădăcinilor a n-a ale unui număr complex ($n \leqslant 4$).
5. Rezolvarea ecuaţiilor de gradul I şi de gradul II cu coeficienţi complecşi; calculul părţilor reale şi imaginare ale rădăcinilor; cazul coeficienţilor reali.

II. — Calcul diferenţial

1. Funcţii numerice de o variabilă reală: continuitate. Continuitatea „într-un punct"; continuitatea pe un interval; sumă, produs, cît de funcţii continui; continuitatea funcţiei compuse a două funcţii continui (fără demonstraţie).
Se va admite fără demonstraţie următoarea teoremă: „dacă o funcţie este continuă pe un interval, imaginea prin funcţie a acestui interval este un interval". Aplicaţie la o funcţie continuă şi strict monotonă pe un interval: existenţa funcţiei reciproce; monotonia şi continuitatea acestei funcţii (se va admite continuitatea).
2. Funcţii numerice de o variabilă reală: limite.
Limita unei funcţii atunci cînd variabila tinde spre un număr real dat, spre infinit. Unicitatea.
Cazuri particulare de şiruri.
Limita unei sume, a unui produs, a unui cît (fără demonstraţie).
3. Funcţii numerice de o variabilă reală: derivata. Revederea programei anului I *D*: funcţia lineară tangentă într-un punct la o funcţie dată; notaţia diferenţială; derivata în acest punct.
Funcţia derivată; derivata unei sume, a unui produs, a unui cît de funcţii derivabile. Interpretarea geometrică a derivatei (reper cartezian); ecuaţia tangentei.
Definiţia derivatelor succesive.
Derivata într-un punct a funcţiei compuse a două funcţii derivabile.
Derivata într-un punct a reciprocii unei funcţii derivabile şi strict monotonă.
Se va admite fără demonstraţie că dacă o funcţie numerică este derivabilă pe un interval şi dacă derivata ei este pozitivă sau nulă ea este crescătoare în sens larg pe acest interval.
Compararea a două funcţii care au aceeaşi funcţie derivată pe un interval.
Studiul sensului de variaţie al unei funcţii derivabile cu ajutorul semnului derivatei ei.
Reprezentarea grafică.
4. Funcţii vectoriale de o variabilă reală.
Aplicaţia unei părţi a lui **R** într-un spaţiu vectorial euclidian de dimensiune finită.
Continuitatea într-un punct; limita unei funcţii cînd variabila tinde spre un număr real dat, spre infinit.
Derivata într-un punct; dacă spaţiul vectorial este raportat la o bază, coordonatele, în această bază ale derivatei; funcţia derivată.
Derivata unei sume de funcţii vectoriale derivabile, a produsului unei funcţii vectoriale derivabile printr-o funcţie numerică derivabilă.
Derivata produsului scalar a două funcţii vectoriale derivabile.

Aplicație la căutarea de tangente. Exemple.
5. Cinematica punctului.
Mișcarea unui punct: aplicația unui interval din $\mathbf{R}$ într-un spațiu afin euclidian. Traiectoria.
Vectorul viteză la un moment dat. Fiind ales un reper, coordonatele vectorului viteză în acest reper. Norma vectorului viteză.
Vectorul accelerație la un moment dat. Fiind ales un reper, coordonatele vectorului accelerație în acest reper.
Studiul mișcărilor circulare (viteza unghiulară); studiul mișcărilor helicoidale uniforme.

III. — Calcul integral

1. Definiția sumelor lui Riemann a unei funcții numerice de o variabilă reală pe un interval închis, mărginit. Existența integralei pentru o funcție monotonă; notația $\int_a^b f(t)dt$; primele proprietăți. Se va admite că aceste proprietăți se extind cu funcții continue sau monotone pe porțiuni.
Media unei asemenea funcții pe un interval închis, mărginit.
Legătura cu derivata în puncte în care funcția este continuă.
Primitive; mulțimea primitivelor; egalitatea

$$\int_a^b f(t)dt = F(b) - F(a)$$

f fiind continuă pe $[a, b]$ și admițind pe F ca primitivă.
Calcul de primitive; integrarea prin părți.
2. Se vor enunța fără demonstrație proprietățile ariilor a căror existență este admisă aci (aditivitatea, unitatea de arie...).
Aplicarea calculului integral la evaluarea ariei părții lui $\mathbf{R} \times \mathbf{R}$ definită prin:

$$a \leqslant x \leqslant b, \quad 0 \leqslant y \leqslant f(x),$$

f fiind o funcție pozitivă, monotonă pe porțiuni, apoi o funcție pozitivă continuă.
Extensia la $b < a$ și la o funcție negativă.
3*. Aplicații geometrice, mecanice, fizice etc... (calcul de volume, mase, momente de inerție; viteza și distanța parcursă; intensitatea și cantitatea de electricitate; putere și energie etc...).
Valoarea eficace a unui fenomen periodic.

IV. — Exemple de funcții de o variabilă reală

Anumite rezultate din acest capitol, deja cunoscute elevilor, vor putea să ilustreze capitolele precedente; va fi necesar să se repartizeze diferitele rubrici ale acestui capitol între mai multe etape ale anului.
1. Funcția $x \longmapsto x^n$ $(n \in \mathbf{Z})$; derivata; primitiva.
2. Funcția $x \longmapsto x^r$ $(r \in \mathbf{Q}; x > 0)$; derivata; primitiva.
3. Șiruri aritmetice și geometrice. Suma primilor n termeni.
4. Funcții circulare; derivatele (recapitulare); derivate și primitive ale lui $x \longmapsto \cos(ax + b)$ și $x \longmapsto \sin(ax + b)$.
5. Logaritm neperian (notația Log)

$$\mathrm{Log}\, x = \int_1^x \frac{dt}{t} \quad (x > 0).$$

Limita lui $\mathrm{Log}\, x$ și $\frac{\mathrm{Log}\, x}{x}$, cînd variabila pozitivă x tinde spre infinit.

Limita lui $x \log x$ cînd x tinde spre 0. Reprezentarea grafică.
6. Funcţia exponenţială (notaţia exp).

Proprietăţi; derivata; reprezentarea grafică; numărul e; notaţia e^x; limita lui $\frac{e^x}{x}$ cînd x tinde spre $+\infty$.
7. Alte funcţii logaritmice şi exponenţiale.
Relaţii între funcţiile logaritmice şi exponenţiale de bază a şi cele de bază e.
Notaţia e^{ix} pentru a desemna $\cos x + i \sin x$; ω fiind o constantă reală, derivata funcţiei $x \longmapsto e^{i\omega x}$.
Observaţie: Studiul de exemple de funcţii compuse de tip logaritmic sau exponenţial va fi strict limitat la cazurile în care sînt în cauză intervalele pe care derivata păstrează un semn constant şi în care nedeterminările ce trebuie înlăturate sînt numai acelea care au fost enumerate mai sus.
8. Calcul numeric.
Folosirea riglei de calcul;
Folosirea tabelelor; practica interpolării liniare. Tabele de logaritmi.
Întrebuinţarea maşinilor de calcul de birou.
9*. Ecuaţii diferenţiale.
Căutarea funcţiilor variabilei reale x odată sau de două ori derivabile care verifică ecuaţiile:
$y' = ay$, a fiind o constantă reală,
$y'' + \omega^2 y = 0$, ω fiind o constantă reală nenulă (se va admite că soluţiile formează un spaţiu vectorial de dimensiune 2).

V. Elemente de algebră liniară

1. Geometrie vectorială:
a) revederea capitolului IV din anul I D.
b) se va admite că spaţiul euclidian real este orientabil; produsul vectorial a doi vectori din spaţiul euclidian orientat de dimensiune 3.
2. Baricentru într-un spaţiu afin. Reper afin.
Reducerea în cazul euclidian al lui

$$f(M) = aMA^2 + bMB^2 + cMC^2.$$

3. Interpretarea geometrică a unei aplicaţii $x \longmapsto ax + b$ (a, b complexe), $a \neq 0$, după identificarea planului cu corpul numerelor complexe, datorită alegerii unui reper ortonormat; grupul asemănărilor directe ale planului.

VI. Probabilităţi pe o mulţime finită; statistică

1. Spaţii probabilistice finite $(\Omega, \mathcal{B}(\Omega), p)$.
Aplicaţii măsurabile (sau variabile aleatoare): probabilitatea imagine; funcţia de repartiţie a unei variabile aleatoare reale. Perechi de variabile aleatoare reale, legea perechii. Legi marginale. Pereche independentă. Sistem de n variabile aleatoare independente.
2. Valoarea medie a unei variabile aleatoare cu valori în $\mathbf{R}$ sau $\mathbf{R}^2$.
Valoarea medie a sumei a două variabile aleatoare reale a unei perechi, a produsului în cazul unei perechi independente.
Dispersia, abaterea medie a unei variabile aleatoare reale.
3. Inegalitatea lui Bienaymé-Cebîşev. Experienţe repetate, legea mică a numerelor mari.
4. Descrierea statistică a unei populaţii sau a unui eşantion (revederea programei de statistică din anul I D, titlul VII-1°; exerciţii practice din această programă; calcul de coeficienţi de corelaţie).

TERMINALA C şi E (Preambul)

a) Paragrafele marcate cu o steluţă nu pot face obiectul la cursuri, pentru lucrările scrise sau orale, nici nu pot fi folosite, în matematici, cu ocazia unei probleme sau exerciţiu, la scris sau la oral, la bacalaureat.

SECŢIUNEA C

b) Rubricele programei au o ordine de enumerare. Această ordine este uneori o schiţă din care profesorii s-ar putea inspira, ci nicidecum ceva obligatoriu; este la alegere, de exemplu, să se permute în I.3 cele trei alineate care privesc numerele întregi, III.1 şi 2 (noţiunile de continuitate şi de limită), să se dea în II.3 o altă introducere a numerelor complexe etc....

SECŢIUNEA E

b) Rubricile programei au o ordine de enumerare. Această ordine este uneori o schiţă din care profesorii s-ar putea inspira, ci nicidecum ceva obligatoriu; este la alegere, de exemplu, să se dea în II.3 o altă introducere a numerelor complexe, să se permute în III 1 şi 2 (noţiunile de continuitate şi de limită) etc.
c) Oridecîteori va fi ocazie, se va pune în evidenţă, pe baza exemplelor studiate în diferitele capitole, structurile de grup, subgrup, inel, corp, spaţiu vectorial, precum şi izomorfismele, homomorfismele (nucleul), automorfismele întîlnite.

SECŢIUNEA C

I. — Numere naturale întregi aritmetice
1*. — Enunţul proprietăţilor atribuite mulţimii **N** a întregilor naturali. Raţionament prin recurenţă. Aplicaţii ale lui **N** într-o mulţime X; notaţia indicială; exemple.
2. Inelul **Z** al întregilor relativi; multiplii unui întreg relativ: notaţia $n\mathbf{Z}$.
Congruenţe modulo n; inelul $\mathbf{Z}/n\mathbf{Z}$; împărţirea euclidiană în **Z**, în **N**.
Principiul sistemelor de numeraţie; bază; numeraţii zecimale şi binare.
3. *a)* Numere prime în **Z**; dacă p este prim, $\mathbf{Z}/p\mathbf{Z}$ este un corp.
b) Descompunerea unui număr în factori primi; existenţă, unicitate.
c) Cel mai mare divizor comun şi cel mai mic comun multiplu; numere prime între ele; identitatea lui Bézout. (Ordinea lui a), b), c) este, bine înţeles, lăsată la alegerea profesorului).

SECŢIUNEA E

I. — Numere întregi naturale aritmetice
Exemple de raţionament prin recurenţă.
Exemple de folosire a notaţiei indiciale.
Principiul sistemelor de numeraţie; bază; numeraţie zecimală şi binară.

SECŢIUNEA C ŞI E

II. — Numere reale. Calcul numeric. Numere complexe

1. Enumerarea (fără demonstraţie) a proprietăţilor lui **R**: **R** este un corp comutativ total ordonat (recapitulare); orice parte nevidă majorată, admite un cel mai mic majorant; orice interval din **R** care conţine mai mult de un punct conţine un număr raţional.
2. Valorile zecimale cu aproximaţie de 10^{-n}, prin lipsă şi prin adaos, ale unui număr real. Reprezentarea unui număr real printr-un şir zecimal nelimitat (studiul periodicităţii nu este în programă).
Valorile aproximative ale unui număr real, încadrare, eroare absolută şi relativă.

Valorile aproximative ale unei sume, ale unei diferențe, ale unui produs, ale unui cît de numere reale, ale căror valori cu aproximație se cunosc.
Vor fi făcute numeroase exerciții de calcul numeric cu ocazia studiului funcțiilor uzuale și cu ocazia problemelor, pentru a pune în practică noțiunile de valori aproximative, de încadrare, de ordin de mărime al unui rezultat, de eroare (cf. V.8).
3. Adunarea și înmulțirea matricelor 2×2 înzestrează mulțimea **C** a matricelor cu coeficienți reali de forma $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ cu o structură de corp comutativ. Identificarea lui **R** cu un subcorp al lui **C** prin aplicația $a \longmapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$; **C** este un spațiu vectorial de dimensiune 2 pe **R**.. Notația $a + bi$; numere complexe; numere complexe conjugate; modulul unui număr complex.
4. Homomorfismul 0 al lui **R** pe grupul multiplicativ al numerelor complexe de modul 1 (reamintire din anul I); forma trigonometrică a unui număr complex nenul: $r(\cos x + i \sin x)$ cu $r > 0$ și $x \in \mathbf{R}$; argumentul unui asemenea număr (clasa numerelor x sau, prin abuz de limbaj, unul dintre ele). Calculul lui $\cos nx$ și al lui $\sin nx$ ($x \in \mathbf{R}$, $n = 2, 3, 4$) și liniarizarea polinoamelor trigonometrice.
Existența și reprezentarea geometrică a rădăcinilor de ordinul n ale unui număr complex.
5. Rezolvarea ecuațiilor de gradul I și de gradul II cu coeficienți complecși; calculul părților reale și imaginare ale rădăcinilor; cazul coeficienților reali.

III. — Calcul diferențial

1. Funcții numerice de o variabilă reală: continuitate. Continuitatea „într-un punct"; continuitatea pe un interval; sumă, produs, cît de funcții continui; continuitatea funcției compuse a două funcții continui (fără demonstrație).
Se va admite fără demonstrație următoarea teoremă: „dacă o funcție este continuă pe un interval, imaginea prin funcție, a acestui interval, este un interval". Aplicație la o funcție continuă și strict monotonă pe un interval; existența funcției reciproce; monotonia și continuitatea acestei funcții (se va admite continuitatea).
2. Funcții numerice de o variabilă reală: limite. Limita unei funcții cînd variabila tinde spre un număr real dat, spre infinit. Unicitate. Caz particular de șiruri.
Limita unei sume, a unui produs, a unui cît (fără demonstrație).
3. Funcții numerice de o variabilă reală: derivarea. Revederea programei din anul I: funcția liniară tangentă într-un punct la o funcție dată; notația diferențială; derivata în acest punct. Funcția derivată; derivata unei sume, a unui produs, a unui cît de funcții derivabile. Interpretarea geometrică a derivatei (reper cartezian); ecuația tangentei. Definiția derivatelor succesive.
Derivata într-un punct a funcției compuse a două funcții derivabile.
Derivata într-un punct a reciprocei unei funcții derivabile și strict monotone.
Se va admite fără demonstrație că dacă o funcție numerică este derivabilă pe un interval și dacă derivata ei este pozitivă sau nulă, ea este crescătoare în sens larg pe acest interval.
Compararea a două funcții care au aceeași funcție derivată pe un interval.
Studiul sensului de variație al unei funcții derivabile cu ajutorul semnului derivatei ei.
Reprezentarea grafică; exerciții simple de găsirea asimptotelor.
4. Funcții vectoriale de o variabilă reală.
Aplicația unei părți a lui **R** într-un spațiu vectorial euclidian de dimensiune finită.
Continuitatea într-un punct; limita unei funcții cînd variabila tinde spre un număr real dat, spre infinit.
Derivata într-un punct; dacă spațiul vectorial este raportat la o bază, coordonatele, în această bază ale derivatei; funcția derivată.
Derivata unei sume de funcții vectoriale derivabile, a produsului unei funcții vectoriale derivabile printr-o funcție numerică derivabilă.
Derivata produsului scalar a două funcții vectoriale derivabile.
Aplicație la găsirea de tangente; exemple de conice și de elice circulare.
5. Cinematica punctului.
Mișcarea unui punct; aplicația unui interval din **R** într-un spațiu afin euclidian. Traiectorie.

Vectorul-viteză la un moment dat. Fiind ales un reper, coordonatele vectorului-viteză în acest reper. Norma vectorului-viteză.
Vectorul-accelerație la un moment dat. Fiind ales un reper, coordonatele vectorului-accelerație în acest reper. Studiul mișcărilor circulare (viteza unghiulară); studiul mișcărilor helicoidale uniforme.

IV. — Calcul integral

1. Definiția sumelor Riemann ale unei funcții numerice de o variabilă reală pe un interval închis, mărginit. Existența integralei pentru o funcție monotonă; notația $\int_a^b f(t)dt$; primele proprietăți. Se va admite că aceste proprietăți se extind la funcții continui sau monotone pe porțiuni.
Media unei asemenea funcții pe un interval închis, mărginit.
Legătura cu derivata în puncte în care funcția este continuă.
Primitive; mulțimea primitivelor; egalitatea

$$\int_a^b f(t)dt = F(b) - F(a)$$

f fiind continuă pe $[a, b]$ și admițînd pe F ca primitivă.
Calcul de primitive; integrare prin părți.
2. Se vor enunța, fără demonstrație, proprietățile ariilor a căror existență este admisă aci (aditivitatea, unitatea de arie, ...).
Aplicarea calculului integral la evaluarea ariei părții lui $\mathbf{R} \times \mathbf{R}$ definită prin: $a \leqslant x \leqslant b$ $0 \leqslant y \leqslant f(x)$.
f fiind o funcție pozitivă, monotonă pe porțiuni, apoi o funcție pozitivă continuă. Extensie la $b < a$ și la 0 funcție negativă.

SECȚIUNEA C ȘI E

3*. Aplicații geometrice, mecanice, fizice etc... (calcul de volume, de mase, momente de inerție; viteza și distanța parcursă; intensitatea și cantitatea de electricitate; puterea și energie etc....)
Valoarea eficace a unui fenomen periodic.

V. — Exemple de funcții de o variabilă reală

Anumite rezultate ale acestui capitol, deja cunoscute elevilor, vor putea să ilustreze capitolele precedente; va fi cazul să se repartizeze diferitele rubrici ale acestui capitol între mai multe momente ale anului.
1. Funcția $x \longmapsto x^n$ $(n \in \mathbf{Z})$; derivată; primitive.
2. Funcția $x \longmapsto x^r$ $(r \in \mathbf{Q}: x > 0)$; derivată; primitive.
3. Progresii aritmetice și geometrice. Suma primilor n termeni.
4. Funcții circulare; derivate (recapitulare); derivatele și primitivele lui $x \longmapsto \cos(ax + b)$ și $x \longmapsto \sin(ax + b)$.
5. Logaritmul neperian (notația Log și ln). Lo g$x = \int_1^x \frac{dt}{t}$ $(x > 0)$.
Limita cînd variabila pozitivă x tinde spre infinit a lui Log$x$ și $\frac{\text{Log}\, x}{x}$. Limita lui x Log x cînd x tinde spre 0.
Reprezentarea grafică.
6. Funcția exponențială (notația exp).
Proprietăți; derivata; reprezentarea grafică; notația e^x;

Limita lui $\frac{e^x}{x}$ cînd x tinde spre $+\infty$.

7. Alte funcţii logaritmice şi exponenţiale. Relaţii între funcţiile logaritmice şi exponenţiale de bază a şi acelea de bază e.

SECŢIUNEA C

Definiţia lui x^α unde $\alpha \in \mathbf{R}$; derivata funcţiei $x \longmapsto x^\alpha$.

SECŢIUNEA C ŞI E

* Notaţia e^{ix} pentru a desemna $\cos x + i \sin x$; ω fiind o constantă reală, derivata funcţiei $x \longmapsto e^{i\omega x}$.

Observaţie: Studiul funcţiilor compuse de tip logaritmic sau exponenţial va fi strict limitat la cazurile în care sînt în evidenţă intervalele pe care derivata păstrează semn constant şi în care nedeterminările de înlăturat sînt numai acelea enumerate mai sus.

SECŢIUNEA C

8. Calcul numeric. Folosirea riglei de calcul; folosirea tabelelor practica interpolării liniare. Tabele de logaritmi. Folosirea maşinilor de calcul de birou.

SECŢIUNEA E

8. Calcul numeric. Revederea programelor din anul II T şi anul I E.

SECŢIUNEA C ŞI E

9*. Ecuaţii diferenţiale. Cercetarea funcţiilor numerice, o dată sau de două ori derivabile, de variabilă x care verifică ecuaţiile: $y' = ay$, a fiind o constantă reală. $y'' + \omega^2 y = 0$, ω fiind o constantă reală, nenulă (se va admite că soluţiile formează un spaţiu vectorial de dimensiune 2).

SECŢIUNEA C ŞI E

VI. — Elemente de geometrie afină şi euclidiană

N.B.: În acest paragraf corpul de bază este $\mathbf{R}$ şi dimensiunea n este totdeauna egală cu 2 sau 3. O „transformare a unei mulţimi E" este o bijecţie a lui E pe ea însăşi; o aplicaţie f a lui E în ea însăşi este o involuţie dacă $f \circ f$ este identitate: aceasta este o transformare a lui E.

1. Suma directă a două subspaţii vectoriale; subspaţii vectoriale suplementare. Aplicaţia liniară a unui spaţiu vectorial E într-un spaţiu vectorial F; imagine şi nucleu. Adunarea şi compunerea aplicaţiilor liniare. Grup liniar. Omotetii vectoriale.

2. Baricentru într-un spaţiu afin. Reper afin. Reducerea în cazul euclidian al lui:

$$f(M) = aMA^2 + bMB^2 + cMC^2.$$

3. Aplicaţia afină a unui spaţiu afin E în el însuşi, aplicaţia liniară asociată. Exemple: proiecţia paralelă pe un subspaţiu afin; involuţii afine, punctele lor fixe; translaţii şi omotetii.

4. Aplicaţii liniare ale unui spaţiu vectorial euclidian în el însuşi, păstrînd norma; transformări ortogonale (izometrii vectoriale), grup ortogonal.

Elemente fixe ale transformărilor ortogonale involutive (simetrii) în planul vectorial şi în spaţiul vectorial de dimensiune 3. Orientarea planului vectorial euclidian (reamintire din anul I).

Studiul rotațiilor vectoriale din spațiul vectorial euclidian de dimensiune 3 (prin definiție, o asemenea rotație este fie identitatea, fie o transformare ortogonală, care are ca singure elemente fixe cele două drepte vectoriale); grup de rotații vectoriale; orientarea spațiului. Produs vectorial în spațiul vectorial euclidian orientat, de dimensiune 3.
5. Definiția unei izometrii a spațiului afin euclidian. Orice izometrie este o bijecție afină. Grup de izometrii; subgrup de deplasări.
Simetrii, translații, rotații în planul afin euclidian: orice deplasare este de unul din aceste ultime două tipuri.
Simetrii, translații, rotații, înșurubări în spațiul afin euclidian de dimensiune 3; se va admite că orice deplasare este de unul din aceste ultime trei tipuri.
Exemple simple de grupuri de izometrii care lasă neschimbată o mulțime dată.

VII. — Complemente de geometrie euclidiană plană

1. Unghiul unei perechi de semidrepte vectoriale (reamintire din anul I).
Grupul $\mathcal{A}$ al unghiurilor de semidrepte.
Unghiul unei perechi de drepte vectoriale (mulțimea a două rotații vectoriale care transformă pe prima în a doua).
Grupul $\mathcal{A}'$ al unghiurilor de drepte.
Homomorfismul canonic $\mathcal{A} \longmapsto \mathcal{A}'$; nucleul lui.
Izomorfismul lui $\mathcal{A}'$ pe $\mathcal{A}$ dedus din homomorfismul $\alpha \longmapsto \alpha + \alpha$ al lui $\mathcal{A}$ pe $\mathcal{A}'$.
Condiția, în cazul unghiurilor de drepte, ca patru puncte să fie conciclice.
2. Asemănări plane (adică aplicații ale planului în el însuși, păstrînd rapoartele de distanță). Reprezentarea prin formulele $z' = az + b$ sau $z' = a\bar{z} + b$ atunci cînd planul a fost identificat cu C datorită alegerii unui reper ortonormat.
Punctele fixe ale asemănărilor. Grupul asemănărilor planului și subgrupuri remarcabile.

SECȚIUNEA C

3. Studiul curbelor reprezentate, într-un reper ortonormat, prin ecuații de forma:

$$ax^2 + by^2 + 2cx + 2dy + e = 0 \quad (|a| + |b| \neq 0).$$

Diferitele forme ale acestor curbe; existența axelor sau a centrelor de simetrie, a asimptotelor; ecuații reduse; existența tangentei.
Elipsa, hiperbola, parabola definite prin proprietățile punctelor lor care fac să intervină focarele și directoarele (proprietățile tangentelor la conice sînt în afara programei).
Ecuația hiperbolei raportată la asimptotele ei.

SECȚIUNEA E

3. Studiul curbelor reprezentate, într-un reper ortonormat prin ecuații de forma:

$$ax^2 + by^2 + 2cx + 2dy + e = 0 \quad (|a| + |b| \neq 0).$$

Diferite forme ale acestor curbe; existența axelor sau a centrelor de simetrie, a asimptotelor. Ecuații reduse: elipsa, hiperbola, parabola.
Existența tangentei. Ecuația hiperbolei raportată la asimptotele ei.
4. Geometrie descriptivă. Chestiunile enumerate mai jos vor fi avantajos studiate în legătură cu cursul de geometrie din această clasă și din clasa anterioară; ele vor servi util la ilustrarea ei.
Rotația în jurul unei axe verticale sau de capăt.
Rabaterea unui plan pe un plan orizontal sau frontal.
Distanța a două puncte, a unui punct la o dreaptă, a unui punct la un plan; unghiul a două drepte.
Proiecția unui cerc: epura.
Reprezentarea unui cilindru de revoluție, a unui con de revoluție a cărui bază circulară este planul orizontal de proiecție.

Construcţia prin puncte şi tangente a proiecţiei orizontale (respectiv frontală) a intersecţiei unei asemenea suprafeţe printr-un plan de capăt (respectiv vertical).
Reprezentarea helicei circulare drepte trasată pe un cilindru de revoluţie de axă verticală.

SECŢIUNEA C ŞI E

VIII. — Probabilităţi pe o mulţime finită

1. Spaţii probabilistice finite $(\Omega, \mathcal{B}(\Omega), p)$.
Aplicaţii măsurabile (sau variabile aleatoare): probabilitatea imagine, funcţia de repartiţie a unei variabile aleatoare reale.
Pereche de variabile aleatoare reale, legea perechii. Legi marginale.
Pereche independentă. Sistem de n variabile aleatoare independente.
2. Valoarea medie a unei variabile aleatoare cu valori în $\mathbf{R}$ sau $\mathbf{R}^2$.
Valoarea medie a sumei a două variabile aleatoare reale a unei perechi, a produsului în cazul unei perechi independente.
Dispersia, abaterea medie a unei variabile aleatoare reale.
3. Inegalitatea lui Bienaymé-Cebîşev. Experienţe repetate; legea mică a numerelor mari.

ALFABETUL GREC

Α	α	alfa	a
Β	β,	beta	b
Γ	γ	gama	g
Δ	δ	delta	d
Ε	ε	epsilon	e scurt
Ζ	ζ	zeta	z
Η	η	eta	e lung
Θ	θ	teta	th
Ι	ι	iota	i
Κ	$\varkappa$	kapa	k
Λ	λ	lambda	l
Μ	μ	miu	m
Ν	ν	niu	n
Ξ	ξ	csi	ks
Ο	o	omicron	o scurt
Π	π	pi	p
Ρ	ρ	ro	r
Σ	σ, ς	sigma	s
Τ	τ	tau	t
Υ	υ	ipsilon	ü
Φ	φ	fi	ph, f
Χ	χ	hi	ch
Ψ	ψ	psi	ps
Ω	ω	omega	o lung

1. NUMERE ÎNTREGI NATURALE

1.1. PROPRIETĂŢI ALE MULŢIMII N

1.1.1. Noţiunea de întreg

Avem intuitiv noţiunea de întreg natural. Scopul acestui capitol este de a enunţa anumite proprietăţi ale acestor obiecte matematice, referindu-ne la experienţa noastră personală şi la aceea a matematicienilor care ne-au precedat. Foarte multă vreme, cunoaşterea intuitivă a fost considerată ca suficientă pentru matematicieni foarte mari, ca Pierre de Fermat[1]. Astăzi sîntem în măsură să definim această noţiune şi să facem un studiu pur axiomatic al ei (a se vedea anexa acestui capitol); acest studiu fiind delicat, ne vom mulţumi să enunţăm proprietăţile fundamentale care ne vor permite să demonstrăm logic teoremele principale ale aritmeticii.

PROPRIETATEA 1 / **Numerele întregi naturale formează o mulţime, notată N.**

Această mulţime este cea mai „naturală" dintre toate mulţimile matematice. Această proprietate figurează în toate expunerile (axiomatice sau nu) ale teoriei mulţimilor — uneori sub o formă diferită.

PROPRIETATEA 2 / **Numărul zero, notat 0, este un element privilegiat al mulţimii N.**

La drept vorbind, această proprietate este mai degrabă o manieră de a privilegia un element al lui N decît o „axiomă" în sensul vechi al acestui cuvînt.

[1] *Pierre de Fermat* (1601—1665), jurist şi matematician francez, unul dintre părinţii teoriei numerelor şi a calculului probabilităţilor.

Ea traduce de asemenea o convenție, adoptată astăzi, care nu ține de tradiția după care mulțimea N nu „începea" decît cu numărul 1.

PROPRIETATEA 3 / **Orice întreg n admite un succesor unic, notat n'.**

Această proprietate este legată de ideea naturală după care există o ordine „bună" în N; tehnic, echivalează cu darea unei aplicații f de la N în N, definită prin:

$$f = [n \longrightarrow f(n) = n'].$$

Intuitiv, succesorul lui n se obține „adăugîndu-i" 1.
Vom reveni asupra acestui punct mai tîrziu (a se vedea nr. 1.2.2).

PROPRIETATEA 4 / **Succesorul lui 0 este numărul unu, notat 1.**

Aceasta nu este decît traducerea ideii intuitive a succesiunii naturale a întregilor, aplicate numărului 0. Alte proprietăți echivalente — care nu sînt de fapt decît definiții ascunse, adevărate datorită propoziției 3 — ar putea introduce aici întregii 2, 3, 4 etc...; nu le mai dăm.

PROPRIETATEA 5 / **0 nu este succesorul nici unui număr natural.**

Această proprietate este deja mai puțin evidentă; traduce impresia naivă că șirul întregilor este infinit.
Arată de fapt că, prin aplicația $f = [n \longmapsto n']$, numărul 0 nu este imaginea niciunui alt număr, deci că aplicația f nu este *surjectivă*. Această proprietate este întărită de următoarea:

PROPRIETATEA 6 / **Doi întregi sînt egali dacă și numai dacă succesorii lor sînt egali.**

Prin definiția unei aplicații, avem evident:

$$(n = m) \Longrightarrow (n' = m').$$

Reciproca care constituie proprietatea 6 traduce faptul că aplicația f este *injectivă*.

PROPRIETATEA 7 / **Orice întreg natural diferit de 0 este succesorul unui întreg unic numit predecesorul său.**

0 este singurul număr care nu este succesorul unui alt întreg; adică toți ceilalți întregi se pot obține cu ajutorul aplicației f: vom vedea mai tîrziu că aceasta este posibil cu ajutorul unui „număr finit" de operații succesive.

1.1.2. Principiul inducției

Să rezumăm studiul precedent: cunoașterea numărului natural ne permite următoarea formalizare a proprietăților de mai sus:

PROPRIETATEA 8 / **Întregii naturali formează o mulțime N. Există o aplicație f (succesiune) de la N la N. Aplicația f este injectivă, nu surjectivă. Există în N un element și numai unul, numărul 0, care nu aparține imaginii aplicației.**

Acest enunț conține toate proprietățile precedente (cu excepția corolarelor evidente, ca unicitatea predecesorului unui întreg care este o consecință banală a injectivității succesiunii).
Ne putem întreba dacă această propoziție este suficient de puternică pentru a servi de axiomă care să fundamenteze teoria întregilor. Totuși, așa cum arată exemplul următor, lucrurile nu stau așa.

EXEMPLU. Să considerăm mulțimea A formată din toți întregii naturali și din numerele rationale, pozitive și negative, al căror numărător este impar și numitorul egal cu 2. Definind în A — care este o submulțime a corpului numerelor reale — operația de succesiune prin formula:

$$f(x) = x + 1,$$

este ușor de verificat că această mulțime satisface proprietățile precedente, fără nici o excepție. Mulțimea A nu poate fi totuși identificată cu N, deoarece există în A elemente care nu pot fi obținute printr-un „număr finit" de succesiuni plecînd de la 0.

Acest exemplu și alte exemple analoage arată că proprietatea 8 este insuficientă; proprietatea „ereditară" pe care o traduce această propoziție este verificată de un număr foarte mare de mulțimi între care nu există nici un izomorfism.
Se poate arăta totuși că orice mulțime „ereditară" conține o submulțime izomorfă cu N, care este, într-o oarecare măsură, „cea mai mică" dintre aceste mulțimi. Sîntem deci conduși să enunțăm o nouă proprietate care va preciza această intuiție.
Am plecat de la un număr particular 0, și de la o aplicație f care asociază fiecărui întreg succesorul său. Proprietățile 5 și 6 ne permit să definim astfel, așa cum am văzut, o „infinitate" de întregi prin succesiuni repetate plecînd de la 0.
Dealtfel, sîntem convinși, că abstracție făcînd de timp și de material de scris, acest procedeu permite teoretic de a ajunge la orice întreg. Pentru a traduce această idee, matematicienii au fost conduși la următoarea formalizare: orice mulțime M de întregi care conține pe 0, și în care este definită aplicația f, trebuie obligatoriu să conțină orice întreg. Dacă interzicem lui M să admită alte elemente decît cele care rezultă din aceste succesiuni repetate, trebuie ca M însuși să fie egal cu N. Vom enunța deci proprietatea următoare, sau principiul inducției.

PROPRIETATEA 9 / **Fie M o submulțime a lui N. Dacă 0 aparține lui M și dacă pentru orice element al lui M succesorul acestui element aparține de asemenea lui M, atunci mulțimea M este egală cu mulțimea N.**

Sub formă simbolică:

$$[M \subset N \text{ și } 0 \in M \text{ și } \forall_N n\,(n \in M \Longrightarrow n' \in M)] \Longrightarrow [M = N]$$

Observație. — Exemplul de la nr. **1.1.2.** arată că propoziția 9 nu este deductibilă deloc din propoziția 8, deoarece A satisface acesteia din urmă, dar nu și pe cea a lui N enunțată mai sus: N este într-adevăr o submulțime a lui A care-l conține pe 0 și succesorii elementelor sale, dar este distinctă de A.

1.1.3. Proprietăți recurente

Principiul inducției admite alte formulări echivalente. Vom da mai jos mai multe dintre ele care vor fi aplicate la nr. **1.1.4.**

Primul enunț face să intervină noțiunea de proprietate a unui obiect matematic (a se vedea clasa I CDE, Algebră nr. **1.2.1.**, pag. 26): el spune că orice *proprietate ereditară* — adică adevărată pentru n' dacă este adevărată pentru n — este verificată în toată mulțimea N dacă, și numai dacă, este adevărată pentru 0. Este un corolar simplu al propoziției 9 aplicat la submulțimea M a întregilor pentru care această propoziție este adevărată.

Vom nota cu $\alpha(p)$ faptul că proprietatea α este verificată pentru întregul p. Putem enunța *teorema inducției.*

TEOREMĂ 1 / **Fie o proprietate susceptibilă de a fi verificată de întregii naturali. Dacă se poate demonstra că această proprietate este adevărată pentru întregul n' deîndată ce ea este verificată pentru predecesorul său n, atunci este suficient să se demonstreze că ea este adevărată pentru 0 pentru ca ea să fie adevărată pentru toți întregii.**

Se scrie:

$$[\alpha(0) \text{ și } (\forall_N n)\,\{\alpha(n) \Longrightarrow \alpha(n')\}] \Longrightarrow [(\forall_N n)\,\alpha(n)]$$

EXEMPLU. Teorema inducției nu se aplică mulțimii A de la nr. **1.1.2.** Astfel, proprietatea exprimată prin relația de inegalitate:

$$x \geqslant 0,$$

satisface condițiile teoremei 1:

$$0 \geqslant 0,$$

$$x \geqslant 0 \Longrightarrow x + 1 \geqslant 0,$$

dar proprietatea nu este verificată de toate elementele lui A.

Aşa cum vom vedea, enunţul teoremei este modul cel mai practic de a traduce principiul inducţiei.
Există o versiune mai fină, deşi logic echivalentă, de asemenea foarte folosită. Ea are în vedere proprietăţile întregilor mai mari sau egali cu unul din ei. Deşi nu vom defini inegalitatea între întregi decît în paragraful următor (a se vedea nr. 1.2.4), vom da aici această teoremă numită *teorema inducţiei restrînse*, pe care o vom putea admite şi a cărei demonstraţie o vom găsi în exerciţiu.

TEOREMĂ 2 / **Dacă se poate demonstra că o proprietate este adevărată pentru un întreg n' deîndată ce ea este adevărată pentru predecesorul său n, atunci este suficient să se demonstreze că ea este adevărată pentru întregul p pentru ca ea să fie adevărată pentru toţi întregii mai mari sau egali cu p.**

Se scrie:

$$[\alpha(p) \text{ şi } (\forall_N n)\ \{n \geqslant p \text{ şi } \alpha(n) \Longrightarrow \alpha(n')\}] \Longrightarrow [(\forall_N n)\ \{n \geqslant p \Longrightarrow \alpha(n)\}]$$

Demonstraţia teoremei inducţiei restrînse

Fie α proprietatea studiată. Să numim M reuniunea mulţimii întregilor strict inferiori lui p cu mulţimea întregilor pentru care proprietatea α este adevărată. M îl conţine pe 0 deoarece conţine toţi întregii inferiori lui p şi pe p.
Să presupunem proprietatea adevărată pentru n.
1° Dacă: $n < p$, atunci: $n' \leqslant p$; deci:
a) sau: $n' < p$, atunci n' aparţine lui M;
b) sau: $n' = p$, atunci prin ipoteză n' aparţine lui M.
2° Dacă: $n \geqslant p$, prin ipoteza teoremei numărul n' aparţine lui M. Mulţimea M satisface condiţiilor principiului inducţiei, deci $M = N$, ceea ce demonstrează teorema.

Observaţii. — 1 De fapt, în enunţul acestei teoreme, este suficient să se demonstreze caracterul ereditar al proprietăţii studiate numai pentru întregii superiori lui p.
2 O ultimă extensie a teoremei inducţiei este necesară prin faptul că ipoteza după care proprietatea este ereditară (adică $[\alpha(n) \Rightarrow \alpha(n')]$ este uneori dificil de demonstrat, în timp ce se poate verifica cu uşurinţă proprietatea pentru n' dacă se ştie că ea este verificată pentru *toţi întregii de la* 0 *la* n (şi nu numai pentru n).
Observaţiile 1 şi 2 conduc deci la un enunţ general al inducţiei, care se va putea demonstra riguros plecînd de la principiul inducţiei:

TEOREMĂ 3 / **Dacă o proprietate este adevărată pentru un întreg p, şi dacă este suficient ca ea să fie adevărată pentru toţi întregii mai mari sau egali cu p şi mai mici sau egali cu n pentru ca ea să fie verificată de succesorul lui n, atunci această proprietate este adevărată pentru toţi întregii mai mari sau egali cu p.**

1.1.4. Raționament prin inducție

Vom folosi aici proprietățile puse în lumină la numerele **1.1.2** și **1.1.3.** pe exemple. În acestea, va interveni bineînțeles structura lui **N** în toată generalitatea sa; cum nu este vorba decît de ilustrări, nu se creează astfel cercuri vicioase.

1. *Să se demonstreze inegalitatea*: $2^n > n$.

Proprietatea este adevărată pentru $n = 0$, căci:

$$2^0 = 1 \text{ si } 1 > 0.$$

Proprietatea este adevărată pentru $n = 1$, căci:

$$2^1 = 2 \text{ și } 2 > 1.$$

Să presupunem proprietatea adevărată pentru n; avem:

$$2^n > n.$$

Prin înmulțire cu 2 rezultă:

$$2^{n+1} > 2n.$$

Dar: $2n = n + n$; prin urmare, pentru n mai mare sau egal cu 1:

$$n + n \geqslant n + 1.$$

În final:

$$[n \geqslant 1 \text{ și } 2^n > n] \Longrightarrow [2^{n+1} > n + 1].$$

Proprietatea fiind adevărată pentru 0 și pentru orice întreg mai mare sau egal cu 1, teorema este demonstrată.

2. *Să se demonstreze că orice predecesor al unei puteri a lui zece este un multiplu de nouă.*

Scriem aceasta sub forma implicativă:

$$(\forall_{\mathbf{N}} m)\,[(m = 10^n - 1) \Longrightarrow (9/m)].$$

(Semnul / se citește: „divide").

Această proprietate este adevărată pentru $n = 0$ căci:

$$(0 = 10^0 - 1) \Longrightarrow (9/0).$$

Să o presupunem verificată pentru n. Atunci:

$$10^n - 1 = 9k,$$

$$10^{n'} - 1 = 10^{n+1} - 1 = 10(10^n - 1) + 9 = 90k + 9 = 9(10k + 1).$$

Proprietatea este adevărată în baza teoremei **1.**

3. *Să se demonstreze că orice întreg mai mare sau egal cu 24 se poate scrie sub forma:*

$$n = 5a + 7b \quad (a \in \mathbf{N}, b \in \mathbf{N}).$$

Această proprietate este adevărată pentru $n = 24$ căci:

$$24 = 5 \times 2 + 7 \times 2.$$

S-o presupunem verificată pentru: $n \geqslant 24$ (folosim aici observația **1** de la nr **1.1.4**). Atunci:

$$n' = n + 1 = 5a + 7b + 1 = 5(a - 4) + 7(b + 3) = 5(a + 3) + 7(b - 2).$$

Or, una din cele două relații:

$$a \geqslant 4,\ b \geqslant 2$$

este adevărată, deoarece:

$$(a \leqslant 3 \text{ și } b \leqslant 1) \Longrightarrow (5a + 7b \leqslant 22 < 24).$$

Se pot deci găsi, pentru orice n cel puțin egal cu 24, întregi convenabili. De exemplu:

$$25 = 5 \times (2 + 3) + 7 \times (2 - 2).$$

(Se poate verifica că proprietatea este falsă pentru $n = 23$.)

4. *Să se demonstreze că, între cele N triunghiuri formate de n puncte ale unui plan încît trei dintre ele să nu fie niciodată coliniare, numărul T al triunghiurilor ale căror unghiuri sînt ascuțite*[1] *este astfel încît:*

$$4T \leqslant 3N \quad (n \geqslant 4).$$

Această relație este verificată natural pentru primii întregi ($n \leqslant 2$, $N = 0$, $T = 0$) dar nu pentru $n = 3$, căci s-ar putea să avem atunci:

$$T = N = 1.$$

Vom presupune deci că n este cel puțin egal cu 4. Relația este adevărată pentru $n = 4$, deoarece:

$$N = 4 \text{ și } T \leqslant 3.$$

Aceasta se vede distingînd cazurile în care cele patru puncte formează un patrulater convex — suma unghiurilor acestui patrulater fiind egală cu patru unghiuri drepte, unul dintre ele este obligatoriu drept sau obtuz — și cazurile în care unul dintre puncte este interior triunghiului definit de celelalte trei — suma celor trei unghiuri formate în acest punct fiind egală cu patru unghiuri drepte, unul dintre ele este obligatoriu obtuz.
Fie acum: $n \geqslant 4$; să notăm $M_0, M_1, \ldots, M_{n-1}, M_n$ cele $(n + 1)$ puncte pe care le vom studia. Fiecare din sistemele de n puncte care se obține scoțînd unul din punctele date are, prin ipoteza inducției, T_i triunghiuri ascuțitunghice printre cele N_i, cu:

$$4T_i \leqslant 3N_i.$$

Fiecare din cele T triunghiuri ascuțitunghice aparține la $(n - 3)$ sisteme de n puncte — toate acelea care au fost obținute scoțînd din sistem un punct altul decît un vîrf al triunghiului dat. Se deduce relația:

$$(n - 3)T = T_0 + T_1 + \ldots + T_n.$$

---

[1] Se spune: triunghiuri ascuțitunghice.

Se arată în același fel relația:

$$(n-3)N = N_0 + N_1 + \ldots + N_n.$$

Inegalitatea rezultă atunci dintr-o simplă adunare.

(EXEMPLU: pentru $n = 5$, se găsește $N = 10$ și $T \leqslant 7$.)

5. *Se consideră un șir* (u_n) *care satisface următoarele relații:*

$$u_0 = 1,\ u_n < u_0 + u_1 + u_2 + \ldots + u_{n-1}.$$

Să se compare u_{n+1} și 2^n.

Să studiem primii termeni ai șirului:

$$u_0 = 1,\ u_1 < u_0,$$

deci, deoarece $2^0 = 1$:

$$u_1 < 2^0.$$

Avem:

$$u_2 < u_0 + u_1,$$

deci, deoarece $u_0 = 1$ și $u_1 < 1$:

$$u_2 < 2^1, \text{ etc.}$$

Să presupunem că am demonstrat relațiile:

$$u_1 < 2^0,\ u_2 < 2^1,\ \ldots,\ u_{n-1} < 2^{n-2},\ u_n < 2^{n-1}.$$

Prin adunare deducem:

$$u_{n+1} < u_0 + u_1 + u_2 + \ldots + u_n < 1 + 2^0 + 2^1 + \ldots + 2^{n-1}.$$

Or:

$$1 + 2^0 + 2^1 + \ldots + 2^{n-1} = 1 + (1 + 2 + 2^2 + \ldots + 2^{n-1}) = \\ = 1 + (2^n - 1) = 2^n.$$

Deci:

$$u_{n+1} < 2^n.$$

După teorema 3, rezultă că proprietatea este adevărată pentru orice n.

EXERCIȚII

1.1. Să se demonstreze prin inducție în raport cu n egalitatea:

$$2.6.10\ldots(4n-2) = (n+1)(n+2)\ldots 2n \qquad (n \geqslant 1).$$

1.2. Să se demonstreze prin inducție în raport cu n egalitatea:

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6} \qquad (n \geqslant 1).$$

1.3. Să se demonstreze prin inducție în raport cu n egalitatea:

$$1^3 + 2^3 + \ldots + n^3 = \frac{n^2(n+1)^2}{4} \qquad (n \geqslant 1).$$

1.4. Să se demonstreze prin inducție în raport cu n egalitatea:

$$1 \cdot 2 + 2 \cdot 3 + \ldots + (n-1)\,n = \frac{(n-1)\,n\,(n+1)}{3} \quad (n \geqslant 2).$$

1.5. Să se demonstreze prin inducție în raport cu n că suma unghiurilor interioare ale unui poligon convex cu n laturi este egală cu $(n-2)\,\pi$ radiani ($n \geqslant 3$).
1.6. Să se generalizeze exercițiul nr. 1.5 la poligoane neconvexe, dar nestelate (anumite unghiuri interioare sînt atunci băgate în interior). (Vom fi conduși să considerăm două cazuri în aplicarea inducției.)
1.7. Să se demonstreze prin inducție în raport cu n că, dacă a este un întreg impar, numărul 2^{n+2} divide întregul:

$$a^m - 1,$$

unde $m = 2^n$, cu: $n \geqslant 1$.
1.8. Începînd de la ce valoare a lui n se poate scrie inegalitatea:

$$2^q - 1 > q^n$$

cu $q = 2^n$?

1.2. STRUCTURA LUI N

1.2.1. Axiomele lui Peano[1]

Printre proprietățile de mai sus vom selecționa trei, din care vom deduce logic toate proprietățile lui N (din motive evidente, unele vor fi trecute la exerciții; ele nu prezintă nici o dificultate deosebită.)

DEFINIȚIE 1 / **Se numește N orice mulțime care are următoarele proprietăți:**
A1 Există o injecție f, numită *succesiune*, de la N la N.
A2 Există un element 0, numit zero, care nu este imaginea prin f a niciunui element din N.
A3 Orice submulțime a lui N care-l conține pe 0 și imaginea prin f a tuturor elementelor sale este egală cu N.

Axioma **A1** nu este alta decît proprietatea 6; axioma A2 traduce proprietatea 5; axioma **A3** este principiul inducției (proprietatea 9);

Observație. — Este foarte ușor de arătat că aceste axiome sînt independente, adică există mulțimi E în care se pot verifica două din aceste axiome dar

---

[1] *Giuseppe Peano*, logician și matematician italian (1858—1932)
De fapt, aceste axiome au fost formulate pentru prima dată în 1888 de J.W.R. Dedekind (1831—1916).

nu și a treia. Se cunoaște un exemplu (nr. 1.1.2) unde axioma **A3** nu este verificată în timp ce axiomele **A1** și **A2** sînt verificate. Mulțimea $E = \{0,1\}$ poate servi de exemplu pentru celelalte două cazuri; este suficient să punem:

$$f(0) = 1.$$

Dacă $f(1) = 0$, E verifică *A1* și *A3*, dar nu pe *A2*.
Dacă $f(1) = 1$, E verifică *A2* și *A3*, dar nu pe *A1*.
(Să remarcăm de asemenea că N însuși verifică pe *A1* și *A2* dar nu pe *A3*, dacă punem $f(n) = 2^n$).
Teoremele 1, 2 și 3 sînt adevărate deoarece sînt simple consecințe ale axiomei **A3**, echivalente cu principiul inducției.
Să demonstrăm, ca altă teoremă foarte simplă valabilă în N, că orice întreg diferit de 0 admite un predecesor unic (proprietatea 7).
Numărul 1 are ca predecesor pe 0 deoarece:

$$0' = 1.$$

Dacă n are un predecesor, atunci n', care-l urmează pe n, are ca predecesor pe n. Deci, după teorema 2, orice număr diferit de 0 are un predecesor.
Dacă n ar fi avut ca predecesori pe p și q, am fi avut:

$$p \neq q \Longrightarrow f(p) = f(q) = n,$$

în contradicție cu faptul că f este injectivă.
Vom enunța deci:

TEOREMĂ / Orice întreg diferit de 0 admite un predecesor unic.

4

1.2.2. Adunarea

Acest paragraf este consacrat studiului unei legi de compoziție, numită *adunare*, pe N. O vom nota prin semnul $+$.
Vom construi *suma* a doi întregi naturali cu ajutorul axiomei inducției.
Să punem a priori:

$$\boxed{\forall_N n,\ \forall_N m\colon n + 0 = n,\ n + m' = (n + m)'} \qquad (1), (2)$$

(Reamintim că m' este un simbol echivalent cu $f(m)$, succesorul lui m.) Aceste egalități sînt conforme cu ideea noastră intuitivă despre adunare deoarece m' nu este altceva decît suma $(m + 1)$; dealtfel se poate demonstra imediat, substituind întregul 0 întregului m în egalitatea (2):

$$n + 1 = n + 0' = (n + 0)' = n', \qquad \boxed{n + 1 = n'}$$

(Amintim că 1 a fost definit ca succesor al lui 0.)
Dacă n este dat, cunoaștem deja $(n + 0)$ și $(n + 1)$. Să notăm cu M mulțimea întregilor m pentru care $(n + m)$ este calculabilă; axioma **A3** și ega-

litatea (2) arată că M este egală cu N, deoarece cunoaşterea sumei $(n + m)$ antrenează cunoaşterea sumei:

$$n + m' = (n + m)' = (n + m) + 1.$$

Suma a doi întregi este deci definită pentru orice pereche (n, m). Se poate arăta, prin inducţie în raport cu m, că nu există decît o singură operaţie care să satisfacă axiomele (1) şi (2). (Exerciţiul nr. 1.9.)

1. *Asociativitatea* adunării este o consecinţă a definiţiilor.

Într-adevăr, ştim că:

$$m + (n + 0) = m + n = (m + n) + 0.$$

Egalitatea (unde vom presupune m şi n daţi, şi p variabil):

$$\boxed{m + (n + p) = (m + n) + p} \tag{4}$$

este deci adevărată pentru $p = 0$. Dacă ea este adevărată pentru p, atunci:

$$\begin{aligned} m + (n + p') &= m + (n + p)' \\ &= [m + (n + p)]' = [(m + n) + p]' \\ &= (m + n) + p'. \end{aligned}$$

Teorema 1 arată că egalitatea (4) este adevărată pentru orice întreg p.

2. *Comutativitatea* are o demonstraţie mai lungă. Vom folosi de trei ori inducţia pentru a dovedi egalităţile:

$$\boxed{\begin{aligned} n + 0 &= 0 + n \qquad (5) \\ n + 1 &= 1 + n \qquad (6) \\ n + m &= m + n \qquad (7) \end{aligned}}$$

Egalitatea (5) este adevărată pentru $n = 0$; dacă este adevărată pentru n, atunci:

$$n' + 0 = n' = (n + 0)' = (0 + n)' = 0 + n'.$$

Egalitatea (5) este deci adevărată pentru orice n: 0 este *element neutru.*

Egalitatea (6) este adevărată pentru $n = 0$ din ceea ce precede; dacă ea este adevărată pentru n, atunci:

$$n' + 1 = (n + 1) + 1 = (n + 1)' = (1 + n)' = 1 + n'.$$

Egalitatea (6) este deci adevărată pentru orice n.

În sfîrşit, egalitatea (7) este adevărată pentru $n = 0$ după (5); dacă ea este adevărată pentrn m fixat şi pentru un anumit n, atunci:

$$\begin{aligned} n' + m &= (n + 1) + m = n + (1 + m) = n + (m + 1) \\ &= (n + m) + 1 = (m + n) + 1 \\ &= m + (n + 1) = m + n'. \end{aligned}$$

Egalitatea (7) este deci adevărată pentru orice n.

3. Cu toate că adunarea nu conferă lui N structura de grup, așa cum vom vedea mai jos, fiecare întreg este simplificabil într-o egalitate de sume (se spune că este *regulat* pentru adunare).
Într-adevăr, să demonstrăm echivalența:

$$\boxed{m + n = p + n \Longleftrightarrow m = p} \tag{8}$$

Trebuie să demonstrăm numai implicația ($\Rightarrow$). Ea este adevărată pentru $n = 0$; dacă este adevărată pentru n, atunci:

$$(m + n' = p + n') \Longrightarrow ([m + n]' = [p + n]');$$

de unde, prin aplicarea axiomei **A1**: $(m + n = p + n)$;
aceasta implicînd $(m = p)$, echivalența (8) este demonstrată prin inducție în raport cu n.
4. Să arătăm că, în N, 0 este singurul element care are un *opus*, adică:

$$\boxed{m + n = 0 \Longleftrightarrow m = n = 0} \tag{9}$$

Trebuie demonstrată numai implicația ($\Rightarrow$).
Fie n diferit de 0; există atunci p astfel încît $p' = n$:

$$m + n = m + p' = (m + p)'.$$

Dacă $m + n = 0$, rezultă că $(m + p)$ ar fi predecesorul lui 0, ceea ce este fals; deci:

$$\forall m\ (n \neq 0) \Longrightarrow (m + n \neq 0).$$

Prin contrapoziție rezultă:

$$(m + n = 0) \Longrightarrow (n = 0).$$

Dar:

$$m + 0 = m,$$

deci:

$$(m + 0 = 0) \Longrightarrow (m = 0).$$

De unde rezultatul căutat.
5. Să rezumăm aceste propoziții într-o teoremă.

TEOREMA 5 / **Adunarea a doi întregi este o operație internă definită complet pe N prin egalitățile:**

$$\boxed{n + 0 = n,\ n + m' = (n + m)'}$$

Este asociativă și comutativă; 0 este element neutru și singurul număr care admite un opus (el însuși). Orice element este regulat pentru adunare.

$$\boxed{\begin{array}{l} n + (m + p) = (n + m) + p \\ n + m = m + n \\ n + 0 = 0 + n = n \\ n + p = m + p \Longleftrightarrow n = m \\ n + m = 0 \Longleftrightarrow n = m = 0 \end{array}}$$

EXERCIȚIU. *Să se demonstreze că doi și cu doi fac patru.*
Să revenim la definiții: $1 = 0'$, $2 = 1'$, $3 = 2'$, $4 = 3'$,

$$2 + 2 = 2 + 1' = (2 + 1)' = (2')' = 3' = 4.$$

1.2.3. Înmulțirea

Acest paragraf este consacrat studiului unei legi de compoziție, numită *înmulțire*, pe N. O vom nota prin semnul $\times$.
Vom construi *produsul* a doi întregi naturali cu ajutorul axiomei inducției și a proprietăților adunării. Să punem a priori:

$$\boxed{\forall_{\mathbf{N}} n,\ {}_{\mathbf{N}}m : n \times 0 = 0,\ n \times m' = (n \times m) + n} \quad (10)\ (11)$$

Aceste egalități sînt conforme cu ideea noastră intuitivă despre înmulțire. De exemplu, să substituim întregul 0 întregului m în egalitatea (11):

$$n \times 1 = n \times 0' = n \times 0 + n = 0 + n = n, \qquad \boxed{n \times 1 = n} \quad (12)$$

Dacă n este dat, cunoaștem deja $(n \times 0)$ și $(n \times 1)$. Să notăm cu M mulțimea întregilor m pentru care $(n \times m)$ este calculabil: se arată ca și pentru adunare că $M = \mathbf{N}$.
Produsul a doi întregi este deci bine definit pentru orice pereche (n, m); se demonstrează, ca și pentru adunare, că el este unic.
1. Să demonstrăm mai întîi *distributivitatea la stînga* a înmulțirii în raport cu adunarea, adică egalitatea:

$$\boxed{(m + n)p = mp + np} \quad (13)$$

(Așa cum se obișnuiește, vom scrie de acum încolo de multe ori mn în loc de $m \times n$.)

Egalitatea (13) este adevărată pentru $p = 0$, deoarece:

$$(m + n)0 = 0 = 0 + 0 = m0 + n0.$$

Dacă este adevărată pentru p, atunci:

$$\begin{aligned}(m + n)p' &= (m + n)p + (m + n) = (mp + np) + (m + n)\\ &= mp + [np + (m + n)] = mp + [(np + m) + n]\\ &= mp + [(m + np) + n] = mp + [m + (np + n)]\\ &= (mp + m) + (np + n) = mp' + np'.\end{aligned}$$

Proprietatea este deci demonstrată prin inducție în raport cu p.

2. Să demonstrăm *distributivitatea la dreapta*:

$$\boxed{m(n + p) = mn + mp} \tag{14}$$

Egalitatea (14) este adevărată pentru $p = 0$, deoarece:

$$m(n + 0) = mn = mn + 0 = mn + m0.$$

Dacă este adevărată pentru p, atunci:

$$\begin{aligned}m(n + p') &= m(n + p)' = m(n + p) + m\\ &= (mn + mp) + m = mn + (mp + m)\\ &= mn + mp'.\end{aligned}$$

Proprietatea este deci demonstrată prin inducție în raport cu p.

3. *Asociativitatea* rezultă destul de simplu. Într-adevăr, egalitatea:

$$\boxed{m(np) = (mn)p} \tag{15}$$

este adevărată pentru $p = 0$. Dacă este adevărată pentru p, atunci:

$$\begin{aligned}m(np') &= m(np + n) = m(np) + mn\\ &= (mn)p + (0 + mn) = (mn)p + [(mn)0 + mn]\\ &= (mn)p + (mn)0' = (mn)(p + 0')\\ &= (mn)p'.\end{aligned}$$

Proprietatea este deci demonstrată prin inducție în raport cu p.

4. În scopul studierii *comutativității* înmulțirii, să demonstrăm mai întîi egalitatea:

$$\boxed{0n = 0} \tag{16}$$

Este adevărată pentru $n = 0$; dacă este adevărată pentru n, atunci:

$$0n' = 0n + 0 = 0n = 0,$$

ceea ce demonstrează egalitatea (16) prin inducție în raport cu n.
Se spune că 0 este *absorbant* pentru înmulțire.
5. Regula de *comutativitate:*

$$\boxed{mn = nm} \tag{17}$$

este deci verificată pentru $n = 0$, deoarece:

$$m0 = 0 = 0m.$$

Este verificată prin inducție în raport cu m dacă $n = 1$.
Adăugînd acest rezultat la egalitatea (12), se poate deduce că 1 este element neutru pentru înmulțire:

$$1n = n1 = n.$$

Dacă egalitatea (17) este verificată pentru n, atunci:

$$mn' = mn + m = nm + m = nm + 1m = n'm$$

după egalitatea (13).
Comutativitatea este deci o proprietate a înmulțirii pe N.
6. Produsul a două elemente nenule este nenul, ceea ce se poate traduce prin echivalența:

$$\boxed{nm = 0 \iff n = 0 \text{ sau } m = 0} \tag{18}$$

Trebuie demonstrată numai implicația ($\Longrightarrow$). Deocamdată, *nu vom folosi inducția*; vom folosi numai echivalența (9), definiția înmulțirii și teorema 4.
Pentru $m = 0$, nu este nimic de demonstrat.
Să presupunem deci m nenul: el este succesorul unui întreg p; atunci:

$$\begin{aligned}(nm = 0) &\Longrightarrow (np' = 0) \Longrightarrow (np + n = 0)\\ &\Longrightarrow (np = n = 0)\\ &\Longrightarrow (n = 0).\end{aligned}$$

7. Produsul a două elemente diferite de 1 este diferit de 1, ceea ce se poate traduce prin echivalența:

$$\boxed{nm = 1 \iff n = m = 1} \tag{19}$$

Trebuie demonstrată numai implicația ($\Longrightarrow$). Nu vom folosi, nici aici, inducția; vom folosi numai rezultatul precedent, teorema 4, axioma A1, echivalența (9) și comutativitatea produsului.

Dacă ($nm = 1$), n şi m nu sînt nuli; sînt succesorii a doi întregi p şi q. Să scriem:

$$0' = 1 = nm = p'q' = p'q + p' = (p'q + p)'.$$

În consecinţă:

$$0 = p'q + p,$$

de unde:

$$p = 0,\ n = 1.$$

S-ar putea arăta la fel că:

$$q = 0,\ m = 1.$$

(Se poate observa de asemenea că $p'q = q$ trebuie de asemenea să fie nul, ceea ce nu face să intervină comutativitatea.) 1 este deci singurul element al lui **N** care are un *invers*.

8. Să rezumăm aceste propoziţii într-o teoremă:

TEOREMĂ 6 / **Înmulţirea a doi întregi este o operaţie internă definită complet pe N prin egalităţile:**

$$n0 = 0,\ nm' = nm + n$$

Ea este asociativă, comutativă şi distributivă în raport cu adunarea; 0 este element absorbant; produsul a două elemente nenule este nenul; 1 este element neutru şi singurul număr care admite un invers (el însuşi).

$$n(mp) = (nm)p;\ nm = mn$$
$$n(m + p) = nm + np$$
$$n0 = 0n = 0;\ n1 = 1n = n$$
$$nm = 0 \Leftrightarrow n = 0 \text{ sau } m = 0$$
$$nm = 1 \Leftrightarrow n = m = 1$$

EXERCIŢIU. *Să se demonstreze că doi ori doi fac patru.*

$$2 \times 2 = 2 \times 1' = (2 \times 1) + 2 = 2 + 2.$$

Dar noi ştim că (exerciţiul nr. **1.2.2**):

$$2 + 2 = 4.$$

Vom studia mai departe (nr. **1.2.4**) ecuaţia în numere întregi:

$$n + m = nm.$$

1.2.4. Ordine

Conform unei intuiții foarte simple, vom defini o relație de ordine pe N prin posibilitatea de *scădere* a celui mai mic întreg din cel mai mare:

$$\boxed{\forall_N n,\ \forall_N m : n \geqslant m \Leftrightarrow \exists p,\ n = m + p} \tag{20}$$

Simbolul „$\geqslant$" se citește „mai mare sau egal cu".
Numărul p este *diferența* între n și m (se notează adesea $p = n - m$). El este unic (8).
Această relație dă naștere la o relație *strictă*, asociată:

$$\boxed{(n > m) \Leftrightarrow (n \geqslant m \text{ și } n \neq m) \Leftrightarrow (\exists p \neq 0,\ n = m + p)} \tag{21}$$

Relațiile $(n \geqslant m)$ și $(n > m)$ se mai scriu, respectiv:

$$(m \leqslant n) \text{ și } (m < n).$$

Aceste simboluri au numeroase aplicații imediate. Se vor putea demonstra direct cele care urmează:

$$(n \in \mathbf{N} \Longrightarrow n \geqslant 0),\ (n \neq 0 \Leftrightarrow n > 0 \Leftrightarrow n \geqslant 1),$$
$$[(n + 1 > n),\ (n > 0 \text{ și } m > 0)] \Longrightarrow (n + m > 0), \text{ etc.}$$

Să studiem mai de aproape relația notată: „$\geqslant$".
1. O astfel de relație binară este evident o *relație de ordine*, deoarece:

▪ *Reflexivitate.*

$$n = n + 0 \Longrightarrow \boxed{n \geqslant n} \tag{22}$$

▪ *Tranzitivitate.*

$$(n \geqslant m \text{ și } m \geqslant p) \Longrightarrow (n = m + q \text{ și } m = p + r)$$
$$\Longrightarrow [n = (p + r) + q = p + (r + q)] \Longrightarrow (n \geqslant p).$$

$$\boxed{(n \geqslant m \text{ și } m \geqslant p) \Longrightarrow (n \geqslant p)} \tag{23}$$

▪ *Antisimetrie.*

$$(n \geqslant m \text{ și } m \geqslant n) \Longrightarrow (n = m + p \text{ și } m = n + q)$$
$$\Longrightarrow [n = (n + q) + p = n + (q + p)]$$
$$\Longrightarrow (0 = q + p) \Longrightarrow (0 = p) \Longrightarrow (n = m).$$

$$\boxed{(n \geqslant m \text{ și } m \geqslant n) \Longrightarrow (n = m)} \tag{24}$$

(Am aplicat echivalențele (8) și (9) privind regularitatea întregilor la adunare și unicitatea egalității ($m + n = 0$) în N.)

2. Relația de inegalitate strictă este evident tranzitivă deoarece:

$$(n = m + q, q \neq 0, m = p + r, r \neq 0) \Longrightarrow (n = p + (r + q), r + q \neq 0).$$

$$\boxed{(n > m \text{ și } m > p) \Longrightarrow (n > p)} \tag{25}$$

3. Relația de ordine este *compatibilă* cu adunarea: adunarea unui același, întreg, în cei doi membri ai unei inegalități nu o modifică. De fapt vom demonstra echivalența mai tare:

$$\boxed{n \geqslant m \Longleftrightarrow (n + p) \geqslant (m + p)} \tag{26}$$

Într-adevăr:

$$n \geqslant m \Longleftrightarrow (n = m + q) \Longleftrightarrow [(n + p) = (m + q) + p].$$

Proprietățile adunării ne permit să scriem:

$$(m + q) + p = m + (q + p) = m + (p + q) = (m + p) + q.$$

Cum:

$$[(n + p) = (m + p) + q] \Longleftrightarrow [(n + p) \geqslant m + p],$$

avem:

$$n \geqslant m \Longleftrightarrow (n + p) \geqslant (m + p).$$

La fel, presupunînd p diferit de 0:

$$\boxed{(n > m) \Longleftrightarrow [(n + p) > (m + p)]]} \tag{27}$$

4. Se poate demonstra compatibilitatea relației de ordine cu înmulțirea:

$$\boxed{(n \geqslant m) \Longrightarrow (np \geqslant mp)} \tag{28}$$

Într-adevăr:

$$(n = m + q) \Longrightarrow (np = mp + qp).$$

Produsul a două numere nenule fiind nenul, presupunînd p diferit de 0 și q diferit de 0, deducem implicația:

$$\boxed{(n > m \text{ și } p \neq 0) \Longrightarrow (np > mp)} \tag{29}$$

5. Ordinea pe care o studiem noi este o *ordine totală*, adică doi întregi sînt comparabili întotdeauna:

$$(n \in \mathbf{N} \text{ şi } m \in \mathbf{N}) \Longrightarrow (n \geqslant m \text{ sau } m \geqslant n) \tag{30}$$

Vom demonstra această implicaţie ca o consecinţă a unei implicaţii puţin mai tare:

$$(n \in \mathbf{N} \text{ şi } m \in \mathbf{N}) \Longrightarrow (n > m \text{ sau } n = m \text{ sau } m > n) \tag{31}$$

cele trei eventualităţi excluzîndu-se reciproc.
Demonstraţia se face prin inducţie în raport cu n.
Pentru $n = 0$, implicaţia este adevărată, pentru că:

$$0 = m \text{ dacă } m = 0,\ m > 0 \text{ dacă } m \neq 0.$$

Dacă n este comparabil cu m, să încercăm să comparăm n' şi m. Se prezintă trei cazuri:

■ $n > m$; atunci: $n = m + p,\ p \neq 0,$

şi:

$$n' = m + p',$$

deci:

$$n' > m.$$

■ $n = m$; atunci:

$$n' = m + 1, \text{ deci: } n' > m.$$

■ $m > n$; atunci: $m = n + p,\ p \neq 0$, de unde existenţa unui întreg q astfel încît:

$$p = q',\ m = n + q' = n' + q.$$

(Această egalitate se scrie într-adevăr:

$$n + q' = n + (q + 1) = n + (1 + q) = (n + 1) + q = n' + q).$$

Dacă q este nul, atunci $m = n'$. Dacă nu: $m > n'$; n' este deci întotdeauna comparabil cu m; aceasta încheie aplicarea inducţiei şi demonstrează implicaţiile (31) şi (30).

6. Să studiem acum reciproca implicaţiei (29):

$$(np > mp) \Longrightarrow (n > m \text{ şi } p \neq 0) \tag{32}$$

Dacă am avea ($p = 0$), inegalitatea ($np > mp$) ar fi falsă; p este deci nenul. Dacă am avea ($n = m$) sau ($m > n$), am deduce ($np = mp$) sau ($mp > np$). Cum noi ştim că ordinea este totală, putem trage concluzia că excluderea ipotezelor ($n = m$, $m > n$) antrenează inegalitatea ($n > m$), de unde rezultă teorema.

7. Implicaţia (28) nu admite decît o reciprocă parţială:

$$(np \geqslant mp) \Longrightarrow (n \geqslant m \text{ sau } p = 0) \tag{33}$$

Într-adevăr cazul ($p = 0$) nu poate fi îndepărtat aici. Dacă se presupune $p \neq 0$ nu rezultă că raţionamentul precedent se poate aplica.

O consecinţă importantă a acestei implicaţii are în vedere întregii nenuli: ei sînt *regulaţi* faţă de înmulţire, deoarece se poate scrie:

$$(np = mp) \Longrightarrow (n = m \text{ sau } p = 0) \tag{34}$$

(Se consideră egalitatea ($np = mp$) ca fiind conjuncţia a două inegalităţi ($np \geqslant mp$) şi ($mp \geqslant np$).)

8. Să rezumăm principalele proprietăţi găsite mai sus:

TEOREMĂ 7 / **Relaţia de inegalitate între întregi este bine definită în N prin echivalenţa:**

$$n \geqslant m \Longleftrightarrow \exists p \; n = m + p$$

Este o relaţie de ordine totală, compatibilă cu adunarea şi înmulţirea pe N.

TEOREMĂ 8 / **Orice întreg este regulat pentru adunare.**
Orice întreg nenul este regulat pentru înmulţire.

Relaţie de ordine şi *Compatibilitate* — **Ordine totală**

$$\left\{\begin{array}{l} n \geqslant n;\ (n \geqslant m \text{ şi } m \geqslant p) \Longrightarrow (n \geqslant p) \\ (n \geqslant m \text{ şi } m \geqslant n) \Longleftrightarrow (n = m) \\ (n \in \mathbf{N} \text{ şi } m \in \mathbf{N}) \Longrightarrow (n \geqslant m \text{ sau } m \geqslant n) \\ (n \geqslant m \Longleftrightarrow (n + p \geqslant m + p) \\ (n \geqslant m \Longrightarrow (np \geqslant mp) \\ (np \geqslant mp) \Longleftrightarrow (n \geqslant m \text{ sau } p = 0) \end{array}\right.$$

$$\begin{array}{l} (n > m \text{ şi } m > p) \Longrightarrow (n > p) \\ (n > m) \Longleftrightarrow (n + p > m + p) \\ (n > m \text{ şi } p \neq 0) \Longleftrightarrow (np > mp) \end{array}$$

$$(np = mp) \iff (n = m \text{ sau } p = 0)$$

Să semnalăm de asemenea o implicație care se referă în același timp la inegalitățile nestricte și stricte:

$$(n \geqslant m \text{ și } m > p) \Longrightarrow (n > p) \tag{35}$$

EXERCIȚII. I. *Să se demonstreze implicația precedentă* (35).

Avem:

$$n = m + r,$$
$$m = p + s,\ s \neq 0,$$

deci:

$$n = (p + s) + r = p + (s + r).$$

Se știe că:

$$(s \neq 0) \Longrightarrow (s + r) \neq 0;$$

avem deci:

$$[n \geqslant m \text{ și } m > p] \Longrightarrow (n > p).$$

Se demonstrează la fel implicația analoagă:

$$[n > m \text{ și } m \geqslant p] \Longrightarrow (n > p).$$

II. *Să se compare* $(n + m)$ *și* (nm).
Să studiem diferite valori ale lui m ținînd seama de comutativitatea operațiilor.

Dacă $m = 0$, atunci:

$$nm = 0 \text{ și } n + m = n,$$

deci:

$$nm \leqslant n + m.$$

Cazul $n = 0$ este analog.
Să studiem deci cazurile în care n și m admit predecesorii p și q:

$$n = p',\ m = q',\ n + m = p + q + 2 = 1 + q + p + 1$$
$$nm = p'q' = p'q + p' = pq + q + p + 1.$$

A compara deci $(n + m)$ și (nm) revine deci la a compara pe 1 și pq.
În consecință:

$$(m \geqslant 2 \text{ și } n \geqslant 2) \iff (p \neq 0 \text{ și } q \neq 0) \iff (pq \geqslant 1)$$
$$\iff (mn \neq 0 \text{ și } nm \geqslant n + m).$$

(Celelalte cazuri sînt foarte simple; se verifică că avem:

$$m = 1,\ n \geqslant 1; \qquad n + m > nm;$$
$$m \geqslant 1,\ n = 1; \qquad n + m > nm.)$$

Dacă vrem să ştim cazurile de egalitate între sumă şi produs, deducem ($m = n = 0$) sau, dacă se presupune ($m \geqslant 1$ şi $n \geqslant 1$):

$$(nm = n + m) \Longleftrightarrow (pq = 1) \Longleftrightarrow (p = q = 1)$$
$$\Longleftrightarrow (m = n = 2).$$

Tabloul următor rezumă discuţia (semnul indicat arată simbolul relaţional care trebuie plasat în relaţia:

$$nm? \; n + m).$$

m \ n	0	1	2	$\geqslant 3$
0	=	<	<	<
1	<	<	<	<
2	<	<	=	<
$\geqslant 3$	<	<	>	>

Ecuaţia definită prin ($nm = n + m$) nu are decît două soluţii:

$$0 = 0 \times 0 = 0 + 0; \; 4 = 2 \times 2 = 2 + 2.$$

III. *Să se demonstreze, fără a folosi relaţia de ordine, următorul caz particular al echivalenţei* (34):

$$(n + n = m + m) \Longleftrightarrow (n = m).$$

Să studiem ecuaţia definită prin:

$$x + x = n + n \quad (x \in \mathbf{N}).$$

Aceasta nu admite decît o singură soluţie pentru $n = 0$: ea este $x = 0$.
Să presupunem că unicitatea acestei soluţii mai este verificată pentru n; să studiem atunci ecuaţia:

$$x + x = n' + n' = n + n + 2.$$

Dacă există o soluţie x, acest întreg nu poate fi nul. Este deci succesorul unui anumit întreg y, de unde:

$$y + y + 2 = y' + y' = x' + x' = n + n + 2.$$
$$y + y = n + n.$$

Această ultimă ecuaţie, neavînd decît o singură rădăcină prin ipoteza inducţiei, acelaşi lucru se întîmplă cu:

$$x + x = n' + n'.$$

Cum această soluţie este evidentă (este $x = n'$), am dovedit echivalenţa studiată.

EXERCIȚII

1.9. Să se demonstreze că nu există decît o singură operație în N care să satisfacă axiomele adunării.

1.10. Să se demonstreze că un element neutru definit pentru o operație este unic.

1.11. Aceeași problemă pentru un element absorbant.

1.12. Să se demonstreze direct, plecînd de la axiomele înmulțirii, egalitatea:

$$m'n = mn + n.$$

1.13. Să se demonstreze că nu există nici un întreg m astfel încît:

$$n < m < n + 1 \qquad \text{(unde } n \text{ este dat)}$$

1.14. Să se demonstreze relațiile:

$$(n \in \mathbf{N} \Longrightarrow n \geqslant 0);\ (n \neq 0 \Longleftrightarrow n > 0 \Longleftrightarrow n \geqslant 1);$$
$$(n + 1 > n);\ (n > 0 \text{ și } m > 0 \Longrightarrow n + m > 0).$$

1.15. Să se demonstreze direct, plecînd de la definiția relației de ordine, implicația:

$$(n \in \mathbf{N} \text{ și } m \in \mathbf{N}) \Longrightarrow (n \geqslant m \text{ sau } m \geqslant n).$$

1.16. Să se demonstreze egalitățile:

$$[(m + n) + p] + q = (m + n) + (p + q);$$
$$\{[(m + n) + p] + q\} + r = (m + n) + [(p + q) + r].$$

1.17. Același exercițiu pentru înmulțire.

1.18. Se pune în N:

$$m * n = m + n + 1.$$

Să se studieze proprietățile acestei operații.

1.19. Se pune în N:

$$m = b + c,\ n = c + a,\ p = a + b.$$

Să se compare întregii:

$$(m + a),\quad (n + b),\quad (p + c).$$

1.20. Să se numere perechile de elemente din N definite prin egalitatea (unde n este dat):

$$x + y = n.$$

1.21. Să se demonstreze egalitatea:

$$\{[(1 + 2) + 3] + \ldots + n\} = \{[(n + \{n - 1\}) + \{n - 2\}] + \ldots + 1\}.$$

Să se deducă valoarea comună a celor doi membri.

1.22. Să se reia exercițiul nr. **1.19** înlocuind adunarea cu înmulțirea.

1.23. Cîte bijecții f există de la N pe N astfel încît, pentru orice întreg n:

$$f(n) \leqslant n?$$

1.24. Se pune, în N:

$$a - b = d,\ x - y = z$$

Să se demonstreze implicația:

$$(d > z,\ a > x \text{ și } b > y) \Longrightarrow (a - x > b - y).$$

1.25. Să se numere perechile de elemente din N definite prin relaţiile (unde n şi m sînt daţi):

$$x - y = n, \quad x \leqslant m.$$

1.26. Să se demonstreze direct, fără a folosi relaţia de ordine, echivalenţa:

$$(n + n + n = m + m + m) \Longleftrightarrow (n = m).$$

1.27. Acelaşi exerciţiu cu patru termeni (să se folosească exerciţiul rezolvat III de la nr. 1.2.4).

1.28. Acelaşi exerciţiu pentru echivalenţa:

$$(n^2 = m^2) \Longleftrightarrow (n = m).$$

1.29. Să se rezolve, în N ecuaţia definită prin:

$$x^2 = 18\,713.$$

1.3. SUBMULŢIMI ALE LUI N

1.3.1. Ordine şi predecesor

În N, orice inegalitate strictă poate fi înlocuită prin una nestrictă, şi reciproc. Într-adevăr:

$$\boxed{n \geqslant m + 1 \Longleftrightarrow n > m} \tag{36}$$

(Singura excepţie o formează inegalitatea nestrictă $n \geqslant 0$ care nu se poate scrie sub forma $n > m$.)

Această echivalenţă se demonstrează foarte simplu.
Într-adevăr:

$$(n \geqslant m + 1) \Longleftrightarrow (n = (m + 1) + p)$$
$$\Longleftrightarrow (n = m + (p + 1), \quad p + 1 \neq 0) \Longleftrightarrow (n > m).$$

(În N, noţiunea de *interval* este deci mai simplă ca în alte mulţimi ca de exemplu R; vom reveni asupra acestei probleme la nr. **1.4.1.**)
Această proprietate se poate exprima folosind termenii de *majoranţi* şi *minoranţi*:

DEFINIŢIE 2 / **Un majorant (resp. majorant strict, minorant, minorant strict) al unei submulţimi nevide A a unei mulţimi ordonate E este un element mai mare sau egal (resp. strict mai mare, mai mic sau egal, strict mai mic) ca toate elementele lui A.**

Putem enunţa:

TEOREMĂ 9 / **Succesorul unui întreg este cel mai mic dintre majoranții săi stricți; predecesorul, dacă există, este cel mai mare dintre minoranții săi stricți.**

(Mulțimea A nu are aici decît un singur element.)

1.3.2. Element minimum

Să considerăm o submulțime nevidă A a lui **N**; în două cazuri foarte simple ($A = \mathbf{N}$, $A = \{n\}$), vedem că această mulțime are un *element minimum* (sau cel mai mic element) dacă adoptăm următoarea definiție:

DEFINIȚIE 3 / **Un element al unei submulțimi A a unei mulțimi ordonate E este un element minimum (resp. maximum) al lui A dacă el este un minorant (resp. majorant) al lui A.**

Un minimum, notat:

$$\min A,$$

este deci în mod necesar un element al lui A; el poate să nu existe (exemple: $E = \mathbf{R}$; A fiind mulțimea numerelor pozitive x astfel încît: $x^2 > 2$), dar dacă există este unic — și el va fi numit deci minimum.
În **N**, orice submulțime nevidă admite un minimum. Vom demonstra acest rezultat prin inducție.
Fie $\alpha\,(n)$ următoarea proprietate:
„A (nevidă) *admite un minimum dacă conține un element mai mic sau egal cu* n".
$\alpha\,(0)$ este adevărată, căci A conține atunci pe 0 care este evident minimumul său.
Dacă $\alpha\,(n)$ este adevărată, să considerăm o mulțime A care conține un întreg:

$$m \leqslant n + 1.$$

Dacă se poate găsi un întreg ($m < n + 1$) în A, avem atunci ($m \leqslant n$), de unde rezultă existența minimumului lui A prin ipoteza inducției.
Dacă aceasta este imposibil, din cauză că A nu conține niciunul dintre elementele strict inferioare lui $(n + 1)$, dar conține pe $(n + 1)$; rezultă că $(n + 1)$ este minimumul lui A.
Putem deduce următoarea teoremă:

TEOREMĂ 10 / **Orice submulțime nevidă a lui N admite un element minimum unic.**

(Despre o mulțime ordonată în care este adevărată o proprietate analoagă cu teorema 10, se spune că este *bine ordonată*; aceasta implică că ordinea este totală.)

EXERCIȚIU. *Să se demonstreze teorema 10 folosind mulțimea M a minoranților lui A.*
Mulțimea minoranților lui A:

$$M = \{m;\ n \in A \Longrightarrow m \leqslant n\}$$

conține evident pe 0. Dacă l-ar conține pe $(m + 1)$ de fiecare dată cînd îl conține pe m, M ar fi confundată cu N și A ar fi vidă. Dar, A nu este vidă; deci există un element p al lui M astfel încît $(p + 1)$ nu aparține lui M; p minorează toate elementele lui A; dacă el însuși nu aparține lui A, avem, pentru orice n care aparține lui A:

$$(p < n) \Longrightarrow (p + 1 \leqslant n),$$

ceea ce implică că $(p + 1)$ este un minorant al lui A ceea ce este contrar ipotezei:

$$(p + 1) \notin M.$$

Deci p aparține lui A deci el este minimumul.

1.3.3. Element maximum

Să considerăm o submulțime nevidă și *majorată* A a lui N. Mulțimea majoranților săi este nevidă, prin definiția adjectivului „majorat". Ea admite deci un element minimum m:

$$(n \in A) \Longrightarrow (n \leqslant m).$$

Dacă m nu aparține lui A, putem scrie:

$$(n \in A) \Longrightarrow (n < m) \Longrightarrow (n \leqslant m - 1).$$

(Cazul $m = 0$ este banal: A este formată atunci dintr-un singur element 0.) Acesta arată că $(m - 1)$ este încă un majorant al lui A; cum m este cel mai mic dintre majoranți, avem:

$$m \leqslant m - 1,$$

ceea ce este fals. Prin urmare, m aparține lui A, deci este elementul maximum (în mod necesar unic).

TEOREMĂ 11 / **Orice submulțime nevidă și majorată a lui N admite un element maximum unic.**

EXERCIȚIU. *Să se demonstreze prin inducție teorema 11.*
Fie α (n) următoarea proprietate:
„A (nevidă) admite un maximum dacă ea este majorată de n".
$\alpha(0)$ este adevărată, căci A nu conține atunci decît pe 0.
Dacă α (n) este adevărată, și dacă A nu este vidă și este majorată de $(n + 1)$, atunci:
a) sau n majorează pe A, care admite deci un maximum;
b) sau n nu majorează pe A, ceea ce dovedește că $(n + 1)$ este element al lui A: este maximumul căutat.

Există submulțimi nevide ale lui N care nu au element maximum. Este chiar cazul lui N, căci:

$$(m = max\ \mathrm{N}) \Longrightarrow (m \geqslant m + 1),$$

ceea ce este absurd. În consecință:

TEOREMĂ 12 / **N nu admite element maximum.**

Același lucru se întîmplă cu mulțimi ($p\mathbf{N}$), formate din *multiplii* unui întreg p, în afara cazului cînd $p = 0$. Într-adevăr:

$$(p\mathbf{N}) = \{n;\ \exists m,\ n = pm\},$$
$$(p = 0) \Longrightarrow (p\mathbf{N} = \{0\}).$$

Dacă p este diferit de zero, vom arăta că nici un întreg q diferit de zero nu poate fi un majorant al lui ($p\mathbf{N}$); într-adevăr:

$$(q + 1)\,p = q + p + q(p - 1) \geqslant q + p \geqslant q + 1 > q.$$

Deducem *teorema lui Arhimede:*

TEOREMĂ 13 / **Pentru orice întreg q și orice întreg p nenul, există un întreg n astfel încît:**

$$\boxed{np > b}$$

1.3.4. Axiomatica ordinală a lui N

Să considerăm o mulțime E, înzestrată cu o relație de ordine ($\geqslant$), pentru care sînt adevărate axiomele:
A4 E nu admite element maximum.
A5 Orice submulțime nevidă a lui E admite un element minimum.
A6 Orice submulțime nevidă și majorată a lui E admite un element maximum.
Aceste axiome sînt adevărate pentru N (a se vedea teoremele 12, 10 și 11).
Fie 0 elementul minimum al lui E, care este bine definit.
Ordinea în E este totală, deoarece, în orice mulțime $\{n, m\}$, există un minimum.
a) Fie n un element al lui E, și fie:

$$A = \{m;\ m \leqslant n\}.$$

E neavînd maximum, există în E un element strict superior lui n. Acest element este un majorant strict al lui A; deci mulțimea B a majoranților stricți ai lui A nu este vidă.
Să notăm $\mathrm{f}(n) = n'$ minimumul lui B.
Nu putem avea $\mathrm{f}(n) = 0$, căci:

$$0 \leqslant n < n'.$$

b) Să examinăm egalitatea:

$$\mathrm{f}(n) = \mathrm{f}(m).$$

Dacă n este diferit de m, să scriem de exemplu: $n < m$; de unde:

$$(p \in A) \Longrightarrow (p \leqslant n < m) \Longrightarrow (p < m),$$

adică: $(m \in B)$, deci $\mathrm{f}(n) \leqslant m$ sau în sfîrșit: $\mathrm{f}(m) \leqslant m$, ceea ce este contradictoriu; rezultă că f este injectivă.

c) Fie în sfîrşit M o submulţime a lui E care-l conţine pe 0 şi astfel încît:

$$(n \in M) \Longrightarrow (\mathfrak{f}(n) \in M).$$

Dacă M nu se confundă cu E, *diferenţa*:

$$E - M = \{m;\ m \in E,\ m \notin M\}$$

admite un element minimum p, în mod necesar distinct de 0. Dacă notăm q maximumul submulţimii C nevide a minoranţilor stricţi ai lui p, se vede imediat că q aparţine lui M şi că:

$$\mathfrak{f}(q) = p;$$

aceasta fiind în contradicţie cu faptul că p nu aparţine lui M, diferenţa $(E-M)$ este vidă şi:

$$E = M.$$

E satisface deci axiomelor **A2**, **A1** şi **A3** ale lui Peano.

EXERCIŢIU. *Să se demonstreze egalitatea:* $p = \mathfrak{f}(q)$.

Ştim că:

$$(q \in C) \Longrightarrow (q < p) \Longrightarrow (\mathfrak{f}(q) \leqslant p).$$

Dacă am avea $\mathfrak{f}(q)$ diferit de p, s-ar putea deduce o inegalitate falsă:

$$(\mathfrak{f}(q) < p) \Longrightarrow (\mathfrak{f}(q) \in C \Longrightarrow (\mathfrak{f}(q) \leqslant q).$$

Am fi putut pune deci următoarea definiţie:

DEFINIŢIE 4 / **Se numeşte N orice mulţime ordonată care are următoarele proprietăţi:**
A4 N nu admite element maximum.
A5 Orice submulţime nevidă a lui N admite un element minimum.
A6 Orice submulţime nevidă şi majorată a lui N admite un element maximum.

Oricare ar fi definiţia aleasă-există şi altele combinînd, de exemplu, ordinea totală, existenţa unui minimum pentru N, definiţia lui f dată mai sus în *a)* şi axioma **A3** — este evident că ea nu permite să distingem pe N de o altă mulţime care i-ar fi izomorfă.[1] Dar se poate demonstra că două mulţimi N şi $\overline{\mathrm{N}}$ care satisfac amîndouă aceloraşi axiome (de exemplu acelea din definiţia 1), sînt în mod *necesar izomorfe*. N este deci bine definită în mod „esenţial" unic.
(Să observăm că axiomele structurii de grup nu au aceeaşi proprietate, căci două grupuri oarecare nu sînt obligatoriu izomorfe.)

---

[1] Aceasta este conform cu punctul actual de vedere în algebră.

Unicitatea lui **N.** Să notăm $\mathfrak{f}$ și $\overline{\mathfrak{f}}$ succesiunile în **N** și $\overline{\mathbf{N}}$, 0 și $\overline{0}$ elementele definite prin axioma **A2**, etc.
Vom defini o bijecție g de la **N** pe $\overline{\mathbf{N}}$ care să fie un izomorfism, deci astfel încît:

$$g(0) = \overline{0}, \quad g[\mathfrak{f}(n)] = \overline{\mathfrak{f}}[g(n)].$$

Fie M mulțimea elementelor n pentru care $g(n)$ este calculabil: axioma **A3** arată că $M = N$. Deci aplicația g există; ea este evident unică așa cum arată o inducție simplă în raport cu n. Fie $\overline{M}$ mulțimea imaginilor elementelor lui M prin g; axioma **A3** arată că $\overline{M} = \overline{N}$: g este surjectivă.
Să presupunem în sfîrșit că ecuația, definită prin:

$$g(x) = g(n),$$

nu admite decît o singură soluție, ceea ce este adevărat pentru $n = 0$:

$$(x \neq 0 \Longrightarrow x = \mathfrak{f}(m) \Longrightarrow g(x) \neq \overline{0}).$$

Ecuația $g(x) = g[\mathfrak{f}(n)]$ echivalează atunci cu:

$$g(x) = \overline{\mathfrak{f}}[g(n)].$$

Cum x este diferit de zero, putem pune: $x = \mathfrak{f}(y)$,

de unde:

$$\overline{\mathfrak{f}}[g(n)] = g(x) = g[\mathfrak{f}(y)] = \overline{\mathfrak{f}}[g(y)],$$

fie:

$$g(n) = g(y),$$

și în sfîrșit, prin ipoteza inducției:

$$y = n, \quad x = \mathfrak{f}(n).$$

Prin inducție în raport cu n, aplicația g este injectivă. Ea este deci bijectivă.

Vom da o a treia definiție posibilă, foarte diferită de celelalte, în paragraful nr. **1.5.**

1.3.5. Exponențiere

Mai există pe **N** o operație importantă, *exponențierea.*
O vom defini prin egalitățile:

$$\forall_{\mathbf{N}} n, \quad \forall_{\mathbf{N}} m : \quad m^0 = 1; \quad m^{n'} = m^n m \qquad (37)\ (38)$$

(Anumiți autori refuză egalitatea $0^0 = 1$ căci *ea poate conduce la erori, mai ales în analiză*; deci ne vom putea mărgini la valori m nenule în cele ce urmează, sau să începem cu $m^1 = m$.)

1. Exponenţierea este bine definită pe N, şi în mod unic. Ea are două proprietăţi fundamentale.
Prima are două aspecte:

$$\boxed{m^n m^p = m^{n+p}; \quad (m^n)^p = m^{np}} \qquad (39)\ (40)$$

Demonstraţiile se fac prin inducţie în raport cu p.

Pentru $p = 0$, avem: $m^n m^0 = m^n = m^{n+0}$; $(m^n)^0 = 1 = m^0 = m^{n0}$.
Dacă este adevărată pentru p, atunci:
a) $m^n m^{p+1} = m^n m^p m = m^{n+p} m = m^{n+p+1}$;
b) $(m^n)^{p+1} = (m^n)^p (m^n) = m^{np} m^n = m^{np+n} = m^{n(p+1)}$, prin aplicarea egalităţii (39).

Această lege nu este nici comutativă, nici asociativă, aşa cum arată următoarele exemple:

$$(3^2 = 9) \neq (8 = 2^3); \quad (2^{(3^2)} = 512) \neq (64 = (2^3)^2).$$

(Ca exerciţiu, se va putea justifica, de exemplu, calculul lui $2^{(3^2)}$ plecînd de la definiţiile date aici.)
2, A doua proprietate fundamentală este următoarea:

$$\boxed{m^n p^n = (mp)^n} \qquad (41)$$

Demonstraţia se face prin inducţie în raport cu n.

Pentru $n = 0$, avem:

$$m^0 p^0 = 1 \times 1 = 1 = (mp)^0.$$

Dacă este adevărată pentru n, atunci:

$$m^{n+1} p^{n+1} = m^n m p^n p = (m^n p^n)\, mp = (mp)^n mp = (mp)^{n+1}.$$

---

3. Să mai semnalăm *inegalitatea lui Bernoulli:*

$$\boxed{(m \neq 0) \Longrightarrow [m^n \geqslant 1 + n(m-1)]} \qquad (42)$$

EXERCIȚIU

Să se demonstreze inegalitatea lui Bernoulli.
Este adevărată pentru $n = 0$, deoarece:

$$m^0 = 1 \text{ și } 1 = 1 + 0(m - 1),$$

deci:

$$m^0 \geqslant 1 + 0(m - 1).$$

Să o presupunem verificată pentru n; avem:

$$m^n \geqslant 1 + n(m - 1).$$

Prin înmulțire cu m, deducem:

$$m^{n+1} \geqslant [1 + n(m - 1)][1 + (m - 1)].$$

Avem:

$$[1 + n(m - 1)][1 + (m - 1)] = 1 + (n + 1)(m - 1) + n(m - 1)^2,$$

deci:

$$[1 + n(m - 1)][1 + m - 1] \geqslant 1 + (n + 1)(m - 1).$$

Prin tranzitivitatea relației de ordine, rezultă:

$$m^{n+1} \geqslant 1 + (n + 1)(m - 1).$$

Relația este deci demonstrată prin inducție în raport cu n.
Această inegalitate, banală pentru $n = 0$, rezultă de asemenea din formula binomului:

$$m^n = [1 + (m - 1)]^n = 1 + n(m - 1) + p,$$

unde p este un număr întreg (de exemplu dacă $n = 2$, avem: $p = C_n^2(m - 1)^2$).
Se va arăta ca exercițiu că inegalitatea lui Bernoulli nu este strictă decît pentru:

$$n \geqslant 2 \text{ și } m \geqslant 2.$$

În celelalte cazuri, $m = 1$ sau $n \leqslant 1$, este o egalitate.

Inegalitatea lui Bernoulli ne permite să demonstrăm o implicație analoagă teoremei lui Arhimede:

$$\boxed{(m > 1) \Longrightarrow (\forall_{\mathbb{N}} p,\ \exists n,\ m^n > p)} \tag{43}$$

EXERCIȚIU

Să se demonstreze implicația (43).
1. *Demonstrație directă.*
Să luăm $n = p$; deoarece $m^n = m^p$, și după inegalitatea lui Bernoulli:

$$m^p \geqslant 1 + p(m - 1);$$

dar, deoarece $m > 1$:

$$1 + p(m - 1) = 1 + p + p(m - 2),$$

deci:

$$1 + p(m - 1) \geqslant 1 + p > p.$$

Rezultă:

$$m^p > p.$$

2. Demonstrarea prin inducție în raport cu p a lui $m^p > p$ $(m > 1)$.
Proprietatea este adevărată pentru $p = 0$: $1 > 0$.
Dacă este adevărată pentru p, se poate scrie:

$$(p = 0) \Longrightarrow (m^{p+1} > p + 1) \text{ deoarece } m > 1;$$

$$(p \neq 0) \Longrightarrow (m^p m > pm).$$

Cum:

$$pm = p + 1 + [(m - 1)p - 1],$$

avem:

$$pm \geqslant p + 1,$$

deci:

$$(p \neq 0) \Longrightarrow m^{p+1} > p + 1.$$

---

4. Următoarele exerciții studiază inegalitățile între exponențiale.

EXERCIȚII

I. *Se presupune: $m > n$. Să se compare m^p și n^p.*
Pentru $p = 0$, are loc egalitatea.
Dacă nu, se poate scrie:

$$m^p > n^p,$$

prin inducție restrînsă plecînd de la 1.
Într-adevăr, $m > n$ se scrie:

$$m^1 > n^1;$$

inegalitatea $m^p > n^p$ implică $(m \neq 0)$ și:

$$m^p m > n^p m \geqslant n^p n,$$

deci:

$$m^{p+1} > n^{p+1}.$$

II. *Se presupune: $m > n$. Să se compare p^m și p^n.*
Dacă $p = 0$ și n diferit de 0, are loc egalitatea.
Dacă $p = n = 0$, atunci:

$$p^m = 0^m = 0 \text{ și } p^n = 0^0 = 1,$$

deci

$$p^n > p^m.$$

(Egalitatea $0^0 = 1$ nu este adesea acceptată pentru a evita relațiile ciudate de forma celor de mai sus.)

Fie: $p > 0$; nici o putere a lui p nu este atunci nulă ($p^0 = 1$; $p^{r+1} = p^r p$, mai mare decît 0 prin inducție în raport cu r).
Dacă $p = 1$ are loc egalitatea:

$$p^m = 1 = p^n.$$

Dacă: $p > 1$, numai p^0 este egal cu 1, căci:

$$(s \geqslant 1) \Longrightarrow (s = r + 1) \Longrightarrow (p^r p \geqslant p > 1).$$

Are loc atunci inegalitatea, căci:

$$(m = n + q,\ q > 0) \Longrightarrow (p^n p^q > p^n) \Longrightarrow p^m > p^n.$$

În concluzie:

$$(p = 0 = n) \Longrightarrow (p^m < p^n),$$
$$(p = 0 \neq n) \Longrightarrow (p^m = p^n),$$
$$(p = 1) \Longrightarrow (p^m = p^n),$$
$$(p > 1) \Longrightarrow (p^m > p^n).$$

În rezumat:

TEOREMA 14 / **Exponențierea între întregi este o operație internă bine definită pe N prin egalitățile:**

$$m^0 = 1;\quad m^{n'} = m^n m$$

$$m^n m^p = m^{n+p};\quad (m^n)^p = m^{np}$$
$$m^n p^n = (mp)^n$$

EXERCIȚII

1.30. Să se demonstreze că un element minimum este în mod necesar unic. Același exercițiu pentru un element maximum.
1.31. A și B fiind două submulțimi nevide ale lui N, să se compare:

$$\min A,\ \min B,\ \min (A \cup B),\ \min (A \cap B) \text{ (dacă există)}.$$

1.32. Același exercițiu cu maximumurile a două submulțimi nevide majorate ale lui N.
1.33. Se consideră o mulțime E care are cel puțin două elemente și mulțimea F (înzestrată cu relația de incluziune a părților sale nevide). Să se demonstreze că F este ordonată. Admite ea un element minimum? Să se găsească elementele lui F care nu sînt strict superioare niciunui alt element al lui F (se spune că aceste părți sînt părți minimale pentru incluziune).
1.34. Același exercițiu cu:

$$F' = \mathcal{P}(E) = F \cup \{\varnothing\}.$$

1.35. A și B fiind două submulțimi nevide ale lui N, notăm $(A + B)$ mulțimea întregilor n astfel încît să existe a în A și b în B cu:

$$n = a + b,$$
$$(A + B = \{n;\ \exists a \in A,\ \exists b \in B,\ n = a + b\}).$$

Să se compare:

$$\min (A + B) \text{ și } (\min A + \min B).$$

1.36. Același exercițiu cu maximumurile a două submulțimi nevide majorate ale lui **N**.
1.37. Același exercițiu cu:

$$AB = \{n;\ \exists a \in A,\ \exists b \in B,\ n = ab\},$$

comparînd:

$$\min (AB) \text{ și } (\min A)\ (\min B),$$

apoi:

$$\max (AB) \text{ și } (\max A)\ (\max B).$$

1.38. Să se rezolve, în **N**, inecuația definită prin:

$$5^x < 3\,127.$$

1.39. Să se rezolve, în **N**, inecuația definită prin:

$$a^{x-1} \leqslant x.$$

(Se va discuta după valorile lui a.)

1.4. ȘIRURI NUMERICE

1.4.1. Intervale ale lui N

Să definim noțiunea de interval pentru o mulțime ordonată E (această noțiune a fost deja folosită în clasa I în cazul particular al lui **R**):

DEFINIȚIE 4 / **O submulțime I a unei mulțimi ordonate E este un interval al lui E dacă satisface implicația:**

$$(x \in I \text{ și } y \in I \text{ și } x \leqslant z \leqslant y) \Longrightarrow (z \in I)$$

Cunoaștem anumite intervale ale lui **N**:
a) mulțimea vidă este un interval.
b) **N** este un interval.
c) $[m, n] = \{p;\ m \leqslant p \leqslant n\}$ este un interval mărginit.
d) $[m, +\infty[= \{p;\ m \leqslant p\}$ este un *interval infinit.*
(Se poate scrie, de exemplu: $\mathbf{N} = [0, +\infty[$.)
Să arătăm că aceste cazuri acoperă gama tuturor intervalelor lui **N**.
Orice interval nevid admite un minimum:

$$a = \min I \geqslant 0.$$

Dacă este majorat, admite un maximum:

$$b = \max I \geqslant a,$$

și I se confundă cu intervalul $[a, b]$. Dacă nu, aceasta înseamnă că:

$$\forall_{\mathbf{N}} n,\ \exists m \in I,\ m > n,$$

ceea ce implică că:

$$(n \geqslant a) \Longrightarrow (n \in I).$$

I se confundă atunci cu $[a, +\infty[$.

TEOREMĂ 15 / **Nu există decît trei feluri de intervale ale lui N: intervalul vid, intervalele mărginite $[a, b]$ și intervalele infinite $[a, +\infty[$.**

Observație. — Notația $[m, n]$ nu se folosește, în general, decît pentru $(m \leqslant n)$; dar poate fi comod să punem a priori:

$$[m, n] = [n, m],$$

ceea ce evită distincția între extremitățile m și n.

Intervalele mărginite (se mai spune: *finite*) nevide au o structură simplă: există un întreg p astfel încît $[m, n]$ să fie izomorf cu $[1, p]$. Într-adevăr:

$$(n \geqslant m) \Longrightarrow (n = m + r),$$

și aplicația:

$$\mathfrak{f} = [x \longmapsto x - m + 1]$$

este evident o bijecție crescătoare între $[m, n]$ și $[1, r + 1]$.

Intervalele infinite, ca $[n, +\infty[$, sînt izomorfe cu N prin aplicația

$$\mathfrak{f} = [x \longmapsto x - n].$$

Observație. — Am văzut în clasa I (Algebră, nr. **3.1.1**) că o mulțime este finită dacă și numai dacă există o bijecție între această mulțime și mulțimea vidă sau o mulțime de tipul $[1, p]$; se poate deci defini o mulțime finită ca o mulțime în bijecție cu un interval mărginit al lui N.
Proprietățile mulțimilor finite se pot deduce din axiomele lui Peano.
Reciproc, structura lui N se poate defini plecînd de la proprietățile mulțimilor finite (a se vedea paragraful nr. **1.5**).

EXERCIȚIU

Să se demonstreze, prin inducție, că numărul p definit mai sus este unic (se numește **cardinalul** *lui* I).
Dacă acest rezultat ar fi fals, ar exista doi întregi p și q cu, spre exemplu,: $q < p$, astfel încît să existe o bijecție φ între $[1, q]$ și $[1, p]$.
Aceasta este imposibil pentru $p = 1$. Să admitem că o astfel de imposibilitate este demonstrată pentru p, și să o dovedim pentru $(p + 1)$.
Dacă bijecția φ între $[1, q]$ și $[1, p + 1]$ este astfel încît:
$\varphi(q) = p + 1$, se poate deduce o bijecție între $[1, q - 1]$ și $[1, p]$ ceea ce este imposibil (cazul $q = 0$ este imediat).

Există deci doi întregi u şi v astfel încît:

$$\varphi(u) = p + 1, \varphi(q) = v.$$

Să construim o nouă bijecţie definită prin:

$$\psi(x) = \varphi(x) \text{ pentru: } x \neq u, x \neq q,$$
$$\psi(u) = v, \psi(q) = p + 1.$$

Sîntem readuşi la cazul precedent şi teorema este deci demonstrată prin absurd.

1.4.2. Şiruri

Aplicaţiile de la **N** într-o mulţime X au fost studiate de mult timp, deoarece ele constau doar din a lua elemente ale lui X într-o anumită ordine. Ele au primit un nume particular:

DEFINIŢIE 5 / **Un şir este o aplicaţie de la N (sau de la un interval infinit al lui N) într-o mulţime dată.**
Un şir finit este o aplicaţie de la un interval finit al lui N într-o mulţime dată.

După natura mulţimii valorilor şirului (ex.: **N**, **R**, **C**) vom vorbi de şiruri de numere întregi, reale sau complexe.
Notaţia clasică a aplicaţiilor:

$$\mathbf{u} = [n \longmapsto \mathbf{u}(n)]$$

este puţin folosită; o notaţie veche, desemnînd şirul **u** prin simbolul (u_n), unde:

$$u_n = \mathbf{u}(n) \quad (n\text{: } \textit{indicele} \text{ lui } u_n),$$

este foarte comodă şi încă în uz; ea provoacă totuşi o confuzie regretabilă între şirul **u** şi valoarea pe care o ia pentru un întreg dat.

Observaţie. — Nu trebuie să se confunde noţiunea de şir u_n şi cea de mulţime a valorilor şirului: **u** nefiind neapărat injectivă, pot exista doi indici diferiţi pentru care u_n să ia aceeaşi valoare. Se poate chiar ca mulţimea acestor valori să fie finită, ca în cazul şirului:

$$\mathbf{u} = [n \longmapsto (-1)^n].$$

EXERCIŢII

I. *Să se demonstreze că mulţimea şirurilor în un grup G poate primi structura de grup.*
Ne vom plasa în cazul cel mai frecvent în care şirurile sînt definite pe tot **N**. Grupul G va fi presupus aditiv. Vom defini suma a două şiruri prin formula:

$$\mathbf{u} + \mathbf{v} = [n \longmapsto u_n + v_n].$$

Această definiție este naturală; bineînțeles este cea a sumei a două aplicații, pe care am văzut-o deja într-un caz particular (clasa I, Algebră nr. 6.1.7).
Mulțimea S a șirurilor în G este atunci ea însăși un grup. Într-adevăr adunarea este *asociativă* deoarece:

$$\mathbf{u} + (\mathbf{v} + \mathbf{w}) = [n \longmapsto u_n + (v_n + w_n)],$$
$$(\mathbf{u} + \mathbf{v}) + \mathbf{w} = [n \longmapsto (u_n + v_n) + w_n = u_n + (v_n + w_n)]$$

Elementul neutru este șirul constant care, oricărui n, îi asociază elementul neutru e al grupului G căci:

$$\mathbf{t} = [n \longmapsto e],$$
$$\mathbf{u} + \mathbf{t} = [n \longmapsto u_n + e = u_n],$$
$$\mathbf{t} + \mathbf{u} = [n \longmapsto e + u_n = u_n].$$

În sfîrșit, șirul *opus* șirului u este șirul $(-\mathbf{u})$ astfel încît:

$$-\mathbf{u} = [n \longmapsto -u_n],$$
$$\mathbf{u} + (-\mathbf{u}) = (-\mathbf{u}) + \mathbf{u} = [n \longmapsto e] = \mathbf{t}.$$

Dacă G este un corp K, mulțimea șirurilor în K poate fi înzestrată cu o înmulțire, prin egalitatea:

$$\mathbf{uv} = [n \longmapsto u_n v_n].$$

Totuși, această înmulțire nu conferă lui S o structură de corp, ci o structură de *inel*.
II. *Fie un șir (u_n) majorat de întregul A, cu valori în mulțimea* N. *Să se demonstreze că există un întreg L astfel încît să existe o infinitate de indici m cu:*

$$u_m = L \leqslant A,$$

și un număr finit de indici m cu:

$$u_m > L.$$

Să considerăm un întreg n și mulțimea E_n a întregilor u_m de indice m mai mare sau egal cu n:

$$E_n = \{x;\ \exists m \geqslant n,\ x = u_m\} \subset \mathbf{N}.$$

Această mulțime este nevidă și majorată. Ea admite deci un maximum x_n.
Incluziunea $E_{n+1} \subset E_n$ arată că:

$$x_{n+1} \leqslant x_n \leqslant A.$$

Mulțimea H a întregilor y mai mici sau egali cu toți x_n este nevidă ($0 \in H$) și majorată (de A). Fie L elementul său maximum:

$$L = \max H.$$

L este el însuși un x_n, căci dacă ar fi strict inferior tuturor x_n, $(L + 1)$ ar aparține lui H.
Fie p cel mai mic indice pentru care:

$$L = x_p.$$

Cum avem întotdeauna:

$$(n \geqslant p) \Longrightarrow (L \leqslant x_n \leqslant x_p),$$

deducem:

$$(n \geqslant p) \Longrightarrow (x_n = L).$$

L aparține deci tuturor mulțimilor E_n pentru n mai mare sau egal cu p, ceea ce demonstrează că există o infinitate de indici m cu:

$$u_m = L.$$

Dacă a este un întreg strict superior lui L, ecuația $u_m = a$ implică $(m < p)$, căci:

$$(m \geqslant p) \Longrightarrow (u_m \in E_p) \Longrightarrow (u_m \leqslant x_p = L),$$

ceea ce demonstrează proprietatea.

1.4.3. Notație cu indici

Notația u_n, folosită de obicei, este foarte comodă în anumite expresii algebrice unde figurează sume și produse pe un interval $[a, b]$ de întregi.
Vom nota astfel:

$$\boxed{S = \sum_{n=a}^{b} u_n, \quad P = \prod_{n=a}^{b} u_n}$$

elementele mulțimii X în care este definit șirul finit u astfel încît:

$$\boxed{\begin{aligned} S &= u_a + u_{a+1} + \ldots + u_{b-1} + u_b \\ P &= u_a \times u_{a+1} \times \ldots \times u_{b-1} \times u_b \end{aligned}}$$

(Se presupune că există pe X o adunare și o înmulțire asociativă. Se poate da o definiție precisă a lui S și P prin inducție în raport cu b). Se notează de asemenea:

$$\boxed{S = \sum_{n \in [a, b]} u_n; \quad P = \prod_{n \in [a, b]} u_n.}$$

EXERCIȚIU

X fiind chiar **N**, *să se compare întregii:*

$$h_m = 1 + \sum_{n=0}^{m} u_n, \quad k_m = \prod_{n=0}^{m} (1 + u_n).$$

Pentru $m = 0$, acești întregi sînt egali cu $(1 + u_0)$:

$$k_0 = h_0 = 1 + u_0 \text{ și } 1 + u_0 > 0.$$

Să presupunem că avem:

$$k_m \geqslant h_m > 0.$$

Atunci:

$$k_{m+1} = (1 + u_{m+1})\, k_m = k_m + u_{m+1}\, k_m;$$

avem:

$$k_m + u_{m+1} k_m \geqslant h_m + u_{m+1} k_m,$$

şi deoarece $k_m > 0$:

$$h_m + u_{m+1} k_m \geqslant h_m + u_{m+1};$$

cum:

$$h_m + u_{m+1} = h_{m+1},$$

rezultă:

$$k_{m+1} \geqslant h_{m+1}.$$

Relaţia este deci demonstrată prin inducţie în raport cu m. Egalitatea are loc:
a) sau, pentru că $m = 0$;
b) sau pentru toţi indicii strict inferiori lui m:

$$h_n = k_n,\ u_{n+1} k_n = u_{n+1};$$

c) sau încă, pentru că $u_n = 0$ pentru toţi indicii (în afară poate doar de un singur indice).

Dealtfel:

$$k_m - h_m \geqslant (u_0u_1 + u_0u_2 + \ldots + u_0u_m) + (u_1u_2 + \ldots + u_1u_m) + \ldots + (u_{m-1}u_m)$$

aşa cum se vede dezvoltînd produsul k_m.
Exemplu. $u_n = \lambda - 1$ pentru orice n; atunci:

$$k_{m-1} = \lambda^m;\ h_{m-1} = 1 + m(\lambda - 1),$$

deci:

$$\lambda^m \geqslant 1 + m(\lambda - 1) \text{ (conform nr. 1.3.5).}$$

Notaţia cu indici permite scrierea comodă a *aplicaţiei iterate* a unei aplicaţii f de la o mulţime la ea însăşi. Putem nota astfel:

$$\mathrm{f} = [x \longmapsto \mathrm{f}(x)],\quad (x \in E,\ \mathrm{f}(x) \in E),$$
$$\mathrm{f}_1 = \mathrm{f},\quad \mathrm{f}_{n+1} = [x \longmapsto \mathrm{f}(\mathrm{f}_n(x))],$$

adică:

$$\boxed{\mathrm{f}_1 = \mathrm{f},\quad \mathrm{f}_{n+1} = \mathrm{f} \circ \mathrm{f}_n = \mathrm{f}_n \circ \mathrm{f}}$$

EXERCIŢII

I. f *reprezentînd operaţia de succesiune în* N, *să se demonstreze relaţia:*

$$n = \mathrm{f}_n(0).$$

Este adevărată pentru $n = 1$ căci:

$$1 = 0' = \mathrm{f}(0) = \mathrm{f}_1(0).$$

Dacă este adevărată pentru n, atunci:

$$n + 1 = n' = \mathfrak{f}(n) = \mathfrak{f}(\mathfrak{f}_n(0)) = \mathfrak{f}_{n+1}(0).$$

Orice întreg este deci obținut prin aplicația $\mathfrak{f}$, plecînd de la 0 și printr-un număr finit de operații (conform nr. 1.1.1, Proprietatea 7).

II. *Dacă $\mathfrak{f}$ și $\mathfrak{g}$ comută (adică dacă $f \circ g = g \circ f$), să se demonstreze relația:*

$$(\mathfrak{f} \circ \mathfrak{g})_n = \mathfrak{f}_n \circ \mathfrak{g}_n.$$

Este adevărată pentru $n = 1$, căci:

$$(\mathfrak{f} \circ \mathfrak{g})_1 = \mathfrak{f} \circ \mathfrak{g} = \mathfrak{f}_1 \circ \mathfrak{g}_1.$$

Dacă este adevărată pentru n, este adevărată și pentru $(n + 1)$. Pentru demonstrație, trebuie să verificăm mai întîi (tot prin inducție) că $\mathfrak{g}$ comută cu $\mathfrak{f}_n$; atunci:

$$(\mathfrak{f} \circ \mathfrak{g})_{n+1} = (\mathfrak{f} \circ \mathfrak{g}) \circ (\mathfrak{f}_n \circ \mathfrak{g}_n)$$
$$= \mathfrak{f} \circ (\mathfrak{g} \circ \mathfrak{f}_n) \circ \mathfrak{g}_n = \mathfrak{f} \circ \mathfrak{f}_n \circ \mathfrak{g} \circ \mathfrak{g}_n$$
$$= \mathfrak{f}_{n+1} \circ \mathfrak{g}_{n+1}.$$

De exemplu, dacă $\mathfrak{f}$ are același sens ca în exercițiul I și dacă $\mathfrak{g}$ este definită prin:

$$\mathfrak{g} = [x \longmapsto p + x] \qquad (p \text{ constant}),$$

atunci:

$$\mathfrak{f} \circ \mathfrak{g} = \mathfrak{g} \circ \mathfrak{f} = [x \longmapsto (p + x) + 1 = p + (x + 1)]$$

(aceasta nu este decît una din relațiile de definiție ale adunării).

Deducem egalitatea:

$$(\mathfrak{f} \circ \mathfrak{g})_n = \mathfrak{f}_n \circ \mathfrak{g}_n,$$

sau încă:

$$(\mathfrak{f} \circ \mathfrak{g})_n = [x \longmapsto (np + x) + n].$$

Adesea se completează definiția de mai sus, punînd a priori, aplicația $\mathfrak{f}_0$ egală cu identitatea:

$$\boxed{\mathfrak{f}_0 = [x \longmapsto x]}$$

ceea ce verifică: $\mathfrak{f}_1 = \mathfrak{f} \circ \mathfrak{f}_0 = \mathfrak{f}_0 \circ \mathfrak{f}$.

EXERCIȚII

1.40. Reuniunea, intersecția, diferența a două intervale ale unei mulțimi ordonate sînt intervale?

1.41. Să se demonstreze că toate intervalele care conțin o submulțime finită a lui $\mathbf{N}$ admit ca submulțime comună un interval particular care va fi determinat.

1.42. Să se demonstreze că dacă o proprietate este adevărată pentru un întreg a și dacă din aceea că ea este adevărată pentru toți întregii n astfel încît:

$$a \leqslant n \leqslant m < b \qquad (b \text{ fixat}, a < b)$$

atunci ea este adevărată pentru $(m + 1)$, se poate deduce că ea este adevărată pentru toți întregii intervalului $[a, b]$.

1.43. Să se demonstreze că șirurile definite într-un corp K nu formează, în general, un corp (a se vedea exercițiul nr. 1.4.2).

1.5. MULȚIMI FINITE

1.5.1. Proprietățile mulțimilor finite

Nu vom da aici, fără demonstrație, decît lucruri făcute deja în clasa I (Algebră, capitolul 3).

1. O mulțime E este finită dacă, și numai dacă, există un interval $[1, n]$ al lui N astfel încît să existe o bijecție între această mulțime și acest interval. Întregul n este unic: este *cardinalul* lui E (mulțimea vidă este o mulțime finită, de cardinal 0). Imaginea unei mulțimi finite printr-o aplicație este o mulțime finită.

2. Reuniunea și intersecția a două mulțimi finite sînt mulțimi finite și avem:

$$\text{Card}E + \text{Card}F = \text{Card}(E \cup F) + \text{Card}(E \cap F).$$

Produsul cartezian este de asemenea o mulțime finită:

$$\text{Card}\,(E \times F) = \text{Card}\,E \times \text{Card}\,F,$$

la fel și mulțimea $\mathcal{F}(E, F)$ a aplicațiilor de la E la F:

$$\text{Card}\,\mathcal{F}(E, F) = [\text{Card}\,F]^{\text{Card}\,E}.$$

Există o bijecție între E și F dacă și numai dacă:

$$\text{Card}\,E = \text{Card}\,F.$$

Numărul bijecțiilor este atunci:

$$(\text{Card}\,E)!.$$

Există o injecție între E și F dacă și numai dacă:

$$\text{Card}\,E \leqslant \text{Card}\,F.$$

Numărul injecțiilor este atunci:

$$A_m^n = m(m-1)\ldots(m-n+1),$$

cu:

$$m = \text{Card}\,F, \qquad n = \text{Card}\,E.$$

Există o surjecție de la E pe F dacă și numai dacă:

$$\text{Card}\,E \geqslant \text{Card}\,F.$$

3. Submulțimile lui E formează o mulțime finită de cardinal:

$$\text{Card } \mathcal{P}(E) = 2^{\text{Card } E}.$$

Aceste submulțimi sînt finite; în plus:

$$(F \subset E) \Longrightarrow (\text{Card } F \leqslant \text{Card } E),$$
$$(F \neq E \text{ și } F \subset E) \Longrightarrow (\text{Card } F < \text{Card } E).$$

O aplicație de la E la ea însăși este o bijecție deîndată ce ea este injectivă sau surjectivă; mulțimile finite sînt caracterizate prin această proprietate căci există întotdeauna, într-o mulțime infinită, o injecție care nu e surjecție și o surjecție care nu e injecție (această teoremă are o demonstrație delicată). Dacă $m = \text{Card} E$ și dacă $n \leqslant m$, există:

$$C_m^n = \frac{m(m-1)\dots(m-n+1)}{n!} = \frac{1}{n!} A_m^n$$

submulțimi ale lui E avînd pe n drept cardinal.
Notăm adesea:

$$C_m^n = \binom{m}{n}.$$

1.5.2. Definiție axiomatică

Fără a cunoaște mulțimea **N**, se poate totuși considera noțiunea de mulțime finită care nu depinde de întregii naturali, deoarece putem pleca de la următoarea proprietate:
O mulțime E este finită dacă, și numai dacă, nu există injecții nesurjective de la E la E.
Această definiție este totuși foarte greu de folosit; am putea s-o verificăm încercînd să demonstrăm direct, plecînd de la această definiție, următoarea teoremă foarte simplă: produsul a două mulțimi finite este finit.
O definiție mai bună este folosită de matematicieni în cadrul teoriei cardinalilor unei mulțimi oarecare, dar ea este prea delicată pentru a o putea expune aici.
La un nivel elementar, am putea totuși construi o teorie a mulțimilor finite, inteligibilă, cu condiția să admitem următoarele enunțuri:
a) relația: $(E < F) \Leftrightarrow$ (există o injecție de la E la F) este o relație de ordine totală în clasa tuturor mulțimilor;
b) pentru orice surjecție $\mathfrak{f}$ de la E pe F, există cel puțin o injecție $\mathfrak{g}$ de la F la E astfel încît:

$$[y = \mathfrak{g}(x)] \Longrightarrow [x = \mathfrak{f}(y)]$$

(printre toate rădăcinile ecuației în t:

$$\mathfrak{f}(t) = x,$$

se poate alege una, particulară, pe care o notăm y);

c) o mulțime E este finită dacă și numai dacă o putem înzestra cu o relație de ordine pentru care orice submulțime nevidă admite un maximum și un minimum.
Oricărei mulțimi finite îi atașăm un obiect (de exemplu o mulțime în bijecție cu ea) numit *cardinalul* acestei mulțimi.
Cardinalul este astfel încît două mulțimi legate printr-o bijecție au același cardinal, și reciproc.
Vom admite că aceasta este posibil și că mulțimea cardinalilor mulțimilor finite este și ea o mulțime (care nu este alta decît **N**).
Această mulțime **N** este și ea ordonată prin comparare cu relația „$\prec$".
Această ordine este totală.
Putem demonstra atunci anumite teoreme din paragraful 1.5, de exemplu (E fiind mereu presupusă finită):
1. $(F \subset E) \Rightarrow (F$ finită și Card$F \leqslant$ Card $E)$.
2. Pentru orice F, $E \cap F$ este finită și:

$$\text{Card } (E \cap F) \leqslant \text{Card } E.$$

3. $(F \prec E) \Leftrightarrow (F$ finită și Card $F \leqslant$ Card $E)$.
4. Dacă φ este o aplicație de la E la X, atunci $\varphi(E)$ este finită și de cardinal:

$$\text{Card } \varphi\,(E) \leqslant \text{Card} E.$$

5. Dacă E și F sînt finite, $E \cup F$, $E \cap F$ și $E \times F$ sînt finite.
6. $(m \leqslant n) \Rightarrow ([0,\ m] \subset [0,\ n])$.
7. $[0,\ n]$ este finită (demonstrația este delicată).
8. *Orice submulțime nevidă a lui* **N** *admite un element minimum.*
9. *Orice submulțime nevidă și majorată a lui* **N** *este finită și admite un element maximum.*
10. Orice submulțime **M** a lui **N** care-l conține pe 0, astfel încît:

$$(n \in M \text{ și } n \text{ admite un succesor}) \Longrightarrow (n' \in M),$$

se confundă cu **N** (n' este cel mai mic element, dacă există, strict mai mare ca n).
11. Orice mulțime a părților unei mulțimi finite este finită (demonstrația este delicată).
12. Există o injecție — dar nici o surjecție — a unei mulțimi E în mulțimea $\mathcal{P}(E)$ a părților sale.
13. **N** *nu este majorată.*
14. Mulțimea aplicațiilor unei mulțimi finite într-o mulțime finită este o mulțime finită.
15. Orice element al lui **N** are un succesor.
16. **N** satisface axioma inducției.
17. O mulțime este finită dacă, și numai dacă, este în bijecție cu o submulțime majorată a lui **N**.
18. **N** este infinită.
19. Orice mulțime infinită conține o submulțime în bijecție cu **N**.
20. O mulțime este finită dacă și numai dacă orice injecție internă este o bijecție.
21. O mulțime este finită dacă și numai dacă orice surjecție internă este o bijecție.

22. O mulțime este finită dacă și numai dacă există o injecție — dar nici o surjecție — de la E la mulțimea obținută adăugînd un nou element lui E.
23. n este cardinalul mulțimii $[1, n]$.

Observație. — Proprietățile 8, 9 și 13 antrenează, așa cum știm, axiomele lui Peano (a se vedea nr. 1.3.4). Adoptînd atunci definițiile adunării, înmulțirii și exponențierii, putem demonstra foarte ușor implicația:

$$(\text{Card } E = n \text{ și Card } F = m)$$
$$\Longrightarrow (\text{Card } E \times F = nm \text{ și Card } \mathcal{F}(E, F) = m^n).$$

În plus, dacă E și F au intersecția vidă:

$$n + m = \text{Card } (E \cup F) \qquad (E \cap F = \varnothing).$$

Multe din proprietățile acestor operații se demonstrează foarte ușor plecînd de la aceste relații cu mulțimi. Demonstrațiile sînt mai naturale decît cele prin inducție.

EXERCIȚII

1.44. Se consideră un șir (u_n) de numere întregi astfel încît, pentru toate perechile (n, m):

$$u_n + u_m - 1 \leqslant u_{n+m} \leqslant u_n + u_m + 1, \; u_1 = 1$$

Să se demonstreze dubla inegalitate:

$$1 \leqslant u_n < 2n \quad (n \geqslant 1).$$

1.45. Se consideră un șir (u_n) de numere întregi. Să se compare întregii:

$$a = \left(\sum_{n=0}^{m} u_n\right)^2, \; b = \sum_{n=0}^{m} (u_n)^2.$$

1.46. Se consideră două șiruri (u_n) și (v_n) de numere întregi. Să se compare întregii:

$$a = \left(\sum_{n=0}^{m} u_n\right) \left(\sum_{p=0}^{m} v_p\right), \; b = \sum_{n=0}^{m} u_n v_n.$$

1.47. $\mathfrak{f}$ fiind o aplicație a unei mulțimi în ea însăși, punem:

$$\mathfrak{f}_0 = [x \longmapsto x], \; \mathfrak{f}_{n+1} = \mathfrak{f} \circ \mathfrak{f}_n.$$

Să se demonstreze egalitatea:

$$\mathfrak{f}_n \circ \mathfrak{f}_m = \mathfrak{f}_{n+m}.$$

1.48. Aceeași problemă cu egalitatea:

$$(\mathfrak{f}_n)_m = \mathfrak{f}_{nm}.$$

1.49. Să se calculeze cardinalul intervalului:

$$[m, m + n].$$

Aceeași problemă pentru intervalul:

$$[m, m + n - 1].$$

1.50. Să se demonstreze: cardinalul unei submulțimi a unei mulțimi finite este mai mic sau egal cu cardinalul acestei mulțimi.
1.51. Să se demonstreze că, dacă o mulțime are același cardinal cu o mulțime finită a cărei parte este, aceste două mulțimi sînt egale.
1.52. Să se demonstreze: cardinalul reuniunii a două mulțimi finite este mai mic sau egal cu suma cardinalilor lor. În ce caz are loc egalitatea?
1.53. Se consideră un șir de mulțimi E_n astfel încît E_0 să fie finită și, pentru orice n:

$$E_{n+1} \subset E_n.$$

Să se demonstreze că există un întreg m astfel încît:

$$(n \geqslant m) \Longrightarrow (E_n = E_m).$$

(Să se studieze al doilea exercițiu rezolvat din paragraful nr. **1.4.2** și exercițiul nr. 1.50.)
1.54. Să se demonstreze teoremele enunțate la numerele 1, 2, 3, 4 din paragraful nr. **1.5.2.**

PROBLEME

1.55. 1° Să se demonstreze că există un șir unic de numere reale definit prin relațiile:

$$u_0 = 2, \; u_n = \frac{1}{3 + u_{n-1}} \; (n \geqslant 1).$$

2° Să se demonstreze că, dacă punem:

$$l = \frac{-3 + \sqrt{13}}{2},$$

se pot scrie relațiile:

$$u_{2n} > l, \; u_{2n+2} < u_{2n}, \; u_{2n+1} < l, \; u_{2n+1} > u_{2n-1}.$$

1.56. 1° Să se demonstreze că există un șir unic de numere întregi strict pozitive definit prin relațiile:

$$0 < u_0 = a, \; u_{n+1} = \frac{u_n}{2} \text{ dacă } u_n \text{ este par,}$$

$$u_{n+1} = u_n + 1 \text{ dacă } u_n \text{ este impar.}$$

2° Să se demonstreze că există o infinitate de indici n astfel încît $u_n = 1$.
1.57. 1° Începînd de la ce valoare a lui n se poate scrie inegalitatea:

$$\frac{1}{n^2} < \frac{1}{n^2} - \frac{1}{(n+1)^2} \; ?$$

2° Să se deducă inegalitatea:

$$1 + \frac{1}{2^3} + \frac{1}{3^3} + \ldots + \frac{1}{n^3} < \frac{5}{4},$$

1.58. Să se studieze următorul raționament datorat logicianului și matematicianului *Alfred Tarski:*

„Să presupunem că, pentru orice mulțime E_n de cardinal n, am demonstrat implicația:

$$(p \in E_n \text{ și } q \in E_n) \Longrightarrow (p = q).$$

Această implicație este adevărată pentru $n = 1$. Dacă este adevărată pentru n, să numerotăm elementele unei mulțimi E_{n+1}:

$$E_{n+1} = \{x_1, x_2, \ldots, x_n, x_{n+1}\}.$$

Mulțimile:

$$E_n = \{x_1, x_2, \ldots, x_n\}, \quad E'_n = \{x_2, x_3, \ldots, x_{n+1}\}$$

sînt fiecare de cardinal n. În consecință:

$$x_1 = x_2 = \ldots = x_n,$$

$$x_2 = x_3 = \ldots = x_{n+1},$$

ceea ce demonstrează teorema prin inducție în raport cu n."
Să se găsească greșeala (făcută cu bună știință) în acest raționament.

1.59. Înzestrăm mulțimea $\mathbf{N}$ cu operația, notată cu ajutorul semnului „$*$", definită prin implicațiile:

$$(n \text{ par și } m \text{ par}) \Longrightarrow (n * m = n + m),$$
$$(n \text{ impar și } m \text{ impar}) \Longrightarrow (n * m = n + m + 1),$$
$$(n \text{ par și } m \text{ impar}) \Longrightarrow (n * m = m * n = p),$$

cu:

$$(n > m) \Longrightarrow (p = n - m - 1),$$
$$(m > n) \Longrightarrow (p = m - n).$$

1° Să se demonstreze că $\mathbf{N}$ primește astfel structura de grup comutativ.
2° Să se rezolve ecuația pe $\mathbf{N}$ definită prin:

$$x * (x + 1) = n.$$

1.60. 1° Să se studieze eventuala existență a aplicațiilor $\mathfrak{f}$ de la $\mathbf{N}$ la $\mathbf{N}$ astfel încît; pentru toți întregii n și m:

$$\mathfrak{f}(n + m) = \mathfrak{f}(n) + \mathfrak{f}(m).$$

2° Aceeași problemă cu:

$$\mathfrak{f}(nm) = \mathfrak{f}(n)\mathfrak{f}(m).$$

1.61. Se definește *scăderea*, notată cu ajutorul semnului „$-$", ca o aplicație de la partea $\mathbf{N} \times \mathbf{N}$ definită prin $(n \leqslant m)$ la $\mathbf{N}$, astfel încît:

$$m - n = p \Longleftrightarrow m = n + p.$$

1° Să se demonstreze echivalențele:

$$(m - n = p) \Longleftrightarrow ([m + q] - [n + q] = p)$$
$$\Longleftrightarrow ([m - q] - [n - q] = p) \text{ (pentru } q \leqslant n);$$
$$(m < n) \Longleftrightarrow (m - p < n - p) \text{ (pentru } p \leqslant m);$$
$$(m = n) \Longleftrightarrow (m - p = n - p) \text{ (idem);}$$
$$(m \leqslant n) \Longleftrightarrow (m - p \leqslant n - p) \text{ (idem).}$$

2° Să se demonstreze egalitatea:

$$p(m - n) = pm - pn.$$

1.62. Se consideră doi întregi a și b astfel încît:

$$a^b = b^a,\ a = nb,\ n > 1,\ b \geqslant 3\ (n \in \mathbf{N}).$$

1° Să se demonstreze inegalitatea:

$$3^{n-1} > n.$$

2° Să se demonstreze echivalența:

$$(x^b = y^b) \Longleftrightarrow (x = y).$$

3° Să se demonstreze că a și b nu există.

1.63. 1° Să se determine în $\mathbf{N}$ toate perechile de întregi (x, y) definiți prin:

$$x^y + y^x \leqslant 1\,000.$$

2° Aceeași problemă cu:

$$x^x + y^y \leqslant 1\,000.$$

1.64. Să se determine mulțimile ordonate E care satisfac două axiome luate din axiomele *A4*, *A5*, *A6* (nr. 1.3.4), dar nu și pe a treia. (Se vor putea considera mulțimi finite, sau mulțimea $\mathbf{Z}$, sau mulțimea numerelor reale obținute reunind pe $\mathbf{N}$ cu mulțimea numerelor de forma $\left(-\frac{1}{n}\right)$.

1.65. Se definește un șir (u_n) de numere întregi prin următoarele condiții:
$u_n = 0$ dacă nu există nici un întreg m astfel încît $n = m^2$;
$u_n = 1$ în cazul contrar.

1° Să se demonstreze inegalitatea:

$$\left(\sum_{n=1}^{m} u_n\right)^2 \leqslant m.$$

2° Pentru ce numere întregi m avem egalitate în inegalitatea de mai sus?

3° Să se demonstreze inegalitatea:

$$m < \left(\sum_{n=0}^{m} u_n\right)^2.$$

1.66. 1° Să se demonstreze că, pentru ca un șir (u_n) de numere întregi să satisfacă egalitatea:

$$u_{n+1} + u_{n-1} = 2(u_n + 1),$$

pentru orice întreg n, este necesar și suficient ca să existe doi întregi a și b astfel încît:

$$u_n = an^2 + an + b.$$

Să se calculeze a și b în funcție de u_0 și de u_1.

2° Să se generalizeze la egalitatea:

$$u_{n+1} + u_{n-1} = 2(u_n + k) \qquad (k \text{ întreg fixat}).$$

1.67. 1° Se dă un întreg p strict pozitiv. Fie (u_n) șirul definit prin:

$$u_0 = 1,\ u_1 = 1,\ u_{n+1} = pu_n + u_{n-1}.$$

Să se calculeze u_2, u_3, u_4.

2° Să se demonstreze relațiile:

$$u_{n+1}\,u_{n-1} - u_n^2 = (-1)^{n-1}p;$$

$$u_{n+1}^2 - u_n^2 - pu_nu_{n+1} = (-1)^{n-1}p.$$

3° Punem acum $u_0 = 0$. Să se stabilească relații de recurență analoage cu cele care au fost studiate în a doua problemă.

1.68. 1° Se definește șirul (u_n) prin $u_0 = 0$ și relația de recurență:

$$u_n = u_{n-1} + n(-1)^n.$$

Să se calculeze u_n pentru $n \leqslant 5$.

2° Să se studieze șirul:

$$u_0, u_2, \ldots, u_{2k}, \ldots$$

Să se exprime u_{2k}, u_{2k+1}, u_{2k-1} în funcție de k.

1.69. Fie $u_0 = 1$ și $v_0 = 0$ și formulele de recurență:

$$(E)\begin{cases} u_{n+1} = 2u_n + 3v_n \\ v_{n+1} = u_n + 2v_n \end{cases}$$

care definesc șirurile (u_n) și (v_n).

Să se stabilească:

$$\begin{cases} u_{n+1} + u_{n-1} = 4u_n \\ v_{n+1} + v_{n-1} = 4v_n. \end{cases}$$

Să se demonstreze prin recurență că, notînd prin k un întreg astfel încît $0 \leqslant k \leqslant n$, există un număr m_k astfel încît, oricare ar fi indicele n, să avem:

$$\begin{cases} u_{n-k} + u_{n+k} = m_k u_n \\ v_{n-k} + v_{n+k} = m_k v_n. \end{cases}$$

(Se va stabili relația:

$$m_{k+1} + m_{k-1} = 4m_k$$

și se va deduce că:

$$m_k = 2u_k.)$$

2. NUMERE ÎNTREGI RELATIVE

2.1. DEFINIȚIA MULȚIMII Z

2.1.1. Întregi pozitivi și negativi

Noțiunea de întreg înzestrat cu un *semn* este foarte comună. Fiecare cunoaște semnificația intuitivă a simbolurilor (+3), (—5), (—1), etc.
Următoarea diagramă arată cum se formalizează folosirea lor:

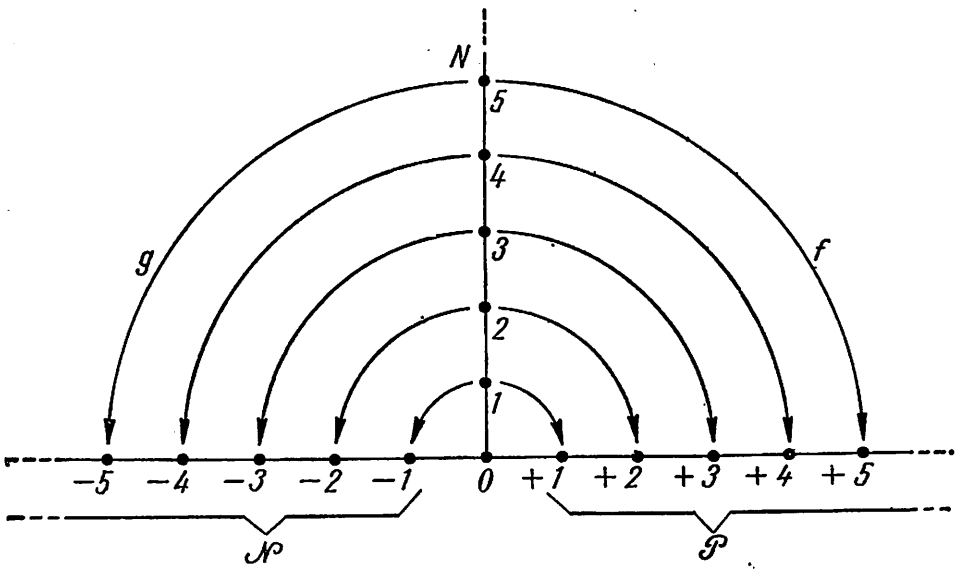


FIG. 1

Două aplicații diferite asociază, aceluiași element n din $\mathbf{N}^*$ (întregi nenuli), cele două simboluri $(+n)$ și $(-n)$. (Semnele „+" și „—" nu au nevoie deocamdată de nici o semnificație specială.)
Imaginile lui $\mathbf{N}^*$ prin aceste două aplicații, care se presupune că sînt *bijective*, sînt notate, de exemplu, $\mathcal{P}$ și $\mathcal{N}$ — pentru întregi strict pozitivi și întregi strict negativi. Vom spune că aceste mulțimi noi sînt copii distincte ale lui $\mathbf{N}^*$, imagini, disjuncte ale lui $\mathbf{N}^*$, prin cele două bijecții:

$$\mathfrak{f} = [n \longmapsto +n],$$

$$\mathfrak{g} = [n \longmapsto -n].$$

La reuniunea $\mathcal{P} \cup \mathcal{N}$ vom adăuga mulțimea $\{0\}$ astfel încît să obținem două copii ale lui $\mathbf{N}$, imagini ale lui $\mathbf{N}$ prin bijecții, notate tot $\mathfrak{f}$ și $\mathfrak{g}$, astfel încît:

$$\mathfrak{f}(0) = +0 = \mathfrak{g}(0) = -0 = 0.$$

Aceste mulțimi, egale respectiv cu $\mathcal{P} \cup \{0\}$ și cu $\mathcal{N} \cup \{0\}$ (întregi *pozitivi sau nuli* și întregi *negativi sau nuli)*, nu sînt disjuncte, deoarece $\{0\}$ este intersecția lor.
Vom numi $\mathbf{Z}$ reuniunea:

$$\boxed{\mathbf{Z} = \mathcal{P} \cup \{0\} \cup \mathcal{N}}$$

Vom rezuma construcția precedentă enunțînd:

DEFINIȚIE 1 / **Mulțimea $\mathbf{Z}$ a întregilor relativi este definită ca reuniunea a trei mulțimi disjuncte dintre care una nu conține decît numărul 0 al lui $\mathbf{N}$, celelalte două fiind legate de $\mathbf{N}^*$ prin bijecții.**

$\mathbf{Z}$ nu este deci definit decît făcînd abstracție de un izomorfism, ca și $\mathbf{N}$. De aceea, în anumite probleme, este comod să luăm drept bijecție $\mathfrak{f}$, identitatea. Atunci:

$$\mathbf{N}^* = \mathcal{P}, \qquad \mathbf{N} = \mathcal{P} \cup \{0\},$$

de unde incluziunea:

$$\boxed{\mathbf{N} \subset \mathbf{Z}}$$

EXERCIȚII

---

1. *Să se demonstreze că există o bijecție între $\mathbf{Z}$ și $\mathbf{N}$.*
Orice element al lui $\mathbf{Z}$ este tipul 0, $+n$ sau $-n$ cu: $n \geqslant 1$. Să punem de exemplu:

$$\varphi(0) = 0, \quad \varphi(+n) = 2n, \quad \varphi(-n) = 2n - 1.$$

Este ușor de văzut că se definește astfel un izomorfism între $\mathbf{Z}$ și $\mathbf{N}$. Să dăm valorile cele mai simple ale funcțiilor φ și φ^{-1}:

x	...	-2	-1	0	$+1$	$+2$	$+3$	...
$\varphi(x)$	...	3	1	0	2	4	6	...

n	0	1	2	3	4	5	...
$\varphi^{-1}(n)$	0	-1	$+1$	-2	$+2$	-3	...

(În consecinţă, N ar fi putut foarte bine să servească de model pentru Z; ar fi fost suficient să punem:

$$f(n) = 2n,\ g(n) = 2n - 1.)$$

II. *Să se definească un model al lui* Z *cu ajutorul produsului cartezian dintre* N *şi o mulţime de două elemente.*
(+) şi (−) fiind două semne oarecare (dar diferite, de exemplu: + = 0, − = 1), se poate construi mulţimea:

$$A = \mathbf{N} \times \{+, -\}.$$

Dacă punem atunci:

$$f(n) = (n, +),\ g(n) = (n, -) \quad (n \neq 0),$$

şi, de exemplu:

$$f(0) = g(0) = (0, +),$$

atunci mulţimea:

$$B = A - \{(0, -)\}$$

este izomorfă cu Z prin bijecţia definită dè egalităţile:

$$\varphi(+n) = (n, +),\ \varphi(-n) = (n, -),\ \varphi(0) = (0, +) \quad (n \in \mathbf{N}^*).$$

2.1.2. Succesor, predecesor şi opus

În construcţia lui N, funcţia de succesiune a jucat un rol esenţial. O vom prelungi la mulţimea Z. Dorind ca $\mathcal{P} \cup \{0\}$ să fie o imagine cît mai exactă a lui N, vom defini *succesorul* x^+ al întregului relativ x în felul următor:

$$\boxed{\begin{array}{l}(+n)^+ = +(n+1) \\ (-n)^+ = -(n-1)\end{array}} \qquad \begin{array}{l}(n \in \mathbf{N}) \\ (n \in \mathbf{N}^*).\end{array}$$

În special:

$$\boxed{(+n)^+ = +(n')} \qquad (n \in N).$$

Aplicaţia astfel definită este o bijecţie între Z şi el însuşi. Într-adevăr, dacă notăm:

$$\mathfrak{f} = [n \longmapsto n^+],$$

imaginea lui $\mathcal{P} \cup \{0\}$ prin f este chiar $\mathcal{P}$, şi orice element al lui $\mathcal{P}$ este imaginea unui element unic al lui $\mathcal{P} \cup \{0\}$ (a se vedea nr. **1.1.1.**, sau nr. **1.2.1.**, Teorema 4). La fel, imaginea lui $\mathcal{N}$ prin f este $\mathcal{N} \cup \{0\}$: $(-n)$ este succesorul lui $-(n+1)$, şi nu este succesorul niciunui alt întreg relativ din $\mathcal{N}$; f este deci surjectivă.
În sfîrşit, $\mathcal{P}$ şi $\mathcal{N} \cup \{0\}$ fiind disjuncte, se poate deduce că f este injectivă. Vom nota cu (x^-) unicul element astfel încît:

$$\boxed{(x^-)^+ = x} \qquad (x \in \mathbf{Z}).$$

Acest *predecesor* al lui x are proprietăți simple:

$$\boxed{\begin{array}{l}(+n)^- = +\,(n-1)\\(-n)^- = -\,(n+1)\\(x^+)^- = x\end{array}} \qquad \begin{array}{l}(n \in \mathbf{N}^*)\\(n \in \mathbf{N})\\(x \in \mathbf{Z}).\end{array}$$

În sfîrșit:

$$\boxed{x = y \iff x^+ = y^+ \iff x^- = y^-}$$

Alături de cele două aplicații definite mai sus, se impune pe $\mathbf{Z}$ o a treia bijecție; oricărui întreg relativ x, îi asociază *opusul* său, notat $(-x)$, astfel încît:

$$\boxed{\begin{array}{l}-(+n) = -\,n,\\-(-n) = +\,n\end{array}} \qquad (n \in \mathbf{N}).$$

Aceasta este evident o bijecție, schimbînd $\mathcal{P}$ cu $\mathcal{N}$, lăsînd pe 0 — și numai pe el — invariant. Ea este involutivă:

$$\left.\begin{array}{l}-\,[-\,(+\,n)] = +\,n,\\-\,[-\,(-\,n)] = -\,n\end{array}\right\} \qquad \boxed{-\,(-\,x) = x}$$

(Semnul „—" folosit aici nu are, a priori, nici o legătură cu semnul „—" care indică bijecția între $\mathbf{N}^*$ și $\mathcal{N}$; vom vedea mai tîrziu în ce raport se află aceste două semne.)
Aceste trei bijecții sînt legate, în particular, prin următoarea relație fundamentală:

$$\boxed{-\,(x^+) = (-\,x)^-}$$

și corolarul său:

$$\boxed{-\,(x^-) = (-\,x)^+}$$

EXERCIȚIU

Să se demonstreze egalitățile precedente:

$$-\,(x^+) = (-\,x)^- \text{ și } -\,(x^-) = (-\,x)^+.$$

Fie relația:

$$y = -\,(x^+) = (-\,x)^-.$$

Dacă x este pozitiv sau nul, atunci:

$$x = +\,n. \quad x^+ = +\,(n+1) \quad (n \in \mathbf{N}),$$

de unde:

$$y = -\,(x^+) = -\,[+(n+1)] = -(n+1),$$

şi:

$$y^+ = [-(n+1)]^+ = -[(n+1)-1] = -n,$$

sau:

$$y^+ = -x,$$

şi:

$$y = (-x)^-.$$

Dacă x este strict negativ, atunci:

$$x = -n, \quad x^+ = -(n-1) \quad (n \in \mathbf{N}^*),$$

$$y = -(x^+) = -[-(n-1)] = +(n-1),$$

$$y^+ = [+(n-1)]^+ = +[(n-1)+1] = +n,$$

$$y^+ = -x, \; y = (-x)^-.$$

A doua relaţie o deducem scriind:

$$z = -x, \quad -z = -(-x) = x.$$

Prima, aplicată lui z, se scrie:

$$(-z)^- = -(z^+), \quad -[(-z)^-] = -[-(z^+)] = z^+,$$

adică:

$$-(x^-) = (-x)^+.$$

Aceste rezultate sînt imediate cu ajutorul unei diagrame:

Vom rezuma aceste proprietăţi enunţînd:

TEOREMA 1 / **Există trei bijecţii remarcabile între Z şi Z. Prima este succesiunea, definită prin:**

$$\boxed{\begin{array}{l}(+n)^+ = +(n+1) \\ (-n)^+ = -(n-1)\end{array}} \qquad \begin{array}{l}(n \in \mathbf{N}) \\ (n \in \mathbf{N}^*).\end{array}$$

A doua este inversa primeia:

$$\boxed{y = x^- \Longleftrightarrow x = y^+}$$

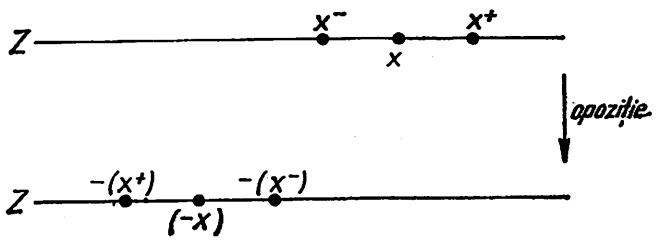


FIG. 2

A treia este opoziția, definită prin:

$$\boxed{-(+n) = -n, \quad -(-n) = +n} \qquad (n \in \mathbf{N})$$

Opoziția schimbă între ele bijecțiile precedente:

$$\boxed{-(x^+) = (-x)^-, \quad -(x^-) = (-x)^+}$$

2.1.3. Principiul dublei inducții

Să considerăm o submulțime nevidă M a lui $\mathbf{Z}$, și fie a unul din elementele sale. Dacă a aparține lui $\mathcal{P} \cup \{0\}$, bijecția:

$$\mathrm{f} = [m \longmapsto +m]$$

asociază lui M o submulțime M' a lui $\mathbf{N}$; întregul m nu aparține lui $\mathbf{M}'$ decît dacă, și numai dacă, $+m$ aparține lui M. De exemplu, M' conține întregul n astfel încît $a = +n$.
Să presupunem că M conține succesorul și predecesorul fiecăruia din elementele sale; M' are atunci aceeași proprietate.
Să considerăm mulțimea nevidă M': ea admite un element minimum q.
Dacă q este diferit de zero, predecesorul $(q - 1)$ al lui q trebuie să aparțină lui M' ca predecesor al unui element al lui M', ceea ce este contradictoriu.
Deducem că q este nul, deci că M' este egală cu N după principiul inducției, sau încă:

$$\mathcal{P} \cup \{0\} \subset M.$$

0 fiind element al lui M, întregul negativ (-1) aparține deci lui M, deoarece:

$$(-1) = 0^-.$$

Același raționament, cu bijecția:

$$\mathrm{g} = [m \longmapsto -m]$$

în loc de f, și (-1) în loc de a, arată că:

$$\mathcal{N} \cup \{0\} \subset M.$$

În final, M și $\mathbf{Z}$ sînt egale. Același raționament se aplică bineînțeles în cazul în care a aparține lui $\mathcal{N} \cup \{0\}$. Putem deci enunța următoarea teoremă:

TEOREMA 2 / **Orice submulțime nevidă a lui Z care conține succesorii și predecesorii elementelor sale se confundă cu mulțimea Z (principiul dublei inducții).**

Observație. — Teorema precedentă rămîne adevărată dacă i se substituie litera N literei Z: este suficient să remarcăm că operația de succesiune în N

se deduce din restricția succesiunii lui **Z** la submulțimea $\mathcal{P} \cup \{0\}$ prin bijecția

$$[+ m \longmapsto m].$$

EXERCIȚII

2.1. Se consideră două mulțimi disjuncte A și B, legate amîndouă de **N** prin bijecțiile φ și ψ. Să se demonstreze că există o bijecție între **Z** și $A \cup B$.

2.2. Să se definească cel puțin trei bijecții diferite între **Z** și **N**.

2.3. Să se demonstreze, prin dublă inducție, că 5 divide pe $x^5 - x$ (vom admite proprietățile cunoscute ale lui **Z**, inel comutativ).

2.4. Să se demonstreze că teorema 2 este adevărată în **N**.

2.5. Se consideră mulțimea $E = \mathbf{N} \times \mathbf{N}$ și, în această mulțime, relația:

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

1° Să se demonstreze că este o relație de echivalență.
2° Să se demonstreze că mulțimea cît a lui E prin această relație (adică mulțimea claselor de echivalență) este izomorfă cu **Z**. Pentru aceasta se va putea arăta că orice clasă are una, și numai una din cele trei forme: clasa lui $(n, 0)$, clasa lui $(0, 0)$, clasa lui $(0, n)$ unde n aparține lui $\mathbf{N}^*$.
(Acest exercițiu constituie prima verigă a unei alte construcții a lui **Z**. Ea va fi completată de exercițiile: 2.20, 2.21, 2.22 și 2.34.)

2.2. STRUCTURA DE INEL

2.2.1. Adunarea

Pe **N** adunarea este definită prin egalitățile:

$$n + 0 = n, \quad n + m' = (n + m)'.$$

Să înlocuim succesiunea în **N**:

$$[n \longmapsto n']$$

cu succesiunea în **Z**:

$$[x \longmapsto x^+],$$

și să mai punem:

$$\boxed{x + 0 = x, \quad x + y^+ = (x + y)^+} \qquad (1)\ (2)$$

Unicitatea adunării pe **N** arată că, pentru doi întregi pozitivi sau nuli, avem:

$$\boxed{(+ n) + (+ m) = + (n + m)} \qquad (3)$$

Aceasta arată că $(+\ n)$ este egal cu:

$$(+\ 0) + (+\ n) = 0 + (+\ n).$$

Pe de altă parte:

$$x + 0^+ = (x + 0)^+ = x^+,$$

sau:

$$\boxed{x^+ = x + (+\ 1)} \tag{4}$$

Să observăm în sfîrşit că se pot scrie egalităţile:

$$(x + y^-)^+ = x + (y^-)^+ = x + y,$$

de unde:

$$\boxed{x + y^- = (x + y)^-} \tag{5}$$

1. *Existenţa* sumei a doi întregi.
Să fixăm pe x. Mulţimea M a întregilor relativi y pentru care $(x + y)$ este calculabilă conţine pe 0, y^+ şi y^- pentru orice y al lui M. Mulţimea M este deci egală cu **Z**, şi se poate calcula $(x + y)$ pentru toate perechile (x, y) ale lui $\mathbf{Z}^2$.

2. *Unicitatea* adunării este evidentă. Să considerăm toate aplicaţiile f ale lui $\mathbf{Z}^2$ în **Z** astfel încît:

$$f(x, 0) = x, \quad f(x, y^+) = [f(x, y)]^+.$$

Mulţimea M a întregilor y pentru care numărul $f(x, y)$ nu depinde decît de x, şi nu de funcţia f, îl conţine pe 0. Dacă îl conţine pe y, ea îl conţine atunci şi pe y^+, şi pe y^-, aşa cum ne arată egalitatea:

$$f(x, y^-) = [f(x, y)]^-.$$

Mulţimea M este deci egală cu **Z**, şi aplicaţia f este unică.

3. *Asociativitatea* adunării se demonstrează ca la nr. 1.2.2; egalitatea:

$$\boxed{x + (y + z) = (x + y) + z} \tag{6}$$

este adevărată pentru $z = 0$. Dacă este adevărată pentru z, atunci:

$$\begin{aligned} x + (y + z^+) &= x + (y + z)^+ = \\ &= [x + (y + z)]^+ = [(x + y) + z]^+ \\ &= (x + y) + z^+. \end{aligned}$$

La fel:

$$x + (y + z^-) = (x + y) + z^-.$$

Mulţimea M a întregilor z pentru care egalitatea (6) este adevărată este deci chiar **Z**.

4. *Comutativitatea* adunării se arată la fel ca şi comutativitatea adunării pe N. Cele trei leme:

$$x + 0 = 0 + x, \quad x + (+1) = (+1) + x,$$

$$\boxed{x + y = y + x} \tag{7}$$

se demonstrează prin dublă inducţie.
Într-adevăr:

$$0 + 0 = 0 + 0,$$

$$[(x + 0) = (0 + x)]$$

$$\Longrightarrow [x^+ + 0 = x^+ = (x + 0)^+ = (0 + x)^+ = 0 + x^+].$$

La fel:

$$[(x + 0) = (0 + x)]$$

$$\Longrightarrow [x^- + 0 = x^- = (x + 0)^- = (0 + x)^- = 0 + x^-].$$

Deci, 0 este *element neutru* pentru adunare, şi egalitatea:

$$[x + (+1) = (+1) + x]$$

este adevărată pentru 0. Dacă este adevărată pentru x, atunci:

$$\begin{aligned} x^+ + (+1) &= [x + (+1)] + (+1) = [x + (+1)]^+ \\ &= [(+1) + x]^+ = (+1) + x^+, \end{aligned}$$

$$\begin{aligned} x^- + (+1) &= x^{-+} = x = x^{+-} = [x + (+1)]^- \\ &= [(+1) + x]^- = (+1) + x^-. \end{aligned}$$

Este deci adevărată pentru x. Egalitatea:

$$x + y = y + x$$

este adevărată pentru $x = 0$. Dacă este adevărată pentru x, atunci:

$$\begin{aligned} x^+ + y &= [x + (+1)] + y = x + [(+1) + y] \\ &= x + [y + (+1)] = x + y^+ = (x + y)^+ \\ &= (y + x)^+ = y + x^+; \end{aligned}$$

$$\begin{aligned} x^- + y &= x^- + y^{-+} = x^- + [y^- + (+1)] = \\ &= x^- + [(+1) + y^-] = [x^- + (+1)] + y^- \\ &= x^{-+} + y^- = x + y^- = (x + y)^- \\ &= (y + x)^- = y + x^-. \end{aligned}$$

Comutativitatea adunării rezultă deci din asociativitatea sa (conform nr. 1.2.2). Să notăm egalitatea:

$$(x + y^- = x^- + y).$$

5. Orice element al lui **Z** are un opus. Într-adevăr, egalitatea:

$$\boxed{x + (-x) = 0} \tag{8}$$

este adevărată pentru $x = 0$, căci 0 este propriul său opus.
Dacă este adevărată pentru x, atunci:

$$x^+ + [-(x^+)] = x^+ + (-x)^- = x^{+-} + (-x)$$
$$= x + (-x) = 0,$$
$$x^- + [-(x^-)] = x^- + (-x)^+ = x + (-x)^{+-}$$
$$= x + (-x) = 0.$$

6. Mulțimea **Z** înzestrată cu adunarea este deci un *grup comutativ*, notat $(\mathbf{Z}, +)$ sau **Z** prin abuz de limbaj:

grup comutativ

$$\begin{cases} x + (y + z) = (x + y) + z & \textit{(asociativitate)} \\ x + 0 = 0 + x = x & \textit{(element neutru)} \\ x + (-x) = (-x) + x = 0 & \textit{(elemente opuse)} \\ x + y = y + x & \textit{(comutativitate)} \end{cases}$$

7. Se deduce imediat *regularitatea* oricărui întreg relativ la adunare. Într-adevăr, dacă se cunoaște egalitatea:

$$(x + y = z + y),$$

se poate scrie:

$$x = x + 0 = x + [y + (-y)] = (x + y) + (-y)$$
$$= (z + y) + (-y) = z + [y + (-y)] = z + 0 = z,$$

și:

$$\boxed{x + y = z + y \iff x = z} \tag{9}$$

8. Vom rezuma aceste proprietăți enunțînd următoarea teoremă:

TEOREMĂ 3 / **Adunarea a doi întregi relativi este o operație internă bine definită pe Z prin egalitățile:**

$$x + 0 = x, \quad x + y^+ = (x + y)^+.$$

Z este un grup comutativ pentru această adunare.

Observație. — Adunarea în **Z** o prelungește pe cea din **N**; aceasta înseamnă că adunarea pe **N** induce, prin bijecția $[m \longmapsto +m]$, o operație în partea $\mathcal{P} \cup \{0\}$ a lui **Z**, care este restricția la această parte a adunării lui **Z**.

De exemplu, echivalența (9) permite să se demonstreze din nou echivalența (8) din capitolul precedent (nr. 1.2.2).

EXEMPLE. I. *Să se studieze, în* $(\mathbf{Z}, +)$, *ecuația:*

$$a + x = b,$$

unde a *și* b *sînt doi întregi relativi dați.*
Dacă această ecuație admite o soluție, trebuie să avem:

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

Reciproc, această valoare convine, deoarece:

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

Ecuația admite deci o soluție unică:

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

Ea nu diferă de ecuația:

$$x + a = b$$

care admite aceeași soluție:

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

În particular, egalitatea adevărată: $x^- + (+1) = x$ dă egalitatea:

$$\boxed{x^- = x + (-1)} \qquad (10)$$

II. *Să se demonstreze că orice mulțime nevidă* G *înzestrată cu o adunare asociativă și comutativă este un grup dacă ecuația:*

$$a + x = b$$

admite întotdeauna cel puțin o soluție.
Să fixăm un element a în G; există atunci un număr e astfel încît:

$$a + e = e + a = a.$$

Pentru orice element b, există un element c astfel încît:

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

Numărul e este deci un element neutru pentru adunare.
Pentru orice element b, există un element c astfel încît:

$$e = b + c = c + b.$$

În consecință, orice element admite un opus. (Este ușor de arătat că e este unic ca fiind opusul unui element dat al lui G.)

III. *Să se rezolve, în* $(\mathbf{Z}, +)$, *ecuația:*

$$x + x = a + a,$$

unde a *este un întreg relativ dat.*

Să punem: $x = a + z$ (conform exercițiului I).

Ecuația este echivalentă cu:

$$z + z = 0.$$

O soluție este $z = 0$ (de unde $x = a$). Dacă nu:

a) sau $z = +n$, cu $n \in N^*$; dar atunci:

$$z + z = +(n + n) \neq 0,$$

căci: $n + n \neq 0$ (conform celor de pe pagina 30);

b) sau $z = -n$, dar avem în mod analog:

$$z + z = -(n + n) \neq 0.$$

Singura soluție este deci $x = a$.

IV. *Să se compare* $(-x) + (-y)$ și $-(x + y)$.

Avem:

$$\begin{aligned}(x + y) + [-(x + y)] &= 0\\ &= x + (-x) = (x + 0) + (-x)\\ &= [x + (y + [-y])] + (-x)\\ &= [(x + y) + (-y)] + (-x)\\ &= (x + y) + [(-y) + (-x)].\end{aligned}$$

Simplificînd cu $(x + y)$, deducem:

$$-(x + y) = (-y) + (-x),$$

fie:

$$\boxed{-(x + y) = (-x) + (-y)} \qquad (11)$$

2.2.2. Înmulțirea

Studiul înmulțirii pe N ne va folosi pentru a defini o înmulțire pe Z care să-i fie o prelungire naturală. Să punem deci.

$$\boxed{x \times 0 = 0, \quad x \times y^+ = (x \times y) + x} \qquad (12)\ (13)$$

De exemplu:

$$\boxed{x \times (+1) = x, \quad (+n) \times (+m) = +(n \times m)} \qquad (14)\ (15)$$

1. Să calculăm suma $(x \times y^-) + x$; se obține:

$$(x \times y^-) + x = x \times (y^-)^+ = x \times y,$$

de unde egalitatea:

$$\boxed{x \times y^- = (x \times y) + (-x)} \tag{16}$$

Produsul $x \times y$ permite deci să se calculeze $x \times y^+$ și $x \times y^-$; se deduce ca și la nr. 2.2.1 că înmulțirea este definită, în mod unic, prin egalitățile (12) și (13).

2. Modificate convenabil, raționamentele de la nr. 1.2.3 permit să se demonstreze că înmulțirea este distributivă la stînga în raport cu adunarea, apoi distributivă la dreapta, în sfîrșit asociativă și comutativă. Aici încă, vom scrie, xy pentru $x \times y$. Egalitatea:

$$\boxed{(x + y)z = xz + yz} \tag{17}$$

este adevărată pentru $z = 0$. Dacă este adevărată pentru z, se poate deduce, ca la nr. 1.2.3, că avem:

$$(x + y)z^+ = xz^+ + yz^+.$$

Pe de altă parte, cu aceeași ipoteză și folosind asociativitatea, comutativitatea și rezultatul din exemplul IV (egalitatea (11)), se poate scrie:

$$\begin{aligned}(x + y)z^- &= (x + y)z + [-(x + y)] \\ &= (xz + yz) + [(-x) + (-y)] \\ &= [xz + (-x)] + [yz + (-y)] \\ &= xz^- + yz^-.\end{aligned}$$

Egalitatea (17), care dovedește *distributivitatea la stînga*, este deci demonstrată prin dublă inducție în raport cu z.

3. *Distributivitatea la dreapta:*

$$\boxed{x(y + z) = xy + xz} \tag{18}$$

este adevărat pentru $z = 0$.

Dacă este adevărată pentru z, avem atunci (nr. 1.2.3):

$$x(y + z^+) = xy + xz^+,$$

și:

$$\begin{aligned}x(y + z^-) = x(y + z)^- &= x(y + z) + [-(x)] \\ &= (xy + xz) + (-x) \\ &= xy + [xz + (-x)] \\ &= xy + xz^-.\end{aligned}$$

Înmulțirea este deci distributivă în raport cu adunarea.

4. Se deduce *asociativitatea:*

$$\boxed{x(yz) = (xy)z} \tag{19}$$

tot prin dublă inducție în raport cu z. Este adevărată pentru $z = 0$. Dacă este adevărată pentru z, avem atunci (nr. 1.2.3):

$$x(yz^+) = (xy)z^+,$$

și:

$$\begin{aligned} x(yz^-) + xy &= x(yz^- + y) \\ &= x(yz^{-+}) = x(yz) = (xy)z; \end{aligned}$$

de unde:

$$x(yz^-) = (xy)z + (-xy) = (xy)z^-.$$

5. Rezultă că 0 este *absorbant:*

$$\boxed{0x = 0} \tag{20}$$

Această proprietate este adevărată pentru $x = 0$; dacă este adevărată pentru x, atunci:

$$\begin{aligned} 0x^+ &= 0x + 0 = 0x = 0, \\ 0x^- &= 0x + (-0) = 0x + 0 = 0x = 0. \end{aligned}$$

6. În sfîrșit, înmulțirea este *comutativă.*
Într-adevăr, egalitatea:

$$\boxed{xy = yx} \tag{21}$$

este adevărată pentru $y = 0$ [(12) și (20)]. Este adevărat pentru $y = 1$, căci $x(+1) = x$, și o dublă inducție arată că: $x = (+1)x$.
(Egalitatea $x = (+1)x$ implică egalitățile:

$$\begin{aligned} x^+ &= x + (+1) = (+1)x + (+1) = (+1)x^+, \\ x^- &= x + (-1) = (+1)x + (-1) \\ &= (+1)x + [-(+1)] = (+1)x^-; \end{aligned}$$

deoarece $0 = (+1)0$, egalitatea este adevărată pentru orice x, și $(+1)$ este element neutru pentru înmulțire.)
7. Să presupunem că egalitatea (21) este adevărată pentru y; atunci:

$$\begin{aligned} xy^+ &= xy + x = xy + (+1)x = yx + (+1)x \\ &= [y + (+1)]x = y^+x \text{ (conform nr. 1.2.3),} \\ xy^- &= xy + (-x) = yx + (-x) = y^{-+}x + (-x) \\ &= [y^- + (+1)]x + (-x) \\ &= [y^-x + (+1)x] + (-x) \\ &= (y^-x + x) + (-x) = y^-x + [x + (-x)] \\ &= y^-x + 0 = y^-x. \end{aligned}$$

Comutativitatea este deci demonstrată pentru orice pereche (x, y).

8. $(\mathbf{Z}, +)$ fiind un grup comutativ, mulțimea $\mathbf{Z}$ înzestrată cu cele două legi studiate formează atunci un *inel comutativ unitar:*

Inel	$(\mathbf{Z}, +)$ **grup comutativ**	
	$x(yz) = (xy)z$	*(asociativitate)*
	$x(y + z) = xy + xz$	*(distributivitate)*
	$(x + y)z = xz + yz$	
comutativ	$xy = yx$	*(comutativitate)*
unitar	$x1 = 1x = x$	*(element neutru)*

9. Vom rezuma aceste propoziții enunțînd următoarea teoremă:

TEOREMA 4 / **Înmulțirea a doi întregi relativi este o operație internă bine definită pe Z prin egalitățile:**

$$x0 = 0, \quad xy^+ = xy + x.$$

Ea este asociativă, comutativă și distributivă în raport cu adunarea; 0 este un element absorbant; 1 este un element neutru; $(\mathbf{Z}, +, \times)$ este un inel comutativ unitar.

Observație. — Adunarea și înmulțirea din $\mathbf{Z}$ prelungesc pe cele din $\mathbf{N}$.

2.2.3. Proprietăți diverse

1. Am notat, în trecere, egalitățile:

$$(+n) + (+m) = +(n + m), \tag{3}$$

$$(+n) \times (+m) = +(nm). \tag{15}$$

La fel, să determinăm suma și produsul a doi întregi negativi; mai întîi:

$$\begin{aligned}(-n) + (-m) &= [-(+n)] + [-(+m)] \\ &= -[(+n) + (+m)] \\ &= -[+(n + m)] \\ &= -(n + m).\end{aligned}$$

$$\boxed{(-n) + (-m) = -(n + m)} \tag{22}$$

2. Determinarea produsului este mai delicată. Să arătăm mai întîi egalitatea importantă:

$$\boxed{-x = (-1)x} \tag{23}$$

care este o simplă consecință a egalităților:

$$x + (-x) = 0 = 0x = [1 + (-1)]x$$
$$= 1x + (-1)x = x + (-1)x.$$

În particular:

$$+1 = -(-1) = (-1)(-1).$$

În consecință:

$$x(-y) = x[(-1)y] = [x(-1)]y$$
$$= [(-1)x]y = (-1)xy = -xy,$$

$$\boxed{x(-y) = -xy} \tag{24}$$

și în final:

$$(-x)(-y) = -[(-x)y] = -[y(-x)]$$
$$= -(-yx) = yx = xy,$$

$$\boxed{(-x)(-y) = xy} \tag{25}$$

Se deduc egalitățile:

$$\boxed{\begin{aligned}(-n)(-m) &= +(nm) \quad (26)\\ (-n)(+m) &= -(nm) \quad (27)\end{aligned}}$$

care constituie „*regula semnelor*" bine cunoscută.

3. Rămîne de determinat suma dintre un întreg pozitiv și un întreg negativ. Sînt două cazuri de examinat:

a) $n \geqslant m \Leftrightarrow n = m + p.$

Atunci: $(+n) + (-m) = +p$; prin inducție simplă în raport cu p:

$$(+m) + (-m) = 0,$$

$$(+[m + p']) + (-m) = (+n') + (-m)$$
$$= (+n)^+ + (-m) = [(+n) + (-m)]^+$$
$$= (+p)^+ = +p'.$$

b) $m \geqslant n \Leftrightarrow m = n + p.$

Atunci: $(+n) + (-m) = -p$; prin inducție simplă în raport cu p:

$$(+m) + (-m) = 0,$$

$$(+n) + (-[n + p']) = (+n) + (-m')$$
$$= (+n) + (-m)^- = [(+n) + (-m)]^-$$
$$= (-p)^- = -(+p)^+ = -p'.$$

În final:

$$\boxed{n \geqslant m \Longrightarrow (+n) + (-m) = +(n - m)} \quad (28)$$

$$\boxed{n \leqslant m \Longrightarrow (+n) + (-m) = -(m - n)} \quad (29)$$

Proprietățile (3), (15), (22), (26), (27), (28) și (29), alăturate comutativității înmulțirii sînt suficiente pentru a defini cele două operații fundamentale pe **Z**. Am fi putut să le luăm ca definiții.

4. În mod obișnuit se confundă practic elementul n al lui **N** cu elementul $(+n)$ al lui **Z**, ceea ce revine la a confunda $\mathcal{P}$ și **N***.
Conform acestui obicei, vom scrie de acum încolo, spre exemplu:

$$(-n)(-m) = nm; \qquad x^{+} = x + 1.$$

Diferența a doi întregi relativi va fi definită prin echivalența:

$$\boxed{x - y = z \Longleftrightarrow x = y + z}$$

sau încă prin egalitatea:

$$\boxed{x - y = x + (-y)} \quad (30)$$

Cu această notație, putem scrie $x^{-} = x - 1$ și:

$$\boxed{x - y = -(y - x)} \quad (31)$$

ceea ce rezumă egalitățile (28) și (29), devenite familiare.
Evident, aceste abuzuri de limbaj și de scriere nu sînt posibile decît pentru că operațiile de adunare, de înmulțire și de scădere pe **Z** prelungesc operațiile cu același nume pe **N** (unde, să observăm, scăderea nu este definită peste tot).

5. În **N**, egalitatea:

$$n + m = 0$$

era echivalentă cu ($n = 0$ și $m = 0$). În **Z** nu este la fel; putem demonstra numai echivalența foarte simplă:

$$\boxed{x + y = 0 \Longleftrightarrow y = -x} \quad (32)$$

(A se vedea exercițiul I de la pagina 84.)

6. Să studiem, pe **Z**, ecuația: $xy = 0$.
Egalitățile (15), (26) și (27) arată că, pentru toate semnele posibile ale lui x și y, această egalitate necesită ca unul din factori să fie egal cu zero.
Se deduce echivalența fundamentală:

$$\boxed{(xy = 0) \Longleftrightarrow (x = 0 \text{ sau } y = 0)} \quad (33)$$

Se spune că $(\mathbf{Z}, +, \times)$ este un *inel integru*.

7. Să studiem pe $\mathbf{Z}$ ecuaţia:

$$xy = 1.$$

Şi aici, studiul diferitelor cazuri arată că singurele soluţii sînt date de echivalenţa:

$$\boxed{(xy = 1) \Longleftrightarrow (x = y = 1 \text{ sau } x = y = -1)} \qquad (34)$$

1 şi (-1) sînt deci singurele elemente inversabile ale lui $\mathbf{Z}$.

EXERCIŢII

I. *Să se demonstreze echivalenţa* (34).
Produsul xy trebuind să fie pozitiv, sîntem conduşi la două cazuri:

a) $x = +n$, $y = +m$, $nm = 1$, de unde: $n = m = 1$;

b) $x = -n$, $y = -m$, $nm = 1$, de unde: $n = m = 1$.

II. *Să se demonstreze că înmulţirea este distributivă în raport cu scăderea.*
Trebuie să demonstrăm egalitatea:

$$x(y - z) = xy - xz,$$

sau încă (30):

$$x[y + (-z)] = xy + (-xz);$$

or:

$$x[y + (-z)] = xy + x(-z) = xy + (-xz). \qquad (24)$$

Proprietatea este deci demonstrată.

III. *Se poate defini o exponenţiere în* $\mathbf{Z}$?
Să punem din nou:

$$y^0 = 1, \; y^{x+} = y^x y.$$

(Astfel exponenţierea o va prelungi pe cea din $\mathbf{N}$.)
În particular, trebuie să dăm un sens lui y^{-1}. Dacă $z = y^{-1}$, trebuie să avem:

$$1 = y^0 = y^{(-1)+} = y^{-1}y = zy.$$

Dacă y nu este egal cu 1 sau -1, această egalitate este falsă. Deci nu putem prelungi la $\mathbf{Z}$ exponenţierea din $\mathbf{N}$.

IV. *Să se dea exemple de inele unitare. Să se compare în aceste inele mulţimea elementelor regulate cu cea a elementelor inversabile.*

a) Să considerăm inelul $(\mathbf{Z}, +, \times)$. În acest inel, orice element nenul este regulat la înmulţire.
Într-adevăr:

$$xy = xz \Longleftrightarrow x(y - z) = 0 \qquad \text{(exerciţiul II)}.$$

Dacă: $x \neq 0$, deducem: $y - z = 0$; de unde:

$$\boxed{(x \neq 0 \text{ şi } xy = xz) \Longleftrightarrow (y = z)} \qquad (35)$$

Pe de altă parte, se știe că 1 și (−1) sînt singurele elemente inversabile (34).
Pentru ca un inel să fie integru, este necesar și suficient ca elementele sale nenule să fie toate regulate la înmulțire.

b) Să considerăm inelul $(\mathbf{D}, +, \times)$ al numerelor zecimale:

$$n = 10^x \cdot y \qquad (x \in \mathbf{Z},\ y \in \mathbf{Z}).$$

Cum este o submulțime a corpului $(\mathbf{Q}, +, \times)$ al numerelor raționale, **D** este un inel integru.
Toate elementele sale nenule sînt regulate.
Elementele inversabile ale lui **D** sînt acelea pentru care se poate scrie o egalitate de genul:

$$|y| = 2^p 5^q \ (p \in \mathbf{N},\ q \in \mathbf{N}).$$

c) Să considerăm un corp $(\mathbf{K}, +, \times)$: orice element nenul este în același timp inversabil și regulat.
Cu toate acestea, inelul matricelor pătrate de ordin 2 cu coeficienți reali (conform Geometriei I, clasa I CDE, pagina 153) nu este un corp; dar există încă identitate între mulțimea elementelor inversabile și aceea a elementelor regulate (sînt matricele de determinant nenul).
În cazul general, orice element inversabil este evident regulat. Exemplele de mai sus arată că nu se poate spune nimic cu privire la reciprocă.

EXERCIȚII

2.6. Să se demonstreze egalitățile:

$$[(x + y) + z] + t = (x + y) + (z + t);$$

$$\{[(x + y) + z] + t\} + s = (x + y) + [(z + t) + s].$$

2.7. Punem în **Z**:

$$x * y = x + y + 1.$$

Să se studieze proprietățile acestei operații.

2.8. O submulțime H a unui grup G este un subgrup dacă nu este vidă și dacă formează un grup pentru restricția la H a operației grupului. Să se demonstreze că elementul neutru al lui H și opusul în H al elementului a din H sînt egale cu elementul neutru al lui G și cu opusul lui a în G.

2.9. Să se determine intersecția tuturor subgrupurilor lui $(\mathbf{Z}, +)$ care conțin întregul (-3). Este aceasta un grup?

2.10. Să se rezolve, în $(\mathbf{Z}, +)$, ecuația:

$$x + x + x = a + a + a.$$

2.11. Plecînd de la axiomele înmulțirii să se demonstreze direct egalitățile:

$$x^+y = xy + y,$$

$$x^-y + y = xy.$$

2.12. Să se reia exercițiul nr. **2.6** pentru înmulțire.

2.13. Să se calculeze prin recurență valoarea expresiei:

$$+(n \times m) + (+n) \times (-m) \qquad (n \in \mathbf{N},\ m \in \mathbf{N}).$$

2.14. Există un inel cu două elemente?
(Se vor găsi două soluții.)

2.15. Să se demonstreze asociativitatea și comutativitatea adunării definite prin egalitățile (3), (22), (28) și (29).

2.16. Să se exprime suma $x + y$ în mod unic cu ajutorul literelor x, y, repetate de atîtea ori de cîte ori este necesar, și al semnului „−".

2.17. Să se studieze, pe $\mathbf{Z}$, ecuația $xy = 2$.

2.18. Același exercițiu pentru $x^2 = x$.

2.19. Să se definească, pe $\mathbf{Z}$, o exponențiere parțială, adică o aplicație de la $\mathbf{Z} \times \mathbf{N}$ la $\mathbf{Z}$, notată $(x, y) \longmapsto x^y$, care prelungește pe cea din $\mathbf{N}$.
Să se calculeze suma:

$$(-2)^n + (-2)^{n+1} + \ldots + (-2)^{n+p}.$$

2.20. *Urmare a exercițiului* nr. 2.5:

3° Să se studieze adunarea definită pe $\mathbf{N} \times \mathbf{N}$ prin egalitatea:

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

4° Să se demonstreze că este compatibilă cu relația de echivalență $\sim$, adică avem:

$$[(a, b) \sim (s, t) \text{ și } (c, d) \sim (u, v)] \Longrightarrow [(a, b) + (c, d)] \sim [(s, t) + (u, v)].$$

5° Să se deducă o adunare în mulțimea cît care face din aceasta un grup comutativ.

2.21. *Urmare a exercițiului* nr. 2.20.

6° Să se studieze înmulțirea definită pe $\mathbf{N} \times \mathbf{N}$ prin egalitatea:

$$(a, b) \times (c, d) = (ac + bd, ad + bc).$$

7° Să se demonstreze că este compatibilă cu echivalența $\sim$.

8° Să se deducă o înmulțire în mulțimea cît care împreună cu adunarea definită la nr. 5°, face din aceasta un inel comutativ unitar.

2.22. *Urmare a exercițiului* nr. 2.21.

9° Să se demonstreze că această mulțime cît conține o submulțime legată de $\mathbf{N}$ printr-o bijecție care respectă adunarea și înmulțirea din $\mathbf{N}$.

10° Să se demonstreze că orice element nenul este regulat la înmulțire.

11° Să se demonstreze că există o bijecție între mulțimea cît și $\mathbf{Z}$ care este un izomorfism pentru adunare și înmulțire.

2.23. Se consideră cele două legi definite pe $\mathbf{Z} \times \mathbf{Z}$ prin egalitățile:

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

$$(a, b) \times (c, d) = (ac, ad + bc).$$

1° Să se verifice că se obține astfel un inel comutativ unitar.

2° Punînd $\varepsilon = (0,1)$, să se calculeze ε^2. Să se compare (a, b) și $[(a, 0) + (b, 0)\,\varepsilon]$.
Să se calculeze $(a, b)^2$.

2.3. INEGALITĂȚI

2.3.1. Ordine

Relația de ordine în $\mathbf{Z}$ este evident la fel cu cea din $\mathbf{N}$.
Prin definiție, vom lua echivalența:

$$\boxed{(x \geqslant y) \Longleftrightarrow [\exists z,\ z \in \mathcal{P} \cup \{0\},\ x = y + z]} \qquad (36)$$

care ne dă o prelungire a relației analoage în N. Vom pune și aici:

$$(x > y) \Longleftrightarrow (x \geqslant y \text{ și } x \neq y) \tag{37}$$

1. Să notăm relațiile imediate:

$$\begin{array}{l} x \in \mathcal{P} \cup \{0\} \Longleftrightarrow x \geqslant 0 \Longleftrightarrow 0 \geqslant -x \\ x \in \mathcal{P} \Longleftrightarrow x > 0 \Longleftrightarrow x \geqslant 1 \\ x \in \mathcal{N} \cup \{0\} \Longleftrightarrow x \leqslant 0 \Longleftrightarrow 0 \leqslant -x \\ x \in \mathcal{N} \Longleftrightarrow x < 0 \Longleftrightarrow x \leqslant -1 \\ x + 1 > x > x - 1 \text{ etc.} \end{array}$$

2. Raționamentele de la paginile 35 și următoarele se aplică integral și arată că relația definită mai înainte este într-adevăr o relație de ordine, compatibilă cu adunarea; se arată de asemenea relațiile:

$$\begin{array}{ll} x \geqslant x; \quad (x \geqslant y \text{ și } y \geqslant z) \Longrightarrow (x \geqslant z) & (38)\ (39) \\ (x \geqslant y \text{ și } y \geqslant x) \Longrightarrow (x = y) & (40) \\ (x > y \text{ și } y > z) \Longrightarrow (x > z) & (41) \\ (x \geqslant y) \Longleftrightarrow (x + z \geqslant y + z) & (42) \\ (x > y) \Longleftrightarrow (x + z > y + z) & (43) \end{array}$$

În particular:

$$\begin{array}{ll} x \geqslant y \Longleftrightarrow -y \geqslant -x & (44) \\ x > y \Longleftrightarrow -y > -x & (45) \end{array}$$

(Să se pună $z = -x - y$ în ultimele două echivalențe.)

3. Să studiem relațiile între înmulțire și ordine pe **Z**: ele fac din $(\mathbf{Z}, +, \times)$ un *inel ordonat*

Știm că produsul a două elemente ale lui $\mathcal{P} \cup \{0\}$ aparține lui $\mathcal{P} \cup \{0\}$, și că produsul a două elemente din $\mathcal{P}$ aparține lui $\mathcal{P}$.

Or:

$$(x \geqslant y \text{ și } z \geqslant 0) \Longleftrightarrow (x - y \in \mathcal{P} \cup (0) \text{ și } z \in \mathcal{P} \cup \{0\});$$

$$(x > y \text{ și } z > 0) \Longleftrightarrow (x - y \in \mathcal{P} \text{ și } z \in \mathcal{P}).$$

În consecință:

$$\begin{array}{ll} (x \geqslant y \text{ și } z \geqslant 0) \Longrightarrow (xz \geqslant yz) & (46) \\ (x > y \text{ și } z > 0) \Longrightarrow (xz > yz) & (47) \end{array}$$

Se pot deduce ușor, cu ajutorul relațiilor:

$$z \geqslant 0 \Longleftrightarrow -z \leqslant 0, \quad (-x)y = -(xy),$$

implicațiile:

$$\boxed{(x \geqslant y \text{ și } z \leqslant 0) \Longrightarrow (xz \leqslant yz)} \quad (48)$$
$$\boxed{(x > y \text{ și } z < 0) \Longrightarrow (xz < yz)} \quad (49)$$

4. Să fixăm un întreg relativ y și un întreg strict pozitiv x; există atunci un întreg natural n astfel încît:

$$(nx > y).$$

Acest rezultat este cunoscut sub numele de *teorema lui Arhimede* (conform paginii 45). O vom demonstra aici, independent de proprietatea analoagă din N.

Dacă y este negativ sau nul, se va lua atunci $n = 1$, căci:

$$x1 = x > 0 \geqslant y,$$

de unde: $(x1 > y)$ (conform implicației (35), exercițiul IV).

Să presupunem deci y *strict pozitiv*.

Atunci, avem:

$$x(y + 1) \geqslant y + 1 > y,$$

și numărul $n = y + 1$ convine.

$$\boxed{(x > 0) \Longrightarrow (\forall_{\mathbf{Z}} y,\ \exists_{\mathbf{N}} n,\ nx > y)} \quad (50)$$

Se spune că $(\mathbf{Z}, +, \times)$ este un *inel arhimedian*.

5. Să arătăm în sfîrșit că ordinea astfel definită este o *ordine totală*. Diferența dintre doi întregi relativi x și y aparține obligatoriu uneia și numai uneia din cele trei mulțimi $\mathcal{P}$, $\{0\}$ sau $\mathcal{N}$. În consecință:

$$\boxed{(x \in \mathbf{Z} \text{ și } y \in \mathbf{Z}) \Longrightarrow (x > y \text{ sau } x = y \text{ sau } y > x)} \quad (51)$$

și:

$$\boxed{(x \in \mathbf{Z} \text{ și } y \in \mathbf{Z}) \Longrightarrow (x \geqslant y \text{ sau } y \geqslant x)} \quad (52)$$

6. Vom rezuma aceste proprietăți enunțînd următoarea teoremă:

TEOREMA 5 / **Relația de inegalitate între întregi relativi este definită în Z prin echivalența:**

$$(x \geqslant y) \Longleftrightarrow [\exists z,\ z \in \mathcal{P} \cup \{0\},\ x = y + z].$$

Este o relație de ordine totală, compatibilă cu adunarea din Z și înmulțirea cu un element pozitiv sau nul, care face din $(\mathbf{Z}, +, \times)$ un inel ordonat arhimedian.

Observație. — Un raționament analog celui de la pagina 38 arată că **Z** este integru.

2.3.2. Valoare absolută

O consecință importantă a teoremei 5 este existența unei *valori absolute* în **Z**. Să punem într-adevăr:

$$\boxed{|+n| = |-n| = n} \qquad (n \in \mathbf{N}) \qquad (53)$$

Egalitățile (15), (26) și (27) dau imediat egalitatea:

$$\boxed{|xy| = |x|\,|y|} \qquad (54)$$

Valoarea absolută este o surjecție de la **Z** pe **N**. Să notăm relațiile imediate:

$$\boxed{\begin{array}{l} |x| \geqslant 0 \\ |x| = 0 \Longleftrightarrow x = 0 \end{array}} \qquad \begin{array}{l} (55) \\ (56) \end{array}$$

Să comparăm în sfîrșit $|x+y|$ și $|x| + |y|$. Egalitățile (3), (22), (28) și (29) arată că:

$$x = +n \text{ și } y = +m \Longrightarrow |x+y| = |x| + |y|;$$

$$x = -n \text{ și } y = -m \Longrightarrow |x+y| = |x| + |y|;$$

$$x = +n \text{ și } y = -m \text{ și } n \geqslant m \Longrightarrow |x+y| = |x| - |y| \leqslant |x| + |y|;$$

$$x = +n \text{ și } y = -m \text{ și } m \geqslant n \Longrightarrow |x+y| = -|x| + |y| \leqslant |x| + |y|.$$

În consecință:

$$\boxed{|x+y| \leqslant |x| + |y|} \qquad (57)$$

această inegalitate fiind, de fapt, o egalitate de fiecare dată cînd x și y sînt amîndoi pozitivi sau nuli sau amîndoi negativi sau nuli. Ea poartă numele de *inegalitatea triunghiului*. Relațiile (54), (55), (56) și (57) fac din $(\mathbf{Z}, +, \times)$ un inel cu *valoare absolută*.

EXERCIȚII

I. *Să se studieze inegalitatea:*

$$x^3 + y^3 + z^3 \geqslant 3xyz.$$

În ce caz are loc egalitatea?

Această inegalitate este echivalentă cu următoarea: $z^3 - (3xy)z + (x^3 + y^3) \geqslant 0$, așa cum se vede adăugînd $(-3xyz)$ în ambii membri. Formula binomului fiind valabilă în orice inel comutativ (a se vedea demonstrația acestei formule în cursul de Algebră I din

clasa I CDE, pagina 108, această demonstrație nefolosind decît distributivitatea, asociativitățile și comutativitățile), putem scrie încă:

$$z^3 - (3xy)z + (x + y)^3 - 3xy\,(x + y) \geqslant 0,$$

sau încă:

$$[z^3 + (x + y)^3] - 3xy\,[z + (x + y)] \geqslant 0,$$

adică:

$$(z + x + y)(z^2 - z[x + y] + [x + y]^2 - 3xy) \geqslant 0,$$

sau în sfîrșit:

$$(x + y + z)(z^2 - [x + y]\,z + x^2 - xy + y^2) \geqslant 0,$$

Să studiem semnul celui de-al doilea factor; este și semnul dublului său:

$$2z^2 - 2(x + y)\,z + 2x^2 - 2xy + 2y^2 = (z - x)^2 + (z - y)^2 + (x - y)^2.$$

După proprietățile lui N, o astfel de sumă de elemente pozitive sau nule (26) este strict pozitivă, în afara cazului cînd întregii x,y și z sînt egali: ea este atunci nulă.
Inegalitatea propusă este deci verificată în următoarele două cazuri:
a) sau: $x = y = z$ (avem atunci egalitate);
b) sau: $x + y + z \geqslant 0$
(atunci nu avem egalitate decît dacă și numai dacă $x + y + z = 0$).

II. *Să se demonstreze inegalitatea lui Cebîșev;*

$$[x_1 \leqslant x_2 \leqslant \ldots \leqslant x_n \text{ și } y_1 \leqslant y_2 \leqslant \ldots \leqslant y_n] \Longrightarrow$$
$$\Longrightarrow [(x_1 + x_2 + \ldots + x_n)(y_1 + y_2 + \ldots + y_n) \leqslant n(x_1y_1 + x_2y_2 + \ldots + x_ny_n)].$$

Să considerăm doi indici i și j, nu neapărat distincți, luați între 1 și n. Putem scrie atunci:

$$x_i - x_j \geqslant 0, \qquad y_i - y_j \geqslant 0,$$

sau:

$$x_i - x_j \leqslant 0, \qquad y_i - y_j \leqslant 0.$$

În amîndouă cazurile, produsul $(x_i - x_j)\,(y_i - y_j)$ este pozitiv sau nul; deci:

$$(x_i - x_j)\,(y_i - y_j) = x_iy_i + x_jy_j - x_iy_j - x_jy_i \geqslant 0.$$

Se obțin astfel n^2 întregi relativi pozitivi sau nuli, care se pot aduna între ei, ceea ce dă inegalitatea:

$$\sum_{i=1}^{n}\sum_{j=1}^{n}(x_iy_i + x_jy_j - x_iy_j - x_jy_i) = \left(2n\sum_{i=1}^{n}x_iy_i\right) - 2\left(\sum_{i=1}^{n}\sum_{j=1}^{n}x_iy_j\right) =$$
$$= 2\left[n\left(\sum_{i=1}^{n}x_iy_i\right) - \left(\sum_{i=1}^{n}x_i\right)\left(\sum_{j=1}^{n}y_j\right)\right] \geqslant 0.$$

De aici se deduce inegalitatea cerută.
Ea nu devine o egalitate decît dacă și numai dacă fiecare din întregii $(x_i - x_j)\,(y_i - y_j)$ este nul, deci dacă și numai dacă toți x_i sînt egali sau dacă și numai dacă toți y_j sînt egali (dacă doi x_i sînt distincți, atunci:

$$(x_1 \neq x_n) \Longrightarrow (y_1 = y_n),$$

de unde:

$$y_1 = y_2 = \ldots = y_{n-1} = y_n).$$

III. *Să se demonstreze inegalitatea în N:*

$$(x_1 + x_2 + \ldots + x_n)^3 \leqslant n^2(x_1^3 + x_2^3 + \ldots + x_n^3).$$

Putem presupune întotdeauna că întregii pozitivi x_i sînt aranjaţi în ordine crescătoare. Să punem atunci $y_j = x_j^2$: întregii y_j sînt aranjaţi în ordine crescătoare. Inegalitatea lui Cebîşev se scrie atunci:

$$n\sum_{i=1}^{n} x_i^3 \geqslant \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} x_i^2\right).$$

Putem scrie din nou inegalitatea lui Cebîşev, luînd de astă dată $y_j = x_j$:

$$n\sum_{i=1}^{n} x_i^2 \geqslant \left(\sum_{i=1}^{n} x_i\right)^2.$$

În final, suma $\left(\sum x_i\right)$ fiind pozitivă sau nulă, putem înmulţi cu ea aceste inegalităţi ceea ce ne dă relaţia cerută.
Nu are loc egalitatea decît dacă numerele x_i sînt toate egale.

IV. *Să se studieze în* **Z** *legea definită prin egalitatea:*

$$x * y = |x - y|.$$

Această lege este comutativă. Nu are element neutru, altfel am avea:

$$e = e * e = |e - e| = 0,$$

şi:

$$x = x * e = |x - 0| = |x|,$$

ceea ce este fals în **Z** pentru x negativ.
Nu este asociativă. Într-adevăr:

$$(1 * 2) * 3 = 1 * 3 = 2,$$

$$1 * (2 * 3) = 1 * 1 = 0.$$

Toate elementele nu sînt regulate la această lege, deoarece:

$$1 * 2 = 1 * 0 \qquad (= 1).$$

În **N**, această lege are o restricţie care admite un element neutru ($e = 0$); orice element are un invers pentru această restricţie, deoarece:

$$x * x = 0 = e.$$

Ecuaţia ($a * x = b$) are întotdeauna cel puţin o soluţie (nu unică în general):

$$x = a + b.$$

(**N**, $*$) are deci unele proprietăţi ale unui grup dar nu pe principala, care este asociativitatea.

V. *Să se demonstreze următoarele relaţii, unde y este un întreg pozitiv:*

$$|x| \leqslant y \iff -y \leqslant x \leqslant y \tag{58}$$

$$|x| \leqslant y \iff x \leqslant y \text{ şi } -x \leqslant y \tag{59}$$

Aceste echivalenţe se folosesc foarte des, deşi nu se demonstrează decît rareori. Este adevărat că sînt foarte uşor de stabilit cu condiţia să distingem două cazuri:

■ $x = +n.$

Avem:

$$|x| \leqslant y \Longleftrightarrow n \leqslant y \Longleftrightarrow x \leqslant y,$$

inegalitatea $(-y \leqslant n)$ fiind atunci imediată, ca şi $(-n \leqslant y)$.

▩ $x = -n$.

Avem:

$$|x| \leqslant y \Longleftrightarrow n \leqslant y \Longleftrightarrow -x \leqslant y \Longleftrightarrow -y \leqslant x,$$

inegalitatea $(x \leqslant y)$ fiind atunci imediată.
De asemenea se pot scrie relaţii analoage cu semnul „<“:

$$\boxed{|x| < y \Longleftrightarrow -y < x < y \Longleftrightarrow x < y \text{ şi } -x < y} \qquad (60)$$

VI. *Să se demonstreze relaţiile:*

$$||x| - |y|| \leqslant |x + y|,$$

$$[|x + y| \leqslant n \text{ şi } |x - y| \leqslant n] \Longleftrightarrow [|x| + |y| \leqslant n].$$

Prima relaţie este o simplă consecinţă a inegalităţii triunghiului; într-adevăr, presupunînd spre exemplu că avem: $|x| \geqslant |y|$, este suficient să scriem:

$$\begin{aligned} ||x| - |y|| &= |x| - |y| \\ &= |(x + y) + (-y)| - |y| \leqslant |x + y| + |-y| - |y| \\ &= |x + y|. \end{aligned}$$

A doua relaţie este foarte diferită (ea ar fi falsă în alte inele cu valoare absolută cum ar fi corpul complecsilor, unde faptul că este falsă se arată de exemplu pentru $x = 2, y = 2i$, $n = 3$). A doua relaţie se poate demonstra după cum urmează:

$$|x + y| \leqslant n \Longrightarrow -n - y \leqslant x \leqslant n - y \text{ (conform exerciţiului V)},$$

$$|x - y| \leqslant n \Longrightarrow -n + y \leqslant x \leqslant n + y,$$

de unde rezultă cele patru inegalităţi:

$$\begin{aligned} &x + y \leqslant n, \\ &x - y \leqslant n, \\ &x + y \geqslant -n \qquad (\Longleftrightarrow -x - y \leqslant n) \\ &x - y \geqslant -n \qquad (\Longleftrightarrow -x + y \leqslant n). \end{aligned}$$

Una din aceste patru inegalităţi este în mod necesar inegalitatea căutată.

2.3.3. Submulţimi ale lui Z

Să considerăm o submulţime nevidă a lui **Z**. Contrar a ceea ce este adevărat în **N**, o astfel de submulţime nu admite în mod necesar un element minimum (este chiar cazul lui **Z**). Putem totuşi stabili două teoreme interesante.
Să presupunem că această submulţime M este minorată; există atunci un întreg relativ a astfel încît:

$$x \in M \Longrightarrow a \leqslant x.$$

Vom demonstra că în M există un element minimum. Pentru aceasta, să considerăm mulțimea M' obținută scăzînd întregul relativ a din toate elementele lui M:

$$y \in M' \iff a + y \in M.$$

M' este o submulțime a lui $\mathcal{P} \cup \{0\}$. Transferînd în $\mathcal{P} \cup \{0\}$ proprietățile lui **N**, se vede că M' admite un element minimum t; numărul $s = a + t$ este atunci un element minimum al lui M; s este evident unic.

TEOREMĂ 6 / **Orice submulțime nevidă și minorată a lui Z admite un element minimum unic.**

Să presupunem acum M nevidă și majorată. Considerînd mulțimea M'' a opușilor elementelor lui M, se deduce următoarea teoremă:

TEOREMĂ 7 / **Orice submulțime nevidă și majorată a lui Z admite un element maximum unic.**

Ca și în **N**, orice inegalitate strictă poate fi scrisă sub forma unei inegalități nestricte, și reciproc (fără nici o excepție de astă dată), datorită echivalențelor:

$$x \geqslant y \iff x > y - 1 \tag{61}$$
$$x \leqslant y \iff x < y + 1 \tag{62}$$

(sînt simple consecințe ale echivalenței:

$$z \geqslant 0 \iff z + 1 > 0).$$

Se deduce structura *intervalelor* lui **Z**, rezumată în următoarea teoremă:

TEOREMĂ 8 / **Nu există decît cinci feluri de intervale ale lui Z: intervalul *vid*, intervalele *mărginite* $[x, y]$, intervalele *infinite la dreapta* $[x, +\infty[$, intervalele *infinite la stînga* $]-\infty, x]$ și Z.**

EXERCIȚII

I. *Să se demonstreze că* **Z** *nu admite nici minimum, nici maximum.*
N neadmițînd element maximum, la fel se întîmplă și cu $\mathcal{P}$, deci și cu **Z**. Din contră, considerînd mulțimea $\mathcal{N}$, pentru care relația de ordine este relația opusă relației din **N**, se arată la fel că **Z** nu are element minimum.

II. *Să se demonstreze teorema* 8.

Orice interval I nemajorat este astfel încît:

$$\forall_{\mathbf{Z}} x, \ \exists_I y \ \ y > x.$$

Prin urmare:

$$(z \in I \text{ și } x \geqslant z) \Longrightarrow (x \in I).$$

Dacă I este nevid și minorat, I admite un minimum s. Deci:

$$x \geqslant s \Longleftrightarrow x \in I,$$

și:

$$I = [s, +\infty[.$$

Dacă I nu este minorat, același raționament arată că:

$$(z \in I \text{ și } x \leqslant z) \Longrightarrow (x \in I),$$

și:

$$I = Z.$$

Să presupunem acum I nevid și majorat. El admite un maximum t. Implicația de mai sus arată că, dacă I nu este minorat, I este egal cu $]-\infty, t]$ (se va pune $z = t$).
Dacă I este în același timp nevid, minorat și majorat (se spune că I este mărginită), el admite un minimum s, de unde:

$$(x \in I) \Longleftrightarrow (s \leqslant x \leqslant t),$$

și:

$$I = [s, t].$$

Observație. — Se poate demonstra că intervalele finite nevide ale lui **Z** sînt intervale mărginite (conform paginii 53), că intervalele infinite la dreapta sau la stînga sînt izomorfe cu **N**, deci cu **Z**.

2.3.4. Definiții axiomatice ale lui Z

Să dăm aici, fără demonstrație, două axiomatizări ale lui **Z** analoage cu axiomatizările lui **N** de la paginile 27 și 45.

A1 Există o bijecție f, numită *succesiune* între Z și Z.

A2 Orice submulțime nevidă a lui Z care conține imaginea prin f și imaginea prin f^{-1} a tuturor elementelor sale se confundă cu Z.

A3 Z este infinită *(această axiomă echivalează, spre exemplu, cu existența unei injecții nesurjective de la Z în Z.)*

Aceste axiome seamănă cu cele ale lui Peano (și le sînt chiar echivalente, în măsura în care există o bijecție între **N** și **Z**). Datorită lor, succesiunea joacă un rol esențial. Se poate verifica că paragrafele 2.2 și 2.3 pot fi stabilite unic cu ajutorul acestor axiome, fără a recurge la teoria lui **N**.

A'1 Z este o mulțime total ordonată.

A'2 Z nu admite nici maximum nici minimum.

A'3 Orice submulțime nevidă și minorată a lui Z admite un element minimum.

A'4 Orice submulțime nevidă și majorată a lui Z admite un element maximum.

Fiecare din aceste două axiomatizări este formată din axiome independente.

EXERCIȚIU

Să se demonstreze independența axiomei A'1 în raport cu axiomele A'2, A'3 și A'4.

Este suficient să considerăm mulțimea (2, 3, 4, 9) înzestrată cu relația de divizibilitate, care este o relație de ordine.

EXERCIȚII

2.24. Să se demonstreze relațiile de la începutul paragrafului nr. **2.3.1.**

2.25. Să se demonstreze direct că relația „$\leqslant$" definită pe **Z** prin următoarele trei proprietăți:

$$m \leqslant n \Longleftrightarrow (+m) \leqslant (+n) \qquad (m \in \mathbf{N},\ n \in \mathbf{N}),$$
$$m \leqslant n \Longleftrightarrow (-n) \leqslant (-m),$$
$$(-m) \leqslant (+n),$$

este o relație de ordine totală, care coincide cu relația definită la nr. **2.3.1.**

2.26. Se pune, în **Z**:

$$x - y = z, \quad u - v = w.$$

Să se demonstreze implicația:

$$(z > w) \Longrightarrow (x - u > y - v).$$

2.27. Să se reia exercițiile nr. 1.30, 1.31, 1.33, 1.34, 1.35 (pagina 51). Cum trebuie modificate enunțurile pentru ca să se aplice la **Z**?

2.28. Să se reia exercițiul nr. 1.39 (pagina 52) în **Z.**

2.29. Să se demonstreze implicațiile (48) și (49).

2.30. Să se rezolve direct exercițiile rezolvate II și III de la paginile 90 și 91 pentru $n = 2$ și $n = 3$.

2.31. Să se demonstreze proprietatea enunțată în observația care termină paragraful nr. **2.3.3.**

2.32. Să se determine în **Z** mulțimea numerelor x astfel încît să avem:

$$x^2 - 3x < 28.$$

2.33. Să se demonstreze, în **Z**, implicațiile:

$$(0 \leqslant x < y) \Longrightarrow (x^2 < y^2),$$
$$(x < y) \Longrightarrow (x^3 < y^3).$$

Ce se poate spune despre reciproce?

2.34. *Urmare a exercițiului* nr. **2.22.**

12° Să se definească, pe mulțimea cît studiată, o relație de ordine care are proprietățile celei definite pe **Z.**

13° Să se extindă izomorfismul definit la 11° la această relație de ordine.

2.4. CONGRUENȚE ȘI ÎMPĂRȚIRE EUCLIDIANĂ

2.4.1. Multipli

Fie x un întreg relativ. Să-i asociem submulțimea notată $x\mathbf{Z}$ a *multiplilor* săi:

$$\boxed{y \in x\mathbf{Z} \iff \exists_{z \in \mathbf{Z}}\, y = xz} \tag{63}$$

Se spune atunci că: y este un multiplu al lui x, x *divide* pe y, x este un *divizor* al lui y, aceste trei expresii fiind echivalente. De exemplu:

$$0\mathbf{Z} = \{0\}, \qquad 1\mathbf{Z} = (-1)\mathbf{Z} = \mathbf{Z}.$$

În cazul general:

$$\boxed{n\mathbf{Z} = (-n)\mathbf{Z}} \qquad (n \in \mathbf{N}). \tag{64}$$

Este deci inutil să studiem mulțimile multiplilor de întregi strict negativi. $2\mathbf{Z}$ este mulțimea numerelor *pare*, $\mathbf{Z} - 2\mathbf{Z}$ acea a numerelor *impare*; 1 este *impar*, căci:

$$(1 = 2z = z + z) \Longrightarrow (z > 0 \text{ și } 1 > z),$$

ceea ce este imposibil (61).
Mulțimea $n\mathbf{Z}$ este *închisă* în raport cu adunarea, adică:

$$\boxed{(x \in n\mathbf{Z} \text{ și } y \in n\mathbf{Z}) \Longrightarrow (x + y \in n\mathbf{Z})} \tag{65}$$

Într-adevăr:

$$(x = nz \text{ și } y = nt) \Longrightarrow [x + y = n(z + t)].$$

Mulțimea $n\mathbf{Z}$ este închisă în raport cu înmulțirea cu un întreg oarecare, adică:

$$\boxed{(x \in n\mathbf{Z} \text{ și } y \in \mathbf{Z}) \Longrightarrow (xy \in n\mathbf{Z})} \tag{66}$$

Într-adevăr:

$$x = nz \Longrightarrow xy = n(zy).$$

Mulțimea $n\mathbf{Z}$ este deci închisă în raport cu înmulțirea, ca și în raport cu opoziția:

$$\boxed{(x \in n\mathbf{Z}) \Longrightarrow (-x \in n\mathbf{Z})} \tag{67}$$

Într-adevăr:

$$x = nz \text{ și } y = nt \Longrightarrow xy = n(nzt)$$
$$(-x) = x(-1).$$

Adunarea și înmulțirea, bine definite pe $n\mathbf{Z}$, au aici proprietățile de asociativitate, de comutativitate și de distributivitate pe care le au în $\mathbf{Z}$. (Totuși nu se păstrează toate proprietățile; astfel, $n\mathbf{Z}$ nu este unitar, în afară de cazul cînd $n = 1$). În consecință, putem enunța:

TEOREMĂ 9 / **Submulțimea $n\mathbf{Z}$ a multiplilor unui întreg pozitiv sau nul este un inel comutativ. Orice mulțime a multiplilor unui întreg relativ este de acest tip.**

Observație. — Pentru a traduce implicația (66), mai tare decît prin simpla închidere relativă la înmulțire, se spune că $n\mathbf{Z}$ este un *ideal* al inelului comutativ $\mathbf{Z}$.

2.4.2. Congruențe

Să considerăm, în $\mathbf{Z}$, relația binară:

$$\boxed{x \equiv y \Longleftrightarrow x - y \in n\mathbf{Z}} \tag{68}$$

Cum ea depinde de numărul pozitiv sau nul n, se notează:

$$x \equiv y \mod n,$$

sau încă:

$$\boxed{x \equiv y \ [n]}$$

(se citește: x este congruent cu y modulo n). Se numește *congruență modulo n*; n este *modulul*.
Congruența modulo 0 este egalitatea. Congruența modulo 1 este verificată pentru orice pereche (x, y).

1. O congruență este o *relație de echivalență*. Într-adevăr:

$$(x - x = 0 \text{ și } 0 \in n\mathbf{Z}) \Longrightarrow \boxed{x \equiv x} \tag{69}$$

$$\begin{aligned}&(x \equiv y \text{ și } y \equiv z)\\ &\Longrightarrow (x - y \in n\mathbf{Z} \text{ și } y - z \in n\mathbf{Z})\\ &\Longrightarrow [(x - y) + (y - z) \in n\mathbf{Z}] \Longrightarrow (x - z \in n\mathbf{Z})\\ &\Longrightarrow (x \equiv z);\end{aligned}$$

$$\boxed{(x \equiv y \text{ și } y \equiv z) \Longrightarrow (x \equiv z)} \tag{70}$$

$(x \equiv y) \Longrightarrow (x - y \in n\mathbf{Z})$
$\Longrightarrow [-(x - y) \in n\mathbf{Z}] \Longrightarrow [(y - x) \in n\mathbf{Z}]$
$\Longrightarrow (y \equiv x)$.

$$\boxed{(x \equiv y) \Longrightarrow (y \equiv x)} \tag{71}$$

Relațiile (69), (70) și (71) traduc respectiv *reflexivitatea*, *tranzitivitatea* și *simetria* relației studiate.

2. Această relație este *compatibilă* cu adunarea. Într-adevăr:

$(x \equiv y) \Longrightarrow [(x - y) \in n\mathbf{Z}]$
$\Longrightarrow [(x + z) - (y + z) \in n\mathbf{Z}]$
$\Longrightarrow (x + z \equiv y + z)$.

Mai general:

$$\boxed{(x \equiv y \text{ și } z \equiv t) \Longrightarrow (x + z \equiv y + t)} \tag{72}$$

(este suficient să operăm în doi timpi).

3. Această relație este compatibilă cu înmulțirea. Într-adevăr:

$(x \equiv y) \Longrightarrow [(x - y) \in n\mathbf{Z}] \Longrightarrow [(x - y)z \in n\mathbf{Z}]$
$\Longrightarrow [xz - yz \in n\mathbf{Z}] \Longrightarrow (xz \equiv yz)$.

Mai general:

$$\boxed{(x \equiv y \text{ și } z \equiv t) \Longrightarrow (xz \equiv yt)} \tag{73}$$

(este suficient să operăm în doi timpi).

4. Vom rezuma aceste propoziții enunțînd următoarea teoremă:

TEOREMĂ 10 / **Relația de congruență modulo n între întregi relativi este definită pe Z prin echivalența:**

$$x \equiv y \quad [n] \Longleftrightarrow x - y \in n\mathbf{Z}.$$

Este o relație de echivalență, compatibilă cu adunarea și înmulțirea pe Z. Se pot aduna sau înmulți membru cu membru două congruențe de același modul.

Relație de echivalență	$x \equiv x$; $(x \equiv y$ și $y \equiv z) \Longrightarrow (x \equiv z)$ $(x \equiv y) \Longrightarrow (y \equiv x)$
Compatibilități	$(x \equiv y$ și $z \equiv t) \Longrightarrow (x + z \equiv y + t)$ $(x \equiv y$ și $z \equiv t) \Longrightarrow (xz \equiv yt)$

EXERCIȚIU

Să se determine toți întregii relativi x astfel încît:

$$x^2 + x + 1 \equiv 0 \quad [4].$$

Dacă această problemă ar avea o soluție, s-ar putea scrie atunci egalitatea:

$$x(x + 1) + 1 = 4y,$$

sau încă:

$$1 = 4y - x(x + 1).$$

Or, numărul $x(x + 1)$ este un număr par. Într-adevăr, aceasta este adevărat pentru $x = 0$; dacă este adevărat pentru x, atunci, este adevărat și pentru $x^+(x^+ + 1)$ și $x\ (x + 1)$, căci:

$$x^+(x^+ + 1) = (x + 1)\ (x + 2) = x(x + 1) + 2(x + 1),$$

$$x^-(x^- + 1) = (x - 1)x = x(x + 1) + 2(-x).$$

1 ar fi deci un număr par, ceea ce nu este adevărat. Problema n-are deci nici o soluție.

2.4.3. Inelul $\mathbf{Z}/n\mathbf{Z}$

Să considerăm mulțimea $\mathbf{Z}/n\mathbf{Z}$, numită *mulțime cît*, a *claselor de echivalență* relative la congruența modulo n. Să alegem două elemente α și β din această mulțime; α este, de exemplu, clasa unui întreg x, și β aceea a unui întreg z. Fie, în mulțimea α și β, doi alți întregi y și t; avem:

$$x \equiv y, \quad z \equiv t.$$

Egalitățile (72) și (73) arată atunci că avem:

$$x + z \equiv y + t, \quad xz \equiv yt.$$

Clasele de echivalență ale întregilor $(x + z)$ și (xz) nu depind deci decît de α și β, și nu de alegerile particulare ale lui x și z în aceste clase. Putem deci defini pe $\mathbf{Z}/n\mathbf{Z}$ două legi cît, notate „$+$" și „$\cdot$", induse de legile inelului $(\mathbf{Z}, +, \cdot)$. Avem:

$$(x \in \alpha \text{ și } z \in \beta) \Longrightarrow [(x + z) \in (\alpha + \beta)]; \tag{74}$$

$$(x \in \alpha \text{ și } z \in \beta) \Longrightarrow x \cdot z \in \alpha \cdot \beta. \tag{75}$$

Notînd $\bar{x}$ clasa întregului x, se pot scrie următoarele egalități:

$$\bar{x} + \bar{y} = \overline{x + y};$$

$$\bar{x} \cdot \bar{y} = \overline{x \cdot y};$$

$$(\bar{x})^n = \overline{x^n}.$$

Observație. — În membrul stîng al fiecărei egalități, adunarea și înmulțirea sînt operații pe $\mathbf{Z}/n\mathbf{Z}$, în timp ce în membrul din dreapta, sînt operații pe inelul $\mathbf{Z}$.

EXERCIȚIU

Să se determine x astfel incît:

$$3^{2n} - 2^n \equiv x \ [7].$$

Avem succesiv:

$$3^{2n} - 2^n = \bar{x},$$

$$(\bar{9})^n - (\bar{2})^n = \bar{x};$$

or:

$$9 \equiv 2 \ [7];$$

de unde:

$$(\bar{9})^n = (\bar{2})^n,$$

deci:

$$\bar{2}^n - \bar{2}^n = \bar{x},$$

sau:

$$\bar{x} = \bar{0}.$$

Să considerăm cele nouă axiome ale inelului comutativ unitar (două asociativități, două comutativități, două existențe de elemente neutre, două distributivități, o existență a opusului). Fiecare dintre ele dă naștere la o axiomă analoagă pentru mulțimea $\mathbf{Z}/n\mathbf{Z}$. De exemplu:

$$(x + z) = (z + x) \Longrightarrow (\alpha + \beta = \beta + \alpha).$$

$\mathbf{Z}/n\mathbf{Z}$ este deci de asemenea un inel comutativ unitar. Elementele neutre din $\mathbf{Z}/n\mathbf{Z}$ sînt respectiv $\bar{0}$ și $\bar{1}$ deoarece, de exemplu:

$$(x + 0 = 0 + x = x) \Longrightarrow (\alpha + \bar{0} = \bar{0} + \alpha = \alpha).$$

Observație. — Nu toate proprietățile lui $\mathbf{Z}$ se conservă obligatoriu în $\mathbf{Z}/n\mathbf{Z}$. Astfel, faptul că $\mathbf{Z}$ este integru:

$$x \neq 0 \text{ și } z \neq 0 \Longrightarrow xz \neq 0$$

nu generează nici o proprietate particulară; aceasta provine din cauza neegalităților în $\mathbf{Z}$ care nu se traduc neapărat în neegalități în $\mathbf{Z}/n\mathbf{Z}$. De altfel, pentru $n = 6$:

$$3 \neq 0, \ 2 \neq 0, \ 6 \neq 0,$$

dar:

$$\bar{3} \neq \bar{0}, \ \bar{2} \neq \bar{0}, \ \bar{6} = \bar{0}.$$

Vom rezuma aceste propoziții enunțînd următoarea teoremă:

TEOREMĂ 11 / **Mulțimea cît definită pe Z prin relația de congruență modulo n este un inel comutativ unitar, notat $(\mathbf{Z}/n\mathbf{Z}, +, \times)$ sau $\mathbf{Z}/n\mathbf{Z}$.**

EXERCIȚII

I. *Să se determine relațiile de ordine totală care se pot defini pe inelul $\mathbf{Z}/n\mathbf{Z}$ $(n \neq 0)$ care sînt compatibile cu adunarea din acest inel.*

Problema nu prezintă interes decît dacă n este mai mare ca 1, căci pentru $n = 1$, $\mathbf{Z}/n\mathbf{Z}$ nu conține decît un singur element: pe $\mathbf{Z}$. Clasa $\overline{1}$ nu este deci $\overline{0}$. Să presupunem că am avea $\overline{1}$ mai mare ca $\overline{0}$ pentru o anumită relație de ordine totală. Atunci:

$$\overline{2} = \overline{1+1} = \overline{1} + \overline{1} > \overline{1} + \overline{0} = \overline{1} > \overline{0},$$

$$\overline{3} = \overline{2+1} = \overline{2} + \overline{1} > \overline{2} > \overline{0}, \text{ etc...}$$

Prin recurență: $\overline{n} = \overline{n-1+1} = \overline{n-1} + \overline{1} > \overline{n-1} > \overline{0}$,

Or: $\overline{n} = \overline{0}$; se ajunge deci la o contradicție. Inelul $\mathbf{Z}/n\mathbf{Z}$ nu poate fi ordonat în acest mod.

Inegalitatea $\overline{1} < \overline{0}$ ar da la fel:

$$\overline{2} = \overline{1+1} = \overline{1} + \overline{1} < \overline{1} + \overline{0} = \overline{1} < \overline{0}, \text{ etc.}$$

II. *Se consideră șirul definit pe $\mathbf{Z}$ prin egalitatea:*

$$u_n = 9n^2 - 6n - 1 + (-2)^n,$$

unde $(-2)^n$ este definit prin relația de recurență:

$$(-2)^0 = 1, \quad (-2)^{n'} = -2(-2)^n.$$

Să se calculeze u_n pentru: $n \leqslant 3$. Să se calculeze $u_{n+1} + 2u_n$.

Să se deducă clasa lui u_n în $\mathbf{Z}/27\mathbf{Z}$.

Calculul ne dă ușor:

$$u_0 = u_1 = 0, \quad u_2 = 27, \quad u_3 = 54.$$

În $u_{n+1} + 2u_n$, termenii în $(-2)^n$ se elimină, și rămîne:

$$u_{n+1} + 2u_n = 9[(n+1)^2 + 2n^2] - 6[n + 1 + 2n] - 3$$

$$= 27\, n^2.$$

În consecință: $\overline{u_{n+1}} = \overline{27n^2} - \overline{2u_n} = -\overline{2u_n}$.

Cum $\overline{u_0} = \overline{0}$, deducem, prin recurență, $\overline{u_n} = \overline{0}$; pentru orice n, există deci un întreg m în $\mathbf{Z}$ astfel încît:

$$u_n = 27m.$$

2.4.4. Împărțire euclidiană pe Z

Să reamintim teorema lui Arhimede:

$$\boxed{(x > 0) \Longrightarrow (\forall_{\mathbf{Z}} y, \, \mathrm{E}_{\mathbf{N}} n, \; nx > y)} \qquad (50)$$

Ea ne va permite să cunoaștem natura lui $\mathbf{Z}/n\mathbf{Z}$, pentru n diferit de zero.

1. Să considerăm doi întregi relativi a și b, cu b diferit de zero, și să definim o mulțime M de întregi relativi prin echivalența:

$$\boxed{(t \in M) \Longleftrightarrow (t \geqslant 0 \text{ și } \exists_{\mathbf{Z}} s,\ t = a - bs)}$$

Mulțimea M nu este vidă; este suficient să aplicăm teorema lui Arhimede întregilor $x = |b|$ și $y = -a$; se deduce existența unui întreg z astfel încît:

$$z\,|b| > -a,$$

sau:

$$t = a + |b|z > 0.$$

Se va lua atunci, după caz, $s = z$ sau $s = -z$. Mulțimea M are un element minimum r, deoarece această submulțime este nevidă și minorată (de 0); r este pozitiv sau nul. Dacă r ar fi mai mare sau egal cu $|b|$, am putea scrie relațiile:

$$r = a - bq \qquad (q \in Z),$$

$$0 \leqslant t = r - |b| = a - bs,$$

cu $s = q + 1$ sau $s = q - 1$ după caz; r n-ar fi atunci elementul minimum al lui M.

Există deci cel puțin o pereche (q, r) de întregi relativi astfel încît:

$$\boxed{a = bq + r, \qquad 0 \leqslant r < |b|} \tag{76}$$

2. Această pereche este unică. Într-adevăr, să presupunem că avem două perechi care satisfac aceleași relații; am putea scrie atunci, de exemplu:

$$0 = b(q_1 - q_2) + (r_1 - r_2),$$

de unde:

$$|b|\,|q_1 - q_2| = |r_2 - r_1|.$$

Dacă $(q_1 - q_2)$ n-ar fi nul, am avea atunci:

$$|q_1 - q_2| \geqslant 1, \quad |b|\,|q_1 - q_2| \geqslant |b|,$$

de unde, de exemplu:

$$|b| > r_2 \geqslant r_2 - r_1 = |r_2 - r_1| \geqslant |b|,$$

ceea ce este contradictoriu.

Deci:

$$q_1 = q_2 \text{ și } r_1 = r_2.$$

3. q și r sînt unice: q este *cîtul* și r este *restul împărțirii euclidiene* a întregului relativ a prin întregul relativ nenul b.

TEOREMĂ 12 / **Oricărei perechi de întregi relativi (a, b), unde b este diferit de zero, putem face să-i corespundă în mod unic o pereche (q, r) de întregi relativi astfel încît:**

$$a = bq + r, \qquad 0 \leqslant r < |b|.$$

Observație. — Cîtul q este bine determinat de dubla inegalitate:

$$0 \leqslant a - bq < |b|.$$

4. Să considerăm un element oarecare x al lui Z și un întreg strict pozitiv n. Împărțirea euclidiană:

$$x = nq + y, \qquad 0 \leqslant y < n$$

arată că x aparține clasei y. Inelul $\mathbf{Z}/n\mathbf{Z}$ conține deci, cel mult, n elemente:

$$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}.$$

Dacă două din aceste clase ar fi confundate, ar exista doi întregi m și p astfel încît:

$$0 \leqslant m < p < n, \; p - m \in nZ,$$

de unde:

$$p = 0n + p, \qquad 0 \leqslant p < n,$$
$$p = kn + m, \qquad 0 \leqslant m < n,$$

ceea ce contrazice unicitatea împărțirii lui p prin n.
$\mathbf{Z}/n\mathbf{Z}$ conține deci exact n elemente:

$$\boxed{\mathbf{Z}/n\mathbf{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}} \qquad (77)$$

TEOREMĂ 13 / **Inelul $\mathbf{Z}/n\mathbf{Z}$ unde n este un întreg strict pozitiv, conține n elemente pe care le putem defini ca fiind clasele întregilor din intervalul $[0, n-1]$.**

EXERCIȚIU

Să se compare cîturile în împărțirile lui a la n $(n \geqslant 1)$, și ale lui $(-a)$ la n.
Să scriem relațiile:

$$a = nq_1 + r_1, \qquad 0 \leqslant r_1 < n,$$
$$-a = nq_2 + r_2, \qquad 0 \leqslant r_2 < n.$$

Rezultă imediat:

$$-a = n(-q_1 - 1) + (n - r_1).$$

Dacă r_1 este diferit de 0, avem deci:

$$0 < n - r_1 < n.$$

Unicitatea împărțirii dă egalitatea:

$$q_2 = -q_1 - 1, \quad r_2 = n - r_1.$$

Dacă r_1 este nul, atunci:

$$-a = n(-q_1) + 0,$$

de unde:

$$q_2 = -q_1, \quad r_2 = r_1 = 0.$$

Suma a două cîturi este deci egală cu (-1), în afară de cazul cînd n divide pe a în care caz ea este nulă.

2.4.5. Împărțire euclidiană pe N

Să presupunem acum a pozitiv sau nul, b strict pozitiv. Împărțirea euclidiană se scrie:

$$a = bq + r, \qquad 0 \leqslant r < b,$$

r este pozitiv sau nul.
Să presupunem q strict negativ; rezultă:

$$q \leqslant -1, \; bq \leqslant -b,$$

$$a = bq + r \leqslant -b + r < 0,$$

ceea ce este fals; q este deci pozitiv sau nul.

TEOREMĂ 14 / **Oricărei perechi de întregi naturali (a, b), unde b este diferit de zero, putem face să-i corespundă în mod unic o pereche (q, r) de întregi naturali astfel încît:**

$$a = bq + r, \; 0 \leqslant r < b.$$

EXERCIȚII

1. *Fie a și b doi întregi strict pozitivi. Să se demonstreze că cel mai mic întreg strict pozitiv n astfel încît b să dividă pe an este un divizor al lui b.*
Să-l împărțim pe b prin n; rezultă:

$$b = nq + r, \quad 0 \leqslant r < n.$$

Întregul b divide pe an. În consecință:

$$an = bc,$$

$$ar = a(b - nq) = b(a - cq).$$

Deci: b divide pe ar.
Dacă r nu este nul, n nu este cel mai mic întreg cu proprietatea dorită; în consecință, $r = 0$ și n divide pe b.
(Existența lui n este asigurată prin faptul că b divide pe ab.)

II. *b fiind un număr strict pozitiv, să se compare cîturile q_1, q_2 și q_3 ale împărțitorilor lui a la b, lui $2a$ la b și lui $(2a + b)$ la $2b$.*

Avem succesiv:

$$a = bq_1 + r_1, \qquad 0 \leqslant r_1 < b;$$
$$2a = bq_2 + r_2, \qquad 0 \leqslant r_2 < b;$$
$$2a + b = 2bq_3 + r_3, \qquad 0 \leqslant r_3 < 2b;$$
$$2a = 2bq_1 + 2r_1, \qquad 2a + b = b(2q_1 + 1) + 2r_1.$$

Să presupunem că avem: $2r_1 < b$. Atunci:

$$b(2q_1) + 2r_1 = bq_2 + r_2$$

implică $2q_1 = q_2$.

Pe de altă parte:

$$2bq_3 + (b + 2r_1) = 2bq_3 + r_3 \ (b + 2r_1 < 2b)$$

implică $q_1 = q_3$.

În acest caz:

$$q_2 = 2q_1 = 2q_3.$$

Să presupunem din contră că avem:

$$b \leqslant 2r_1 < 2b.$$

Atunci:

$$b(2q_1 + 1) + (2r_1 - b) = bq_2 + r_2$$

implică $2q_1 + 1 = q_2$.

Pe de altă parte:

$$2b(q_3 + 1) + (2r_1 - b) = 2bq_3 + r_3$$

implică $q_1 + 1 = q_3$.

În acest caz:

$$q_2 = 2q_1 + 1 = 2q_3 - 1.$$

Să notăm spre exemplu, relația generală:

$$q_1 + q_3 = q_2.$$

III. *c fiind un număr strict pozitiv, a și b doi întregi relativi astfel încît:*

$$a \leqslant b,$$

să se demonstreze că numărul multiplilor lui c cuprinși între a și b (posibil egali) este egal cu $(1 + q_1 + q_2)$, unde q_1 și q_2 sînt cîturile împărțirilor lui $(-a)$ și lui b la c.

Să punem:

$$-a = cq_1 + r_1, \qquad 0 \leqslant r_1 < c;$$
$$b = cq_2 + r_2, \qquad 0 \leqslant r_2 < c.$$

Inegalitatea $a \leqslant b$ implică:

$$q_1 + q_2 > -2.$$

Se poate scrie:

$$a \leqslant cn \leqslant b,$$

dacă și numai dacă:

$$0 \leqslant c(n + q_1) + r_1, \qquad 0 \leqslant c(q_2 - n) + r_2,$$

sau încă:

$$-c < -r_1 \leqslant c(n + q_1), \qquad c(n - q_2) \leqslant r_2 < c,$$

ceea ce echivalează cu inegalitățile:

$$0 \leqslant c(n + q_1), \qquad c(n - q_2) \leqslant 0,$$

adică în sfîrșit:

$$0 \leqslant n + q_1, \qquad n - q_2 \leqslant 0,$$

sau:

$$-q_1 \leqslant n \leqslant q_2,$$

ceea ce demonstrează teorema studiată, chiar dacă $q_2 = -q_1 - 1$.
Se poate deduce că, pentru $a = b$, q_1 și q_2 sînt opuși dacă și numai dacă c divide pe a. Dacă nu: $q_1 = -q_2 - 1$ (conform exercițiului de la paragraful **2.4.4**, pagina 103).

IV. *b și c fiind două numere strict pozitive, să se compare cîtul q_1 al împărțirii unui întreg a a bc cu cîtul q_2 al împărțirii la c a cîtului q_3 al împărțirii lui a la b.*

*I*Avem succesiv:

$$a = bcq_1 + r_1, \qquad 0 \leqslant r_1 < bc;$$
$$a = bq_3 + r_3, \qquad 0 \leqslant r_3 < b;$$
$$q_3 = cq_2 + r_2, \qquad 0 \leqslant r_2 < c - 1.$$

Rezultă:

$$a = b(cq_2 + r_2) + r_3 = bcq_2 + (br_2 + r_3)$$
$$a \leqslant bcq_2 + b(c - 1) + r_3$$
$$a < bcq_2 + b(c - 1) + ba < bcq_2 + bc.$$

După unicitatea cîtului, se deduce egalitatea $q_1 = q_2$.

EXERCIȚII

2.35. În enunțul exercițiului nr. 2.8, cuvintele „inel" și „subinel" le înlocuim cu „grup" și „subgrup"; să se studieze intersecția tuturor subinelelor lui $(\mathbf{Z}, +, \times)$ care conțin întregul (-3).

2.36. Dacă un același număr pozitiv divide termenii congruenței:

$$x \equiv y \quad [z],$$

să se demonstreze că se obține tot o congruență împărțind fiecare din cei trei întregi x, y și z prin divizorul lor comun.

2.37. Să se reamintească regula „probei prin nouă" a unei adunări și a unei înmulțiri. Să se exprime în termenii congruențelor. Să se demonstreze.

2.38. Același exercițiu pentru „proba prin unsprezece".

2.39. Să se calculeze restul împărțirii prin 7 a numărului 247^{349}.

2.40. Să se dea tablele de adunare și de înmulțire pentru inelele $\mathbf{Z}/n\mathbf{Z}$, cu $n \leqslant 6$.

2.41. Să se rezolve, în fiecare din aceste inele, ecuația: $x^2 = x$.

2.42. Să se caute, în fiecare din aceste inele, mulțimea U_n a elementelor inversabile. Să se verifice că aceste mulțimi sînt grupuri comutative pentru înmulțire. Ce se poate spune despre grupurile:

$$U_3 \text{ și } U_4 ? \quad U_3 \text{ și } U_6 ?$$

2.43. Se împart cei doi întregi x și y prin diferența lor $x - y$, presupusă nenulă. Să se compare cîturile și resturile obținute.

2.44. Pe N, se împarte a la b. Să se compare a cu dublul restului.

2.45. Se împart două numere a și b prin același număr c. Să se compare suma cîturilor obținute cu cîtul lui $(a + b)$ prin c.

2.46. Cunoscînd cîtul și restul împărțirii lui a la b, se poate deduce cîtul și restul împărțirii lui a la cîtul lui a prin b?

Aplicații.

$$a = 589,\ b = 275;\ a = 718,\ b = 39.$$

2.47. Din exercițiul rezolvat IV care încheie paragraful 2.4, să se deducă o regulă care să dea, pe N, cîtul în împărțirea unui întreg la un produs de mai mulți întregi.

2.48. Fie o împărțire pe N. Ce devine cîtul:

a) dacă se mărește întregul a fără a modifica pe b?

b) dacă se mărește b fără a modifica pe a?

În ce cazuri cîtul rămîne constant?

Aplicații.

$$a = 581,\ b = 17;\ a = 483,\ b = 75;\ a = 12\,809,\ b = 628.$$

2.49. Să se calculeze b și q știind că avem:

$$a = 557,\ r = 89.$$

2.50. Să se calculeze b și r știind că avem:

$$a = 1\,517,\ q = 75.$$

2.51. Să se rezolve, pe N, ecuația:

$$4\,231 = 713x + y.$$

2.52. Același exercițiu pe Z.

2.53. Să se calculeze q știind că q și r rămîn invarianți dacă se mărește a cu 52 și b cu 4.

2.54. Să se calculeze a și b știind că:

$$q = 82,\ r = 47,\ 0 < a < 300.$$

2.55. Să se găsească întregii a astfel încît să avem:

$$1\,000 \leqslant a \leqslant 2\,000,\ b = 127,\ q = r.$$

2.56. Să se calculeze a și b știind că:

$$a - b = 538,\ q = 13,\ r = 22.$$

2.57. Același exercițiu cu:

$$a + b = 2\,096,\ q = 5,\ r = 206.$$

2.58. Să se calculeze cîturile în împărțirile lui 36 la 8 și lui 36 la 9. Să se deducă cîtul împărțirii lui 3 643 la 878.

2.59. Să se determine întregii congruenți cu 1 modulo 27 și cu 13 modulo 17.

2.60. Să se reia exercițiul precedent studiind dacă cîturile în împărțirile la 27 și 17 pot fi egale.

2.61. Să se studieze congruența:

$$x^2 + x + 1 \equiv 0 \quad [n]$$

pentru următoarele valori ale lui n:

$$n \in \{2, 3, 5\}.$$

2.62. Același exercițiu cu:

$$x^2 + 2x + 1 \equiv 0 \quad [n].$$

2.63. În exercițiul rezolvat II (pagina 105), să se găsească toți întregii α, β, γ, astfel încît să avem în cele două cazuri studiate:

$$\alpha q_1 + \beta q_3 = \gamma q_2.$$

2.64. Să se rezolve, pe $\mathbf{Z}/4\mathbf{Z}$, ecuația:

$$x^2 + px + q = 0 \quad (p \in \mathbf{Z}/4\mathbf{Z},\ q \in \mathbf{Z}/4\mathbf{Z}).$$

Să se discute.

2.65. Să se demonstreze că suma a două numere impare consecutive este divizibilă cu 4. Reciproca este adevărată?

2.66. Să se demonstreze că produsul a două numere consecutive este divizibil cu 2. Cîtul său prin 2 se poate termina printr-o cifră oarecare?

2.67. 1° Care poate fi restul împărțirii la 5 al pătratului unui număr întreg?

2° Care poate fi restul împărțirii la 8 al pătratului unui număr impar?

2.68. Care sînt resturile împărțirii la 7 ale cuburilor numerelor întregi?

2.69. A este un număr impar, egal cu suma a două pătrate. Care este restul împărțirii sale la 4?

2.70. Să se găsească două numere întregi a și b știind că: $a^2 - b^2 = 24$.

2.71. Să se determine n astfel încît:

a) $n + 8$ să fie divizibil cu n;

b) $n + 11$ să fie divizibil cu $n - 1$;

c) $3n + 24$ să fie divizibil cu $n - 4$.

2.72. 1° Să se determine resturile împărțirii lui 37^n la 11 cînd se dau lui n valorile: 1, 2, 3, 4, 5.

2° Să se deducă resturile împărțirii la 11 ale lui:

$$37^{23},\ 37^{24},\ 37^{25},\ 37^{26},\ 37^{27}.$$

3° Să se generalizeze la 37^n pentru n întreg oarecare.

2.73. Care este restul împărțirii la 11 a lui N^5 cu $N = 705\,432$?

2.74. Care este restul împărțirii la 8 a lui $13^{23} \times 27^{41}$?

2.75. Care este restul împărțirii la 7 a numărului $(32)^{48}$?

2.76. Care este restul împărțirii lui $(57\,383)^4$ la 19?

2.77. Să se găsească ultimele două cifre ale numărului:

$$7^{9^9}$$

2.78. Să se determine n astfel încît împărțirea lui n la 64 să dea un rest egal cu cubul cîtului.

2.79. Să se demonstreze că numărul $n(n + 1)(2n + 1)$ este divizibil cu 6.

2.80. Să se demonstreze că numărul $10^n(9n - 1) + 1$ este divizibil cu 9.

2.81. Să se demonstreze că, dacă a divide pe $x - x'$, $y - y'$, $z - z'$, atunci divide pe: $xyz - x'y'z'$.

2.82. Să se demonstreze că, dacă n este un număr întreg oarecare, produsul $n(2n + 1)(7n+1)$ este divizibil cu 6.

2.83. Care este restul împărțirii la 3 a numărului:

$$\frac{n(n + 1)}{2}?$$

2.84. Să se demonstreze următoarele congruențe:

a) $x(x^4 - 1) \equiv 0$ [5];

b) $x(x^6 - 1) \equiv 0$ [7];

c) $4x + 15x - 1 \equiv 0$ [9] (pentru $x \geqslant 1$);

d) $2^{2x-1}\,3^{x+2} + 1 \equiv 0$ [11] (pentru $x \geqslant 1$);

e) $xy(x^2 - y^2) \equiv 0$ [3].

2.85. Să se determine n, știind că:

$$m \equiv 0 \quad [p],$$

în următoarele cazuri:

a) $m = n^2 - n + 1, \quad p = 7;$

b) $m = 19^n - 2, \quad p = 7;$

c) $m = n^2 + n + 1, \quad p = 13;$

d) $m = 2^n - 1, \quad p = 9$

(în acest caz, să se determine clasele de echivalență ale lui m pe $\mathbf{Z}/7\mathbf{Z}$ și $\mathbf{Z}/21\mathbf{Z}$.)

e) $m = n^3 + 3n^2 + 3n - 7$, $p = 8$ (să se calculeze $(n + 1)^3$).

2.5. NUMERAȚIA

2.5.1. Numerația pozițională

Să considerăm un număr întreg b mai mare sau egal cu 2: îl vom numi *bază* a unui *sistem de numerație*, algoritm care realizează o bijecție între $\mathbf{N}$ și șirurile care iau valori pe mulțimea $\{0, 1, 2, ..., b - 1\}$ și ale căror elemente sînt toate nule începînd cu un anumit rang[1].

1. Să amintim mai întîi o proprietate a lui $\mathbf{N}$ (pagina 49):

$$\boxed{b > 1 \Longrightarrow \forall_{\mathbf{N}} n,\ \exists_{\mathbf{N}} m,\ b^m > n}$$

Mulțimea întregilor p, astfel încît: $b^p \leqslant n$, este vidă dacă n este egal × cu 0, nevidă dacă n este mai mare sau egal cu 1. În acest ultim caz, ea este majorată conform proprietății precedente căci:

$$p \geqslant m \text{ și } b^m > n \Longrightarrow b^p > n.$$

---

[1] Aceste șiruri sînt deci polinoame particulare.

Această mulțime are un element maximum pe care-l vom nota k:

$$b^k \leqslant n < b^{k+1}.$$

Să-l împărțim pe n la b^k; deducem:

$$n = a_k b^k + n_k, \qquad 0 \leqslant n_k < b^k.$$

Cum n este strict mai mic decît b^{k+1}, a_k este strict mai mic ca b. Pe de altă parte, a_k este strict pozitiv; de unde:

$$0 < a_k < b.$$

2. Să-l împărțim pe n_k la b^{k-1}; deducem:

$$n_k = a_{k-1} b^{k-1} + n_{k-1}, \quad 0 \leqslant n_{k-1} < b^{k-1}.$$

Se deduce de aici dubla inegalitate:

$$0 \leqslant a_{k-1} < b.$$

(Aici, a_{k-1} poate fi nul, ceea ce a fost imposibil pentru a_k). Reîncepînd cu n_{k-1}, este posibil să construim un șir finit $(a_k, a_{k-1}, \ldots, a_h, \ldots, a_0)$ cu:

$$0 < a_k < b, \ 0 \leqslant a_h < b \qquad (0 \leqslant h < k),$$

și:

$$n_{h+1} = a_h b^h + n_h, \qquad 0 \leqslant n_h < b^h.$$

În particular, n_0 este nul.

3. Să adunăm membru cu membru egalitățile:

$$\begin{aligned}
n &= a_k b^k + n_k \\
n_k &= a_{k-1} b^{k-1} + n_{k-1} \\
&\vdots \\
n_{h+1} &= a_h b^h + n_h \\
&\vdots \\
n_1 &= a_0 b^0
\end{aligned}$$

(de fapt este vorba de o recurență deghizată).
Se găsește egalitatea:

$$\boxed{n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_0 b^0 = \sum_{h=0}^{k} a_h b^h} \tag{78}$$

EXERCIȚIU

Să se regăsească egalitatea (78) printr-o metodă care nu folosește implicația amintită.
Să presupunem de asemenea că n este nenul. Să împărțim pe n la b:

$$n = bq_1 + a_0 \ (0 \leqslant a_0 < b).$$

Să reîncepem cu q_1:

$$q_1 = bq_2 + a_1 \ (0 \leqslant a_1 < b),$$

și așa mai departe:

$$q_h = bq_{h+1} + a_h \ (0 \leqslant a_h < b).$$

Se găsesc astfel egalități de tipul:

$$n = a_0 + ba_1 + b^2a_2 + \ldots + b^ha_h + b^{h+1}q_{h+1}.$$

Cum b este mai mare ca 1, întregii q_h descresc strict:

$$n > q_1 > q_2 > \ldots > q_h.$$

Prin inducție se poate deduce inegalitatea:

$$q_h \leqslant n - h.$$

Există deci un rang k pentru care q_{k+1} este nul (se poate chiar preciza inegalitatea $k \leqslant n - 1$), de unde egalitatea căutată:

$$n = a_0 + ba_1 + \ldots + b^ka_k.$$

Dacă k este cel mai mare indice pentru care q_k nu este nul, se poate deduce că a_k nu este nul căci $q_k = a_k$.

---

4. Putem să dăm acum definiția completă a sistemului de numerație de bază b. Întregului n îi vom face să-i corespundă:
a) șirul nul $u_h = 0$ dacă $n = 0$;
b) șirul definit prin:

$$u_0 = a_0, \ u_1 = a_1, \ \ldots, \ u_k = a_k,$$

și $u_h = 0$ pentru h strict mai mare decît k.

5. De obicei acest șir se scrie în felul următor:

$$\ldots 000 \ldots 0a_ka_{k-1}\ldots a_h\ldots a_2a_1a_0$$

prescurtat în:

$$a_ka_{k-1}\ldots a_2a_1a_0.$$

Dacă se poate face confuzie (în special cu produsul întregilor a_h), se va scrie:

$$\overline{a_k \ \ldots \ a_2a_1a_0}$$

sau (precizînd baza):

$$\overline{a_k\ldots a_2a_1a_0}_{(b)}.$$

Numărul cel mai din stînga este întotdeauna diferit de 0, în afara cazului cînd este zero pe care-l reprezentăm prin 0. Fiecăruia dintre numerele de la 0 la $(b - 1)$, i se asociază un simbol tipografic special, numit cifră. Orice întreg este deci reprezentat printr-un șir finit de cifre alăturate, cu o bară deasupra eventual.

6. Această reprezentare este surjectivă; simbolului $\overline{a_k...a_1a_0}$ i se asociază întregul:

$$n = \sum_{h=0}^{k} a_h b^h$$

a cărui reprezentare se verifică ușor, este cea de la care s-a plecat.
Ea este injectivă. Să considerăm două reprezentări diferite ale aceluiași întreg:

$$n = \sum_{h=0}^{k} a_h b^h = \sum_{h=0}^{l} c_h b^h.$$

Fie m primul rang plecînd de la care ele diferă:

$$a_0 = c_0,\ a_1 = c_1,\ ...,\ a_{m-1} = c_{m-1},\ a_m \neq c_m.$$

Să scriem atunci egalitățile:

$$n = (a_0 + a_1 b + ... + a_{m-1}b^{m-1}) + b^m(a_m + bx)$$
$$= (a_0 + a_1 b + ... + a_{m-1}b^{m-1}) + b^m(c_m + by).$$

Din regularitatea lui b^m la înmulțire, deducem egalitatea:

$$a_m + bx = c_m + by = z,$$

cu:

$$0 \leqslant a_m < b,\ 0 \leqslant c_m < b.$$

Unicitatea restului împărțirii lui z la b arată că avem $a_m = c_m$. Coeficienții a_m și c_m fiind egali contrar ipotezei, reprezentarea lui n este unică.

TEOREMĂ 15 / **b fiind un întreg strict mai mare ca 1, orice întreg strict pozitiv n se poate reprezenta în mod unic prin simbolul $a_k ...a_2a_1a_{0(b)}$ unde întregii a_k și b sînt astfel încît:**

$$n = a_k b^k + ... + a_2 b^2 + a_1 b^1 + a_0$$

cu:

$$0 < a_k < b,\ 0 < a_h < b \text{ pentru } 0 \leqslant h < k.$$

2.5.2. Sistem zecimal și sistem binar

Cele două sisteme cele mai folosite sînt sistemul zecimal ($b = 10$) și sistemul binar ($b = 2$). Această carte este scrisă în sistemul zecimal; cifrele sînt simbolurile bine cunoscute:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Sistemul binar nu are decît două cifre: 0 și 1.

Tabloul de corespondență de mai jos dă scrierea, în sistemul binar, a întregilor cuprinși între 0 și 99 (zecile se vor citi pe linie iar unitățile pe coloane):

	Unități									
	0	1	2	3	4	5	6	7	8	9
0	0	1	10	11	100	101	110	111	1000	1001
1	1010	1011	1100	1101	1110	1111	10000	10001	10010	10011
2	10100	10101	10110	10111	11000	11001	11010	11011	11100	11101
3	11110	11111	100000	100001	100010	100011	100100	100101	100110	100111
4	101000	101001	101010	101011	101100	101101	101110	101111	110000	110001
5	110010	110011	110100	110101	110110	110111	111000	111001	111010	111011
6	111100	111101	111110	111111	1000000	1000001	1000010	1000011	1000100	1000101
7	1000110	1000111	1001000	1001001	1001010	1001011	1001100	1001101	1001110	1001111
8	1010000	1010001	1010010	1010011	1010100	1010101	1010110	1010111	1011000	1011001
9	1011010	1011011	1011100	1011101	1011110	1011111	1100000	1100001	1100010	1100011

De exemplu: $\overline{100}_{(10)} = \text{o sută} = \overline{1100100}_{(2)} = 2^6 + 2^5 + 2^2$

$$= \overline{64}_{(10)} + \overline{32}_{(10)} + \overline{4}_{(10)}.$$

EXERCIȚII

1. *Să se demonstreze că un întreg scris cu p cifre în sistemul zecimal necesită cel puțin $(3p - 2)$ cifre și cel mult $4p$ cifre în sistemul binar.*

Pentru n mai mic sau egal cu 10, enunțul este adevărat, căci p este atunci egal cu 1. Să presupunem deci: $n > 10$, și:

$$10^{p-1} \leqslant n < 10^p \qquad (p > 1),$$

se deduc imediat inegalitățile:

$$2^{3p-3} = 8^{p-1} < 10^{p-1} \leqslant n,$$

$$n < 10^p < 16^p = 2^{4p}.$$

Dacă avem: $2^{q-1} \leqslant n < 2^q,$

se deduc inegalitățile:

$$3p - 3 < q, \qquad q^{-1} < 4p,$$

$$3p - 2 \leqslant q \leqslant 4p,$$

care permit demonstrarea proprietății enunțate.

II. *Există oare un sistem de bază b în care să se poată scrie o egalitate de forma:*

$$\overline{xxx} \times \overline{xxx} = \overline{yyyyyy}?$$

O astfel de egalitate se scrie:

$$x^2(b^2 + b + 1)^2 = y(b^5 + b^4 + b^3 + b^2 + b + 1)$$
$$= y(b^2 + b + 1)(b^3 + 1).$$

Se deduce egalitatea:

$$x^2(b^2 + b + 1) = y(b^3 + 1).$$
$$= y(b^3 - 1) + 2y$$
$$= y(b - 1)(b^2 + b + 1) + 2y.$$

$(b^2 + b + 1)$ divide pe $2y$ deoarece avem:

$$2y = (b^2 + b + 1)(x^2 - y[b - 1]).$$

Or, noi știm că: $0 < y < b$,

de unde:

$$0 < 2y < 2b \leqslant b^2 + 1 < b^2 + b + 1.$$

În consecință, egalitatea propusă este imposibil de scris oricare ar fi baza.
Egalitatea $\overline{xx} \times \overline{xx} = \overline{yyyy}$ are, din contră, o infinitate de soluții; de exemplu:

$$\overline{55}_{(7)} \times \overline{55}_{(7)} = \overline{4444}_{(7)}$$

Într-adevăr, această egalitate se scrie în numerație zecimală:

$$(5 \times 7 + 5)^2 = (4 \times 7^3 + 4 \times 7^2 + 4 \times 7 + 4)$$

sau încă:

$$40^2 = 4 \times (343 + 49 + 7 + 1).$$

III. *Să se demonstreze că, pentru orice întreg n strict pozitiv, există un întreg k și un întreg t strict pozitivi astfel încît, pentru orice întreg x:*

$$(m \geqslant k) \Longrightarrow (n \text{ divide } x^{m+t} - x^m).$$

Să considerăm șirul u_m definit prin: $m \longmapsto u_m = (a_m, b_m, c_m, \ldots, h_m)$, unde a_m, b_m, ..., h_m sînt cifrele din dreapta ale numerelor 0^m, 1^m, ..., $(n-1)^m$ scrise în sistemul de bază n (pentru $n = 1$, enunțul nu prezintă interes). Acești întregi sînt cifrele din dreapta ale tuturor numerelor x^m. Dacă două elemente ale șirului sînt egale, și succesorii lor sînt egali: $u_m = u_\mu \Longrightarrow u_{m+1} = u_{\mu+1}$, și așa mai departe.
Or, numărul valorilor lui u_m este limitat căci există cel mult n^n șiruri finite de n cifre.
Aplicația:

$$u = [m \longmapsto u_m]$$

nu este deci injectivă; se pot găsi deci doi întregi k și t astfel încît:

$$u_k = u_{k+t} \qquad (t \geqslant 1),$$

ceea ce demonstrează proprietatea.
Acest exercițiu se poate interpreta în inelul $\mathbf{Z}/n\mathbf{Z}$; aplicațiile $[m \longmapsto x^m]$ admit aici o perioadă comună t plecînd de la rangul k.
Într-adevăr, $\bar{a}_m$, $\bar{b}_m$, ..., $\bar{h}_m$ sînt clasele lui 0^m, 1^m, ..., $(n-1)^m$ modulo n.

Determinarea lui k și t începînd de la n, depinde în general de descompunerea lui n în factori primi. Pentru $n = 72$, găsim spre exemplu $k = 3$ și $t = 6$.

IV. *Să se calculeze numărul:*

$$\left(1 - \frac{1}{8}\right)^2 \left(1 + \frac{2}{8} + \frac{3}{8^2} + \frac{4}{8^3} + \frac{5}{8^4} + \frac{7}{8^5}\right)$$

Să se deducă dezvoltarea octală infinită a numărului $\frac{1}{49}$ *(sistemul octal are ca bază pe 8).*

Notă. — Acest exercițiu face să intervină numerele raționale.
Se găsește ușor:

$$\left(1 - \frac{1}{8}\right)\left(1 + \frac{2}{8} + \frac{3}{8^2} + \frac{4}{8^3} + \frac{5}{8^4} + \frac{7}{8^5}\right) = 1 + \frac{1}{8} + \frac{1}{8^2} + \frac{1}{8^3} + \frac{1}{8^4} + \frac{1}{8^5} + \frac{1}{8^6} +$$

$$\left(1 - \frac{1}{8}\right)\left(1 + \frac{1}{8} + \frac{1}{8^2} + \frac{1}{8^3} + \frac{1}{8^4} + \frac{1}{8^5} + \frac{1}{8^6}\right) = 1 - \frac{1}{8^7}.$$

Or:

$$\frac{1}{49} = \frac{1}{8^2\left(1 - \frac{1}{8}\right)^2} = \frac{1}{8^2}\left(1 + \frac{2}{8} + \frac{3}{8^2} + \frac{4}{8^3} + \frac{5}{8^4} + \frac{7}{8^5}\right) + \frac{1}{8^9\left(1 - \frac{1}{8}\right)^2}$$

$$= \left(\frac{1}{8^2} + \frac{2}{8^3} + \frac{3}{8^4} + \frac{4}{8^5} + \frac{5}{8^6} + \frac{7}{8^7}\right) + \frac{1}{8^7} \cdot \frac{1}{49}$$

Se deduce următoarea dezvoltare octală (49 se scrie 61 în sistem octal):

$$\frac{1}{61} = 0{,}012345701234570123457...$$

(Se va putea compara cu dezvoltarea zecimală:

$$\frac{1}{81} = 0{,}012\ 345\ 679\ 012\ 345\ 679\ 012\ 3...)$$

EXERCIȚII

2.86. Un număr $n = \overline{xyz}$ (în sistemul zecimal) este astfel încît:

$$n + 36 = \overline{xzy},\quad n - 270 = \overline{yxz}.$$

Ce se poate spune despre numărul $\overline{zyx}$?

2.87. x și y au respectiv 5 și 3 cifre (în sistemul zecimal).

1° Ce se poate spune de numărul cifrelor:

lui $x + y$? lui xy? lui y^x?

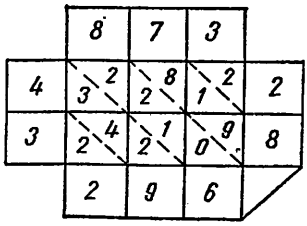
2° Ce se poate spune despre cîtul şi restul împărţirii lui x prin y?

2.88. 1° Să se găsească numerele de trei cifre (în sistemul zecimal) al căror produs prin 8 se termină prin 896.

2° Să se găsească un număr de patru cifre al cărui produs prin 7 se termină cu 4 894.

3° Să se găsească un număr de trei cifre al cărui produs cu 87 se termină cu 658.

2.89. 1° Să se interpreteze schema următoare (înmulţirea musulmană) care dă produsul lui 873 cu 34:



$(873 \times 34 = 29\,682)$

2° Să se enunţe regula şi să se aplice la produsul:

$$3\,524 \times 237 = 835\,188.$$

2.90. În împărţirea pe **N** (sistem zecimal):

$$a = bq + r, \quad 0 \leqslant r < b,$$

a are α cifre, b are β cifre. Ce se poate spune despre numărul de cifre al lui q?

2.91. Acelaşi exerciţiu în sistemul binar, apoi în sistemul octal.

2.92. Să se scrie numărul $\overline{4207}_{(8)}$ în sistem binar:

1° Trecînd prin sistemul zecimal.

2° Direct.

2.93. Să se rezolve ecuaţia definită prin:

$$\overline{23}_{(10)} = \overline{27}_{(b)}.$$

2.94. Să se rezolve ecuaţia definită prin:

$$\overline{136}_{(10)} = \overline{253}_{(b)}.$$

2.95. Să se rezolve ecuaţia definită prin:

$$\overline{303}_{(b)} = \overline{523}_{(b)}.$$

2.96. Să se exprime în sistem zecimal, reguli simple care dau clasele modulo n pentru:

$$n \in \{2, 5, 10, 4, 25, 100\}.$$

2.97. Același exercițiu pentru $n = 11$ (se va calcula restul modulo 11 al lui $10^n - (-1)^n$).

Exemplu:

$$278\,531;\ 753\,457;\ 559\,721.$$

2.98. Același exercițiu pentru: $n \in \{99, 999, 9\,999\}$.

2.99. Să se împartă 111 111 la 111, și 3 003 la 33.

2.100. Să se demonstreze că 6 divide pe n dacă și numai dacă 6 divide multiplul de patru al sumei cifrelor lui n mai puțin de trei ori cifra din dreapta (sistem zecimal).

2.101. Să se compare resturile împărțirii lui n la 111 și al lui $(1\,000n)$ la 111.
Să se calculeze resturile împărțirilor lui $(10^8 + 10^4 + 1)$ la 111 și lui $(10^{10} + 10^5 + 1)$ la 111.

2.102. Să se demonstreze că, dacă d și u sînt cifrele zecilor și unităților unui număr, acest număr este divizibil cu 4 dacă $2d + u$ este multiplu de 4.

2.103. Să se demonstreze că, dacă c, d, u sînt cifrele sutelor, zecilor și unităților unui număr, acest număr este divizibil cu 8 dacă:

$$4c + 2d + u \text{ este multiplu de 8.}$$

2.104. Fie n întreg, $n > 6$. Să se scrie $(n + 1)^4$ în sistemul de bază n.

2.105. Un număr N se scrie $\overline{abc}$ în sistemul de bază treisprezece (numerele zece, unsprezece și doisprezece sînt reprezentate respectiv de cifrele α, β, γ).
În ce condiție N este divizibil cu: treisprezece? cu pătratul lui treisprezece?
Să se scrie numărul 1001 din sistemul zecimal în sistemul cu baza treisprezece.

2.106. Să se împartă la 7 numerele 10, 100, 1 000, 10 000 etc.
Să se deducă un criteriu de divizibilitate cu 7.

2.107. Să se determine cifrele x și y ale numărului $\overline{28\,x\,75\,y}$ pentru ca acest număr să fie divizibil cu 3 și cu 11.

2.108. Să se determine cifrele x, y și z ale numărului $\overline{13\,xy\,45\,z}$ pentru ca acest număr să fie divizibil cu 8, 9 și 11.

2.109. Două numere sînt scrise cu aceleași cifre într-o ordine diferită. Să se demonstreze că diferența lor este un multiplu de 9. Se întîmplă același lucru cu suma?

2.110. 1° Cum se poate face proba prin 5 a unei înmulțiri și a unei împărțiri? Această probă are vreo însemnătate?

2° Aceeași întrebare pentru proba prin 3.

2.111. Se face produsul lui 15 724 cu 307 scriind din greșeală cifra 2 a celui de al doilea produs parțial nenul în coloana zecilor în loc să-l scriem în coloana sutelor. Să se demonstreze că proba prin 9 reușește. Să se spună de ce?
Proba prin 11 va semnala eroarea?

2.112. 1° Să se calculeze în orice sistem de numerație a cărui bază este mai mare ca 4, pătratele numerelor 11, 111, 1 111.
(Vom nota că, în produsul 111×111, nu există cifră de transport.)

2° Să se deducă de aici că în orice sistem de numerație a cărui bază este mai mare ca 4, numerele 121, 12 321, 1 234 321 sînt pătrate perfecte.

2.113. Din egalitatea:

$$1\,001 = 7 \times 11 \times 13,$$

să se deducă un criteriu de divizibilitate cu 7 și cu 13.

2.114. Care sînt resturile împărțirii puterilor lui 10 la 45?
Să se deducă un criteriu de divizibilitate cu 45.

2.115. Să se împartă 1 000 la 37. Să se deducă un criteriu de divizibilitate cu 37.

2.116. Să se interpreteze egalitatea:

$$b^n - 1 = (b - 1)(b^{n-1} + b^{n-2} + \ldots + b^2 + b + 1)$$

pentru:

$$b \in \mathbf{N} \text{ și } b \geqslant 2.$$

2.117. În ce sistem de numerație numărul unsprezece se scrie 102?

2.118. În ce sistem de numerație numărul 10 000 din sistemul zecimal se scrie 14 641?

2.119. Să se scrie numărul 68 425 din sistemul zecimal în sistemul cu baza opt și în sistemul cu baza doisprezece.

2.120. Numărul 16 524 este scris în sistemul cu baza șapte. Să se scrie în sistemul cu baza nouă.

2.121. În ce sistem de numerație avem:

$$21 \times 12 = 1\,022?$$

2.122. În ce sistem de numerație avem:

$$31 \times 43 = 443?$$

2.123. În ce sistem de numerație avem:

$$324 + 223 = 1\,102?$$

2.124. În sistemul cu baza doisprezece, un număr se scrie $\overline{abc}$. În sistemul cu baza cinci, același număr se scrie $\overline{abco}$. Care este acest număr?

2.125. Cîte numere de trei cifre avem într-un sistem de bază n?

2.126. Să se verifice că:

$$x(x + 1)(x + 2)(x + 3) + 1 = (x^2 + 3x + 1)^2.$$

Să se deducă de aici că, în orice sistem de numerație a cărui bază este mai mare ca 3, avem:

$$\overline{10} \times \overline{11} \times \overline{12} \times \overline{13} + 1 = (\overline{131})^2.$$

2.127. În ce sisteme de numerație numărul unsprezece se scrie cu două cifre?

2.128. Să se demonstreze că, în orice sistem de numerație a cărui bază este mai mare ca trei, numărul $\overline{1331}$ este cubul unui număr întreg x. Să se determine acest număr x.

2.129. Care sînt numerele, în sistemul zecimal, care se scriu cu patru cifre în sistemul binar și două în sistemul duodecimal?

2.130. 1° Să se formeze tabela de adunare în sistemul cu baza cinci.

2° Să se calculeze suma numerelor: 3 402 + 231 + 2 034 scrise în sistemul cu baza cinci, folosind tabela precedentă.

2.131. Să se efectueze scăderea $4\,123 - 204$, numerele fiind scrise în sistemul cu baza cinci.

2.132. 1° Să se formeze tabela de înmulțire în sistemul cu baza șapte.

2° Să se folosească această tabelă pentru a calcula produsul numerelor care se scriu, în acest sistem, 43 și 25. Să se verifice rezultatul calculînd în sistemul zecimal.

2.133. Să se efectueze următoarele operații în sistemul binar:

$$10 + 10; \qquad 100 \times 10; \qquad 111 \times 11.$$

2.134. Să se rezolve ecuația (în sistemul zecimal) definită prin

$$\overline{1abcde} \times \overline{3} = \overline{abcde1}.$$

2.135. Același exercițiu pentru ecuația definită prin:

$$\overline{xy} = (\overline{2} \times \overline{yx}) + \overline{1}.$$

PROBLEME

2.136. Fie a, b, c, d întregi relativi fixați. Oricărei perechi (x, y) de întregi relativi, i se asociază perechea (X, Y) definită prin:

$$X = ax + by; \qquad Y = cx + dy.$$

1° Să se demonstreze că se obține astfel o aplicație φ de la $\mathbf{Z} \times \mathbf{Z}$ la el însuși.

2° Să se scrie matricial egalitățile precedente. Care sînt proprietățile lui φ care o apropie de o aplicație liniară? De ce $\mathbf{Z} \times \mathbf{Z}$ nu este un spațiu vectorial?

3° În ce condiție φ este injectivă?

4° În ce condiție φ este surjectivă?

5° Să se demonstreze că mulțimea aplicațiilor φ poate primi o structură de grup comutativ.

6° Să se demonstreze că această mulțime poate primi o structură de inel unitar necomutativ.

7° Să se determine aplicațiile φ astfel încît, pentru orice altă aplicație ψ a mulțimii, să avem:

$$\varphi \circ \psi = \psi \circ \varphi.$$

8° Să se demonstreze că, dacă φ este dat, există doi întregi relativi λ și μ, astfel încît:

$$\varphi^2 = \lambda\varphi + \mu i,$$

unde $\varphi^2 = \varphi \circ \varphi$ și unde i este elementul neutru pentru înmulțirea definită la 6°.

2.137. Se consideră matricile:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix},$$

și mulțimea matricilor $M = 3xI + yA$, unde x și y sînt întregi relativi arbitrari.

1° Să se demonstreze că mulțimea matricilor M formează un inel necomutativ Acest inel este unitar?

2° Să se determi:e matricile M, dacă există, astfel încît să existe o matrice M' din aceeași mulțime cu:

$$MM' = M'M = I.$$

3° Să se demonstreze că inelul este integru. (Se vor folosi proprietățile numerelor prime din capitolul 3.)

2.138. Se consideră n întregi relativi $x_1, x_2, ..., x_n$, astfel încît, pentru orice indice i:

$$|x_i| \leqslant 1.$$

1° Să se demonstreze că, dacă suma $x_1 + x_2 + ... + x_n$ este nulă, atunci suma

$$x_1 + 2x_2 + 3x_3 + ... + nx_n$$

este mai mică sau egală ca cel mai mare întreg care este mai mic sau egal cu $\frac{n^2}{4}$.

2° Să se construiască mulțimile $\{x_1, x_2, ..., x_n\}$ pentru care a doua sumă este efectiv egală cu cel mai mare întreg mai mic sau egal cu $\frac{n^2}{4}$.

2.139. Fie A un inel.

1° Să se demonstreze că mulțimea A^E a aplicațiilor unei mulțimi fixate E în A este un inel. Ce se poate spune despre A^E: dacă A este unitar? dacă A este comutativ?
Să se studieze cazul în care A este integru.

2° Se presupune că E este înzestrată cu o lege multiplicativă față de care este un grup G. Se presupune că G este finită, și se pune în A^G:

$$(f * g)(x) = \sum_{y \in G} f(xy^{-1})\ (g(y).$$

Să se demonstreze că această lege, adăugată la adunarea naturală, face din A^G un inel distinct de cel care a fost studiat la 1°. Ce se poate spune despre acest inel: dacă A este unitar? dacă A și G sînt comutative?

2.140. A este un inel unitar, A^* este mulțimea elementelor lui A care admit un invers în A.

1° Ce se poate spune despre A^*: dacă $A = \mathbf{Z}$? dacă A este un corp?

2° Să se demonstreze că A^* este un grup multiplicativ.

3° Înzestrăm produsul cartezian $A^* \times A$ cu legea:

$$(a, b) \times (c, d) = (ac, bc + d).$$

Să se demonstreze că se definește astfel un grup. Este el comutativ?

4° Să se studieze mulțimea matricilor:

$$\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix},$$

unde a și b sînt numere reale cu: $a \neq 0$.

5° Ce se poate spune despre grupul construit la 3° pe mulțimea $\mathbf{Z}^* \times \mathbf{Z}$? ($\mathbf{Z}^*$ are aici sensul definit la începutul problemei, și nu cel de $\mathbf{Z} - \{0\}$.)

3. NUMERE ÎNTREGI PRIME

3.1. ÎNTREGI PRIMI NATURALI

3.1.1. Divizibilitate în N

Am definit la numărul **2.4.1.** divizibilitatea în **Z** : x divide y(y este un multiplu de x) dacă, și numai dacă, există un întreg z astfel încît:

$$y = xz.$$

Se notează: $x \mid y$; simbolul „$\mid$" înseamnă „divide". Vom nota de asemenea cu $x \nmid y$, „x nu divide pe y".

Cînd x divide pe y, convenim să notăm cîtul: $z = \frac{y}{x}$.

De exemplu:

$$\boxed{(x \in \mathbf{Z}) \Longrightarrow (x \mid 0)} \tag{1}$$

În afara acestei proprietăți să mai notăm două relații foarte simple:

$$\boxed{x \mid x} \tag{2}$$

$$\boxed{(x \mid y \text{ și } y \mid z) \Longrightarrow (x \mid z)} \tag{3}$$

care sînt consecințe imediate ale definiției.
În sfîrșit:

$$\boxed{(x \in \mathbf{Z}) \Longrightarrow (1 \mid x \text{ și } (-1) \mid x)} \tag{4}$$

Divizibilitatea păstrează următorul sens în **N**: întregul natural n divide întregul natural m dacă, şi numai dacă, $(+n)$ divide $(+m)$; notăm: $n \mid m$. După *regula semnelor* de la nr. 2.2.3, se poate scrie:

$$\boxed{n \mid m \Longleftrightarrow (\exists_{\mathbf{N}}{}^{d}\ nd = m) \qquad (n \in \mathbf{N},\ m \in \mathbf{N})} \tag{5}$$

Relaţiile: $n \mid 0$, $n \mid n$, $1 \mid n$

şi: $(n \mid m \text{ şi } m \mid r) \Longrightarrow (n \mid r)$

evident sînt valabile în **N**. Dar divizibilitatea între întregii naturali este mai simplă ca între întregi relativi căci ea defineşte o *relaţie de ordine parţială* în **N**. Într-adevăr, după nr. 1.2.3, ştim că avem în **N**:

$$(nm = 1) \Longleftrightarrow (n = m = 1).$$

Să presupunem deci că doi întregi naturali n şi m se divid unul pe altul:

$$n \mid m \Longrightarrow m = nu \quad (u \in \mathbf{N}),$$

$$m \mid n \Longrightarrow n = mv \quad (v \in \mathbf{N});$$

rezultă: $$m = nu = (mv)u = m(vu).$$

Dacă m nu este nul, deducem:

$$(1 = vu) \Longrightarrow (v = 1) \Longrightarrow (n = m).$$

Dacă m este nul, atunci:

$$n = mv = 0v = 0 = m.$$

În toate cazurile, n şi m sînt egale:

$$\boxed{(n \mid m \text{ şi } (m \mid n) \Longrightarrow (n = m)} \tag{6}$$

Relaţiile (2), (5) şi (6) permit enunţarea următoarei teoreme:

TEOREMĂ 1 / **Relaţia de divizibilitate în N este o relaţie de ordine parţială.**

Teorema 1 este adevărată şi în $\mathbf{N}^*$. Se poate chiar demonstra relaţia următoare:

$$\boxed{(m \neq 0 \text{ şi } n \mid m) \Longrightarrow (n \neq 0 \text{ şi } n \leqslant m)} \tag{7}$$

Într-adevăr:

$$(m = nd \neq 0) \Longrightarrow (n \neq 0 \text{ şi } d \neq 0)$$

$$\Longrightarrow (d \geqslant 1) \Longrightarrow (m \geqslant n).$$

(Relaţiile (6) şi (7) sînt evident false în **Z**; într-adevăr:

$$(-1) \mid 1,\ 1 \mid (-1),\ 1 \neq (-1),\quad 1 \not\leqslant (-1)).$$

Să semnalăm în sfîrșit trei consecințe imediate ale definiției, adevărate în **N** ca și în **Z**:

$$(x \mid y) \Longrightarrow (x \mid yz) \tag{8}$$
$$(x \mid y) \Longrightarrow (xz \mid yz) \tag{9}$$
$$(x \mid y) \text{ și } (x \mid z) \Longrightarrow (x \mid y + z) \tag{10}$$

3.1.2. Numere prime în N

Orice întreg natural n îi are pe 1 și n ca divizori [(2) și (4)]. Dacă n nu este egal cu 1, admite deci cel puțin doi divizori. Unii întregi au și mai mulți: 0 are o infinitate de divizori în **N** (orice întreg îl divide pe 0); 24 are 8 divizori în **N**:

$$div\ 24 = \{1, 2, 3, 4, 6, 8, 12, 24\}.$$

În acest paragraf, simbolul div n reprezintă mulțimea divizorilor întregi naturali ai lui n. Să convenim, pentru a simplifica, să numim „divizor" și „întreg" divizorii întregi naturali și numerele întregi naturale, pentru tot paragraful 3.1.

Anumiți întregi, ca 13, nu au decît doi divizori:
$div\ 13 = \{1, 13\}$. Astfel de întregi sînt numiți *întregi naturali primi* (prescurtat: numere prime, în tot acest paragraf); 24 nu este deci număr prim: el este numit compus; 0 și 1 nu sînt numere prime[1], dar în general nu sînt considerate nici numere compuse.

Comportamentul lor față de împărțirea în **N** este mai special și constituie o sursă de dificultăți de limbaj.

Să rezumăm aceste noțiuni enunțînd:

DEFINIȚIA 1 / **Un întreg natural este numit număr prim dacă are numai doi divizori care aparțin lui N. Un întreg mai mare ca 2 este numit compus dacă nu este prim.**

Relația (7) între întregi nenuli:

$$n \mid m \Longrightarrow n \leqslant m,$$

este esențială pentru studiul numerelor prime căci ea dovedește că un întreg are un număr finit de divizori. Încercările permit deci să se determine dacă un întreg dat este prim (a se vedea nr. **3.1.4**). Un tabel de numere prime mai mici ca 5 000 este dat la pagina 192 și următoarele; extragem de acolo următoarele numere:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29. 31, 37, 41, 43, 47.

Se poate construi un șir:

$$n \longmapsto p_n,$$

[1] Convenția care-l exclude pe 1 din mulțimea numerelor prime nu este absolut universală.

astfel încît $p_1 = 2$ și unde p_{n+1} este cel mai mic număr prim strict mai mare ca p_n; astfel:

$$p_2 = 3, \quad p_{11} = 31, \quad p_{23} = 83,$$
$$p_{253} = 1\,607, \quad p_{664\,999} = 10\,006\,721.$$

3.1.3. Divizori primi în N

Am observat deja că întregul n ar putea avea cel mult n divizori (7). Să presupunem: $n \geqslant 2$, și fie p cel mai mic dintre divizorii săi diferit de 1. Dacă p ar fi compus, am putea scrie:

$$n = pd, \; p = ab, \text{ cu: } p \geqslant 2,$$

și de exemplu:

$$p > a \geqslant b > 1;$$

de unde:

$$n = pd = (ab)d = a(bd),$$

cu:

$$p > a > 1.$$

Aceasta contrazice faptul că p este minimal: p este deci prim.

TEOREMĂ 2 / **Orice întreg mai mare sau egal cu 2 admite cel puțin un divizor prim.**

Întregii 2, 3, 4, 5, 6 se pot scrie ca produse de numere prime. Vom spune, prin abuz de limbaj, că un întreg poate fi considerat ca un produs de „un" factor. Ținînd seama de aceste două observații, se poate scrie:

$$2 = 2, \quad 3 = 3, \quad 4 = 2 \times 2,$$
$$5 = 5, \quad 6 = 3 \times 2, \ldots$$

Să admitem că această proprietate este adevărată pentru toți întregii mai mici sau egali cu n (conform teoremei 3, nr. **1.1.3**), și să considerăm întregul $(n + 1)$. Dacă acesta nu este prim, se poate scrie atunci egalitatea:

$$n + 1 = uv,$$

cu:

$$u < n + 1.$$

Întregul u se poate deci scrie ca produs de numere prime; la fel și întregul v, deci și $(n + 1)$. Dacă $(n + 1)$ este prim, se poate scrie:

$$n + 1 = p, \qquad p \text{ prim.}$$

În final, orice întreg n mai mare sau egal cu 2 este egal cu un produs de numere prime. Un divizor prim putînd să apară de mai multe ori în descompunere, se regrupează divizorii egali între ei. De exemplu:

$$72 = 2 \times 2 \times 2 \times 3 \times 3 = 2^3 \times 3^2.$$

TEOREMĂ 3 / **Orice întreg mai mare sau egal cu 2 se poate scrie ca produs de numere prime naturale.**

Se poate demonstra teorema 3, altfel, ca un corolar al teoremei 2.

Să presupunem într-adevăr, că există doi întregi pentru care teorema 3 este falsă. Fie n cel mai mic dintre ei; n nefiind prim admite totuşi un divizor prim p. Dar atunci:

$$n = pm, \quad m < n.$$

Teorema 3 fiind adevărată pentru m, se ajunge la o contradicţie.

O altă consecinţă a teoremei 2 este importantă. Să presupunem că nu există decît s numere prime $p_1, p_2, \ldots, p_s$, şi să considerăm întregul:

$$n = p_1 p_2 \ldots p_s + 1;$$

n admite un divizor prim p. Totuşi, fiecare din egalităţile:

$$p = p_1, \quad p = p_2, \ldots, \quad p = p_s$$

este evident falsă, deoarece p nu divide pe 1. Există deci o infinitate de numere prime (sau încă: există un număr prim mai mare ca un întreg dat). Enunţăm:

TEOREMĂ 4 / **Există o infinitate de numere prime naturale.**

EXERCIŢIU

Să se demonstreze inegalitatea:

$$p_n < 2^m \ (n \geqslant 1), \text{ unde } m = 2^n.$$

Această inegalitate este adevărată pentru $n = 1$ căci:

$$p_1 = 2 \text{ şi } 2 < 2^2.$$

Să o presupunem adevărată pentru n; atunci întregul:

$$a = p_1 p_2 \ldots p_n + 1$$

admite un divizor prim q strict mai mare ca p_n.
Dar se poate scrie:

$$p_{n+1} \leqslant q \leqslant a < 2^2 2^4 2^8 \ldots 2^{2^n} + 1.$$

Avem:

$$2^2 2^4 \ldots 2^{2^n} = 2^{(2^{n+1}-2)},$$

deci a fortiori:

$$a < 4 \times 2^{(2^{n+1}-2)},$$

sau:

$$a < 2^r,$$

cu:

$$r = 2^2 \times 2^{(2^{n+1}-2)} = 2^{2^{n+1}},$$

ceea ce demonstrează inegalitatea:

$$p_{n+1} < 2^{2^{n+1}},$$

și proprietatea cerută.

Să mai dăm încă o demonstrație, puțin diferită, a teoremei 4. Să presupunem într-adevăr că toate numerele prime sînt mai mici ca un anumit întreg m. Atunci, întregul:

$$n = m! + 1$$

admite cel puțin un divizor prim p, care este în mod necesar strict mai mare ca m, de unde o contradicție.

3.1.4. Proprietăți diverse

1. Căutarea numerelor prime este delicată. Să reamintim principiul *ciurului lui Eratostene;* pentru a determina dacă un număr fixat (419 de exemplu) este prim, trebuie încercați toți divizorii eventuali d astfel încît:

$$d < 419.$$

De fapt, este suficient să-i căutăm pe aceia care sînt astfel încît:

$$d^2 < 419,$$

căci o descompunere: $419 = d \times n$
este astfel încît, dacă d este cel mai mic dintre cei doi divizori, atunci:

$$d \times n \geqslant d^2, \text{ deci: } d^2 \leqslant 419.$$

Este deci suficient să luăm: $d < 21$ căci $21^2 > 419$.
Pe de altă parte, teorema 2 arată că este suficient să ne limităm la valorile lui d care sînt numere prime (cel mai mic divizor al lui 419 este prim).
Pe un tabel care dă întregii de la 1 la 419, se taie deci multiplii lui 2 (plecînd de la $4 = 2^2$), apoi aceia ai lui 3 (plecînd de la $9 = 3^2$) etc.
În cazul ales, se consideră deci succesiv multiplii lui 2, 3, 5, 7, 11, 13, 17 și 19. Numerele netăiate sînt numerele prime mai mici sau egale cu 419. Cum 419 nu este tăiat, el este prim.
O așezare regulată a numerelor atrage după sine o așezare regulată a multiplilor lui 2, 3, 5 etc. Ea ne poate ajuta în cele de mai sus.
2. Putem îmbunătăți puțin această metodă căutînd numerele prime numai în anumite șiruri aritmetice; astfel, numerele de forma:

$$2n + 0, \quad 3n + 0, \quad 6n + 0,$$
$$6n + 2, \quad 6n + 3, \quad 6n + 4$$

sînt evident compuse (în afara valorilor excepționale, ca $n = 0$). De aceea se caută numerele prime numai în cele două șiruri:

$$n \longmapsto 6n + 1, \qquad n \longmapsto 6n + 5$$

(numai 2 și 3 nu sînt în aceste șiruri).

3. Se poate arăta că se obține cea mai mare eficacitate în căutarea numerelor prime mai mici sau egale decît întregul a studiind șirurile de forma:

$$n \longmapsto \lambda n + \mu,$$

unde λ este un produs de numere prime.
De exemplu, să luăm $\lambda = 30 = 2 \times 3 \times 5$;
μ nu poate lua decît valorile:

$$\mu \in \{1, 7, 11, 13, 17, 19, 23, 29\}$$

(numai 2, 3, 5 nu sînt în aceste opt șiruri).
Pentru $a = 419$, este suficient să mărginim valorile lui n la 13 căci:

$$30 \times 14 > 419.$$

4. *Numere prime mai mici ca* 420.
$p = 2, 3, 5$ și:

n \ μ	1	7	11	13	17	19	23	29
0		7	11	13	17	19	23	29
1	31	37	41	43	47		53	59
2	61	67	71	73		79	83	89
3		97	101	103	107	109	113	
4		127	131		137	139		149
5	151	157		163	167		173	179
6	181		191	193	197	199		
7	211			223	227	229	233	239
8	241		251		257		263	269
9	271	277	281	283			293	
10		307	311	313	317			
11	331	337			347	349	353	359
12		367		373	379		383	389
13		397	401			409		419

5. Distribuția numerelor prime nu este regulată. Astfel, se pot construi șiruri de n întregi consecutivi compuși toți (este suficient să punem $m = (n + 1)!$, și să considerăm șirul finit:

$$m + 2, m + 3, m + 4, \ldots, m + n - 1, m + n, m + n + 1).$$

Se pot totuși demonstra anumite teoreme, foarte dificile, ca:

a) Dacă a și b nu au divizori comuni, există o infinitate de numere prime de forma:

$$p = an + b \quad \text{(Dirichlet)}.$$

b) Între n și $2n$, există cel puțin un număr prim:

$$n < p < 2n \qquad \text{(Cebîșev)}.$$

c) Orice număr impar mai mare ca $3^{3^{15}}$ este suma a trei numere prime (Vinogradov).

d) Pentru m fixat, avem:

$$\lim_{+\infty}\left[n \longmapsto \frac{mp_n + np_m}{p_{nm}}\right] = 1. \text{ (Hadamard, de la Vallée Poussin)}.$$

De exemplu:

$$\frac{11p_{23} + 23p_{11}}{p_{253}} = \frac{11 \times 83 + 23 \times 31}{1\,607} = \frac{1\,626}{1\,607} \approx 1{,}01.$$

Acest ultim rezultat este o consecință a egalității:

$$\lim_{+\infty}\left[n \longmapsto \frac{p_n}{n\log n}\right] = 1.$$

EXERCIȚIU

Să se demonstreze că există o infinitate de numere prime de forma:

$$p = 4n + 3.$$

Să presupunem că ipoteza este falsă și să considerăm produsul a al numerelor prime:

$$3,\ 7,\ 11,\ 19,\ \ldots,$$

de forma $(4n + 3)$. Atunci întregul impar:

$$b = 4a - 1$$

nu are decît divizori primi de forma:

$$q = 4n + 1,$$

căci nici un număr prim de forma $(4n + 3)$ nu-l poate divide pe b.

Dar deoarece $q \equiv 1$ [4], egalitatea $b \equiv q_1 q_2 \ldots q_m$ conduce la congruența:

$$b \equiv 1 \quad [4]$$

care este falsă; această contradicție demonstrează rezultatul enunțat.

EXERCIȚII

3.1. Să se rezolve ecuația definită pe **Z** prin:

$$9x - 15y = 1.$$

3.2. Întregii 2 309, 2 501, 4 825, 7 281 sînt primi?

3.3. Întregii 111,1 111,11 111,111 111,1 111 111 sînt primi?

3.4. Să se demonstreze că într-un grup de zece numere ca cele de mai sus nu pot să existe mai mult de patru numere prime.

3.5. Să se demonstreze că există o infinitate de numere prime de forma:

$$p = 4n - 1.$$

3.6. Să se demonstreze că există o infinitate de numere prime de forma:

$$p = 6n - 1.$$

3.7. Să se demonstreze că, dacă p și $8p - 1$ sînt prime, $8p + 1$ este compus. (Să se studieze congruențele modulo 3.)

3.8. Să se demonstreze că, dacă p și $8p^2 + 1$ sînt prime, $8p^2 - 1$ este compus.

3.9. Să se demonstreze că descompunerea din teorema 3 este unică.
(Se va considera cel mai mic întreg a care admite două descompuneri distincte:

$$a = m_1 m_2 \ldots m_p, \qquad m_1 \leqslant m_2 \leqslant \ldots \leqslant m_p,$$

$$a = n_1 n_2 \ldots n_q, \qquad n_1 \leqslant n_2 \leqslant \ldots \leqslant n_q,$$

și se va arăta succesiv că m_1 este distinct de n_1, că m_1 nu poate divide cîtul lui a prin n_1 și că egalitățile $m_1 < n_1$ și $n_1 < m_1$ sînt false amîndouă.)

3.10. Să se descompună în factori următorii întregi:

450, 480, 1 600, 1 848, 3 960, 6 006, 8 200, 1 332, 8 472, 18 840, 16 808, 111 111, 111 333
125 250, 125 375, 183 652, 288 144, 360 360.

3.11. Să se descompună în factori fără să se calculeze, întregii $n!$, cu n mai mic sau egal cu 15.

3.12. Să se determine exponentul întregului 3 în descompunerea numărului 100!

3.13. Să se demonstreze că suma a doi întregi impari consecutivi este divizibilă cu 4.

3.14. Care este restul modulo 3 al întregului $\frac{x(x+1)}{2}$?

3.15. Să se calculeze restul modulo 7 al întregului $(32)^{48}$.

3.16. Ce se poate spune despre restul modulo 5 al pătratului unui număr întreg? Ce se poate spune despre restul modulo 8 al pătratului unui număr impar?

3.17. Să se rezolve congruențele:

$$x^2 \equiv 0 \quad [7];$$

$$x^2 \equiv 1 \quad [7];$$

$$x^2 \equiv 2 \quad [7];$$

$$x^2 \equiv 3 \quad [7].$$

3.18. Care sînt întregii relativi a astfel încît congruența:

$$x^3 \equiv a \quad [7]$$

să aibă cel puțin o soluție?

3.19. Să se demonstreze că dacă un întreg x divide întregii $a'-a$, $b'-b$ și $c'-c$, el divide atunci întregii $a'b'c' - abc$ și $(a'b'c')^n - (abc)^n$ $(n \in \mathbf{N})$.

3.20. Care sînt întregii n:

a) astfel încît n să dividă pe $(n + 8)$?

b) astfel încît $(n - 1)$ să dividă pe $(n + 11)$?

c) astfel încît $n - 4$ să dividă pe $3n + 24$?

3.21. Să se demonstreze că întregul $x(x + 1)(x + 2)$ este divizibil cu 2 și cu 3.

3.22. Să se rezolve congruența:

$$x(x + 1)(2x + 1) \equiv 0 \quad [6].$$

3.23. Să se demonstreze că întregul $x(x + 1)(x + 2)(x + 3)(x + 4)$ este divizibil cu 3 cu 5 și cu 8.

3.24. Să se demonstreze că întregul:

$$10^n(9n - 1) + 1, \quad (n \in \mathbf{N})$$

este un multiplu de 9.

3.25. Să se demonstreze că întregul relativ:

$$x(2x + 1)(7x + 1), \quad x \in \mathbf{Z}$$

este divizibil cu 2 și cu 3.

3.26. Să se demonstreze că întregul relativ:

$$xy(x^2 - y^2)$$

este un multiplu de 3, $(x, y) \in \mathbf{Z}^2$.

3.27. Să se demonstreze că, pentru ca un număr scris în sistemul zecimal să fie divizibil cu 6, este necesar și suficient ca suma dintre cifra unităților și de patru ori suma celorlalte cifre să fie divizibilă cu 6.

3.28. Să se demonstreze că, oricare ar fi n aparținînd lui **N**:

$$7^n - 7^{n-2} \equiv 12 \quad [36];$$

$$9^n - 9^{n-2} \equiv 16 \quad [64];$$

$$11^n - 11^{n-2} \equiv 20 \quad [100];$$

$$(2m+1)^n - (2m+1)^{n-2} \equiv 4m \quad [4m^2],\ m \in \mathbf{N}.$$

3.29. Să se demonstreze că întregul: $a = p_n + p_{n+1}$ nu este prim și că divizorii săi primi sînt strict mai mici ca p_n (p_n este al n-lea număr prim natural).

3.30. Să se demonstreze că egalitatea:

$$p_{n+1} = p_n + 2$$

implică una din cele trei congruențe:

$$p_n \equiv -1 \quad [30],\ p_n \equiv 11 \quad [30],\ p_n \equiv 17 \quad [30].$$

3.31. Să se determine două numere prime naturale p și q astfel încît:

$$p^2 = 8q + 1.$$

3.32. Să se demonstreze că, dacă $a^n - 1$ este prim, a trebuie să fie egal cu 2.
Să se demonstreze că, dacă n este compus, $2^n - 1$ nu este prim.
Să se demonstreze că, dacă p este prim, $2^p - 1$ este prim pentru anumite valori ale lui p și este compus pentru alte valori ale lui p.
(Numerele prime de forma $2^p - 1$ sînt numite *numerele lui Mersenne*,)

3.33. Să se demonstreze că, dacă $2^n + 1$ este prim, n trebuie să fie o putere a lui 2. (Numerele prime de forma $2^{2^n} + 1$ sînt numite *numerele lui Fermat*.)
Să se verifice, prin congruențe modulo 641, congruența:

$$2^{32} + 1 \equiv 0 \quad [641].$$

Există numere prime de forma $a^n + 1$, cu: $a > 2$?

3.34. Să se descompună în factori toate numerele:

$$n = a^4 + 4 \quad (0 \leqslant a \leqslant 6).$$

Există numere prime de această formă?

3.35. Să se demonstreze că, dacă p, q, r sînt trei numere prime mai mari sau egale ca 5, întregul $p^2 + q^2 + r^2$ este compus.

3.36. Să se demonstreze că suma a cel puțin doi întregi impari consecutivi este compusă.

3.37. Să se determine restul modulo 5 al întregului:

$$(2\,222)^{3\,\overbrace{333}} + (3\,333)^{2\,222}.$$

3.38. Să se determine întregii n astfel încît 13 să dividă întregul:

$$3^{2^n} + 3^n + 1.$$

3.39. Să se calculeze produsul:

$$(a^3 - a + 1)(a^2 + a + 1).$$

Numărul $a^4 + a^2 + 1$ poate fi prim?

3.40. Să se demonstreze că, dacă p este un număr prim:

$$(p \mid 1\,806) \Longleftrightarrow (p - 1 \mid 1\,806).$$

3.2. ÎNTREGI PRIMI RELATIVI

3.2.1. Numere prime în Z

Orice întreg relativ x are 1,(−1), x şi $(-x)$ ca divizori care aparţin lui **Z**. Anumiţi întregi au şi mai mulţi; de exemplu, 24 are 16 divizori, care formează mulţimea (conform nr. 3.1.2):

$$\text{div } 24 = \{1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 8, -8, 12, -12, 24, -24\}.$$

(Aici, div x este mulţimea divizorilor lui x care aparţin lui **Z**.)
Implicaţia:

$$(x = yz) \Longrightarrow (|x| = |y|\ |z|)$$

arată că mulţimea div x este formată din divizorii lui $|x|$ care aparţin lui **N** şi din opuşii lor.
Anumiţi întregi, ca (−13) sau (+17), nu au decît patru divizori, de exemplu:

$$div(-13) = \{+1,\ -1,\ +13,\ -13\}.$$

Putem stabili imediat teorema următoare:

TEOREMA 5 / **Un întreg relativ este numit prim dacă el are exact patru divizori care aparţin lui Z. Un întreg relativ este prim dacă şi numai dacă valoarea sa absolută este un număr prim natural; el este compus dacă şi numai dacă valoarea sa absolută este compusă.**

Teorema 4 se generalizează imediat. Teorema 3 poate fi extinsă şi ea la **Z**. Introducem pentru aceasta noţiunea de unitate în **Z**; o unitate este un divizor al lui 1, deci unul din cele două numere 1 şi (−1). Deducem atunci imediat teorema următoare:

TEOREMA 6 / **Orice întreg relativ diferit de −1, 0 sau 1 se poate scrie ca produs de numere prime naturale şi de o unitate.**

Divizibilitatea în **Z** se reduce imediat la divizibilitatea în **N** şi la considerarea semnelor factorilor.

În anumite probleme, poate fi avantajos să considerăm congruenţe de module negative. De aceea convenim spre exemplu să punem:

$$\boxed{\mathbf{Z}/x\mathbf{Z} = \mathbf{Z}/(-x)\mathbf{Z}} \tag{11}$$

(cu condiţia de a identifica, bineînţeles, pe $\mathbf{N}$ cu $\mathfrak{Z} \cup \{0\}$. Astfel, studiul inelelor $\mathbf{Z}/p\mathbf{Z}$, unde p este prim în $\mathbf{Z}$, este identic cu cel al inelelor $\mathbf{Z}/p\mathbf{Z}$, unde p este prim în $\mathbf{N}$.

3.2.2. Corpuri Z/pZ

Să considerăm un element α nenul al inelului $\mathbf{Z}/p\mathbf{Z}$, unde p este un întreg relativ diferit de 0 sau 1.

1. Să presupunem că există un element β *nenul* al acestui inel astfel încît:

$$\alpha\beta = \bar{0}.$$

(De exemplu, în $\mathbf{Z}/30\mathbf{Z}$, putem scrie:

$$\alpha = \bar{3},\ \beta = \bar{20},\ \alpha\beta = \bar{3} \times \bar{20} = \bar{60} = \bar{0}).$$

β este clasa unui întreg b, cu:

$$0 < b < |\,p\,|.$$

Fie c cel mai mic întreg astfel încît:

$$0 < c < |\,p\,|,\quad \gamma = \bar{c},\quad \alpha\gamma = \bar{0}.$$

Cum α nu este clasa nulă, c este diferit de 1:

$$1 < c < |\,p\,|.$$

Să împărţim pe p la c:

$$p = cq + r,\quad 0 \leqslant r < c.$$

Atunci:

$$\alpha\bar{r} = \alpha(\overline{p - cq}) = \bar{0} - \alpha\gamma\bar{q} = \bar{0}.$$

Cum c este minimum, avem deci $r = 0$, şi c divide pe $|\,p\,|$ (conform exerciţiului 1, nr. 2.4.5). Pentru $p = 30$, $\alpha = \bar{3}$, se găseşte, într-adevăr, $c = 10$.

2. Să presupunem p prim; c este atunci egal cu 1 sau cu $|\,p\,|$, dar cele două cazuri sînt excluse de inegalitatea:

$$1 < c < |\,p\,|.$$

În inelul $\mathbf{Z}/p\mathbf{Z}$, produsul a două elemente nenule este deci de asemenea nenul; $\mathbf{Z}/p\mathbf{Z}$ este un inel integru dacă p este prim. Dacă p este compus, $\mathbf{Z}/p\mathbf{Z}$ nu este integru căci:

$$(p = ab) \Longrightarrow (\bar{a} \times \bar{b} = \overline{ab} = \bar{0}).$$

3. Aplicația definită prin:

$$\mathfrak{f} = [\beta \longmapsto \alpha\beta] \quad (\alpha \neq 0)$$

este *injectivă* căci:

$$(\alpha\beta = \alpha\gamma) \Longleftrightarrow (\alpha(\beta - \gamma) = 0) \Longleftrightarrow (\beta - \gamma = 0).$$

Imaginea lui $\mathbf{Z}/p\mathbf{Z}$ prin $\mathfrak{f}$ are deci același cardinal ca $\mathbf{Z}/p\mathbf{Z}$, care are p elemente; Aplicația $\mathfrak{f}$ este deci *surjectivă*. Există deci o clasă β astfel încît: $\alpha\beta = \bar{1}$. Cum $\bar{1}$ este element neutru pentru înmulțire, α este deci inversabil în $\mathbf{Z}/p\mathbf{Z}$, care este un corp cu p elemente. Se notează în general F_p.
Reciproc, dacă $\mathbf{Z}/p\mathbf{Z}$ este un corp, este a fortiori un inel integru, căci:

$$(\alpha \neq \bar{0} \text{ și } \alpha\beta = \bar{0}) \Longrightarrow (\beta = \alpha^{-1}(\alpha\beta) = \alpha^{-1}\ \bar{0} = \bar{0}).$$

Am văzut că aceasta interzicea lui p să fie compus.
4. $\mathbf{Z}/0\mathbf{Z}$ este un inel izomorf cu $\mathbf{Z}$; acest inel este deci integru, dar nu este corp.
$\mathbf{Z}/1\mathbf{Z}$ este o mulțime cu un singur element: nu este corp, căci grupul multiplicativ al unui corp nu este vid. Este deci un inel integru care nu este corp.

TEOREMA 7 / **Inelul $\mathbf{Z}/p\mathbf{Z}$ este un corp, notat F_p, dacă și numai dacă p este prim. Este un inel integru dacă și numai dacă p nu este compus.**

5. Să transcriem teorema 5 în $\mathbf{Z}$. Dacă p este un număr prim, și dacă produsul: $\alpha\beta = \bar{a} \times \bar{b} = \overline{ab}$
este clasa nulă (adică dacă p divide pe ab), atunci $\alpha = \bar{0}$ sau $\beta = \bar{0}$ (adică p divide pe a sau p divide pe b).

$$\boxed{(p \text{ prim și } p \mid ab) \Longrightarrow (p \mid a \text{ sau } p \mid b)}. \tag{12}$$

TEOREMA 8 / **Un număr prim nu divide un produs de factori decît dacă, și numai dacă, divide cel puțin unul din ei.**

6. Să presupunem că un întreg n mai mare sau egal ca 2 admite două descompuneri distincte în produs de numere prime naturale (nu vom distinge descompunerile care diferă numai prin ordine): presupunem deci că există un număr prim p cu un exponent k în unul, și cu un exponent h (care poate fi nul) în altul, astfel încît:

$$n = p^h m = p^h r, \quad k > h \geqslant 0.$$

Deducem:

$$r = p^{k-h} m, \quad k - h \geqslant 1.$$

p divide deci pe r; or r este un produs de numere prime distincte de p; prin inducție în raport cu numărul de divizori primi ai lui r, se arată ușor că se contrazice teorema 6. În final:

TEOREMA 9 / **Descompunerea unui număr întreg mai mare sau egal cu 2 într-un produs de numere prime naturale este posibilă într-un mod unic, atunci cînd se face abstracție de ordinea factorilor.**

7. Putem extinde teorema 9 la **Z**, în același mod în care am trecut deja de la teorema 3, valabilă în **N**, la teorema 6, valabilă în **Z**.
Putem deci enunța:

TEOREMA 10 / **Descompunerea unui număr întreg relativ diferit de −1, 0 sau 1 într-un produs de numere prime naturale și de o unitate este posibilă într-un mod unic, atunci cînd se face abstracție de ordinea factorilor.**

Să dăm alte două demonstrații ale faptului că $\mathbf{Z}/p\mathbf{Z}$ este un corp pentru p prim.

■ Se demonstrează, cum am făcut-o mai înainte, că $\mathbf{Z}/p\mathbf{Z}$ este integru.
Să considerăm atunci o clasă nenulă α, și puterile sale succesive:

$$\alpha,\ \alpha^2,\ \alpha^3,\ \ldots,\ \alpha^u,\ \ldots,\ \alpha^v,\ \ldots$$

Cum numărul elementelor lui $\mathbf{Z}/p\mathbf{Z}$ este finit, există în mod obligatoriu doi exponenți u și v astfel încît:

$$u < v, \qquad \alpha^u = \alpha^v,$$

sau încă:

$$\overline{0} = \alpha^u(\alpha^{v-u} - \overline{1}),$$

ceea ce implică, deoarece α este diferit de $\overline{0}$:

$$\overline{0} = \alpha^{v-u} - \overline{1}.$$

Prin urmare:

$$\alpha \times \alpha^{v-u-1} = \overline{1};$$

deci α este inversabil; $\mathbf{Z}/n\mathbf{Z}$ este un corp.
■ A doua demonstrație arată altfel. Fie submulțimea G a multiplilor lui α care aparțin lui $\mathbf{Z}/p\mathbf{Z}$; G este un grup aditiv căci îl conține pe $\overline{0}$ și:

$$\alpha\beta + \alpha\gamma = \alpha(\beta + \gamma),$$
$$\alpha(-\beta) = -(\alpha\beta).$$

Relația, definită în inelul $\mathbf{Z}/p\mathbf{Z}$ prin:

$$\beta - \gamma \in G,$$

este o relație de echivalență (conform demonstrației date la nr. **2.4.2**). Fiecare din clase conține același număr de elemente, egal cu cardinalul lui G. Acest cardinal divide deci pe $|\ p\ |$, cardinal al inelului $\mathbf{Z}/p\mathbf{Z}$; el este deci egal cu 1 sau $|\ p\ |$.
Dacă α nu este clasa nulă, G conține pe $\overline{0}$ și α; cardinalul său este deci $|\ p\ |$; de unde:

$$G = \mathbf{Z}/p\mathbf{Z}.$$

Rezultă existența unui element β astfel încît:

$$\alpha\beta = \overline{1} \in G.$$

La numărul **3.4.3.** vom da a patra demonstrație a acestei teoreme fundamentale.

3.2.3. Exerciții referitoare la divizibilitate

Problemele referitoare la divizibilitatea în **Z**, și mai ales acelea referitoare la numere prime, sînt foarte numeroase. Noi am grupat aici cîteva exerciții tipice în care nu intervin noțiunile de c.m.M.d.c și c.m.m.m. c pe care le vom trata mai tîrziu.

EXERCIȚII

I. *Cu ajutorul exercițiului nr. 1.62 (pagina 52), să se rezolve ecuația definită pe* $\mathbf{N}$ *prin:*

$$x^y = y^x.$$

Să presupunem: $x \geqslant y > 0$.
Egalitatea $x^y = y^y \times y^{x-y}$ arată că y^y divide pe x^y. Fie p un divizor prim al lui y; el figurează cu exponentul m. În y^y figurează deci divizorul p^{my}. Fie k exponentul lui p în x ($k = 0$ dacă p nu divide pe x). Datorită unicității descompunerii, p^{ky} figurează în x^y și avem deci:

$$(my \leqslant ky) \Longrightarrow (m \leqslant k).$$

Această relație fiind adevărată pentru orice divizor prim al lui y, se poate deduce că y divide pe x; de unde egalitatea:

$$x = ny.$$

Exercițiul nr. 1.62 arată că această egalitate nu este verificată pentru n mai mare ca 1 și y mai mare sau egal cu 3.
Cazul $n = 1$ dă soluția imediată $x = y$ (chiar pentru $y = 0$).
Cazul $y = 1$ este de asemenea imediat:

$$x = x^1 = 1^x = 1 = y.$$

În sfîrșit, pentru $y = 2$, avem:

$$x = 2n, \quad x^2 = 2^x,$$
$$4n^2 = 2^{2n} \text{ sau } (2n)^2 = (2^n)^2,$$

fie:

$$2n = 2^n \text{ (exercițiul nr. 1.28, pagina 42)},$$
$$n = 2^{n-1}.$$

Or știm (nr. 1.3.5, pagina 48) că aceasta echivalează cu $n = 1$ (de unde $x = y = 2$) sau cu $n = 2$ (de unde $x = 4$, $y = 2$).
În final ecuația $x^y = y^x$ admite soluțiile $x = y$ și:

$$x = 4 \text{ și } y = 2, \qquad x = 2 \text{ și } y = 4.$$

II. *Să se demonstreze că, pentru* x, y, z, t *elemente ale lui* $\mathbf{Z}$, *egalitatea:*

$$x^2 + 5y^2 = 2(z^2 + 5t^2)$$

este echivalentă cu:

$$x = y = z = t = 0.$$

Să punem: $n = x^2 - 2z^2 = (-5)(y^2 - 2t^2)$. Mulțimea M a întregilor nenuli n care se pot scrie sub această dublă formă este, poate, vidă. Dacă nu este vidă, să considerăm întregul n din această mulțime care are cea mai mică valoare absolută. Atunci:

$$x^2 \equiv 2z^2 \ [5].$$

Să presupunem mai întîi că 5 divide pe z; atunci:

$$x^2 \equiv 0 \ [5].$$

Întregul 5 fiind prim, deducem $x \equiv 0$; de unde:

$$x = 5u,\ z = 5v,\ n = -5m$$

$$(\text{cu } m = 10v^2 - 5u^2),$$

și:

$$m = y^2 - 2t^2 = (-5)\,(u^2 - 2v^2).$$

Întregul n fiind minim, această egalitate este contradictorie căci:

$$|\,m\,| = |\,\frac{-n}{5}\,| < |\,n\,|.$$

Deci, 5 nu divide pe z. Dar atunci, $\bar{z}$ are un invers $\bar{w}$ care aparține lui $\mathbf{Z}/5\mathbf{Z}$; de unde:

$$\bar{2} = (\bar{x})^2\,(\bar{w})^2 = (\overline{xw})^2.$$

Dar pătratele elementelor lui $\mathbf{Z}/5\mathbf{Z}$ sînt respectiv egale cu:

$$\bar{0}^2 = \bar{0},\quad \bar{1}^2 = \bar{4}^2 = \bar{1},\quad \bar{2}^2 = \bar{3}^2 = \bar{4},$$

și nici unul din ele nu este egal cu 2.
În final, n este nul; de unde:

$$x^2 - 2z^2 = 0,$$

$$y^2 - 2t^2 = 0.$$

Egalitatea $x^2 = 2z^2$ arată, ca și în exercițiul precedent, că z divide pe x (se vor considera toți divizorii primi ai lui z); de unde egalitățile:

$$x = kz,\ k^2 = 2\ (\text{dacă } z \neq 0).$$

Nu există întregi astfel încît $k^2 = 2$; deducem că z și x sînt nuli.
Se întîmplă același lucru cu y și t.

III. *Să se rezolve ecuația definită pe* **N** *prin:*

$$x^2 + y^3 = y^6.$$

Să o scriem sub forma:

$$x^2 = y^3(y^3 - 1).$$

y^2 divide pe x^2. Deci, y divide pe x; să punem:

$$x = \lambda y,\ \lambda^2 = y(y^3 - 1)\ (\text{dacă } y \neq 0).$$

Printre divizorii primi ai lui y, să-i grupăm pe toți care sînt la pătrat pentru a forma un număr u^2, citul lui y prin u^2 neavînd nici un divizor la pătrat altul decît 1, de exemplu:

$$y = 360 = 2^3 3^2 5 = (2 \times 3)^2\,(2 \times 5).$$

Se poate scrie atunci:

$$(y = u^2v) \Longrightarrow (u^2 \mid \lambda^2) \Longrightarrow (u \mid \lambda).$$

Punînd în sfîrșit $\lambda = \mu u$, deducem:

$$\mu^2 = v(y^3 - 1) = v(u^6v^3 - 1) \qquad (u \neq 0).$$

Cum v nu admite nici un divizor la pătrat, trebuie ca $(u^6v^3 - 1)$ să fie multiplu de v; dar aceasta implică v divide pe 1, deci că $v = 1$ (sîntem în N), sau în sfîrșit:

$$\mu^2 = u^6 - 1,$$

$$(u^3 + \mu)(u^3 - \mu) = 1.$$

$u^3 + \mu$ și $u^3 - \mu$ fiind atunci în mod obligatoriu egale (fie cu 1, fie cu -1), deducem $\mu = 0$; de unde:

$$\lambda = 0 \text{ și } x = 0.$$

Singurele soluții ale ecuației sînt deci:

$$(y = 0,\ x = 0) \text{ sau } (y = 1,\ x = 0).$$

IV. *Același exercițiu ca precedentul, x și y aparținînd lui* **Z**.
Sînt valabile aceleași raționamente cu condiția de a admite că v poate fi atunci negativ. Dar condiția $(v \mid 1)$ conduce la $v = 1$ sau $v = -1$. În acest ultim caz:

$$\mu^2 = u^6 + 1,$$

$$(\mu + u^3)(\mu - u^3) = 1;$$

de unde $u = 0$ și, în sfîrșit:

$$y = x = 0.$$

Trecerea de la **N** la **Z** nu dă soluții noi.

V. *A și B fiind doi întregi strict pozitivi care nu sînt multipli ai unui număr prim p, să se demonstreze că ecuația definită prin $p = Ax^2 + By^2$ nu are decît cel mult o soluție care aparține lui* **N**.
Să presupunem că există două soluții:

$$p = Ax^2 + By^2 = Aa^2 + Bb^2,$$

$$(b^2 - y^2)p = b^2(Ax^2 + By^2) - y^2(Aa^2 + Bb^2)$$

$$= A(b^2x^2 - a^2y^2).$$

Există deci o unitate:

$$\varepsilon \in \{-1,\ +1\}$$

astfel încît p divide $(bx + \varepsilon ay)$. Să punem:

$$bx + \varepsilon ay = \lambda p.$$

Să folosim această relație în egalitatea, ușor de verificat:

$$(Aax - \varepsilon Bby)^2 + AB(bx + \varepsilon ay)^2 = (Aa^2 + Bb^2)(Ax^2 + By^2).$$

Deducem:

$$(Aax - \varepsilon Bby)^2 + AB\lambda^2 p^2 = p^2,$$

de unde:

$$AB\lambda^2 \leqslant 1.$$

Pentru $\lambda = 0$, se găsește $\varepsilon = -1$, și egalitățile:

$$bx = ay,$$

$$\left(\frac{a}{x}\right)^2 = \left(\frac{b}{y}\right)^2 = \frac{Aa^2 + Bb^2}{Ax^2 + By^2} = 1,$$

de unde:

$$x = a,\ y = b.$$

Pentru $\lambda = A = B = 1$, găsim:

$$ax = \varepsilon by,\ \varepsilon = +1,$$

de unde:

$$\left(\frac{a}{y}\right)^2 = \left(\frac{b}{x}\right)^2 = \frac{a^2 + b^2}{y^2 + x^2} = 1$$

și:

$$x = b,\ y = a.$$

În particular, un număr prim nu este suma a două numere la pătrat ($A = B = 1$) decît într-un singur mod (exemplu: $29 = 5^2 + 2^2$) sau în nici unul (exemplu: $7 = x^2 + y^2$ nu are soluții).

VI. *Să se demonstreze că numărul $p = 2n + 1$ este prim dacă și numai dacă nu figurează în următorul tablou infinit:*

$$\begin{pmatrix} 4 & 7 & 10 & 13 & 16 & \dots \\ 7 & 12 & 17 & 22 & 27 & \dots \\ 10 & 17 & 24 & 31 & 38 & \dots \\ 13 & 22 & 31 & 40 & 49 & \dots \\ 16 & 27 & 38 & 49 & 60 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

unde a m-a linie este o progresie aritmetică de rație $(2m + 1)$, prima coloană fiind progresia aritmetică de rație 3, cu primul termen 4.
Se poate arăta ușor că primul termen al liniei a m-a este egal cu:

$$3m + 1.$$

Deducem atunci termenul de rang k din a m-a linie:

$$a_{m,k} = (k - 1)(2m + 1) + (3m + 1)$$
$$= 2mk + m + k.$$

Dacă p este compus, el este produsul a doi întregi obligatoriu impari:

$$p = (2m + 1)(2k + 1);$$

de unde:

$$n = \frac{p-1}{2} = \frac{4mk + 2k + 2m}{2} = a_{m,k}.$$

Reciproc, $n = a_{m,k}$ implică că p este compus.

VII. *Se consideră șirul definit prin:*

$$m \longmapsto u_m = \frac{m(m+1)}{2}.$$

Să se demonstreze că numărul $p = 2n + 1$ *este prim dacă și numai dacă primii* n *termeni ai șirului au resturi distincte în împărțirea la* p.

Dacă p este prim și dacă:

$$1 \leqslant m < k \leqslant n,$$

atunci:

$$2(u_k - u_m) = (k - m)(k + m + 1),$$

cu:

$$1 \leqslant k - m < k \leqslant n < p,$$

și:

$$4 \leqslant k + m + 1 \leqslant n + m + 1 \leqslant 2n < p.$$

p nu divide deci nici unul din termenii produsului $2(u_k - u_m)$, și nu divide deci nici pe $u_k - u_m$.

Dacă p este compus, să punem:

$$p = ab \ (a \geqslant 3,\ b \geqslant 3).$$

a și b sînt impare, $a - 2b$ nu este nul. Distingem mai multe cazuri:

■ $a - 2b > 1$.

Să punem atunci:

$$m = \frac{a-1}{2} - b,\ k = \frac{a-1}{2} + b;$$

găsim:

$$1 \leqslant m < k \leqslant n,\ u_k - u_m = ab = p.$$

■ $a - 2b < -1$.

Să punem atunci:

$$m = b - \frac{a+1}{2},\qquad k = b + \frac{a+1}{2};$$

găsim:

$$1 \leqslant m < k \leqslant n,\ u_k - u_m = ab = p.$$

Dacă $a - 2b$ este egal cu 1 sau cu -1, se vede atunci ușor că avem:

sau: $$b - 2a > 1,$$

sau: $$b - 2a < -1.$$

și continuăm în același mod. (Acest rezultat se pare că este datorat lui Guillaume.)

VIII. *Să se demonstreze că nu există nici un întreg n astfel încît mulțimea:*

$$E = \{n, n + 1, n + 2, n + 3, n + 4, n + 5\}$$

să se poată descompune în două submulțimi complementare astfel încît produsele elementelor din aceste submulțimi să fie egale.

Mulțimea E care conține cel mult un multiplu de 7, nu trebuie să conțină nici un multiplu de 7. Deci:

$$n \equiv 1, \ [7],$$
$$m = n(n + 1)(n + 2)(n + 3)(n + 4)(n + 5)$$
$$1 \times 2 \times 3 \times 4 \times 5 \times 6 = 720 \equiv 6 \ [7].$$

Dar, prin ipoteză, m este un pătrat perfect:

$$m = k^2 \equiv 6 \ [7].$$

Or în $\mathbf{Z}/7\mathbf{Z}$:

$$\bar{0}^2 = \bar{0}, \ \bar{1}^2 = \bar{6}^2 = \bar{1}, \ \bar{2}^2 = \bar{5}^2 = \bar{4}, \ \bar{3}^2 = \bar{4}^2 = \bar{2}.$$

Deci nu există nici un număr k astfel încît $k^2 \equiv 6 \ [7]$.

EXERCIȚII

3.41. Să se demonstreze că întregul natural n este prim sau egal cu 9 dacă, și numai dacă, el nu divide întregul $m!$, unde m este definit prin $n = 2m + 1$.

3.42. Să se demonstreze că întregul natural n divide întregul $m!$, unde m este astfel încît $n = 2m$, în afară de cazul cînd $n = 2$ sau $n = 4$.

3.43. Să se calculeze exponentul numărului natural prim p în produsul:

$$(n + 1)(n + 2) \ldots (m + 1)m,$$

unde $m = pn$.

3.44. Să se demonstreze că aplicația:

$$(a, b) \longmapsto 2^a(2b + 1)$$

este o bijecție între $\mathbf{N} \times \mathbf{N}$ și $\mathbf{N}$.

3.45. Să se demonstreze că relația pe $\mathbf{N} \times \mathbf{N}$, definită prin:

$$[(a, b) \leqslant (c, d)] \Longleftrightarrow [2^d(2a + 1) \leqslant 2^b(2c + 1)],$$

este o relație de ordine totală; $\mathbf{N} \times \mathbf{N}$ nu are atunci nici cel mai mare nici cel mai mic element.

3.46. Să se demonstreze egalitatea, în inelul $\mathbf{Z}/48\mathbf{Z}$:

$$x^3 + 3x^2 = x + 3.$$

3.47. n fiind cubul unui număr prim p, să se rezolve în inelul $\mathbf{Z}/n\mathbf{Z}$ ecuațiile definite prin:

$$x^2 = x, \ x^2 = 0, \ x^2 = 1.$$

3.48. În corpul $\mathbf{Z}/7\mathbf{Z}$ să se rezolve ecuația definită prin:

$$x^3 = 3x^2 + 2.$$

3.49. Se consideră mulțimea E a ecuațiilor de gradul doi definite prin:

$$x^2 + ax + b = 0,$$

unde a și b sînt elemente ale corpului $\mathbf{Z}/p\mathbf{Z}$. Să se numere elementele din mulțimea E.

3.50. În corpul $\mathbf{Z}/p\mathbf{Z}$ să se numere elementele din mulțimea F a polinoamelor de forma:

$$(x - u)(x - v).$$

Să se deducă de aici că în acest corp există ecuații de gradul doi care nu admit nici o soluție.

3.3. MULTIPLI ȘI DIVIZORI COMUNI

3.3.1. Subgrupuri ale lui Z

Știm că adunarea face din $\mathbf{Z}$ un grup aditiv. O submulțime ca $n\mathbf{Z}$, unde n este un întreg natural, este încă un grup în raport cu restricția acestei adunări. Într-adevăr, suma a două elemente din $n\mathbf{Z}$ aparține lui $n\mathbf{Z}$; ea este și asociativă. Pe de altă parte, 0 este element neutru în $n\mathbf{Z}$ ca și în $\mathbf{Z}$, și opusul unui element din $n\mathbf{Z}$ este de asemenea element din $n\mathbf{Z}$ (conform nr. **2.4.1**, pagina 96):

$$\begin{cases} nx + ny = n(x + y) \\ 0 = n0 \\ -(nx) = n(-x). \end{cases}$$

Vom spune că $n\mathbf{Z}$ este un *subgrup* al lui $\mathbf{Z}$. În general, o submulțime H a unui grup G înzestrat cu o lege „$*$“ este un subgrup dacă și numai dacă H conține elementul neutru al lui G, opușii elementelor sale, și dacă H este considerat în raport cu legea „$*$“.

EXERCIȚIU

Să se demonstreze că H este un subgrup al grupului multiplicativ $(G, \times)$ dacă și numai dacă:

$$H \neq \varnothing \text{ și } (a \in H \text{ și } b \in H) \Longrightarrow (a \times b^{-1} \in H).$$

■ Mulțimea H nu este vidă. Fie a un element care aparține lui H; prin ipoteză:

$$(a \in H) \Longrightarrow (e = a \times a^{-1} \in H);$$

deci, H conține elementul neutru.
■ Avem acum:

$$(e \in H \text{ și } a \in H) \Longrightarrow (e \times a^{-1} \in H);$$

or:

$$e \times a^{-1} = a^{-1};$$

deci, H conține opusul lui a.
În sfîrșit:

$$(a \in H \text{ și } b \in H) \Longrightarrow (a \in H \text{ și } b^{-1} \in H)$$
$$\Longrightarrow [a \times b = a \times (b^{-1})^{-1} \in H];$$

deci, H conține produsul lui a cu b.
Reciproc, aceste condiții suficiente sînt evident necesare.
În cazul unui grup aditiv, ele se scriu:

$$H \neq \varnothing, \ (a \in H \text{ și } b \in H) \Longrightarrow (a - b \in H).$$

Ele sînt verificate evident pentru $\mathbf{Z}$ și $n\mathbf{Z}$ căci:

$$0 \in n\mathbf{Z}, \ (nx) - (ny) = n(x - y),$$

și $n(x - y)$ aparține lui $n\mathbf{Z}$.

Să demonstrăm că $\mathbf{Z}$ nu admite alte subgrupuri decît grupurile $n\mathbf{Z}$.
Într-adevăr, fie H un subgrup al lui $\mathbf{Z}$. Dacă nu este egal cu $\{0\} = 0\mathbf{Z}$, el conține cel puțin un element nenul.
Fie n cel mai mic întreg strict pozitiv astfel încît să existe în H un element de valoare absolută n:

$$x \in H, \qquad |x| = n.$$

Dacă avem $x = n$ sau $x = -n$, se deduce în ambele cazuri că n aparține lui H. Se întîmplă deci același lucru cu toate numerele de forma:

$$y = nk, \qquad (k \in \mathbf{Z}).$$

Într-adevăr este suficient să o demonstrăm prin inducție dublă în raport cu k:

$$n(k + 1) = nk + n,$$

deci:

$$(nk \in H) \Longrightarrow (n(k + 1) \in H);$$
$$n(k - 1) \Longrightarrow nk + (-n),$$

deci:

$$(nk \in H) \Longrightarrow (n(k - 1) \in H).$$

Fie în sfîrșit un element oarecare z al lui H. Împărțind pe z la n, deducem:

$$z = nk + r, \qquad 0 \leqslant r < n,$$

sau:

$$r = z - nk = z + n(-k);$$

deci:

$$r \in H.$$

Întregul n fiind minim, deducem $r = 0$, de unde $z = nk$; H și $n\mathbf{Z}$ sînt egale.
Deci toate mulțimile $n\mathbf{Z}$ sînt subgrupuri ale lui $\mathbf{Z}$ (la fel de altfel ca și subinelele și idealele lui $\mathbf{Z}$, considerat ca inel). Se spune că n este *generatorul* lui $n\mathbf{Z}$.

TEOREMA 11 / **Subgrupurile grupului aditiv Z sînt mulțimile $n\mathbf{Z}$ de multipli ai întregilor naturali n.**

3.3.2. Cel mai mic multiplu comun (c. m. m. m. c.)

Chiar definiția unui subgrup arată că *intersecția* unei familii de subgrupuri, adică mulțimea elementelor care aparțin tuturor subgrupurilor familiei, este tot un subgrup. (Aceasta este adevărat chiar și pentru o familie infinită).

1. Să considerăm deci o familie nevidă A de întregi relativi. Mulțimea multiplilor comuni tuturor elĕmentelor lui A este tot un subgrup, de forma $n\mathbf{Z}$. Generatorul n al lui $n\mathbf{Z}$ este numit *cel mai mic multiplu comun* al elementelor lui A (prescurtat: c.m.m.m.c); el divide toți multiplii comuni.

TEOREMA 12 / **Mulțimea multiplilor comuni ai elementelor unei familii nevide de întregi relativi este formată din multiplii unui întreg natural, numit c.m.m.m.c al elementelor familiei.**

De exemplu, dacă $A = \mathbf{Z}$, c.m.m.m.c este egal cu 0, singurul element comun tuturor $n\mathbf{Z}$.
Dacă $A = \{x\}$, c.m.m.m.c este egal cu $|x|$.

2. Dacă familia A este infinită, c.m.m.m.c este în mod obligatoriu 0, căci c.m.m.m.c are o infinitate de divizori.
Din contră, dacă familia A este finită, produsul tuturor elementelor lui A este evident un multiplu comun: c.m.m.m.c nu este nul decît în cazul în care A îl conține pe 0.

TEOREMA 13 / **C.m.m.m.c al elementelor unei familii este diferit de 0 dacă și numai dacă această familie este finită și nu conține pe 0. El divide atunci produsul elementelor familiei.**

3. Pentru două elemente a și b, c.m.m.m.c se notează prin simbolul „$\smile$"; de exemplu:

$$10 \smile 6 = 30,$$

deoarece $(10\mathbf{Z}) \cap (6\mathbf{Z}) = 30\mathbf{Z}$.
Se obțin imediat egalitățile:

$$a \smile b = b \smile a \tag{13}$$
$$a \smile a = a \smile 1 = |a| \tag{14}$$
$$a \smile 0 = 0 \tag{15}$$

și relațiile:

$$a \mid (a \smile b), \qquad b \mid (a \smile b) \tag{16) (17}$$
$$(a \smile b) \mid ab \tag{18}$$
$$(a \mid x \text{ și } b \mid x) \Longleftrightarrow ([a \smile b] \mid x) \tag{19}$$

Relația de definiție a c.m.m.m.c se poate scrie:

$$\boxed{a\mathbf{Z} \cap b\mathbf{Z} = (a \smile b)\mathbf{Z}} \tag{20}$$

4. Aceste relații se pot obține printr-un calcul simplu cu mulțimi. Într-adevăr, egalitățile (13), (14) și (15) sînt simple traduceri ale egalităților:

$$a\mathbf{Z} \cap b\mathbf{Z} = b\mathbf{Z} \cap a\mathbf{Z},$$
$$a\mathbf{Z} \cap a\mathbf{Z} = a\mathbf{Z} \cap 1\mathbf{Z} = |\, a \,|\mathbf{Z},$$
$$a\mathbf{Z} \cap 0\mathbf{Z} = 0\mathbf{Z}.$$

Pe de altă parte, relația $(a \mid b)$ este echivalentă cu $(b = ac)$; orice element al lui $b\mathbf{Z}$ este deci multiplu de a; de unde incluziunea:

$$b\mathbf{Z} \subset a\mathbf{Z}.$$

Reciproc, această incluziune implică b aparține lui $a\mathbf{Z}$, și este deci multiplu de a. Prin urmare:

$$\boxed{(a \mid b) \Longleftrightarrow (b\mathbf{Z} \subset a\mathbf{Z})} \tag{21}$$

5. Această echivalență ne permite să scriem imediat relațiile (16), (17) și (19) cu ajutorul mulțimilor:

$$(a \smile b)\mathbf{Z} \subset a\mathbf{Z},\ (a \smile b)\mathbf{Z} \subset b\mathbf{Z},$$
$$[(x\mathbf{Z} \subset a\mathbf{Z}) \text{ și } (x\mathbf{Z} \subset b\mathbf{Z})] \Longleftrightarrow [x\mathbf{Z} \subset (a \smile b)\mathbf{Z}].$$

Traducerea cu ajutorul mulțimilor a relației (18) este mai puțin evidentă:

$$(ab)\mathbf{Z} \subset (a \smile b)\mathbf{Z}.$$

Ea provine din cele două incluziuni:

$$(ab)\mathbf{Z} \subset a\mathbf{Z},\ (ab)\mathbf{Z} \smile b\mathbf{Z}$$

care implică relația:

$$(ab)\mathbf{Z} \subset (a\mathbf{Z} \cap b\mathbf{Z}) = (a \smile b)\mathbf{Z}.$$

6. Să notăm în sfîrșit echivalența importantă:

$$\boxed{(a \mid b) \Longleftrightarrow (a \smile b) = |\, b \,|)} \tag{22}$$

deoarece:

$$(a \mid b) \Longleftrightarrow (b\mathbf{Z} \subset a\mathbf{Z}) \Longleftrightarrow (a\mathbf{Z} \cap b\mathbf{Z} = |\, b \,|\mathbf{Z}).$$

(Să reamintim că c.m.m.m.c este obligatoriu pozitiv sau nul.)

7. Intersecția a trei mulțimi A, B și C se poate scrie într-una din cele două forme echivalente:

$$A \cap (B \cap C) = (A \cap B) \cap C,$$

De exemplu:

$$(a\mathbf{Z}) \cap [(b\mathbf{Z}) \cap (c\mathbf{Z})] = [(a\mathbf{Z}) \cap b\mathbf{Z})] \cap (c\mathbf{Z}).$$

C.m.m.m.c a trei întregi se poate deci scrie într-una din următoarele două forme echivalente:

$$\boxed{a \smile (b \smile c) = (a \smile b) \smile c} \qquad (23)$$

TEOREMA 14 / **C.m.m.m.c a doi întregi defineşte o lege comutativă şi asociativă în Z, notată prin semnul „$\smile$".**

Această lege are un element absorbant, care este 0. Dar nu are element neutru în Za$\smile$e) este pozitiv sau nul şi nu poate fi egal cu a dacă a este strict negativ). Din contră, există o restricţie la N a legii c. m. m. m. c pentru care 1 este neutru:

$$n \smile 1 = 1 \smile n = n \quad (n \geqslant 0.)$$

1 este de altfel singurul element care are un invers în N faţă de această lege, căci:

$$(n > 1) \Longrightarrow (n \smile 1 \geqslant n > 1).$$

Nici un element nu este regulat la această lege căci:

$$a \smile 1 = a \smile (-1) = |\, a \,|.$$

EXERCIŢII

I *Să se compare întregii* $(a \smile b) \times (c \smile d)$ şi $(ac \smile bd)$.
Să punem:

$$u = a \smile b, \; v = c \smile d, \; w = uv.$$

u este multiplu de a, v este multiplu de c : w este deci multip lu de ac. La fel, w este multiplu de bd. Prin urmare, $(ac \smile bd)$ divide pe w:

$$(ac \smile bd) \;/\; (a \smile b)\,(c \smile d).$$

În general nu are loc egalitatea, aşa cum arată următorul exemplu numeric.
Fie:

$$a = 1, \; b = c = 2, \; d = 3.$$

Avem:

$$ac \smile bd = 2 \smile 6 = 6,$$
$$a \smile b = 1 \smile 2 = 2,$$
$$c \smile d = 2 \smile 3 = 6,$$
$$(a \smile b)\,(c \smile d) = 12.$$

II. *Legea c.m.m.m.c este distributivă în raport: cu adunarea pe* Z? *cu înmulţirea pe* Z?
Egalitatea evidentă: $2 \smile (n + n) = 2 \smile n$ ($2 \smile n$ este egal cu n dacă n este par, şi cu $2n$ dacă n este impar) arată că prima distributivitate studiată nu este verificată în general. A doua nu este nici ea verificată, după cum arată exemplul:

$$[2 = 2 \smile (1 \times 1)] \neq [(2 \smile 1)\,(2 \smile 1) = 2^2 = 4].$$

3.3.3. Cel mai mare divizor comun (c. m. M. d. c.)

În timp ce intersecția unei familii de subgrupuri este un subgrup, *reuniunea* acestor subgrupuri nu este întotdeauna un grup. De exemplu, $\{\bar{0}, \bar{3}\}$ și $\{\bar{0}, \bar{2}, \bar{4}\}$ sînt subgrupuri ale lui $\mathbf{Z}/6\mathbf{Z}$, dar reuniunea lor $\{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$ nu este subgrup al lui $\mathbf{Z}/6\mathbf{Z}$.
Cel mai mic subgrup aditiv care conține o familie de subgrupuri — pe care o vom presupune finită pentru simplificare — este mulțimea sumelor de elemente luate din fiecare din subgrupuri. (Exercițiul nr. **3.57**, permite găsirea unei demonstrații a acestui rezultat.)

1. A fiind o familie finită de întregi relativi:

$$A = \{a, b, c, ..., l\},$$

cel mai mic subgrup H care conține:

$$a\mathbf{Z} \cup b\mathbf{Z} \cup c\mathbf{Z} \cup ... \cup l\mathbf{Z}$$

este deci mulțimea H a numerelor de forma:

$$x = \alpha a + \beta b + \gamma c + ... + \lambda l,$$

unde $\alpha, \beta, \gamma, ..., \lambda$ sînt întregi relativi.
Să verificăm că H este un subgrup al lui $\mathbf{Z}$:

$$0 = 0a + 0b + 0c + ... + 0l,$$
$$-x = (-\alpha)a + (-\beta)b + (-\gamma)c + ... + (-\lambda)l,$$
$$x + x' = (\alpha + \alpha')a + (\beta + \beta')b + ... + (\lambda + \lambda')l.$$

(Este inutil să verificăm asociativitatea adunării, căci ea este adevărată pe $\mathbf{Z}$.)

2. Mulțimea H este deci de forma $n\mathbf{Z}$, cu n aparținînd lui $\mathbf{N}$. Generatorul n al lui H este numit *cel mai mare divizor comun* al elementelor lui A (prescurtat: c.m.M.d.c); el divide toate *combinațiile liniare*:

$$x = \alpha a + \beta b + ... + \lambda l.$$

Întregul n aparține și el lui H; el se poate deci scrie sub forma:

$$\boxed{n = ua + vb + ... + tl} \qquad (24)$$

3. De exemplu, a aparține lui H, deoarece se poate scrie:

$$a = 1a + 0b + ... + 0l.$$

Deci, n divide pe a; la fel, n divide toate celelalte elemente ale lui A: este un divizor comun. La fel, orice divizor al lui n divide toate elementele lui A. *Reciproc*, orice divizor comun elementelor lui A divide pe n după relația (24), pe care o numim *identitatea lui Bezout* (datorată de fapt lui Bachet).
Deducem egalitatea importantă în care intervin mulțimi:

$$\boxed{div\ n = (div\ a) \cap (div\ b) \cap ... \cap (div\ l)} \qquad (25)$$

TEOREMA 15 / **Mulțimea divizorilor comuni elementelor unei familii finite nevidă de întregi relativi este formată din divizorii unui întreg natural, numit c.m.M.d.c al elementelor familiei.**
El generează subgrupul combinațiilor liniare ale elementelor familiei.

Restricția care impune familiei A să fie finită nu este esențială; este suficient în acest caz să-l definim pe H ca mulțimea combinațiilor liniare ale elementelor lui A în care numărul coeficienților nenuli este finit (de exemplu, mulțimea polinoamelor este egală cu aceea a combinațiilor liniare de monoame $a_n x^n$, care satisfac această condiție).

---

4. Pentru două elemente a și b c.m.M.d.c se notează cu semnul „$\frown$"; de exemplu:

$$10 \frown 6 = 2,$$

deoarece $(div\ 10) \cap (div\ 6) = div\ 2$.
Se obțin imediat egalitățile:

$$\boxed{\begin{array}{l} a \frown b = b \frown a \\ a \frown a = a \frown 0 = |\, a \,| \\ a \frown 1 = 1 \end{array}} \qquad \begin{array}{l} (26) \\ (27) \\ (28) \end{array}$$

și relațiile:

$$\boxed{\begin{array}{l} (a \frown b) \mid a \,(a \frown b) \mid b \\ x \mid a \text{ și } x \mid b) \Longleftrightarrow (x \mid [a \frown b]), \end{array}} \qquad \begin{array}{l} (29)\ (30) \\ (31) \end{array}$$

5. Egalitățile (25), (27) și (28) sînt simple transcrieri ale egalităților:

$$div\ a \cap div\ b = div\ b \cap div\ a,$$
$$div\ a \cap div\ a = div\ a \cap div\ 0 = div\ |a\ |,$$
$$div\ a \cap div\ 1 = div\ 1.$$

Pe de altă parte, relația $(a \mid b)$ este echivalentă cu $(b = ac)$; orice divizor al lui a divide deci pe b; de unde incluziunea: $div\ a \subset div\ b$.
Reciproc, această incluziune implică a aparține lui $div\ b$, și divide deci pe b.
Prin urmare:

$$\boxed{(a \mid b) \Longleftrightarrow (div\ a \subset div\ b)} \qquad (32)$$

6. Această echivalență permite scrierea imediată a relațiilor (29), (30) și (31) cu ajutorul mulțimilor:

$$div(a \frown b) \subset div\ a,\ div(a \frown b) \subset div\ b,$$
$$[(div\ x \subset div\ a) \text{ și } (div\ x \subset div\ b)] \Longleftrightarrow [div\ x \subset div\ (a \frown b)].$$

Să notăm în sfîrșit echivalența importantă:

$$\boxed{(a \mid b) \Longleftrightarrow (a \frown b) = |\, a \,|} \tag{33}$$

deoarece:

$$(a \mid b) \Longleftrightarrow (div\ a \subset div\ b) \Longleftrightarrow (div\ a \cap div\ b = div\ |a|).$$

(Să reamintim că c.m.M.d.c este obligatoriu pozitiv sau nul.)

7. Reuniunea a trei mulțimi A, B și C se poate scrie sub una din cele două forme echivalente:

$$A \cup (B \cup C) = (A \cup B) \cup C.$$

De exemplu:

$$(div\ a) \cup [(div\ b) \cup (div\ c)] = [(div\ a) \cup (div\ b)] \cup (div\ c).$$

C.m.M.d.c a trei întregi se poate deci scrie sub una din cele două forme echivalente:

$$\boxed{a \frown (b \frown c) = (a \frown b) \frown c} \tag{33}$$

TEOREMĂ 16 / **C.m.M.d.c a doi întregi definește o lege comutativă și asociativă pe Z, notată prin semnul „$\frown$".**

Această lege are un element absorbant care este 1. Dar nu are element neutru în Z. Din contră, există o restricție la N a legii c.m.M.d.c pentru care 0 este neutru:

$$n \frown 0 = 0 \frown n = n \qquad (n \geqslant 0).$$

Elementul 0 este de altfel singurul element care are un invers în N pentru această lege căci:

$$(n \frown m = 0) \Longrightarrow (0 \mid n) \Longrightarrow (n = 0).$$

Nici un element nu este regulat la această lege, căci:

$$a \frown 1 = a \frown (-1) = 1, \text{ deși } 1 \neq -1.$$

■ **O proprietate importantă a c.m.m.m.c și a c.m.M.d.c.**

Vom demonstra egalitățile următoare pentru c.m.m.m.c. și c.m.M.d.c.:

$$\boxed{\begin{array}{l} |\, a \,|(b \smile c) = ab \smile ac \\ |\, a \,|\, (b \frown c) = ab \frown ac \end{array}} \qquad \begin{array}{l} (34) \\ (35) \end{array}$$

Să studiem prima egalitate:

$$\begin{aligned} [n \in (ab\mathbf{Z} \cap ac\mathbf{Z})] &\Longleftrightarrow \left[\frac{n}{a} \in (b\mathbf{Z} \cap c\mathbf{Z})\right] \\ &\Longleftrightarrow \left(([b \smile c] \,\middle|\, \frac{n}{a}\right) \\ &\Longleftrightarrow (a[b \smile c] \mid n). \end{aligned}$$

Egalitatea (34) se deduce observînd inegalitatea:

$$| a | (b \smile c) \geqslant 0.$$

A doua s-ar putea demonstra analog folosind mulțimile *div b* și *div c*. Dar se poate obține și direct plecînd de la combinațiile liniare:

$$\beta ab + \gamma ac = a(\beta b + \gamma c).$$

Mulțimea multiplilor lui $(ab \frown ac)$ se obține deci înmulțind cu a multiplii lui $(b \frown c)$; se deduce egalitatea (35) deoarece:

$$| a | (b \frown c) \geqslant 0.$$

Înmulțireaeste deci distributivă, pe N, în raport cu legile c.m.m.m.c. și c.m.M.d.c.

EXERCIȚII

I. *Să se determine c.m.m.m.c și c.m.M.d.c al numerelor:*

$$a^2,\ ab,\ b^2,$$

cunoscînd: $a \frown b$ și $a \smile b$.
Putem scrie:

$$\begin{aligned}[a^2 \smile ab] \smile b^2 &= [a^2 \smile (ab \smile ab)] \smile b^2 \\ &= [a^2 \smile ab] \smile [ab \smile b^2] \\ &= [\ | a | (a \smile b)] \smile [| b | (a \smile b)] \\ &= [\ | a | \smile | b | \ ][a \smile b] \\ &= [a \smile b][a \smile b] = (a \smile b)^2.\end{aligned}$$

Se poate demonstra analog egalitatea:

$$a^2 \frown ab \frown b^2 = (a \frown b)^2.$$

(Se va putea studia ca exercițiu c.m.m.m.c. și c.m.M.d.c. al întregilor:

$$a^3,\ a^2b,\ ab^2,\ b^3 \text{ etc.})$$

II. *Să se rezolve, pe* N *ecuația definită prin:*

$$x + y - 1 = x \smile y.$$

$(x - 1)$ este un multiplu de y deoarece:

$$x - 1 = (x \smile y) - y.$$

Să punem deci:

$$x - 1 = \lambda y.$$

La fel:

$$y - 1 = \mu x.$$

Să studiem cazurile în care $(x = 0)$ sau $(y = 0)$;
Deducem atunci:

$$(x = 0) \Longrightarrow (y - 1 = 0 \smile y = 0) \Longrightarrow (y = 1),$$
$$(y = 0) \Longrightarrow (x - 1 = x \smile 0 = 0) \Longrightarrow (x = 1).$$

Abstracție făcînd de aceste două cazuri, λ și μ sînt pozitivi sau nuli. Însă avem egalitatea:

$$y = 1 + \mu x = 1 + \mu(1 + \lambda y),$$
$$(\lambda\mu - 1)y + \mu + 1 = 0.$$

Cum $(\mu + 1)$ este strict pozitiv, trebuie ca $(\lambda\mu - 1)$ să fie strict negativ; de unde:

$$0 \leqslant \lambda\mu < 1,$$

sau încă:

$$\lambda\mu = 0.$$

Deducem atunci:

$$(\lambda = 0) \Longrightarrow (x = 1) \Longrightarrow (y = 1 \smile y),$$
$$(\mu = 0) \Longrightarrow (y = 1) \Longrightarrow (x = x - 1).$$

Ecuația are aceeași mulțime de soluții ca:

$$(x - 1)(y - 1) = 0$$

III. *Să se rezolve, pe* **Z**, *ecuația definită prin:*

$$x + y + 1 = x \frown y.$$

C.m.M.d.c. $(x \frown y)$ divide pe x și y, deci pe $(x + y)$. Prin urmare îl divide pe 1 și este deci egal cu 1. Deducem:

$$x \frown y = 1, \quad x + y = 2.$$

Să-l fixăm pe x care aparține lui **Z**. Dacă x este par, y este de asemenea par și c.m.M.d.c. nu este egal cu 1. Trebuie deci ca x să fie impar. În acest caz, orice divizor pozitiv comun lui x și lui $y = 2 - x$ trebuie să dividă suma lor egală cu 2. Cum 2 nu-l divide pe x, avem:

$$x \frown y = 1.$$

Există deci o infinitate de soluții date prin:

$$x = 1 + 2z, \; y = 1 - 2z \; (z \in \mathbf{Z}).$$

EXERCIȚII

3.51. Să se demonstreze implicația:

$$(x \frown y = x \smile y) \Longrightarrow (|\, x \,| = |\, y \,|).$$

Reciproca este adevărată?

3.52. Să se compare întregii:

$$a \frown b \frown c, \quad (a + nb) \frown b \frown c.$$

3.53. Să se demonstreze egalitatea:

$$[a \smile b \smile c] = [(a \smile b) \smile (b \smile c)].$$

3.54. Să se demonstreze pe **Z** egalitatea:

$$x \frown (x + 1) = x \frown (2x + 1).$$

2.55. m și n fiind întregi naturali distincți, să se calculeze c.m.M.d.c. al întregilor $(mx + 1)$ și $(nx + 1)$.

3.56. Să se verifice egalitatea:

$$14 \frown 611 = 1$$

Să se stabilească numărul:

$$322 \frown 546 \frown 611.$$

3.57. Să se demonstreze că $\mathbf{Z}/p\mathbf{Z}$ care este corp admite două subgrupuri aditive şi numai două. Să se determine subgrupurile aditive ale inelului $\mathbf{Z}/12\mathbf{Z}$.

3.58. Să se demonstreze că Q, corpul numerelor raţionale, admite un subgrup aditiv (de exemplu, acela al numerelor zecimale) care nu este mulţimea multiplilor unui raţional dat.

3.4. ÎNTREGI PRIMI ÎNTRE EI

3.4.1. Identitatea lui Bezout

Vom spune că întregii sînt *primi între ei în ansamblul lor* (prescurtat: primi între ei) dacă c.m.M.d.c. al lor este egal cu 1.

DEFINIŢIA 2 / **Elementele unei familii finite nevide de întregi sînt prime între ele dacă şi numai dacă c.m.M.d.c al lor este egal cu 1.**

1. Pentru ca un subgrup al lui $\mathbf{Z}$ să fie egal cu $1\mathbf{Z}$, este necesar şi suficient ca el să-l conţină pe 1. Pentru ca întregii relativi $(a, b, c, \ldots, l)$ să fie primi între ei, este necesar şi suficient ca să existe întregi relativi $u, v, w, \ldots, t$ astfel încît:

$$1 = au + bv + cw + \ldots + lt \tag{36}$$

TEOREMA 17 / **Pentru ca nişte întregi să fie primi între ei, este necesar şi suficient să existe o combinaţie liniară de aceşti întregi cu coeficienţi întregi care să fie egală cu 1** *(teorema lui Bachet-Bezout)*, **sau să nu existe nici un divizor comun al acestor întregi.**

EXEMPLU. Întregii 6, 10 şi 15 sînt primi între ei deoarece se poate scrie egalitatea:

$$1 \times 6 + 1 \times 10 + (-1) \times 15 = 1.$$

Să observăm totuşi că nu sînt *primi între ei doi cîte doi*, deoarece:

$$6 \frown 10 = 2, \quad 6 \frown 15 = 3, \quad 10 \frown 15 = 5.$$

Cu toate acestea:

$$6 \frown 10 \frown 15 = 1.$$

2. Cazul a doi întregi este mai simplu; a şi b sînt primi între ei dacă şi numai dacă există doi întregi u şi v astfel încît:

$$au + bv = 1 \tag{37}$$

De obicei, această egalitate poartă numele de *identitatea lui Bezout.*
Să notăm că a şi b sînt primi între ei dacă şi numai dacă, $|a|$ şi $|b|$ sînt primi între ei.
0 este prim cu 1 şi cu (-1); 1 şi (-1) sînt prime cu toţi întregii relativi.

3. Să îndepărtăm aceste cazuri și să luăm:

$$|a| \geqslant 2, \qquad |b| \geqslant 2.$$

Să plecăm de la o pereche (u_0, v_0) astfel încît:

$$au_0 + bv_0 = 1.$$

Să împărțim pe u_0 la b; deducem:

$$u_0 = bq + u, \qquad 0 \leqslant u < |b|.$$

$u = 0$ nu convine, căci b ar divide pe au_0 și bv_0 deci pe 1.
În consecință:

$$0 < u < |b|.$$

Să punem atunci:

$$v = v_0 + aq.$$

Deducem:

$$au + bv = a(u_0 - bq) + b(v_0 + aq) = au_0 + bv_0 = 1.$$

Avem:

$$|bv| = |1 - au| \text{ și } |1 - au| \leqslant 1 + |au|,$$

sau:

$$|bv| \leqslant 1 + |a|\,u.$$

Deoarece: $0 < u < |b|$, avem:

$$u \leqslant |b| - 1,$$

deci:

$$|bv| \leqslant 1 + |a|\,(|b| - 1).$$

Deoarece: $|a| \geqslant 2$, avem:

$$|bv| \leqslant |ab| - 2 + 1 < |ab|.$$

În consecință:

$$0 \leqslant |v| < |a|.$$

$v = 0$ nu convine căci au ar fi egal cu 1, de unde $|a| = 1$.
Se vede deci că putem găsi o pereche (u, v) astfel încît:

$$\boxed{au + bv = 1,\ 0 < u < |b|,\ 0 < |v| < |a|} \qquad (38)$$

cînd a și b sînt diferiți de 0, 1 și -1.

4. Dacă avem:

$$a \geqslant 2 \text{ și } b \geqslant 2,$$

deducem atunci:

$$bv = 1 - au \text{ și } 1 - au < (1 - u)a \leqslant 0;$$

de unde relațiile:

$$\boxed{0 < u < b,\ 0 < -v < a} \tag{39}$$

(Se obișnuiește atunci schimbarea lui v în $(-v)$, cu scopul de a obține o egalitate între numere pozitive. De exemplu:

$$(9 \frown 13 = 1) \Longrightarrow (9 \times 3 - 13 \times 2 = 1)).$$

3.4.2. Teorema lui Gauss

Identitatea lui Bezout are un corolar fundamental cunoscut sub numele de *teorema lui Gauss*, cu toate că fusese deja folosită de Euclid (această teoremă ar fi putut fi demonstrată direct ca o consecință a teoremei 8 (pagina 134), așa cum a făcut-o Gauss în *Disquisitiones Arithmeticae)*.
Să presupunem că întregul a divide produsul (bc) și este prim cu b:

$$a \mid bc \qquad a \frown b = 1.$$

Putem scrie egalitățile:

$$ad = bc \qquad au + bv = 1,$$
$$acu + bcv = c,$$
$$a(cu + dv) = c.$$

Rezultă că a divide pe c.

TEOREMĂ 18 **Dacă a divide pe (bc) și este prim cu b, atunci a divide pe c (teorema lui *Gauss*).**

De asemenea se poate deduce teorema lui Gauss din egalitatea (35).
Într-adevăr:

$$(a \frown b = 1) \Longrightarrow (ac \frown bc = |\, c\,|).$$

Dar, a divide pe ac și bc; el divide atunci și c.m.M.d.c. al lor, $|\, c\,|$.
Se deduce imediat că a divide pe c.

Această teoremă este folosită în majoritatea raționamentelor de aritmetică. Teorema 8 este un simplu corolar al ei.

EXERCIȚII

I. *Să se studieze ecuația definită pe* $\mathbf{Z}$ *prin:*

$$ax + by = c \qquad (ab \neq 0).$$

Dacă această ecuație are o soluție, c este o combinație liniară de a și b, deci un multiplu al c.m.M.d.c. al lor d.
Să presupunem că această condiție necesară este îndeplinită și să punem:

$$a = d\alpha,\ b = d\beta,\ c = d\gamma,$$

de unde ecuația echivalentă (căci d este diferit de zero):

$$\alpha x + \beta y = \gamma.$$

α și β sînt prime între ele căci orice divizor comun δ al lui α și al lui β este astfel încît ($d\delta$) divide a și b, deci pe d.
Există deci u și v astfel încît:

$$\alpha u + \beta v = 1.$$

Putem deci obține o soluție particulară:

$$x_0 = \gamma u, \quad y_0 = \gamma v.$$

Pentru a obține toate soluțiile, să scriem:

$$0 = \alpha x + \beta y - \alpha x_0 - \beta y_0;$$
$$\alpha(x - x_0) = \beta(y_0 - y).$$

α este prim cu β și divide pe $\beta(y_0 - y)$.
Trebuie deci să avem:

$$y_0 - y = \lambda\alpha \qquad (\lambda \in \mathbf{Z}),$$

de unde:

$$y = y_0 - \lambda\alpha,$$
$$\alpha(x - x_0) = \beta\lambda\alpha,$$
$$x - x_0 = \lambda\beta \qquad (\alpha \neq 0).$$

Dacă α și d sînt diferiți de 0, se obțin deci toate soluțiile cu ajutorul formulelor:

$$x = \frac{cu + \lambda b}{d}, \qquad y = \frac{cv - \lambda a}{d}.$$

Ecuația nu are soluții dacă d nu divide pe c.

II. *Să se demonstreze că, dacă a și b sînt prime între ele și mai mari sau egale ca 2, există o pereche unică (u, v) astfel încît:*

$$au - bv = 1, \quad 0 < u < b, \quad 0 < v < a.$$

Existența a fost demonstrată în paragraful precedent. Unicitatea este o consecință imediată a teoremei lui Gauss; într-adevăr:

$$(au - bv = ax - by) \iff (a[u - x] = b[v - y]).$$

b trebuie deci să dividă pe $(u - x)$; de unde:

$$x = nb + u.$$

Condiția: $0 < x < b$ dă singura soluție:

$$x = u.$$

III. *Să se rezolve ecuația definită pe* $\mathbf{Z}$ *prin:*

$$\frac{x}{9} - \frac{y}{4} = 3, \qquad x \frown y = 18.$$

Ecuația se mai scrie:

$$4x - 9y = 108, \quad 9 \mid x, 4 \mid y, \quad x \frown y = 18$$

Exercițiul I ne permite să o rezolvăm; într-adevăr:

$$4 \times 7 - 9 \times 3 = 1,$$

de unde:

$$x = 108 \times 7 + 9\lambda,\ y = 108 \times 3 + 4\lambda\ (\lambda \in \mathbf{Z}),$$

sau încă:

$$\frac{x}{9} = 84 + \lambda, \qquad \frac{y}{4} = 81 + \lambda.$$

Rămîne de rezolvat ecuația în λ:

$$(756 + 9\lambda) \frown (324 + 4\lambda) = 18.$$

18 trebuie să dividă pe 9λ și 4λ : λ trebuie să fie multiplu de 2 și de 9, deci de 18, căci:

$$(18 \mid 9\lambda) \Longrightarrow (2 \mid \lambda),\ (18 \mid 4\lambda) \Longrightarrow (9 \mid 2\lambda) \Longrightarrow (9 \mid \lambda)$$

Să punem:

$$\lambda = 18\mu.$$

Rezultă, după relația (35):

$$(42 + 9\mu) \frown (18 + 4\mu) = 1.$$

Dacă μ este un multiplu de 2 sau de 3, nu există soluții căci 6 divide 42 și 18. Deci μ este de forma:

$$\mu = 6t + 1 \text{ sau } \mu = 6t - 1.$$

Să încercăm $\mu = 6t + 1$; deducem:

$$3(18t + 17) \frown 2(12t + 11) = 1,$$

ceea ce este exact deoarece se poate scrie:

$$4 \times [3(18t + 17)] - 9[2(12t + 11)] = 6,$$

și divizorii lui 6 nu pot divide nici pe $3(18t + 17)$, nici pe $2(12t + 11)$. Să încercăm de asemenea pe $\mu = 6t - 1$; rezultă:

$$3(18t + 11) \frown 2(12t + 7) = 1,$$

ceea ce este exact deoarece se poate scrie:

$$4 \times [3(18t + 11)] - 9[2(12t + 7)] = 6,$$

și divizorii lui 6 nu pot divide nici pe $3(18t + 11)$, nici pe $2(12t + 7)$.
În concluzie, $\mu = 6t \pm 1$ convine; de unde soluțiile:

$$\begin{cases} x = 54(18t + 17), & y = 36(12t + 11); \\ x = 54(18t + 11), & y = 36(12t + 7) \qquad (t \in \mathbf{Z}). \end{cases}$$

3.4.3. Elementele inversabile ale lui $\mathbf{Z}/n\mathbf{Z}$

1. Să considerăm un element α al inelului $\mathbf{Z}/n\mathbf{Z}$; α este clasa unui întreg a.
Să presupunem că α este inversabil, deci există o clasă β cu: $\alpha\beta = \overline{1}$.
β fiind clasa unui întreg b putem scrie:

$$ab \equiv 1\ [n],$$

sau încă:

$$n \mid ab - 1,$$

adică:

$$1 = ab - nm.$$

Întregii a și n sînt deci primi între ei, după identitatea lui Bezout.
Reciproc, dacă a și n sînt primi între ei, există întregii b și m astfel încît:

$$1 = ab - nm,$$

$$\bar{a}\bar{b} = \bar{1}.$$

TEOREMA 19 / **Clasa unui întreg a este inversabilă în inelul $\mathbf{Z}/n\mathbf{Z}$ dacă și numai dacă a și n sînt primi între ei.**

2. Elementele inversabile ale lui $\mathbf{Z}/n\mathbf{Z}$ formează un grup multiplicativ. În adevăr, produsul a două elemente inversabile este inversabil, deoarece:

$$(\alpha\beta = \bar{1},\ \gamma\delta = \bar{1}) \Longrightarrow ([\alpha\gamma][\beta\delta] = \bar{1}).$$

Acest produs este asociativ și comutativ, deoarece acest lucru are loc în $\mathbf{Z}/n\mathbf{Z}$; $\bar{1}$ este inversabil, căci:

$$\bar{1}\bar{1} = \bar{1}.$$

În sfîrșit, fiecare element inversabil are, chiar prin definiție, un invers care este și el inversabil.

TEOREMA 20 / **Elementele inversabile ale inelului $\mathbf{Z}/n\mathbf{Z}$ formează un grup comutativ pentru înmulțire.**

3. Să considerăm aplicația:

$$\mathfrak{f} = [\xi \longmapsto \alpha\xi]$$

definită pe $\mathbf{Z}/n\mathbf{Z}$, unde α este inversabil $(\alpha\beta = \bar{1})$.
Această aplicație este injectivă, căci:

$$(\alpha\xi = \alpha\eta) \Longrightarrow (\alpha[\xi - \eta] = \bar{0}) \Longrightarrow (\xi - \eta = \beta\alpha[\xi - \eta] = \bar{0}).$$

Dacă ξ este inversabil, atunci $\mathfrak{f}(\xi)$ este inversabil, căci:

$$(\xi\eta = \bar{1}) \Longrightarrow ([\alpha\xi]\,[\beta\eta] = \bar{1}).$$

Imaginea prin $\mathfrak{f}$ a mulțimii:

$$\{\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_m\}$$

de elemente inversabile ale lui $\mathbf{Z}/n\mathbf{Z}$ este deci chiar această mulțime.
Prin urmare:

$$\alpha_1\alpha_2\ldots\alpha_m = \mathfrak{f}(\alpha_1)\mathfrak{f}(\alpha_2)\ldots\mathfrak{f}(\alpha_m) = \alpha^m(\alpha_1\alpha_2\ldots\alpha_m).$$

Produsul $(\alpha_1\alpha_2\ldots\alpha_m)$ este inversabil. Se poate deci simplifica această egalitate și se obține:

$$\alpha^m = 1.$$

Această relație este cunoscută sub numele de *teorema lui Euler; m* este *indicatorul* lui n; se notează adesea:

$$m = \varphi(n).$$

4. Să reamintim teorema următoare a cărei demonstrație este imediată.

TEOREMA 21 / Un număr prim este prim cu orice întreg pe care nu-l divide.

Să presupunem n prim. Vom pune $n = p$. Printre cele p clase:

$$\{\bar{0}, \bar{1}, \bar{2}, ..., \overline{p-1}\},$$

există $(p-1)$ care sînt inversabile, căci întregii $(1, 2, ..., p-1)$ sînt primi cu p.
Teorema lui Euler se scrie deci acum:

$$(p \nmid a) \Longrightarrow (\bar{a}^{p-1} = \bar{1}),$$

sau încă:

$$\boxed{(p \text{ prim și } p \nmid a) \Longrightarrow (a^{p-1} \equiv 1[p])} \qquad (40)$$

Accasta este celebra *teoremă a lui Fermat.*
Această teoremă are corolarul imediat:

$$\boxed{(p \text{ prim și } a \in \mathbf{Z}) \Longrightarrow (a^p \equiv a[p])} \qquad (41)$$

Toate elementele lui $\mathbf{Z}/p\mathbf{Z}$, cu excepția lui $\bar{0}$, avînd un invers, se regăsește deci că $\mathbf{Z}/p\mathbf{Z}$ este un corp cînd p este prim.

5. Să considerăm elementele nenule ale lui $\mathbf{Z}/p\mathbf{Z}$:

$$\{\bar{1}, \bar{2}, \bar{3}, ..., \overline{p-1}\}.$$

Produsul lor este egal cu:

$$\bar{1} \times \bar{2} \times ... \times \overline{p-1} = \overline{1 \times 2 \times ... \times (p-1)} = \overline{(p-1)!}.$$

Dar fiecare dintre ele are inversul diferit de el însuși, cu excepția cazului:

$$\bar{x}^2 = \bar{1},$$

care este echivalent cu:

$$\bar{0} = (\bar{x}^2 - \bar{1}) = (\bar{x} - \bar{1})(\bar{x} + \bar{1}),$$

deci cu:

$$\bar{x} = \bar{1} \text{ sau } \bar{x} = -\bar{1} = \overline{p-1}.$$

Putem deci asocia două cîte două elementele inversibile în acest produs; rămîne:

$$\bar{1} \times \overline{p-1} = -\bar{1}.$$

De unde se deduce *teorema lui Wilson*:

$$\overline{(p-1)!} = \overline{-1},$$

sau încă:

$$(p \text{ prim}) \Longrightarrow [(p-1)! \equiv -1 \ [p]].$$

Exemplu. $p = 13$.

$$\overline{1}\times\overline{2}\times\overline{3}\times\overline{4}\times\overline{5}\times\overline{6}\times\overline{7}\times\overline{8}\times\overline{9}\times\overline{10}\times\overline{11}\times\overline{12} =$$

$$= \overline{1}\times\overline{12} \times [\overline{2}\times\overline{7}] \times [\overline{3}\times\overline{9}] \times [\overline{4}\times\overline{10}] \times [\overline{5}\times\overline{8}] \times [\overline{6}\times\overline{11}] = \overline{12} = -\overline{1}.$$

---

6. Să considerăm un întreg a neprim cu n, dar nu multiplu al lui n:

$$\alpha = \bar{a} \neq \bar{0}.$$

Să punem:

$$d = a \frown n \text{ şi } d > 1.$$

d divide în acelaşi timp a şi n; în consecinţă:

$$a \times \frac{n}{d} = n \times \frac{a}{d},$$

sau încă:

$$a \times \frac{n}{d} \equiv 0 \quad [n].$$

Întregul $\frac{n}{d}$ nu este un multiplu de n; clasa sa β este deci nenulă; dar $\alpha\beta = \bar{0}$.
Se spune că α este un divizor al lui zero, adică un element nenul care divide pe $\bar{0}$ în $\mathbf{Z}/n\mathbf{Z}$.
7. Pentru ca $\bar{a}$ să fie un divizor al lui zero, este deci suficient (şi necesar după teorema **19** deoarece un element inversabil nu poate fi un divizor al lui $\bar{0}$) ca a şi n să nu fie primi între ei, şi ca n să nu dividă pe a.
Să presupunem că n este compus. Există atunci elemente $\bar{a}$, divizori ai lui zero care aparţin lui $\mathbf{Z}/n\mathbf{Z}$:

$$(n = ab) \Longrightarrow (\bar{n} = \bar{a}\bar{b} = \bar{0}).$$

Produsul:

$$\bar{a}(\bar{1} \times \bar{2} \times \ldots \times \overline{n-1}) = \overline{a(n-1)!}$$

este deci nul, deoarece $\bar{b}$ figurează în mulţimea $(\bar{1}, \bar{2}, \ldots, \bar{n} - 1)$.
Prin urmare, $\overline{(n-1)!}$ nu poate fi egal cu $(\overline{-1})$. Reciproca teoremei lui Wilson este deci adevărată; de unde:

$$\boxed{(p \text{ prim}) \Longleftrightarrow ([p-1]! \equiv -1 \ [p])} \qquad (42)$$

De altfel se poate verifica că:

$(p = 1) \Longrightarrow (p-1)! \equiv 0 \ [1]]$;
$(p = 4) \Longrightarrow (p-1)! \equiv 2 \ [4]]$;
$(p$ compus, diferit de $4) \Longrightarrow [(p-1)! \equiv 0 \ [p]]$.

3.4.4. Proprietăți diverse

1. Să considerăm o familie de întregi nu toți nuli $(a, b, c, ..., l)$ și c.m.M.d.c. al lor n, care este deci nenul:

$$n = au + bv + cw + ... + lt.$$

Împărțim prin n, ceea ce este posibil deoarece $a, b, c, ..., l$ sînt multipli ai lui n:

$$1 = \frac{a}{n}u + \frac{b}{n}v + ... + \frac{l}{n}t.$$

Întregii $\left(\frac{a}{n}, \frac{b}{n}, \frac{c}{n}, ..., \frac{l}{n}\right)$ sînt deci primi între ei.

Reciproc, să considerăm întregii $(a', b', c', ..., l')$ primi între ei (deci nu sînt toți nuli):

$$1 = a'u + b'v + ... + l't.$$

Înmulțim cu un întreg strict pozitiv n; se obține:

$$n = au + bv + ... + lt,$$

cu $a = na'$, $b = nb'$, ..., $l = nl'$.
Întregul n este un multiplu al c.m.M.d.c. al $(a, b, c, ..., l)$; dar n divide evident $(a, b, c, ..., l)$ și divide deci acest c.m.M.d.c.
Prin urmare n, care este pozitiv, este c.m.M.d.c. studiat.

TEOREMA 22 / **Întregul strict pozitiv n este c.m.M.d.c. al unei familii finite de întregi nu toți nuli $(a, b, c, ..., l)$ dacă și numai dacă cîturile $\left(\frac{a}{n}, \frac{b}{n}, \frac{c}{n}, ..., \frac{l}{n}\right)$ sînt prime între ele.**

2. Să considerăm o familie de întregi nenuli $(a, b, c, ..., l)$ și c.m.m.m.c. al lor m, care este deci nenul; întregii $\left(\frac{m}{a}, \frac{m}{b}, ..., \frac{m}{l}\right)$ au un c.m.M.d.c. egal cu d, nenul. Dacă d este diferit de 1, se vede că întregul:

$$m' = \frac{m}{d} < m$$

este un multiplu comun al întregilor $(a, b, c, ..., l)$, căci:

$$(m = aa') \Rightarrow \left(m' = a \times \frac{a'}{d}\right).$$

Cum orice multiplu comun trebuie să fie un multiplu al c.m.m.m.c., m' trebuie să fie un multiplu al lui m, ceea ce este contradictoriu.
3. Reciproc, dacă m este un multiplu comun strict pozitiv al întregilor $(a, b, c, ..., l)$ astfel încît cîturile $a' = \frac{m}{a}$, $b' = \frac{m}{b}$, ..., $l' = \frac{m}{l}$ să fie prime între ele, atunci m este c.m.m.m.c.

În adevăr, dacă μ este c.m.m.m.c., μ divide pe m:

$$m = k\mu,\ k > 0.$$

Să considerăm cîturile $\left(\alpha = \frac{\mu}{a}, \beta = \frac{\mu}{b}, ..., \lambda = \frac{\mu}{l}\right)$:

$$(m = ka\alpha) \Longrightarrow (a' = k\alpha) \Longrightarrow (k \mid a')$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$(m = kl\lambda) \Longrightarrow (l' = k\lambda) \Longrightarrow (k \mid l').$$

(a', b', ..., l') fiind primi între ei, k divide pe c.m.M.d.c. al lor, 1; de unde:

$$(k = 1) \Longrightarrow (m = \mu) \quad (k > 0).$$

Observație. Aceeași metodă conduce la următoarea identitate mai generală unde μ este c.m.m.m.c.:

$$(\mu \mid m) \Longrightarrow \left[m = \mu\left(\frac{m}{a} \frown \frac{m}{b} \frown \cdots \frown \frac{m}{l}\right)\right].$$

În adevăr, k este c.m.M.d.c. al lui a', b', ..., l' deoarece $\alpha \frown \beta \frown \cdots \frown \lambda = l$.

TEOREMA 23 / **Întregul strict pozitiv m este c.m.m.m.c. al unei familii finite de întregi nenuli $(a, b, c, ..., l)$ dacă și numai dacă cîturile $\left(\frac{m}{a}, \frac{m}{b}, \frac{m}{c}, ..., \frac{m}{l}\right)$ sînt prime între ele (sau străine).**

4. Să considerăm cazul a doi întregi nenuli a și b. Să notăm, clasic, cu d și m respectiv c.m.M.d.c. și c.m.m.m.c. al lor:

$$d > 0,\ a = da',\ b = db',\ a' \frown b' = 1.$$

Fie:

$$m' = ab' = a\frac{b}{d} = \frac{a}{d}b = a'b.$$

m' este un multiplu comun al lui a și al lui b; se poate deci scrie: $m \mid m'$.

Pe de altă parte:

$$a' = \frac{m'}{b} = \frac{m'}{m} \times \frac{m}{b},\ b' = \frac{m'}{a} = \frac{m'}{m} \times \frac{m}{a}.$$

$\frac{m'}{m}$ divide pe a' și b' și este deci egal cu 1 sau cu -1. Se deduce egalitatea (care reiese de fapt din condiția $\frac{m'}{a} \frown \frac{m'}{b} = 1$):

$$m = |\, m' \,|,$$
$$|\, ab \,| = dm.$$

Dacă unul din numere este nul, c.m.m.m.c. este nul şi formula este de asemenea adevărată:

$$\boxed{|ab| = (a \frown b)\,(a \smile b)} \tag{43}$$

TEOREMA 24 / **Produsul dintre c.m.M.d.c. şi c.m.m.m.c. a doi întregi este egal cu produsul valorilor lor absolute.**

EXERCIŢII

I. *$(a_1, a_2, \ldots, a_n)$ fiind întregi strict pozitivi, M unul din multiplii lor comuni strict pozitivi, d, c.m.M.d.c. al lor, b_i câtul $\frac{M}{a_i}$ şi μ c.m.m.m.c. al întregilor b_i. Să se demonstreze relaţia: $M = d\mu$.*

Să notăm:

$$\mu = b_i\beta_i = \frac{M}{a_i}\beta_i,\ \beta_1 \frown \beta_2 \frown \ldots \frown \beta_n = 1.$$

M este un multiplu comun al întregilor b_i, deci un multiplu al c.m.m.m.c. al lor:

$$(M = k\mu) \Longrightarrow (a_i = k\beta_i).$$

k divide pe fiecare din întregii a_i; câturile β_i fiind prime între ele, k este deci c.m.M.d.c. al acestor întregi; de unde:

$$k = d,\ M = d\mu,$$

$$\boxed{M = (a_1 \frown a_2 \frown \ldots \frown a_n)\left(\frac{M}{a_1} \smile \frac{M}{a_2} \smile \ldots \smile \frac{M}{a_n}\right)}$$

De exemplu, pentru $n = 2$, dacă M este c.m.m.m.c. al lui a_1 şi a_2, se obţine:

$$a_1 \smile a_2 = (a_1 \frown a_2)\left[\frac{a_1 \smile a_2}{a_1} \times \frac{a_1 \smile a_2}{a_2}\right]$$

$\left(\text{deoarece } \frac{M}{a_1} \text{ şi } \frac{M}{a_2} \text{ sînt aici primi între ei}\right)$, sau încă:

$$a_1a_2 = (a_1 \frown a_2)\,(a_1 \smile a_2).$$

Schimbînd a_i cu $\frac{M}{a_i}$, M rămînînd acelaşi, se obţine:

$$\boxed{M = (a_1 \smile a_2 \smile \ldots \smile a_n)\left(\frac{M}{a_1} \frown \frac{M}{a_2} \frown \ldots \frown \frac{M}{a_n}\right)}$$

De exemplu ($n = 3$, $M = abc$):

$$abc = (a \frown b \frown c)\,(bc \smile ac \smile ab) = (a \smile b \smile c)\,(bc \frown ac \frown ab)$$

(A se vedea observația din paragraful 8.)

II. *Să se demonstreze, cu ajutorul exercițiului I, egalitatea:*

$$\boxed{k \frown (a_1 \smile a_2 \smile \ldots \smile a_n) = (k \frown a_1) \smile \ldots \smile (k \frown a_n)}$$

Să notăm:

$$m = a_1 \smile a_2 \smile \ldots \smile a_n,$$

$$m = a_i b_i, \quad (b_1 \frown b_2 \frown \ldots \frown b_n = 1),$$

$$k \frown a_i = c_i,$$

$$k = c_i d_i,$$

$$a_i = c_i e_i \quad (d_i \frown e_i = 1).$$

Atunci:

$$k \frown m = c_i(d_i \frown b_i e_i) = c_i([d_i \frown d_i b_i] \frown b_i e_i) =$$
$$= c_i(d_i \frown b_i[d_i \frown e_i]) = c_i(d_i \frown b_i).$$

Să înlocuim, în formula a doua din exercițiul precedent, M prin $(k \frown m)$, a_i prin c_i; se obține:

$$k \frown m = (c_1 \smile c_2 \smile \ldots \smile c_n)\,([d_1 \frown b_1] \frown \ldots \frown [d_n \frown b_n]).$$

Dar, întregii b_i sînt primi între ei; avem deci:

$$(d_1 \frown b_1) \frown \ldots \frown (d_n \frown b_n) = (b_1 \frown b_2 \frown \ldots \frown b_n) \frown (d_1 \frown \ldots \frown d_n) =$$
$$= 1 \frown (d_1 \frown \ldots \frown d_n) = 1,$$

sau:

$$k \frown m = c_1 \smile c_2 \smile \ldots \smile c_n,$$

care este egalitatea căutată.

---

5. Locuțiunile „cel mai *mic* multiplu comun" și „cel mai *mare* divizor comun" nu se referă, cum s-ar putea crede, la relația de ordine ($\leqslant$) pe $\mathbf{Z}$, ci la relația ($|$) de divizibilitate. Dacă ne mărginim la $\mathbf{N}$, relația ($|$) este o relație de ordine (parțială); adjectivele „mic" și „mare" se referă la această relație de ordine. De exemplu:

$$(n \mid 0) \Longrightarrow (0 \text{ este mai „mare" ca } n).$$

Evident, dacă ne limităm la întregi strict pozitivi, implicația:

$$(n \mid m) \Longrightarrow (n \leqslant m)$$

arată că c.m.m.m.c. și c.m.M.d.c. sînt, în acest caz, cel mai mic multiplu comun și cel mai mare divizor comun și în sensul relației de ordine uzuală ($\leqslant$).

EXERCIȚII

3.59. Să se demonstreze că produsul a trei numere pare consecutive este un multiplu de 48

3.60. Să se determine întregii congruenți cu 5 modulo 12 și cu 14 modulo 15.

3.61. Să se calculeze restul împărțirii lui $x(x + 1)(2x + 1)$ prin 6, și restul împărțirii cîtului prin 5. (Se vor distinge mai multe cazuri).

3.62. Să se demonstreze că 120 divide întregul:

$$x(x + 1)(x + 2)(x + 3)(x + 4).$$

3.63. Să se determine cel mai mic întreg pozitiv congruent cu 4 modulo 12, 17, 45 și 70.

3.64. Să se determine întregii n astfel încît:

$$1\,000 \leqslant n \leqslant 2\,000,$$
$$n \equiv -1 \quad [m],$$

pentru toate valorile lui m din mulțimea:

$$\{15, 18, 25\}.$$

3.65. Să se demonstreze congruența:

$$x^2(x^2 - 1)(x^4 - 16) \equiv 0 \quad [860].$$

3.66. Să se rezolve ecuația definită pe $\mathbf{Z}$ prin:

$$x^2 - y^2 = 24.$$

3.67. Să se rezolve, în inelul $\mathbf{Z}/30\mathbf{Z}$, ecuația definită prin:

$$x^5 = x.$$

3.68. Să se rezolve, în $\mathbf{Z}$, ecuația definită prin:

$$3x - 4y = 1.$$

3.69. Același exercițiu cu ecuația definită prin:

$$7x - 9y = 1.$$

3.70. Să se demonstreze implicația:

$$(a \frown b = 1) \Longrightarrow (a^n \frown b^n = 1).$$

3.71. Să se calculeze numărul:

$$(15a + 4b) \frown (11a + 3b),$$

în funcție de întregul $(a \frown b)$.

3.72. Să se generalizeze exercițiul nr. 3.69 pentru numerele:

$$(pa + qb) \frown (ra + sb),$$

cu:

$$ps - qr = 1.$$

3.73. Să se rezolve ecuația definită prin:

$$x^2 - x = 10^4 n, \; x \in \mathbf{Z},$$

cu $10^3 < n < 10^4$.

3.74. Să se calculeze numărul:

$$x \smile (x + 1) \smile (x + 2).$$

3.75. Să se calculeze numărul:

$$(a + b) \frown (a - b),$$

în funcție de $d = a \frown b$.

3.76. Să se rezolve ecuația definită pe $\mathbf{Z}$ prin:

$$x^2 - y^2 = p,$$

unde p este un număr prim dat.

3.77. Să se verifice egalitatea:

$$6 \times 7 \times 13 = 546.$$

Să se deducă congruența:

$$x^{13} \equiv x \pmod{546}.$$

3.78. Să se determine întregii x astfel încît:

$$5 \mid 4x^2 + 1, \qquad 13 \mid 4x^2 + 1.$$

3.79. Să se calculeze restul împărțirii întregului:

$$3^{3n+3} - 26n - 27$$

prin 169.

3.80. Să se demonstreze implicația:

$$(a \frown b = 1) \Longrightarrow [(a^2b + ab^2) \frown (a + ab + b) = 1].$$

3.81. Să se demonstreze că, dacă p este un număr prim mai mare sau egal cu 5, 24 divide pe $(p^2 - 1)$.

3.82. Să se demonstreze că, a și b fiind primi între ei, $(a^2 - b^2)$ nu este un pătrat perfect decît dacă și numai dacă, $(a + b)$ și $(a - b)$ sînt pătrate perfecte, sau dacă sînt pătrate perfecte înmulțite cu 2.

3.83. a și b fiind prime între ele, să se demonstreze relația:

$$[(a + b) \frown (a^2 + ab + b^2)] \mid 3.$$

3.84. Să se demonstreze implicația:

$$(a \frown b \frown c = 1) \Longrightarrow (abc \frown [ab + bc + ca] = 1).$$

3.85. Să se demonstreze că, dacă p este un număr prim, coeficienții binomiali C_p^1, C_p^2, ..., ... , C_p^{p-1} sînt divizibili prin p.

3.86. Să se demonstreze că, dacă există doi întregi a și b astfel încît:

$$n^2 = a^2 + 2b^2 \ (n \in \mathbf{N}),$$

se pot determina doi întregi α și β astfel încît:

$$n = (a \frown b)\ (\alpha^2 + 2\beta^2).$$

3.87. Să se demonstreze că ecuația, definită pe **Z** prin:

$$3x^2 = y^2 + z^2,$$

nu admite nici o soluție.

3.88. Să se rezolve ecuația definită pe **Z** prin:

$$xn^2 - y(n + 1)^2 = 1,$$

unde n este un întreg dat.

3.89. Să se rezolve ecuația definită pe **Z** prin:

$$(x - y)^2 = x + y.$$

3.90. Să se demonstreze egalitatea:

$$a \frown (b \smile c) = (a \frown b) \smile (a \frown c).$$

3.91. Să se determine toți întregii naturali n astfel încît orice divizor prim al lui $(n^6 - 1)$ să dividă pe $(n^2 - 1)\ (n^3 - 1)$.

3.92. Să se calculeze numărul:

$$(2^{n+2} - 2^n) \frown (3^{n+2} - 3^n).$$

3.93. Cunoscînd întregul natural n și întregul prim natural p, să se determine întregii a, b, c astfel încît:

$$|\, a - b \,| = 1,\ c \frown n = 1,$$
$$c \mid a^2 - b^2 \mid = npab.$$

3.94. a și b fiind primi între ei, se ia:

$$au + bv = 1.$$

Să se determine toți întregii x astfel încît:

$$x \in \mathbf{Z},\ x \equiv 1 \ [a],\ x \equiv 1 \ [b].$$

Să se generalizeze la congruențele:

$$x \equiv \alpha \ [a], \ x \equiv \beta \ [b].$$

3.95. Să se rezolve ecuația definită pe Z prin:

$$xy = 5x + 3y + 75.$$

3.96. Să se demonstreze că, dacă p și q sînt numere prime mai mari sau egale cu 7, numărul:

$$(p^2 - 1)(q^2 - 1)(p^6 - q^6)$$

este un multiplu de 580 608.

3.5. ALGORITMI

3.5.1. Algoritmul lui Euclid

Un algoritm este o mulțime de reguli care permit unui automat sau unui calculator uman, acționînd ca un automat — să efectueze un anumit calcul.

1. Un prim algoritm constă în calculul c.m.M.d.c. al mai multor numere; calculul acestui c.m.M.d.c. poate fi redus la mai multe calcule ale c.m.M.d.c. a cîte două numere, deoarece operația de intersecție a mulțimilor este asociativă:

$$(div\ a) \cap (div\ b) \cap (div\ c) = (div\ a) \cap [(div\ b) \cap (div\ c)] =$$
$$= (div\ a) \cap (div[b \frown c]).$$

Pe de altă parte, egalitatea:

$$a \frown b = |a| \frown |b|$$

permite să ne ocupăm de întregi pozitivi; o fiind atunci neutru pentru operația c.m.M.d.c., putem presupune a și b strict pozitivi, cu: $a \geqslant b$.

2. Să considerăm o egalitate de forma:

$$a = bq + r.$$

Este evident că avem:

$$(\text{div } a) \cap (div\ b) = (div\ b) \cap (div\ r),$$

deoarece:

$$(a = \lambda a' \text{ și } b = \lambda b') \Longrightarrow (r = \lambda[a' - b'q]),$$
$$(b = \lambda b' \text{ și } r = \lambda r') \Longrightarrow (a = \lambda[b'q + r']).$$

Să efectuăm deci împărțirile euclidiene succesive:

$$\begin{aligned} a &= bq_1 + r_1, & 0 \leqslant r_1 < b, \\ b &= r_1q_2 + r_2, & 0 \leqslant r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, & 0 \leqslant r_3 < r_2, \\ &\vdots & \vdots \\ r_{k-2} &= r_{k-1}q_k + r_k, & 0 \leqslant r_k < r_{k-1}. \end{aligned}$$

De unde se pot deduce, în special, inegalitățile următoare:

$$r_1 \leqslant b - 1,\ r_2 \leqslant b - 2,\ \ldots,\ r_k \leqslant b - k.$$

3. După un anumit număr de etape (cel mult b împărțiri), există deci un întreg n astfel încît:

$$r_{n+1} = 0, \qquad r_n \neq 0 \quad (\text{dacă } n \neq 0).$$

Atunci egalitatea:

$$r_{n-1} = r_nq_{n+1} \ (\text{cu } r_0 = b,\ r_{-1} = a)$$

arată că:

$$(div\ a) \cap (div\ b) = (div\ b) \cap (div\ r_1) = (div\ r_1) \cap (div\ r_2) = \ldots =$$
$$= (div\ r_{n-1}) \cap (div\ r_n) = (div\ r_n), \text{ căci } r_n \mid r_{n-1}.$$

Întregul r_n, care este strict pozitiv, este deci c.m.M.d.c. al lui a și b:

$$\boxed{r_n = a \frown b} \tag{44}$$

EXEMPLU. $a = 30576$, $b = 6600$.
Vom așeza:

a) în prima linie, citurile $q_1q_2 \ldots q_{n+1}$;

b) în a doua, întregii a, b, r_1, r_2, ..., r_{n-1}, r_n;

c) în a treia, produsele bq_1, r_1q_2, ..., $r_{n-1}q_n$, r_nq_{n+1};

d) în ultima, în sfîrșit, resturile r_1, r_2, ..., r_{n-1}, r_n, 0.

	4	1	1	1	2	1	1	1	1	5
30576	6600	4176	2424	1752	672	408	264	144	120	24
26400	4176	2424	1752	1344	408	264	144	120	120	
4176	2424	1752	672	408	264	144	120	24	0	

$(n = 9)$

Deci:

$$30576 \frown 6600 = 24.$$

Verificare:

$$30576 = 24 \times 1274;\ 6600 = 24 \times 275;$$

$$1274 \frown 275 = 1, \text{ căci } 1274 \times 49 - 275 \times 227 = 1.$$

---

4. Algoritmul precedent este cunoscut sub numele de *algoritmul* lui *Euclid*. El permite să regăsim identitatea lui Bezout. În adevăr:

$$a = a \cdot 1 + b \cdot 0,\ b = a \cdot 0 + b \cdot 1,$$

$$r_1 = a + (-q_1)b,\ r_2 = b - r_1 q_2 = (-q_2)a + (1 + q_1 q_2)b.$$

Să presupunem că avem, datorită ipotezei inducției:

$$r_{k-2} = au_{k-2} + bv_{k-2},\ r_{k-1} = au_{k-1} + bv_{k-1};$$

rezultă că:

$$r_k = r_{k-2} - r_{k-1}q_k = a(u_{k-2} - u_{k-1}q_k) + b(v_{k-2} - v_{k-1}q_k) =$$

$$= au_k + bv_k.$$

În particular:

$$a \frown b = r_n = au_n + bv_n.$$

EXEMPLU. Să reluăm: $a = 30576$, $b = 6600$.

$r_1 = 4176 = a - 4b$; $r_2 = b - r_1 = 5b - a$;

$r_3 = r_1 - r_2 = 2a - 9b$; $r_4 = r_2 - r_3 = 14b - 3a$;

$r_5 = r_3 - 2r_4 = 8a - 37b$; $r_6 = r_4 - r_5 = 51b - 11a$;

$r_7 = r_5 - r_6 = 19a - 88b$; $r_8 = r_6 - r_7 = 139b - 30a$;

$r_9 = r_7 - r_8 = 49a - 227b$.

În adevăr:

$$24 = 49 \times 30576 - 227 \times 6600.$$

Algoritmul lui Euclid dă imediat regula:

$$(a > 0 \text{ și } b > 0 \text{ și } c > 0) \Longrightarrow (ab \frown ac = a[b \frown c]).$$

(Se poate deduce de aici teorema lui Gauss: a se vedea pagina 154).

5. C.m.m.m.c. a două numere se obține prin formula:

$$m = \frac{ab}{d}\ (a > 0,\ b > 0).$$

Se poate deduce c.m.m.m.c. al mai multor întregi (în număr finit), deoarece de exemplu:

$$a\mathbf{Z} \cap b\mathbf{Z} \cap c\mathbf{Z} = a\mathbf{Z} \cap [b\mathbf{Z} \cap c\mathbf{Z}] = a\mathbf{Z} \cap [(b \smile c)\mathbf{Z}] \text{ etc.}$$

EXEMPLU. Fie tot: $a = 30576$, $b = 6600$.

Avem:

$$m = \frac{ab}{d} = \frac{ab}{24} = \frac{a}{24} b = 1274 \times 6600.$$

de unde: $m = 8408400$.

6. Pentru a verifica că d este c.m.M.d.c. al lui a şi b, trebuie să arătăm că d divide pe a şi b, şi că:

$$\frac{a}{d} \frown \frac{b}{d} = 1,$$

deci, de exemplu, să găsim u şi v astfel încît:

$$\frac{a}{d} u + \frac{b}{d} v = 1.$$

O astfel de căutare se poate face în mai multe feluri; algoritmul lui Euclid furnizează, cum s-a văzut, o soluţie a acestei ecuaţii în u şi v. Dar se pot folosi de asemenea congruenţele care micşorează numărul tatonărilor necesare.

EXEMPLU. *Să se rezolve ecuaţia definită prin:*

$$1274u + 275v = 1, \qquad 0 < u < 275.$$

275 este vizibil divizibil prin 5; de unde:

$$1274u \equiv 1 \ [5]$$
$$-u \equiv 1 \ [5]$$
$$u \equiv 4 \ [5].$$

275 este vizibil divizibil prin 11; de unde:

$$1274u \equiv 1 \ [11]$$
$$9u \equiv 1 \ [11]$$
$$u \equiv 5 \ [11].$$

Trebuie deci să rezolvăm dubla congruenţă:

$$u \equiv 4 \ [5], \ u \equiv 5 \ [11],$$

fie:

$$u = 5\lambda + 4 = 11\mu + 5,$$
$$5\lambda - 11\mu = 1.$$

O soluţie evidentă este:

$$\lambda = -2, \ \mu = -1,$$

de unde:

$$5(\lambda + 2) = 11(\mu + 1),$$

și, după teorema lui Gauss:

$$\mu + 1 = 5\nu.$$
$$u = 11\mu + 5 = 55\nu - 6 \equiv 49 \ [55].$$

Pentru $\nu = 1$, se găsește $u = 49$, care convine efectiv. Se găsește apoi $\nu = -227$.

3.5.2. Divizori primari

Printre toți întregii, se distinge o familie particulară, care este aceea a întregilor naturali care nu admit decît un singur divizor prim. Să enunțăm:

DEFINIȚIA 3 / **Un număr primar este o putere de exponent mai mare sau egal cu zero a unui număr prim.**

Există o infinitate de numere primare; să notăm cu P mulțimea formată cu aceste numere:

$$P = \{1, 2, 2^2, 2^3, ..., 2^n, ..., 3, 3^2, ..., 3^n, ..., 5, 5^2, ..., 7, ..., 11, ...\}.$$

1. Orice întreg altul decît 0 este un produs dintre o unitate și un produs de numere primare; de exemplu:

$$-18\,900 = (-1)2^2 \cdot 3^3 \cdot 5^2 \cdot 7.$$

Divizorii primari ai întregului natural: $n = p^\alpha q^\beta r^\gamma$, unde p, q, r sînt numere prime, sînt numerele:

$$\{1, p, p^2, p^3, ..., p^{\alpha-1}, p^\alpha, q, q^2, ..., q^\beta, r, r^2, ..., r^\gamma\}.$$

Să notăm cu f aplicația de la mulțimea N^* la mulțimea $\mathcal{P}(P)$ a submulțimilor lui P care, la orice întreg strict pozitiv, asociază mulțimea divizorilor săi primari: De exemplu:

$$\mathfrak{f}(1) = \{1\}, \ \mathfrak{f}(2) = \{1, 2\}.$$
$$\mathfrak{f}(3) = \{1, 3\}, \ \mathfrak{f}(6) = \{1, 2, 3\},$$
$$\mathfrak{f}(12) = \{1, 2, 3, 4\},$$
$$\mathfrak{f}(18900) = \{1, 2, 4, 3, 9, 27, 5, 25, 7\}.$$

Cardinalul lui $\mathfrak{f}(p^\alpha q^\beta r^\gamma)$ este egal cu:

$$\alpha + \beta + \gamma + 1.$$

2. Aplicația $\mathfrak{f}$ este injectivă. În adevăr, doi întregi diferiți au descompuneri diferite în numere prime; există un număr prim p și un număr primar p^α care divide pe unul dintre întregi și nu pe celălalt; de exemplu:

$$120 = 2^3 \cdot 3 \cdot 5, \qquad 60 = 2^2 \cdot 3 \cdot 5,$$
$$8 \mid 120, \qquad 8 \nmid 60.$$
$$8 \in \mathfrak{f}(120), \qquad 8 \notin \mathfrak{f}(60).$$

Aplicația f *nu este surjectivă*; mulțimea {1, 4} nu este imaginea prin f a nici unui întreg, deoarece:

$$4 \mid n \Longrightarrow 2 \mid n.$$

3. Să presupunem că m divide pe n:

$$n = m \times k.$$

Divizorii primari ai lui m sînt divizorii primari ai lui n;
deci:

$$(m \mid n) \Longrightarrow [\mathfrak{f}(m) \subset \mathfrak{f}(n)].$$

Reciproca este adevărată; Să presupunem în adevăr că m are trei divizori primi (p, q, r), de unde egalitățile:

$$m = p^\alpha q^\beta r^\gamma, \quad \mathfrak{f}(m) = \{1, p, p^2, ..., p^\alpha, q, ..., q^\beta, r, ..., r^\gamma\}.$$

p^α, q^β și r^γ divid pe n; de exemplu:

$$n = p^\alpha u.$$

q^β divide pe n și este prim cu p^α (prin definiția c.m.M.d.c.); q^β divide deci pe u (teorema lui Gauss):

$$u = q^\beta v.$$

De asemenea, r^γ divide pe n, deci pe u și v:

$$v = r^\gamma w, \quad n = p^\alpha q^\beta r^\gamma w = mw.$$

(Demonstrația se adaptează ușor, prin inducție, la un număr oarecare de divizori ai lui m). În sfîrșit:

$$\boxed{(m \mid n) \Longleftrightarrow (\mathfrak{f}(m) \subset \mathfrak{f}(n))} \qquad (45)$$

Această implicație permite să regăsim că f este injectivă deoarece, în **N**:

$$(m \mid n) \text{ și } (n \mid m) \Longrightarrow (n = m).$$

4. Să considerăm o familie finită A de întregi strict pozitivi (a, b, c,...), și intersecția:

$$\mathcal{J} = \mathfrak{f}(a) \cap \mathfrak{f}(b) \cap \mathfrak{f}(c) \cap ...$$

Intersecția $\mathcal{J}$ este finită, căci este o submulțime a mulțimii finite $\mathfrak{f}(a)$. Fie p, q, r, ... numerele prime care figurează în $\mathcal{J}$. Întregul primar p^k aparține lui $\mathcal{J}$ dacă și numai dacă p^k divide toți întregii din familia A.
Fie α cel mai mare întreg astfel ca p^α să aparțină lui $\mathcal{J}$; după observația precedentă, se poate scrie incluziunea:

$$\{1, p, p^2, ..., p^\alpha\} \subset \mathcal{J}.$$

p^α este cea mai mare putere a lui p care divide toți întregii lui A.

Să calculăm la fel numerele q^β, r^γ, ..., care constituie cele mai mari puteri ale numerelor prime q, r, ... care divid toți întregii lui A; se poate scrie:

$$\mathcal{J} = \{1,\ p,\ p^2,\ ...,\ p^\alpha,\ q,\ q^2,\ ...,\ q^\beta,\ r,\ ...,\ r^\gamma,...\}.$$

Fie n produsul (finit)

$$n = p^\alpha \times q^\beta \times r^\gamma \times ...$$

Se deduce egalitatea: $\mathcal{J} = \mathfrak{f}(n)$,
apoi incluziunile:

$$\mathfrak{f}(n) \subset \mathfrak{f}(a),\ \mathfrak{f}(n) \subset \mathfrak{f}(b),\ \mathfrak{f}(n) \subset \mathfrak{f}(c),\ ...,$$

și relațiile: $n \mid a$, $n \mid b$, $n \mid c$, ...

5. n este deci un divizor comun al lui a, b, c, ... Orice divizor comun m este astfel încît:

$$m \mid a,\ m \mid b,\ m \mid c,\ ...,$$

deci astfel încît:

$$\mathfrak{f}(m) \subset \mathfrak{f}(a),\ \mathfrak{f}(m) \subset \mathfrak{f}(b),\ \mathfrak{f}(m) \subset \mathfrak{f}(c),\ ...,$$

adică: $\mathfrak{f}(m) \subset \mathcal{J}$.

Cum $\mathcal{J} = \mathfrak{f}(n)$, avem:

$$\mathfrak{f}(m) \subset \mathfrak{f}(n);$$

deci, m este un divizor al lui n.
Divizorii comuni elementelor lui A sînt divizorii lui n, și reciproc. Am definit astfel din nou c.m.M.d.c. al elementelor lui A:

$$\boxed{n = a \frown b \frown c \frown ...}$$

În particular:

$$\boxed{\mathfrak{f}(a \frown b) = \mathfrak{f}(a) \cap \mathfrak{f}(b)} \quad (a > 0,\ \ b > 0) \tag{46}$$

TEOREMA 25 / **C.m.M.d.c. al unei familii finite de întregi strict pozitivi este produsul numerelor primare p^α, q^β, r^γ, ... unde α, β, γ, ... sînt cei mai mari întregi astfel încît aceste numere să dividă toți întregii familiei.**

EXEMPLU. $a = 30576$, $b = 6600$.
Știm că c.m.M.d.c. este egal cu 24 (a se vedea paragraful precedent, pagina 205).
În adevăr:

$$a = 2^4 \cdot 3^1 \cdot 7^2 \cdot 13^1,\ b = 2^3 \cdot 3^1 \cdot 5^2 \cdot 11^1.$$

de unde:

$$a \frown b = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^0 = 2^3 \cdot 3 = 24.$$

Aici:

$$\mathfrak{f}(a) = \{1, 2, 4, 8, 16, 3, 7, 49, 13\},$$
$$\mathfrak{f}(b) = \{1, 2, 4, 8, 3, 5, 25, 11\},$$
$$\mathfrak{f}(a \frown b) = \{1, 2, 4, 8, 3\}.$$

---

7. Teoria precedentă se poate extinde la întregi negativi, punînd:

$$\mathfrak{f}(-n) = \mathfrak{f}(n),$$

(atunci $\mathfrak{f}$ nu mai este injectivă) și la zero, punînd:

$$\mathfrak{f}(0) = P$$

(care redă, de exemplu, egalitatea:

$$0 \frown a = |\, a \,|).$$

Toate proprietățile c.m.M.d.c. sînt atunci imediate, căci ele se reduc la proprietățile bine cunoscute de la mulțimi:

$$a \frown b = b \frown a, \quad a \frown 1 = 1,$$
$$a \frown (b \frown c) = (a \frown b) \frown c,$$
$$a \frown a = |\, a \,| \text{ etc.}$$

EXERCIȚIU

n fiind un întreg strict pozitiv, fie $v_p(n)$ întregul pozitiv sau nul α astfel încît p^α divide pe n, iar $p^{\alpha+1}$ nu divide pe n (p fiind un număr prim).
Să se studieze proprietățile aplicației v_p
Dacă $\alpha = v_p(n)$, atunci $\{1, p, p^2, \ldots, p^\alpha\}$ este submulțimea lui $\mathfrak{f}(n)$ care conține puterile lui p care divid pe n; α este egal cu 0 dacă p nu divide pe n.
Dacă m divide pe n, atunci:

$$v_p(m) \leqslant v_p(n),$$

pentru orice întreg prim p.
Reciproc, dacă această inegalitate este adevărată pentru toți întregii primi, atunci m divide pe n; m este egal cu n dacă și numai dacă:

$$v_p(m) = v_p(n),$$

pentru orice întreg prim p, căci:

$$n = p^{v_p(n)} q^{v_q(n)} r^{v_r(n)} \ldots$$

Dacă d este c.m.M.d.c. al lui m și n, atunci pentru orice p, $v_p(d)$ este cel mai mic dintre cei doi întregi $v_p(m)$ și $v_p(n)$; d' este un divizor comun al lui m și al lui n dacă și numai dacă pentru orice întreg prim p:

$$v_p(d') \leqslant v_p(m), \qquad v_p(d') \leqslant v_p(n).$$

Să considerăm produsul mn; atunci:

$$v_p(mn) = v_p(m) + v_p(n).$$

Dacă s este suma dintre m și n, atunci:

$$v_p(m) \leqslant v_p(s), \qquad v_p(n) \leqslant v_p(s).$$

De exemplu:

$$m = 45,\ n = 216,\ s = 261,$$
$$v_3(m) = 2,\ v_3(n) = 3,\ v_3(s) = 2.$$
$$m = 45,\ n = 207,\ s = 252,$$
$$v_3(m) = 2,\ v_3(n) = 2,\ v_3(s) = 2.$$
$$m = 45,\ n = 198,\ s = 243,$$
$$v_3(m) = 2,\ v_3(n) = 2,\ v_3(s) = 5.$$

Dacă: $v_p(m) < v_p(n)$, atunci:

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

Dacă: $v_p(m) = v_p(n)$, atunci:

$$v_p(m + n) \geqslant v_p(n).$$

v_p este o valoare relativă la numărul prim p.

3.5.3. Aplicații

1. Divizorii primari permit să se calculeze și c.m.m.m.c. al elementelor unei familii finite A de întregi strict pozitivi (a, b, c, ...). În adevăr, să considerăm *reuniunea*:

$$\mathcal{R} = \mathfrak{f}(a) \cup \mathfrak{f}(b) \cup \mathfrak{f}(c) \cup \ldots$$

Reuniunea $\mathcal{R}$ este finită, căci familia A este finită, și fiecare din mulțimile $\mathfrak{f}(a)$ este finită. Fie p, q, r, ..., numerele prime care figurează în $\mathcal{R}$. Întregul primar p^h aparține lui $\mathcal{R}$ dacă și numai dacă p^h divide cel puțin un întreg din A.
Fie α cel mai mare întreg astfel că p^α aparține lui $\mathcal{R}$; după observația precedentă, se poate scrie incluziunea:

$$\{1,\ p,\ p^2,\ \ldots,\ p^\alpha\} \subset \mathcal{R}.$$

p^α este cea mai mare putere a lui p care divide cel puțin un întreg din A. Să calculăm la fel q^β, r^γ, ... care constituie cele mai mari puteri ale primilor q, r, ... care divid cel puțin un întreg din A.
Se poate scrie:

$$\mathcal{R} = \{1,\ p,\ p^2,\ \ldots,\ p^\alpha,\ q,\ q^2,\ \ldots,\ q^\beta,\ r,\ \ldots,\ r^\gamma,\ldots\}.$$

Fie m produsul (finit):

$$m = p^\alpha \times q^\beta \times r^\gamma \times \ldots$$

Se deduce de aci egalitatea:

$$\mathcal{R} = \mathfrak{f}(m),$$

apoi incluziunile:

$$\mathfrak{f}(a) \subset \mathfrak{f}(m),\ \mathfrak{f}(b) \subset \mathfrak{f}(m),\ \mathfrak{f}(c) \subset \mathfrak{f}(m),\ \ldots$$

și relațiile:

$$a \mid m,\ b \mid m,\ c \mid m,\ \ldots$$

2. m este un multiplu comun al lui a, b, c, ... Orice multiplu comun n este astfel încît:

$$a \mid n,\ b \mid n,\ c \mid n,\ \ldots,$$

deci astfel încît:

$$\mathfrak{f}(a) \subset \mathfrak{f}(n),\ \mathfrak{f}(b) \subset \mathfrak{f}(n),\ \mathfrak{f}(c) \subset \mathfrak{f}(n),\ \ldots,$$

adică: $\mathcal{R} \subset \mathfrak{f}(n)$.
Cum $\mathcal{R} = \mathfrak{f}(m)$, avem:

$$\mathfrak{f}(m) \subset \mathfrak{f}(n);$$

de unde rezultă că n este un multiplu al lui m. Multiplii comuni ai elementelor lui A sînt multiplii lui m, și reciproc. Am definit astfel, din nou, c.m.m.m.c. al elementelor lui A:

$$\boxed{m = a \smile b \smile c \smile \ldots}$$

În particular:

$$\boxed{\mathfrak{f}(a \smile b) = \mathfrak{f}(a) \cup \mathfrak{f}(b)} \quad (a > 0,\ b > 0) \tag{47}$$

TEOREMA 26 / **C.m.m.m.c. al unei familii finite de întregi strict pozitivi este produsul numerelor primare p^α, q^β, r^γ, ..., unde α, β, γ, ... sînt cei mai mari întregi astfel că numerele p^α, q^β, r^γ, ... divid cel puțin un întreg al familiei.**

EXEMPLU. $a = 30576$, $b = 6600$.
Știm că c.m.m.m.c. al acestor două numere este egal cu 8408400 (a se vedea paragraful nr. **3.5.1,** pagina 170). În adevăr:

$$a = 2^4 \cdot 3^1 \cdot 7^2 \cdot 13^1,\ b = 2^3 \cdot 3^1 \cdot 5^2 \cdot 11^1,$$

de unde:

$$a \smile b = 2^4 \cdot 3^1 \cdot 5^2 \cdot 7^2 \cdot 11^1 \cdot 13^1 = 8408400.$$

Aici:

$$\mathfrak{f}(a) = \{1, 2, 4, 8, 16, 3, 7, 49, 13\},$$
$$\mathfrak{f}(b) = \{1, 2, 4, 8, 3, 5, 25, 11\},$$
$$\mathfrak{f}(a \smile b) = \{1, 2, 4, 8, 3, 5, 25, 7, 49, 11, 13\}.$$

---

3. Teoremele 25 și 26 se pot formula sub forma unei reguli care se folosește foarte des.
1° Pentru a calcula c.n.M.d.c. al unei familii finite de întregi strict pozitivi, se *înmulțesc* divizorii primi care divid toți întregii familiei cu exponentul cel mai mic cu care ei apar în descompunerile elementelor familiei.

2° Pentru a calcula c.m.m.m.c. al unei familii finite de întregi strict pozitivi, se înmulțesc divizorii primi care divid cel puțin unul din întregii familiei cu exponentul cel mai mare cu care ei apar în descompunerile elementelor familiei.

Astfel, în cazul a doi întregi:

$$a = p^{\alpha}q^{\beta}r^{\gamma},\ b = p^{\alpha'}q^{\beta'}r^{\gamma'}.$$

se poate scrie:

$$a \smile b = p^{u}q^{v}r^{w}\ (u = \sup(\alpha, \alpha'),\ v = \sup(\beta, \beta'),\ w = \sup(\gamma, \gamma'))$$

$$a \frown b = p^{u'}q^{v'}r^{w'}\ (u' = \inf(\alpha, \alpha'),\ v' = \inf(\beta, \beta'),\ w' = \inf(\gamma, \gamma'))$$

Cum avem evident:

$$\sup(x, y) + \inf(x, y) = x + y,$$

rezultă formula cunoscută:

$$ab = (a \smile b)(a \frown b) \quad (a > 0,\ b > 0).$$

4. Extinzînd aplicația f la zero și la întregii negativi, se regăsesc imediat egalitățile:

$$0 \smile a = 0,$$

$$a \smile b = b \smile a,\ a \smile 1 = |\, a \,|,$$

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

$$a \smile a = |\, a \,| \text{ etc.}$$

Observație. Această extensie permite să se considere și c.m.M.d.c. al unei familii infinite de întregi relativi, căci intersecția $\mathcal{J}$ este întotdeauna finită. Dimpotrivă, *ea nu mai dă pe c.m.m.m.c. al unei familii infinite* (care este nul dacă familia conține o infinitate de întregi diferiți) cum arată exemplul familiei A a numerelor prime naturale, pentru care $\mathcal{R}$ este diferit de f(0).

5. Aplicația f permite să se demonstreze instantaneu relații importante ca acestea:

$$a \frown (a \smile b) = |\, a \,| \tag{48}$$

$$a \frown (b \smile c) = (a \frown b) \smile (a \frown c) \tag{49}$$

Este suficient să verificăm aceste formule în cazul cînd întregii sînt strict pozitivi (cazul $abc = 0$ fiind foarte simplu se examinează direct). Punînd: $A = \mathfrak{f}(a)$, $B = \mathfrak{f}(b)$, $C = \mathfrak{f}(c)$, este destul să se scrie relațiile din teoria mulțimilor:

$$A \smile (A \frown B) = A,$$

$$A \smile (B \frown C) = (A \smile B) \frown (A \smile C).$$

Se arată în mod analog egalitățile:

$$a \smile (a \frown b) = |a| \tag{50}$$
$$a \smile (b \frown c) = (a \smile b) \frown (a \smile c) \tag{51}$$

TEOREMA 27 / **Operațiile binare definite prin c.m.m.m.c. și c.m.M.d.c. sînt distributive una în raport cu cealaltă.**

(Ne putem referi și la exercițiul nr. **3.120** de la pagina 180).

6. În general, aplicația f este un izomorfism între $\mathbf{N}^*$ și imaginea sa, care este o submulțime a mulțimii părților lui P. Operațiilor (c.m.m.m.c., c.m.M.d.c.) le corespund operațiile (reuniune, intersecție); numărului 0 îi corespunde mulțimea $\{1\}$; relației de divizibilitate îi corespunde relația de incluziune.
Orice propoziție relativă la divizibilitatea în $\mathbf{N}^*$ se poate traduce printr-o propoziție în $\mathfrak{f}(\mathbf{N}^*)$, și reciproc. Aceste două mulțimi sînt numite *latici* (distributive); ele sînt izomorfe.

EXERCIȚII

I. *Să se calculeze valoarea v_p a c.m.m.m.c. al întregilor m și n.*
Teorema 26 arată imediat că $v_p(m \smile n)$ este cel mai mare dintre întregi $v_p(m)$ și $v_p(n)$, în particular:

$$v_p(m) + v_p(n) = v_p(m \smile n) + v_p(m \frown n).$$

Aceasta este relația pe care am folosit-o pentru a regăsi egalitatea:

$$ab = (a \smile b)(a \frown b).$$

II. *Se consideră doi întregi strict pozitivi a și b, primi între ei. Să se demonstreze egalitatea:*

$$a \frown bx = a \frown x.$$

Această egalitate este adevărată pentru $x = 0$. Dacă x nu este nul, este suficient să presupunem că x este strict pozitiv. Orice divizor comun lui a și lui x divide evident pe a și pe bx. *Reciproc*, să considerăm un întreg n, care divide pe a și pe bx. Cum:

$$\mathfrak{f}(a) \cap \mathfrak{f}(b) = \{1\} \text{ și } \mathfrak{f}(n) \subset \mathfrak{f}(a),$$

rezultă:

$$\mathfrak{f}(n) \cap \mathfrak{f}(b) = \{1\},$$

sau:

$$n \overset{*}{\frown} b = 1.$$

n divizînd pe bx și fiind prim cu b divide deci pe x. Mulțimile ($div\ a \cap div\ bx$) și ($div\ a \cap div\ x$) fiind egale, cei mai mari divizori comuni sînt deci egali.

III. *Să se regăsească rezultatul exercițiului* II *de mai sus cu ajutorul identității lui Bezout.*
Să luăm:

$$au + bv = 1.$$

Orice număr de forma $(\lambda a + \mu bx)$ este evident de forma $(\lambda' a + \mu' x)$.
Reciproc:

$$n = \lambda' a + \mu' x = \lambda' a + \mu'(au + bv)x = (\lambda' + \mu' ux)a + (\mu' v)bx = \\ = \lambda a + \mu bx.$$

Generatorii grupurilor combinațiilor liniare ale lui (a, bx) și ale lui (a, x) sînt deci egali, ceea ce demonstrează egalitatea studiată.

EXERCIȚII

3.97. Să se determine întregii n astfel ca să avem, în inelul $\mathbf{Z}/n\mathbf{Z}$, echivalența:

$$(\exists y \neq \overline{0},\ xy = \overline{0}) \Longleftrightarrow \exists m,\ x^m = \overline{0}).$$

3.98. Dacă n este un întreg primar, $n = p_m$, să se demonstreze implicația:

$$(n \nmid a) \Longrightarrow ([a^{p-1} - 1]^m \equiv 0 \quad [n]).$$

3.99. Să se determine c.m.M.d.c. și c.m.m.m.c. al numerelor familiei (240, —252, 792).

3.100. Aceeași problemă pentru familiile:

(6652, 924), (27634, 6551), (49980, 28420),

(180, 606, 750), —(390, —720, —450),

(540, 1008, 756), (49980, 33810, 28420, 4116).

3.101. Să se determine numerele inferioare lui 50 și prime cu 80.

3.102. Să se rezolve în $\mathbf{N}$ ecuația definită prin:

$$380 \frown x = 5, \qquad x \leqslant 100.$$

3.103. Să se rezolve în $\mathbf{N}$ ecuația definită prin:

$$m + n = 420,\ m \frown n = 12.$$

3.104. Aceeași problemă pentru:

$$144 = m \geqslant n,\ m \frown n = 16.$$

3.105. Aceeași problemă pentru:

$$mn = 6480,\ m \frown n = 18.$$

3.106. Să se rezolve în $\mathbf{Z}$ sistemul de ecuații definit prin:

$$x \frown y = y \frown z = z \frown x = 17,$$
$$x + y + z = 225,\ x \smile y \smile z = 1785.$$

3.107. Să se rezolve în $\mathbf{Z}$ sistemul de congruențe definit prin:

$$x \equiv 1 \quad [74],\ x \equiv -1 \quad [8].$$

3.108. Să se rezolve, în inelul $\mathbf{Z}/n\mathbf{Z}$, ecuațiile definite prin:

$$x^2 = x,\ x^2 = \overline{1},\ x^2 = \overline{0},$$

știind că n este produsul a două numere prime distincte (exemple: $n = 6$, $n = 15$, $n = 803$).

3.109. Să se calculeze numerele întregi:

$$a^n \frown b^n,\ a^n \smile b^n,$$

în funcție de $d = a \frown b$, $m = a \underset{\sim}{\smile} b$.

3.110. Să se calculeze numerele întregi:

$$108 \smile 144,\ 128 \smile 230,\ 1848 \smile 1950,$$
$$480 \smile 874 \smile 1028,\ 480 \smile 210 \smile 735 \smile 491.$$

3.111. Să se rezolve în $\mathbf{Z}$ ecuația definită prin:

$$6 \smile x = 96.$$

3.112. Să se rezolve în **Z** sistemele definite prin:

1° $xy = 1512$, $x \smile y = 252$.

2° $xy = 300$, $x \smile y = 60$.

3° $x + y = 276$, $x \smile y = 1440$.

4° $(x \smile y) - (x \frown y) = 187$.

5° $(x \smile y) - 3(x \frown y) = 108$. $10 < x \frown y < 15$.

6° $x \frown y = 5$, $x \smile y = 30$.

7° $x \frown y = 30$, $x \smile y = 300$.

8° $x \frown y = 60$, $x \smile y = 300$.

3.113. Să se determine un întreg n care să admită 10 divizori în **Z**, știind că $(n - 16)$ este produsul a doi întregi naturali primi.

3.114. Să se rezolve în **N** ecuația definită prin:

$$x^2 - y^2 = 240.$$

3.115. n fiind unul din următoarele trei numere întregi 28, 496 sau 8128, să se calculeze semisuma divizorilor săi (astfel de întregi se numesc perfecți).

3.116. Aceeași problemă pentru întregii 220 și 284 (care se numesc amiabile).
Aceeași problemă pentru 18416 și 17296.
Aceeași problemă pentru $2^2 \times 37$ și $2 \times 5 \times 11^2$.

3.117. Se dau relațiile:

$$0 < m < n,\ n \mid m^2,$$
$$d = m \frown n,\ m = dm_1,\ n = dn_1.$$

Să se demonstreze că n_1 divide pe d, și că n are un divizor un pătrat mai mare ca **1**.

3.118. Să se demonstreze egalitatea:

$$xyz(x \frown y \frown z) = (x \smile y \smile z)\,(x \frown y)\,(y \frown z)\,(z \frown x).$$

3.119. Să se demonstreze egalitatea:

$$(x \frown y)\,(y \frown z)\,(z \frown x) = (x \frown y \frown z)\,(xy \frown yz \frown zx).$$

3.120. Să se demonstreze egalitatea:

$$(x \frown y) \smile (y \frown z) \smile (z \frown x) = (x \smile y) \frown (y \smile z) \frown (z \smile x).$$

Se pot schimba rolurile simbolurilor $\frown$ și $\smile$?

3.121. Să se demonstreze implicația:

$$[(a \frown x) = (a \frown y) \text{ și } (a \smile x) = (a \smile y)] \Longrightarrow [\,|\,x\,| = |\,y\,|\,].$$

3.122. x, y, z fiind mulțimi, iar simbolurile $\frown$ și $\smile$ reprezentînd atunci intersecția și reuniunea, relațiile din exercițiile de la **3.118.** la **3.121** mai sînt exacte? Dacă da, să fie demonstrate direct.

3.123. p, q, r fiind trei numere prime, α, β, γ fiind trei întregi, să se demonstreze că întregul:

$$s = (p - 1) \smile (q - 1) \smile (r - 1)$$

este astfel încît întregul:

$$t = (p^\alpha - p^{\alpha-1}) \smile (q^\beta - q^{\beta-1}) \smile (r^\gamma - r^{\gamma-1})$$

divide întregul:

$$n = p^{\alpha-1} q^{\beta-1} r^{\gamma-1} s.$$

3.124. Să se rezolve în **N** ecuația definită prin:

$$x^2 + y^2 + z^2 = 2(xy + yz + zx).$$

(Să se observe că $4xy$ este un pătrat.)

3.125. Dacă întregul $a^m + b^n$ este un număr prim, c.m.M.d.c. al lui m și n este o putere a lui 2.

3.126. Să se rezolve în **Z** sistemul definit prin:

$$x^2 - y^2 = 7344, \quad x \frown y = 12.$$

3.127. Să se determine întregii naturali m și n care au 45 divizori comuni astfel încît:

$$m + n = 127008.$$

3.128. Să se demonstreze că, dacă d este c.m.M.d.c. al întregilor naturali m și n, $(a^d - b^d)$ este c.m.M.d.c. al întregilor $(a^m - b^m)$ și $(a^n - b^n)$ dacă a este mai mare decît b.

3.129. Să se demonstreze că existența întregilor u și v astfel încît:

$$0 = au - bv, \quad 0 < |u| < b, \quad 0 < |v| < a$$

echivalează cu relația:

$$(a \frown b) > 1.$$

3.130. Numărul 37 se bucură de curioasa proprietate ilustrată prin egalitatea:

$$3 \times 7 \times 37 = 777.$$

Există alți întregi mai mici ca 100 cu aceeași proprietate?

3.131. Să se rezolve în **N** ecuația definită prin:

$$(10x + y)(x + y) = x^3 + y^3.$$

3.132. a și b fiind primi între ele, a' și b' fiind de semenea primi între ele, să se demonstreze echivalența:

$$(b \frown b' = 1) \Longleftrightarrow [bb' \frown (ab' + a'b) = 1].$$

3.133. Să se demonstreze în **N** implicația:

$$(x^2 + y^2 = 2z^2) \Longrightarrow (x^2 \equiv y^2 \quad [48]).$$

3.134. Să se demonstreze implicația:

$$(x^2 + y^2 = z^2) \Longrightarrow (xy = 0 \quad [6] \text{ și } xyz \equiv 0 \quad [30]).$$

3.135. Să se demonstreze implicația:

$$(x^2 + y^2 = z^2 \text{ și } z \equiv 0 \quad [6]) \Longrightarrow (xyz \equiv 0 \quad [1080]).$$

3.136. Să se determine întregii n astfel încît:

$$10^4 \leqslant n^2 < 10^5, \quad n^2 \equiv 0 \quad [54].$$

3.137. Să se determine întregii relativi x și y astfel încît:

$$x \smile y = 340, \quad x(y + 25) = y(x + 20).$$

3.138. Să se rezolve în **N** ecuația definită prin:

$$(2x + 1)(2y + 1) = (x + 1)(y + 1)z.$$

3.139. Să se rezolve în **N** ecuația definită prin:

$$(x - 27)(y + 12) = xy.$$

Să se calculeze $x \frown y$ pentru fiecare dintre soluții.

3.140. Să se demonstreze că a și b fiind numere întregi prime între ele c.m.M.d.c. al lui $(a-b)$ și $\dfrac{a^n-b^n}{a-b}$ divide pe n.

PROBLEME

3.141. Fie a și b doi întregi naturali primi între ei. Se consideră numerele $(a, 2a, 3a, \ldots, \ldots, (b-2)a, (b-1)a)$ și resturile acestor numere la împărțirea prin b.
1° Să se demonstreze că toate resturile sînt diferite.
2° Să se deducă existența unui număr x astfel încît:

$$b \mid (ax-1),\ 1 \leqslant x < b.$$

3° *Aplicație.* $a = 13$, $b = 8$.
4° Să se regăsească prin această metodă identitatea lui Bachet-Bezout.

3.142. Se consideră șirul (u_n) definit prin:

$$u_0 = 0,\ u_1 = 1,\ u_n = u_{n-1} + u_{n-2} \quad (n \geqslant 2).$$

1° Să se calculeze u_n pentru n mai mic sau egal cu 10.
2° Să se demonstreze relațiile:

$$u_0 + u_1 + u_2 + \ldots + u_{n-1} = u_{n+1} - 1 \quad (n \geqslant 1);$$
$$u_n u_{n-2} - u_{n-1}^2 = (-1)^{n-1} \quad (n \geqslant 2);$$
$$u_{n+p-1} = u_{n-1}u_{p-1} + u_n u_p \quad (n \geqslant p \geqslant 1).$$

3° Să se calculeze numărul:

$$u_n \frown u_{n+1}.$$

4° Să se demonstreze implicația:

$$(n \frown m = d) \Longrightarrow (u_n \frown u_m = u_d).$$

(Acest șir se numește șirul lui *Fibonacci.*)

3.143. a, b, c sînt respectiv cifrele unităților, zecilor și sutelor ale unui număr întreg n. Să se calculeze a, b, c în fiecare din cazurile următoare:

1° $a = c$, $n \equiv 0$ [3], $n \equiv 0$ [5].

2° $a = c$, $n \equiv 0$ [3], $n \equiv 0$ [11].

3° $n \equiv 0$ [3], $n \equiv 0$ [5], $n \equiv 0$ [11].

4° $n \equiv 0$ [3], $n \equiv 0$ [5], $n = m^2$ $(m \in \mathbf{N})$.

3.144. 1° Să se rezolve ecuația definită pe inelul $\mathbf{Z}/5\mathbf{Z}$ prin: $x^4 = \overline{k}$, unde k este un întreg dat.
2° Se consideră doi întregi naturali a și b astfel ca a^5 și b^5 să aibă aceeași cifră a unităților în scrierea zecimală. Să se demonstreze că $a - b$ este divizibil prin 10, și că $a^2 - b^2$ este divizibil prin 20.
3° Să se calculeze atunci a și b știind că:

$$a^2 - b^2 = 1940.$$

4° Aceeași problemă pentru:

$$a^2 - b^2 = 1920.$$

3.145 Se consideră șirul (u_n) definit prin:

$$u_0 = 1,\ u_1 = 1,\ u_n = u_{n-1} + 2u_{n-2} \quad (n \geqslant 2).$$

1° Să se determine clasa lui u_n modulo 2.
2° Să se calculeze numerele:

$$u_n \frown u_{n+1}, \quad u_n \frown u_{n+3}.$$

3° Să se demonstreze egalitatea:

$$u_{n+p} = u_{n+1}u_p + 2u_n u_{p-1} \quad (p \geqslant 1),$$

4° Să se calculeze numărul:

$$u_n \frown u_{n+3}.$$

3.146. 1° Să se rezolve ecuația definită pe inelul $\mathbf{Z}/4\mathbf{Z}$ prin:

$$x^2 = \overline{k},$$

unde k este un întreg dat.
2° Se consideră sistemul definit pe $\mathbf{Z}$ prin:

$$\begin{cases} x^2 + y^2 = z^2, \\ x \frown y \frown z = 1. \end{cases}$$

Să se demonstreze că z este impar, ca și unul dintre cei doi întregi x și y, celălalt fiind par.
3° Se presupune că y este par. Să se calculeze:

$$(y + z) \frown (y - z).$$

4° Să se demonstreze atunci că se poate scrie:

$$y + z = u^2, \quad y - z = v^2, \quad u \frown v = 1,$$

u și v fiind doi întregi impari.
5° Să se determine toate soluțiile problemei în funcție de doi parametri arbitrari u și v, întregi impari.
6° Să se determine efectiv toate soluțiile astfel încît:

$$0 < x < 20, \quad 0 < y < 20, \quad 0 < z < 20.$$

7° Să se rezolve ecuația definită pe $\mathbf{Z}$ prin:

$$x^2 + y^2 = z^2.$$

8° Se pune atunci:

$$r(|x| + |y| + |z|) = |xy|, \quad xyz \neq 0.$$

Să se demonstreze că r este un întreg natural.
3.147. 1° m și n fiind doi întregi naturali astfel încît: $n \geqslant 2$, se consideră întregii:

$$a = mn, \quad b = m(n - 1).$$

Să se calculeze $(a \frown b)$ în funcție de m și n, apoi de a și b.
2° Să se rezolve ecuația definită pe $\mathbf{Z}$ prin:

$$x \frown y = x - y.$$

3° *Aplicație.* Să se determine efectiv toate soluțiile știind că:

$$x \frown y = 30.$$

4° Se consideră întregii:

$$a = 24x(5y + 3), \quad b = 15x(8y + 5), \quad c = 40x(3y + 2),$$

unde x, y, z sînt întregi naturali. Să se calculeze cei mai mari divizori comuni ai numerelor a și b, b și c, c și a și diferențele dintre aceste numere.

5° Să se calculeze numărul:

$$a \frown b \frown c.$$

3.148. Se dau întregii naturali nenuli:

$$a > b, \quad a \frown b = d, \quad a \smile b = m.$$

1° n fiind un întreg dat astfel încît:

$$a = n(2n - 1), \quad b = (n - 1)(2n - 1),$$

să se calculeze d și m.
2° Se presupune acum că:

$$m(a + b) = abd. \tag{1}$$

Să se calculeze a și b în funcție de $p = \frac{a}{d}$ și $q = \frac{b}{d}$.

3° a și b satisfăcînd relația (1), se presupune că se mai poate scrie:

$$d = a - b. \tag{2}$$

Să se calculeze a și b.
4° Să se deducă relația:

$$(a - b)^2 = a + b. \tag{3}$$

5° Se presupune că a și b satisfac relația (3). Egalitățile (1) și (2) sînt satisfăcute?
6° Se dă atunci restul r împărțirii lui a prin b. Să se calculeze a și b știind că r nu este nul.
7° *Aplicație.* $r = 11$.

3.149. n este un întreg natural. Se consideră ecuația definită pe $\mathbf{Z}$ prin:

$$(x - 2n)(y - 2n) = 2n^2.$$

1° Se pune:

$$d = (x - 2n) \frown (y - 2n).$$

Să se demonstreze relația: $d \mid (x \frown y)$.
2° Să se demonstreze relația:

$$x^2 + y^2 = (x + y - 2n)^2.$$

Să se deducă că $(x \frown y)$ divide pe d.
3° Să se demonstreze că $(x \frown y)$ divide pe n.
4° Să se calculeze x și y, știind că:

$$x \frown y = 1, \quad n = 30.$$

3.150. m este un întreg pozitiv dat.
1° Să se demonstreze relația:

$$\sum_{i=1}^{m} i = \frac{m(m+1)}{2} = S \quad (m \geqslant 1).$$

2° a fiind un întreg impar, să se demonstreze implicația:

$$(n \equiv m \ [a]) \Longrightarrow (S_n \equiv S_m \ [a]).$$

Să se deducă soluțiile ecuației definită pe corpul $\mathbf{Z}/11\mathbf{Z}$ prin:

$$\bar{S}_m = \bar{k},$$

unde k este un întreg dat.

3° x fiind un întreg strict mai mare ca 1, să se demonstreze că există un întreg m unic astfel încît:

$$S_m \leqslant x < S_{m+1}.$$

4° Se consideră:

$$\mathrm{I}(x) = S_m.$$

Să se demonstreze inegalitatea:

$$[x - \mathrm{I}(x) - 1]^2 < 2x.$$

5° Se presupune pe viitor că există un întreg n astfel încît:

$$S_m = n^2.$$

Să se demonstreze că unul dintre numerele m și $(m + 1)$ este un pătrat perfect impar.
Exemplu: $m = 8$.
6° Să se demonstreze atunci că, dacă m este par și că dacă $m' = 4m(m + 1)$, $S_{m'}$ este un pătrat perfect.
Să se deducă că există o infinitate de întregi m astfel ca S_m să fie un pătrat perfect.
7° Să se demonstreze implicația:

$$(S_m = n^2) \Longrightarrow (\exists_{\mathrm{N}} k,\ \exists_{\mathrm{N}} h,\ m = 4k(k + 1),\ S_k = h^2).$$

3.151. x, y, z sînt trei întregi pozitivi astfel încît:

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{z}.$$

Să se demonstreze că există întregi a, b, c astfel încît:

$$x = a(a + b)c,\ y = b(a + b)c,\ z = abc.$$

3.152. n este un întreg nenul a cărui descompunere în factori primi se scrie sub forma:

$$n = p^\alpha q^\beta r^\gamma \quad (\alpha > 0,\ \beta > 0,\ \gamma > 0).$$

1° Să se demonstreze că numărul divizorilor lui n este dat prin egalitatea:

$$\mathrm{N} = (\alpha + 1)(\beta + 1)(\gamma + 1).$$

Aplicație. $n = 300$.
2° Ce se poate spune despre N dacă n este un pătrat perfect? Să se studieze reciproca.
3° Să se generalizeze la întregii n având un număr oarecare de divizori primi.
4° Să se determine cei mai mici întregi având respectiv 18 și 100 divizori.
5° n având aceeași formă ca la 1°, să se determine că suma divizorilor săi este dată prin egalitatea:

$$S = \frac{(p^{\alpha+1} - 1)(q^{\beta+1} - 1)(r^{\gamma+1} - 1)}{(p - 1)(q - 1)(r - 1)}$$

6° p fiind produsul divizorilor lui n, să se demonstreze egalitatea: $p^2 = n^{\mathrm{N}}$.
3.153. Să se determine un întreg n astfel încît:

$$\mathrm{N} = 9,\ n = 39p + 1,$$

unde p este prim (acest exercițiu folosește rezultatele problemei nr. **3.152**).
3.154. 1° a și b sînt doi întregi primi între ei, astfel încît: $a < b$.
Să se demonstreze că resturile la împărțirile prin b ale numerelor

$$(k,\ a + k,\ 2a + k,\ \ldots,\ (b - 2)a + k,\ (b - 1)a + k)$$

sînt toate distincte dacă: $0 \leqslant k < a$.

2° $\varphi(n)$ fiind numărul întregilor m astfel încît:

$$0 < m \leqslant n, \quad m \frown n = 1 \quad (n \geqslant 1),$$

să se demonstreze implicația:

$$(a \frown b = 1) \Longrightarrow \varphi(ab) = \varphi(a)\varphi(b)).$$

3° p fiind un număr prim, să se calculeze numărul:

$$\varphi(p^\alpha) \quad (\alpha \in \mathbf{N}).$$

q și r fiind alte două numere prime, să se calculeze numărul:

$$\varphi(p^\alpha q^\beta r^\gamma).$$

Aplicație. $n = 300$.

4° Să se demonstreze relațiile:

$$\varphi(mn) \geqslant \varphi(m)\varphi(n);$$
$$[\varphi(mn) = \varphi(m)\varphi(n)] \Longleftrightarrow [m \frown n = 1];$$
$$(m \mid n) \Longrightarrow (m\varphi(n) \leqslant n\varphi(m));$$
$$(m \mid n \Longrightarrow (\varphi(m)\varphi(n);$$
$$[\varphi(m \frown n)]] [\varphi(m) \frown \varphi(n)];$$
$$[\varphi(m) \frown \varphi(n)] \mid [\varphi(m \frown n)].$$

5° Să se demonstreze echivalența:

$$[m^k\varphi(m) = n^k\varphi(n)] \Longleftrightarrow [m = n] \quad (k \geqslant 1).$$

(Se va considera cel mai mare număr prim p care divide pe mn, și exponentul α astfel încît, de exemplu, p^α divide pe m, $p^{\alpha+1}$ nu divide nici pe m nici pe n.)

6° Se notează $n = p^\alpha q^\beta r^\gamma (\alpha \geqslant \beta \geqslant \gamma)$,
unde p, q, r sînt trei numere prime diferite. Să se demonstreze inegalitatea:

$$\varphi(n) \leqslant n - \alpha.$$

3.155. a și b sînt doi întregi astfel încît:

$$a > b > 1, \qquad a \frown b = 1.$$

1° Să se demonstreze că există doi întregi λ și μ astfel încît:

$$\lambda a - \mu b = 1, \; 0 < \lambda < b, \; 0 < \mu < a;$$

2° Să se demonstreze că ecuația definită pe $\mathbf{N}$ prin:

$$ax + by = n$$

are cel puțin o pereche soluție (x, y) dacă n este mai mare sau egal cu ab, și cel mult o pereche (x, y) drept soluție în caz contrar.

3° Să se demonstreze că ecuația $ax + by = n$ admite exact o soluție pentru:

$$(a - 1)(b - 1) \leqslant n < ab.$$

Aplicație. $a = 13$, $b = 20$. Să se calculeze x și y, în cazul în care există pentru: $n < ab$.

3.156. Să se studieze în $\mathbf{Z}$ ecuația definită prin:

$$x^2 + 5y^2 = z^2.$$

Se notează $\delta = x \frown z$.

1° Să se demonstreze că este suficient să se studieze cazul $\delta = 1$;

2° Se notează atunci:

$$d = (z - x) - (z + x).$$

Să se demonstreze că d divide pe 2.

3° Să se demonstreze că, dacă $d = 1$, există două numere impare u și v astfel încît:

$$y = uv, \ 2z = 5u^2 + v^2.$$

4° Să se demonstreze că, dacă $d = 2$, există două numere impare u și v astfel încît:

$$y = 2uv, \ z = 5u^2 + v^2,$$

5° Să se rezolve ecuația propusă.

3.157. 1° Se consideră ecuația definită pe N prin:

$$xyz = x + y + z - 2.$$

Să se demonstreze că se poate scrie, de exemplu:

$$1 \leqslant x \leqslant y \leqslant z \leqslant 5.$$

2° Să se determine toate soluțiile (se vor găsi zece).

3° Se consideră ecuația definită pe N prin:

$$a \frown b \frown c = a + b + c.$$

Să se demonstreze că a divide pe $(b + c)$, b divide pe $(c + a)$ și c divide pe $(a + b)$.

4° Să se folosească primele două chestiuni pentru a rezolva ecuația propusă.

3.158. Să se rezolve sistemul definit pe N prin:

$$\begin{cases} xy + yz + zx = xyz + 2. \\ x + y + z = xyz. \end{cases}$$

3.159. Se consideră ecuația definită pe N prin:

$$x^2 + y^2 = 2z^2, \ 0 < x < y, \ x \frown y \frown z = 1.$$

1° Să se demonstreze că există doi întregi u și v astfel încît:

$$x = u + v, \ y = u - v.$$

2° Să se deducă din rezultatele problemei nr. **3.144** că există doi întregi h și k astfel încît:

$$x = h^2 - 2hk - k^2, \ y = h^2 + 2hk - k^2, \ z = h^2 + k^2.$$

3.160. Fie un inel comutativ unitar $(A, +, \cdot)$, unde elementul neutru al adunării este notat 0, iar elementul neutru al înmulțirii este notat e. Fie α un element al lui A.

A. 1° Fie $\mathscr{A}$ produsul cartezian $A \times A$. Se înzestrează această mulțime cu o adunare și o înmulțire definite prin:

$$(a, b) + (c, d) = (a + c, b + d),$$
$$(a, b)(c, d) = (ac + \alpha bd, ad + bc).$$

Să se demonstreze că $(\mathscr{A}, +, \cdot)$ este un inel comutativ unitar.

2° Fie $\mathscr{A}_*$ produsul $A \times \{0\}$. Să se demonstreze că se poate defini, prin restricția la $\mathscr{A}_*$ a legilor lui $\mathscr{A}$, o structură de inel.

Dacă se notează:

$$\mathfrak{f} = [a \longmapsto (a, 0)]$$

$\mathfrak{f}$ este un izomorfism între A și $\mathscr{A}_*$. Se vor identifica pe viitor A și $\mathscr{A}_*$.

3° Fie $\omega = (0, e)$. Să se demonstreze egalitatea:

$$\omega^2 = (\alpha, 0).$$

4° Se presupune pe viitor că A este un inel integru și că egalitatea $(2x = 0)$ implică egalitatea cu 0 a lui x.
Să se rezolve ecuația definită prin:

$$(x, y)\,(x, y) = (\alpha, 0).$$

Să se deducă că orice element z al lui $\mathcal{A}$ se poate scrie sub forma:

$$z = a + \omega b \quad (a \in A,\ b \in A,\ \omega^2 = \alpha).$$

B. Se presupune, în această chestiune, că α este nul și că A este corpul numerelor reale; $\mathcal{A}$ este atunci mulțimea *numerelor duale.*

1° Să se demonstreze că $\mathcal{A}$ nu este integru.

2° Să se determine elementele lui $\mathcal{A}$ care admit un invers la înmulțire.

3° Să se studieze unicitatea descompunerii:

$$z = a + \varepsilon b, \quad \varepsilon = (0, 1).$$

4° Să se studieze existența rădăcinilor pătrate ale numărului dual:

$$z = a + \varepsilon b.$$

5° Să se rezolve ecuația de gradul doi definită pe $\mathcal{A}$ prin:

$$z^2 + pz + q = 0 \quad (p \in \mathcal{A},\ q \in \mathcal{A}).$$

C. Se presupune că A este integru, că nu există nici un element β în A astfel că $\alpha^2 = \beta$, și că egalitatea $(2x = 0)$ implică egalitatea cu 0 a lui x.

1° Să se studieze unicitatea descompunerii:

$$z = a + \omega b \quad (a \in A,\ b \in A,\ \omega^2 = \alpha).$$

2° Se va nota pe viitor:

$$\bar{z} = a - \omega b.$$

Să se demonstreze că aplicația:

$$\mathfrak{f}[z \longmapsto \bar{z}]$$

satisface egalitățile:

$$\mathfrak{f}(z + z') = \mathfrak{f}(z) + \mathfrak{f}(z'),\ \mathfrak{f}(zz') = \mathfrak{f}(z)\mathfrak{f}(z').$$

Care este natura lui $\mathfrak{f}$?

3° Se pune $\varphi(z) = z\bar{z}$. Să se demonstreze egalitățile:

$$\varphi(z) = a^2 - \alpha b^2;$$

$$\varphi(zz') = \varphi(z)\varphi(z').$$

4° Să se demonstreze că elementul z admite un invers în $\mathcal{A}$ dacă și numai dacă $\varphi(z)$ admite un invers în A. Să se deducă că $\mathcal{A}$ este un corp dacă A este un corp.

D. Se presupune că A este un corp, că nu există nici un element β în A astfel ca $\alpha^2 = \beta$ și că egalitatea $(2x = 0)$ implică egalitatea cu 0 a lui x.
Se consideră mulțimea $\mathcal{M}(\alpha)$ a matricelor pătrate de ordinul doi cu elemente în A de forma:

$$M(a, b) = \begin{pmatrix} a & \alpha b \\ b & a \end{pmatrix}.$$

1° Să se definească pe $\mathcal{M}(\alpha)$ o adunare și o înmulțire, inspirate din acele ale matricelor reale, care îi dau o structură de inel comutativ.

2° Să se demonstreze că $\mathcal{M}(\alpha)$ este un corp.

3° Să se regăsească acest rezultat considerînd aplicația:

$$g = [a + \omega b \longmapsto M(a, b)].$$

4° Să se rezolve ecuația definită pe $\mathcal{A}$ prin:

$$z^2 - \alpha = 0.$$

5° *Aplicație.* Se ia $A = \mathbf{Z}/3\mathbf{Z}$. Să se demonstreze că se poate lua $\alpha = 2$. Cîte elemente are $\mathcal{A}$? Să se alcătuiască tabelele acestui corp.

6° Să se examineze cazul cînd A este unul dintre corpurile Q sau $\mathbf{R}$ (numere raționale sau reale) și în care $\alpha = -1$.

3.161. Fie $\mathbf{R}^2$ produsul cartezian al mulțimii realilor prin ea însăși. Un element al lui $\mathbf{R}^2$ este notat $z = (\alpha, \beta)$.
Fie $\mathfrak{T}$ transformarea lui $\mathbf{R}^2$ care, lui $z = (\alpha, \beta)$, face să-i corespundă $z' = (\alpha', \beta')$ astfel încît:

$$\alpha' = a\alpha + b\beta$$
$$\beta' = c\alpha + d\beta,$$

unde a, b, c sînt întregi relativi.

La fiecare transformare $\mathfrak{T}$, se asociază matricea pătrată de ordinul doi $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, al cărei determinant este notat

$$\Delta = ad - bc.$$

Se notează prin $(\mathfrak{T})$ mulțimea transformărilor $\mathfrak{T}$.

I. 1° O transformare $\mathfrak{A}$ aparținînd lui $(\mathfrak{T})$ lasă fiecare pereche invariantă. Care este matricea sa U?

2° Să se demonstreze echivalența:

$$\mathfrak{T} = \mathfrak{T}' \Longleftrightarrow T = T'.$$

3° Să se demonstreze că matricea lui $\mathfrak{T}'' = \mathfrak{T}' \circ \mathfrak{T}$ este $T'' = T'T$, unde $T'T$ reprezintă produsul matricei T' prin matricea T. Se reamintește că produsul matricelor este, în general, necomutativ.
Să se calculeze determinanții Δ, Δ' și Δ'' asociați lui T, T' și T''.
Să se exprime Δ'' cu ajutorul lui Δ și Δ'.

4° Se compun un număr oarecare de transformări ale familiei $(\mathfrak{T})$.
Notația $\mathfrak{T}^p$ arată că transformarea $\mathfrak{T}$ s-a efectuat de p ori.
Matricea lui $\mathfrak{T}^p$ este notată T^p. Să se demonstreze că acest produs este asociativ.

5° Să se demonstreze că transformarea $\mathfrak{T}$ admite o transformare inversă $\mathfrak{T}^{-1}$ dacă și numai dacă matricea T este inversabilă, adică dacă, lui T i se poate asocia T^{-1} astfel încît:

$$T^{-1}T = TT^{-1} = U.$$

Se va demonstra că este astfel, dacă și numai dacă, $\Delta = 1$ sau $\Delta = -1$. Matricea T^{-1} este inversabilă? Dacă da, care este matricea sa inversă?

II. În această secțiune, se restrîng transformările considerate ale familiei $(\mathfrak{T})$ la acelea a căror matrice este inversabilă ($\Delta = 1$ sau $\Delta = -1$).
T se numește pară dacă $\Delta = 1$ și impară dacă $\Delta = -1$.

1° Să se demonstreze că, dacă $\mathfrak{T}$ și $\mathfrak{T}'$ aparțin acestei familii restrînse, atunci $\mathfrak{T}'' = \mathfrak{T}' \circ \mathfrak{T}$, aparține de asemenea acestei familii. Să se studieze paritatea lui T'' după parităților lui T și lui T'.

2° Se consideră mulțimea E a patru matrice U:

$$I = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \quad J = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad K = IJ.$$

Să se demonstreze că, pentru produsul matricelor, E este un grup comutativ. Se va întocmi tabela înmulțirii lui E.

III. În această secțiune, se studiază matricele T ale căror elemente a, b, c, d fiind numere întregi sînt numai pozitive sau nule, și mai mult satisfac condiția $\Delta = 1$ (matrice pare). Se pune:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ și } \bar{A} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

1° Să se studieze legea de formare a lui TA și a lui $T\bar{A}$. Să se calculeze A^p și $\bar{A}^q$.

2° Să se demonstreze că, dacă matricea T este diferită de U, se poate determina, într-un singur mod, o matrice T' astfel ca să avem una și numai una dintre următoarele, două relații:

$$T = T'A \text{ sau } T = T'\bar{A}.$$

Să se deducă că este posibil să se descompună T într-un singur mod într-un produs finit de matrice A și $\bar{A}$.

Exemplu:

$$T = \begin{pmatrix} 377 & 70 \\ 70 & 13 \end{pmatrix}.$$

3° Fie ecuația definită pe N prin:

$$73y - 47x = 1.$$

Să se determine toate soluțiile. În acest scop, se va aplica o descompunere de tipul precedent al matricei $T = \begin{pmatrix} 73 & 47 \\ x & y \end{pmatrix}$.

4° Fie T_1 și T_2 două matrice comutabile ($T_2T_1 = T_1T_2$). Să se demonstreze, folosind o descompunere de tipul III, 2°, că există atunci o matrice T_3 astfel că, sau $T_1 = T_2T_3$, sau $T_2 = T_1T_3$. Să se demonstreze că T_1, T_2, T_3 sînt permutabile două cîte două.

IV. Printre matricele definite în secțiunea III, se consideră familia $(\mathcal{F})$ formată din cele care sînt de forma:

$$F = \begin{pmatrix} a & kc \\ c & a \end{pmatrix}, \quad \Delta = a^2 - kc^2 = 1,$$

unde k este un întreg fixat, strict pozitiv, și a și c doi întregi strict pozitivi.

Nu se cere aici să se demonstreze existența întregilor a și c care verifică relația $a^2 - kc^2 = 1$; această existență va fi admisă în cazul general și verificată mai tîrziu pe un exemplu numeric.

1° Fie T o matrice diferită de U și care verifică restricțiile din III. Să se demonstreze că T comută cu o matrice F dacă și numai dacă T aparține ea însăși familiei $(\mathcal{F})$.

Care este produsul a două matrice care aparțin familiei $(\mathcal{F})$?

Să se demonstreze că toate matricele familiei $(\mathcal{F})$ sînt de forma F_0^p, unde p este un întreg pozitiv oarecare și $F_0 = \begin{pmatrix} a_0 & kc_0 \\ c_0 & a_0 \end{pmatrix}$, unde a_0 și c_0 sînt cei mai mici întregi pozitivi care verifică $a_0^2 - kc_0^2 = 1$, acceptînd perechea banală (1,0).

2° Să se deducă din aceste proprietăți o metodă care să permită să se determine toate perechile (x, y) de întregi pozitivi, soluții ale ecuației definite pe N prin:

$$x^2 - ky^2 = 1,$$

începînd cu soluția (x_0, y_0) formată din întregii pozitivi cei mai mici posibili, exceptînd perechea banală (1, 0).

Exemplu. Să se determine prin acest procedeu alte două perechi, soluții întregi ale ecuației definite prin:

$$x^2 - 15y^2 = 1,$$

pornind de la soluția (4, 1).

4° Să se demonstreze că, în descompunerea lui F în produse de factori de tipul A și $\bar{A}$, cei echidistanți de extremi sînt identici. Să se verifice această proprietate pe exemplul:

$$F = \begin{pmatrix} 31 & 120 \\ 8 & 31 \end{pmatrix}.$$

N.B. Se spune că perechea (x, y) este mai mică decît perechea $(x' y')$ dacă:

sau:

$$x < x',$$

sau:

$$x = x' \text{ și } y < y'.$$

3.162. Fie n un întreg scris în sistem zecimal:

$$n = \overline{a_k a_{k-1} \ldots a_2 a_1 a_0}.$$

1° Să se demonstreze că resturile lui n la împărțirile prin 2 și prin 5 sînt egale cu acelea ale lui a_0.

2° Să se demonstreze că resturile lui n la împărțirile prin 3 și prin 9 sînt egale cu acelea ale lui:

$$s = a_0 + a_1 + a_2 + \ldots + a_k.$$

3° Să se demonstreze că restul lui n la împărțirea prin 11 este egal cu acela al lui:

$$t = a_0 - a_1 + a_2 - \ldots + (-1)^k a_k.$$

4° Să se deducă echivalențele următoare:

$$2 \mid n \Longleftrightarrow a_0 \in \{0,2,4,6,8\};$$

$$5 \mid n \Longleftrightarrow a_0 \in \{0,5\};$$

$$3 \mid n \Longleftrightarrow a_0 + a_1 + a_2 + \ldots + a_k \equiv 0 \quad [3];$$

$$11 \mid n \Longleftrightarrow a_0 - a_1 + a_2 - \ldots + (-1)^k a_k \equiv 0 \quad [11].$$

5° Să se dea regulile care permit să se găsească resturile lui n la împărțirile prin 4, 8, 25 și criteriile de divizibilitate prin aceste numere.

Tabela numerelor prime de la 17 la 5000.

Această tabelă permite *descompunerea unui întreg natural în divizori primari.* Fiind dat un întreg (fie, de exemplu, $n = 86020$), se caută divizorii săi primi *începînd cu cel mai mic,* Trebuie deci să efectuăm un anumit număr de tatonări împărțind prin 2, 3, 5, 7, 11 etc. pînă se obține un rest nul. Se reîncepe apoi operația asupra cîtului.
Astfel:

$$n = 86020 = 2 \times 43010, \quad 43010 = 2 \times 21505,$$

$$21505 = 5 \times 4301, \quad 4301 = 11 \times 391,$$

$$391 = 17 \times 23,$$

de unde:

$$n = 2^2 \times 5 \times 11 \times 17 \times 23.$$

Cîturile și divizorii succesivi se așază într-un tablou vertical:

86020	2
43010	2
21505	5
4301	11
391	17
23	23
1	

Tabela permite o căutare rapidă a celui mai mic divizor prim al unui întreg natural. Dacă acesta este unul din numerele 2, 3, 5 sau 11, exercițiul nr. 3.162 (pagina 190) dă imediat criteriile care permit să-l recunoască. Dacă nu e cazul, se divide atunci întregul studiat prin numărul:

$$1001 = 7 \times 11 \times 13.$$

Este atunci foarte simplu de verificat dacă întregul este divizibil prin 7 sau prin 13.
Dacă aceste încercări nu dau rezultat și dacă întregul este mai mic sau egal cu 5000, tabela conține în paranteze, cel mai mic divizor al acestui întreg (care este obligatoriu un număr prim cel puțin egal cu 17). Dacă numărul y figurează în tabelă fără nici o indicație, rezultă că este număr prim. Astfel, de exemplu:

a) 3413 este prim.

b) 3427 admite pe 23 ca cel mai mic divizor:

$$3427 = 23 \times 149;$$

149 este prim, cum se poate verifica cu ajutorul tabelei; dar aceasta nu este necesar, căci egalitatea $3427 = 23ab$ $(23 \leqslant a \leqslant b)$ ar da $149 = ab \geqslant 23^2$, ceea ce este vizibil inexact.

Pentru acelaşi motiv toate numerele care figurează în tabelă sînt prime sau produse de două numere prime (distincte sau nu) cu excepţia lui 4913 care este cubul lui 17.

17	101	211	307	401	503	601	701	809	901 (17)
19	103	223	311	409	509	607	703 (19)	811	907
23	107	227	313	419	521	613	709	817 (19)	911
29	109	229	317	421	523	617	713 (23)	821	919
31	113	233	323 (17)	431	527 (17)	619	719	823	929
37	127	239	331	433	529 (23)	629 (17)	727	827	937
41	131	241	337	437 (19)	541	631	731 (17)	829	941
43	137	251	347	439	547	641	733	839	943 (23)
47	139	257	349	443	551 (19)	643	739	841 (29)	947
53	149	263	353	449	557	647	743	851 (23)	953
59	151	269	359	457	563	653	751	853	961 (31)
61	157	271	361 (19)	461	569	659	757	857	967
67	163	277	367	463	571	661	761	859	971
71	167	281	373	467	577	667 (23)	769	863	977
73	173	283	379	479	587	673	773	877	983
79	179	289 (17)	383	487	789 (19)	677	779 (19)	881	989 (23)
83	181	293	389	491	593	683	787	883	991
89	191		391 (17)	493 (17)	599	691	797	887	997
97	193		397	499		697 (17)	799 (17)	893 (19)	
	197							899 (29)	
	199								

1 003 (*17*)	1 103	1 201	1 301	1 403 (*23*)	1 501 (*19*)	1 601	1 709	1 801	1 901
1 007 (*19*)	1 109	1 207 (*17*)	1 303	1 409	1 511	1 607	1 711 (*29*)	1 811	1 907
1 009	1 117	1 213	1 307	1 411 (*17*)	1 513 (*17*)	1 609	1 717 (*17*)	1 817 (*23*)	1 909 (*23*)
1 013	1 121 (*19*)	1 217	1 319	1 423	1 517 (*37*)	1 613	1 721	1 819 (*17*)	1 913
1 019	1 123	1 219 (*23*)	1 321	1 427	1 523	1 619	1 723	1 823	1 919 (*19*)
1 021	1 219	1 223	1 327	1 429	1 531	1 621	1 733	1 829 (*31*)	1 921 (*17*)
1 031	1 139 (*17*)	1 229	1 333 (*31*)	1 433	1 527 (*29*)	1 627	1 739 (*37*)	1 831	1 927 (*41*)
1 033	1 147 (*31*)	1 231	1 343 (*17*)	1 439	1 541 (*23*)	1 633 (*23*)	1 741	1 843 (*19*)	1 931
1 037 (*17*)	1 151	1 237	1 349 (*19*)	1 447	1 543	1 637	1 747	1 847	1 933
1 039	1 153	1 241 (*17*)	1 357 (*23*)	1 451	1 549	1 643 (*31*)	1 751 (*17*)	1 849 (*43*)	1 943 (*29*)
1 049	1 159 (*19*)	1 247 (*29*)	1 361	1 453	1 553	1 649 (*17*)	1 753	1 853 (*17*)	1 949
1 051	1 163	1 249	1 363 (*29*)	1 457 (*31*)	1 559	1 657	1 759	1 861	1 951
1 061	1 171	1 259	1 367	1 459	1 567	1 663	1 763 (*41*)	1 867	1 957 (*19*)
1 063	1 181	1 271 (*31*)	1 369 (*37*)	1 471	1 571	1 667	1 769 (*29*)	1 871	1 961 (*37*)
1 069	1 187	1 273 (*19*)	1 373	1 481	1 577 (*19*)	1 669	1 777	1 873	1 973
1 073 (*29*)	1 189 (*29*)	1 277	1 381	1 483	1 579	1 679 (*23*)	1 783	1 877	1 979
1 081 (*23*)	1 193	1 279	1 387 (*19*)	1 487	1 583	1 681 (*41*)	1 787	1 879	1 987
1 087		1 283	1 399	1 489	1 591 (*37*)	1 691 (*19*)	1 789	1 889	1 993
1 091		1 289		1 493	1 597	1 693		1 891 (*31*)	1 997
1 093		1 291		1 499		1 697			1 999
1 097		1 297				1 699			

2 003	2 111	2 201 (*31*)	2 309	2 407 (*29*)	2 501 (*41*)	2 603 (*19*)	2 701 (*37*)	2 801	2 903
2 011	2 113	2 203	2 311	2 411	2 503	2 609	2 707	2 803	2 909
2 017	2 117 (*29*)	2 207	2 323 (*23*)	2 413 (*19*)	2 507 (*23*)	2 617	2 711	2 809 (*53*)	2 911 (*41*)
2 021 (*43*)	2 129	2 209 (*47*)	2 329 (*17*)	2 417	2 521	2 621	2 713	2 813 (*29*)	2 917
2 027	2 131	2 213	2 333	2 419 (*41*)	2 531	2 623 (*43*)	2 719	2 819	2 921 (*23*)
2 029	2 137	2 221	2 339	2 423	2 533 (*17*)	2 627 (*37*)	2 729	2 831 (*19*)	2 923 (*37*)
2 033 (*19*)	2 141	2 227 (*17*)	2 341	2 437	2 537 (*43*)	2 633	2 731	2 833	2 927
2 039	2 143	2 231 (*23*)	2 347	2 441	2 539	2 641 (*19*)	2 741	2 837	2 929 (*29*)
2 047 (*23*)	2 147 (*19*)	2 237	2 351	2 447	2 543	2 647	2 747 (*41*)	2 839 (*17*)	2 939
2 053	2 153	2 239	2 357	2 449 (*31*)	2 549	2 657	2 749	2 843	2 941 (*17*)
2 059 (*29*)	2 159 (*17*)	2 243	2 363 (*17*)	2 459	2 551	2 659	2 753	2 851	2 953
2 063	2 161	2 251	2 369 (*23*)	2 461 (*23*)	2 557	2 663	2 759 (*31*)	2 857	2 957
2 069	2 173 (*41*)	2 257 (*37*)	2 371	2 467	2 567 (*17*)	2 669 (*17*)	2 767	2 861	2 963
2 071 (*19*)	2 179	2 263 (*31*)	2 377	2 473	2 573 (*31*)	2 671	2 771 (*17*)	2 867 (*47*)	2 969
2 077 (*31*)	2 188 (*37*)	2 267	2 381	2 477	2 579	2 677	2 773 (*47*)	2 869 (*19*)	2 971
2 081		2 269	2 383	2 479 (*37*)	2 581 (*29*)	2 683	2 777	2 879	2 983 (*19*)
2 083		2 273	2 389	2 489 (*19*)	2 591	2 687	2 789	2 881 (*43*)	2 987 (*29*)
2 087		2 279 (*43*)	2 393	2 491 (*47*)	2 593	2 689	2 791	2 887	2 993 (*41*)
2 089		2 281	2 399		2 599 (*23*)	2 693	2 797	2 897	2 999
2 099		2 287				2 699			
		2 291 (*29*)							
		2 293							
		2 297							

3 001	3 103 (*29*)	3 203	3 301	3 401 (*19*)	3 503 (*31*)	3 607	3 701	3 803	3 901 (*17*)
3 007 (*31*)	3 109	3 209	3 307	3 403 (*41*)	3 511	3 611 (*23*)	3 709	3 811 (*37*)	3 907
3 011	3 119	3 217	3 313	3 407	3 517	3 613	3 713 (*47*)	3 821	3 911
3 013 (*23*)	3 121	3 221	3 317 (*31*)	3 413	3 527	3 617	3 719	3 823	3 917
3 019	3 127 (*53*)	3 229	3 319	3 427 (*23*)	3 529	3 623	3 721 (*61*)	3 827 (*43*)	3 919
3 023	3 131 (*31*)	3 233 (*53*)	3 323	3 431 (*47*)	3 533	3 629 (*19*)	3 727	3 833	3 923
3 037	3 137	3 239 (*41*)	3 329	3 433	3 539	3 631	3 733	3 841 (*23*)	3 929
3 041	3 139 (*43*)	3 247 (*17*)	3 331	3 439 (*19*)	3 541	3 637	3 737 (*37*)	3 847	3 931
3 043 (*17*)	3 149 (*47*)	3 251	3 337 (*47*)	3 449	3 547	3 643	3 739	3 851	3 937 (*31*)
3 049	3 151 (*23*)	3 253	3 343	3 457	3 551 (*53*)	3 649 (*41*)	3 743 (*19*)	3 853	3 943
3 053 (*43*)	3 161 (*29*)	3 257	3 347	3 461	3 557	3 659	3 149 (*23*)	3 859 (*17*)	3 947
3 061	3 163	3 259	3 349 (*17*)	3 463	3 559	3 667 (*19*)	3 761	3 863	3 953 (*59*)
3 067	3 167	3 271	3 359	3 467	3 569 (*43*)	3 671	3 763 (*53*)	3 869 (*53*)	3 959 (*37*)
3 071 (*37*)	3 169	3 277 (*29*)	3 361	3 469	3 571	3 673	3 767	3 877	3 961 (*17*)
3 077 (*17*)	3 173 (*19*)	3 281 (*17*)	3 371	3 473 (*23*)	3 581	3 677	3 769	3 881	3967
3 079	3 181	3 287 (*19*)	3 373	3 481 (*49*)	3 583	3 683 (*29*)	3 779	3 889	3 973 (*29*)
3 083	3 187	3 293 (*37*)	3 379 (*31*)	3 491	3 587 (*17*)	3 691	3 781 (*19*)	3 893 (*17*)	3 977 (*41*)
3 089	3 191	3 299	3 383 (*17*)	3 499	3 589 (*37*)	3 697	3 791 (*17*)		3 979 (*17*)
3 097 (*19*)	3 193 (*31*)		3 389		3 593		3 793		3 989
	3 197 (*23*)		3 391		3 599 (*59*)		3 797		
			3 397 (*34*)				3 799 (*29*)		

4 001	4 111	4 201	4 307 (*59*)	4 409	4 507	4 601 (*43*)	4 703	4 801	4 903
4 003	4 117 (*23*)	4 211	4 309 (*31*)	4 421	4 513	4 603	4 709 (*17*)	4 811 (*17*)	4 909
4 007	4 127	4 217	4 313 (*19*)	4 423	4 517	4 607 (*17*)	4 717 (*53*)	4 813	4 913 (*17*)
4 009 (*19*)	4 129	4 219	4 321 (*29*)	4 427 (*19*)	4 519	4 619 (*31*)	4 721	4 817	4 919
4 013	4 133	4 223 (*41*)	4 327	4 429 (*43*)	4 523	4 621	4 723	4 819 (*61*)	4 931
4 019	4 139	4 229	4 331 (*61*)	4 439 (*23*)	4 531 (*23*)	4 633 (*41*)	4 727 (*29*)	4 831	4 933
4 021	4 141 (*41*)	4 231	4 337	4 441	4 541 (*19*)	4 637	4 729	4 841 (*47*)	4 937
4 027	4 153	4 237 (*19*)	4 339	4 447	4 547	4 639	4 733	4 843 (*29*)	4 943
4 031 (*29*)	4 157	4 241	4 343 (*43*)	4 451	4 549	4 643	4 747 (*47*)	4 847 (*37*)	4 951
4 033 (*37*)	4 159	4 243	4 349	4 453 (*61*)	4 553 (*29*)	4 649	4 751	4 853 (*23*)	4 957
4 049	4 163 (*23*)	4 247 (*31*)	4 351 (*19*)	4 457	4 559 (*47*)	4 651	4 757 (*67*)	4 859 (*43*)	4 967
4 051	4 171 (*43*)	4 253	4 357	4 463	4 561	4 657	4 759	4 861	4 969
4 057	4 177	4 259	4 363	4 469 (*41*)	4 567	4 661 (*59*)	4 769 (*19*)	4 867 (*31*)	4 973
4 061 (*31*)	4 181 (*37*)	4 261	4 369 (*17*)	4 471 (*17*)	4 573 (*17*)	4 663	4 777 (*17*)	4 871	4 981 (*17*)
4 063 (*17*)	4 183 (*47*)	4 267 (*17*)	4 373	4 481	4 577 (*23*)	4 673	4 783	4 877	4 987
4 073	4 187 (*53*)	4 271	4 379 (*29*)	4 483	4 579 (*19*)	4 679	4 787	4 883 (*19*)	4 993
4 079	4 189 (*59*)	4 273	4 387 (*41*)	4 489 (*67*)	4 583	4 681 (*31*)	4 789	4 889	4 997 (*19*)
4 087 (*61*)		4 283	4 391	4 493	4 591	4 697 (*43*)	4 793	4 891 (*67*)	4 999
4 091		4 289	4 393 (*23*)		4 597	4 691	4 799	4 897 (*59*)	
4 093		4 297	4 397			4 699 (*37*)			
4 097 (*17*)			4 399 (*53*)						
4 099									

INDEX

Tabla de materii

Nr. colilor de tipar : 12,5
Tiraj : 24.080 ex.
Bun de tipar : 17.09.1974

Combinatul Poligrafic
„CASA SCÎNTEII"
București — R.S.R.
Com. nr. 40 262/6 953