CAPITOLUL I. PRELIMINARII

1.1. Elemente de teoria mulțimilor

1. Mulțimi

Prin **mulțime** vom înțelege o colecție (set, ansamblu) de obiecte (elementele mulțimii), bine determinate şi considerate ca o entitate. Se subânțelege faptul că elementele unei aceleiaşi mulțimi sunt distincte între ele. Mai mult presupunem că se poate deduce dacă un obiect oarecare aparține sau nu colecției şi că un acelaşi obiect nu poate constitui simultan şi o colecție şi un element al acestei colecții. Spunem şi că un obiect capătă "calitatea" de element prin conştientizarea faptului că face parte dintr-o colecție (mulțime).

Vom nota mulțimile cu literele mari A, B,....., iar elementele lor cu literele mici a, b, ..., x, y,.....

A determina o mulțime înseamnă a preciza individual elementele sale sau a preciza o proprietate caracteristică (pe care o au elementele mulțimii respective şi numai acestea). Menționăm că nu orice proprietate (în sensul uzual al cuvântului) determină o mulțime însă se acceptă că orice proprietate determină o clasă (clasa obiectelor ce satisfac proprietatea respectivă). Amintim, de exemplu, că nu se poate vorbi de mulțimea tuturor mulțimilor ci de clasa tuturor mulțimilor. Restricțiile ce se impun asupra proprietăților pentru ca acestea să determine mulțimi derivă din presupunerile enunțate în primul alineat al paragrafului. În general se consideră proprietăți desdpre care să se poată spune dacă sunt sau nu îndeplinite (altă posibilitate neexistând) şi care se referă la obiecte dintr-un "univers de discurs" precizat (pentru "uivers de discrus" se poate accepta înțelesul de "totalitate a obiectelor de întreg pentru un domeniu dat", admițând că se poate vorbi de această "totalitate").

Precizăm că noțiunile şi rezultatele ce urmează pot fi date şi în cadrul claselor (uneori chiar vor fi folosite în acest context).

Dacă A este o mulțime, iar a este un element al mulțimii A, vom nota $a \in A$, iar în caz contrar notăm $a \notin A$.

Semnul "$\in$" reprezintă scrierea stilizată a primei litere din cuvântul grecesc "$\varepsilon \sigma \tau \nu$" (este) şi a fost propus de G. Peano.

Dacă A şi B sunt două mulţimi, vom scrie $A \subseteq B$ şi vom citi "A este înclus în B" dacă pentru orice $x \in A$ rezultă $x \in B$. Dacă $A \subseteq B$, atunci A mai este numită **submulţime** a lui B.

Admitem existenţa unei mulţimi care nu are nici un element, numită mulţimea **vidă**. Va fi notată $\varnothing$ (ultima litera a alfabetului danezo-norvegian).

Pentru orice mulţime A, are loc $\varnothing \subseteq A$. Spunem că mulţimile A şi B coincid şi scriem A = B dacă $A \subseteq B$ şi $B \subseteq A$.

Date mulţimile A şi B, vom nota cu $A \cap B$ mulţimea $\{x \mid x \in A \text{ şi } x \in B\}$ şi o vom numi **intersecţia** mulţimilor A şi B.

Dacă $A \cap B = \varnothing$ vom spune că A şi B sunt **disjuncte**.

Vom nota cu $A \cup B$ mulţimea $\{ x \mid x \in A \text{ sau } x \in B\}$ şi o vom numi **reuniunea** mulţimilor A şi B .

Mulţimea $\{ x \mid x \in B , x \notin A\}$ este numită **diferenţa** mulţimilor B şi A şi este notată B - A. Dacă $A \subseteq B$, atunci B - A se mai notează $\mathbf{C}_B A$ şi este numită **complementara lui A relativ la B**.

Dacă pentru un context dat se are în vedere o mulţime U (numită şi mulţimea universală) ce conţine ca submulţimi toate mulţimile în discuţie în contextul respectiv şi $A \subseteq U$, atunci $\mathbf{C}_U A$ se mai notează $\mathbf{C}A$ şi este numită, simplu, **complementara lui A**.

Pentru orice mulţimi A, B, D au loc următoarele proprietăţi:

1) $\varnothing \cap A = \varnothing$; $A \cap U = A$; $\varnothing \cup A = A$; $A \cup U = U$; $A - \varnothing = A$; $A - A = \varnothing$;
2) $A \cap B \subseteq A$; $A \cap B \subseteq B$; $A \subseteq A \cup B$; $B \subseteq A \cup B$;
3) $A \cap (A \cup B) = A = A \cup (A \cap B)$;
4) $A \cup B = B \cup A$; $A \cap B = B \cap A$;
5) $(A \cap B) \cap D = A \cap (B \cap D)$; $(A \cup B) \cup D = A \cup (B \cup D)$;
6) $A \cup A = A = A \cap A$;
7) $A \subseteq B \Rightarrow A \cup D \subseteq B \cup D$; $A \cap D \subseteq B \cap D$; $CB \subseteq CA$;
8) $A \cap (B \cup D) = (A \cap B) \cup (A \cap D)$; $A \cup (B \cap D) = (A \cup B) \cap (A \cup D)$;
9) $\mathbf{C}(A \cup B) = \mathbf{C}A \cap \mathbf{C}B$; $\mathbf{C}(A \cap B) = \mathbf{C}A \cup \mathbf{C}B$; $\mathbf{C}(\mathbf{C}A) = A$;
10) $B - A = B \cap \mathbf{C}A$.

Când elementele unei mulţimi sunt ele însele mulţimi, se foloseşte termenul de **familie** de mulţimi. O familie de mulţimi

$M = \{ M_i \mid i \in I \}$, unde M_i sunt mulțimi, iar I este o mulțime nevidă (**mulțime de indici**), mai este numită **familie indexată de mulțimi**.

Pentru o familie de mulțimi $M = \{ M_i \mid i \in I\}$ $(I \neq \varnothing)$ definim $\bigcup_{i\in I} A_i$ prin $\bigcup_{i\in I} A_i = \{x \mid$ există $i \in I$, așa încât $x \in A_i\}$ și $\bigcap_{i\in I} A_i$ prin $\bigcap_{i\in I} A_i = \{x \mid$ pentru orice $i \in I$, $x \in A_i\}$.

Au loc proprietățile:

1) $A_i \subseteq \bigcup_{i\in I} A_i$ și $\bigcap_{i\in I} A_i \subseteq A_i$ pentru orice $i \in I$;

2) $B \cap \left(\bigcup_{i\in I} A_i \right) = \bigcup_{i\in I} (B \cap A_i)$

$B \cup \left(\bigcap_{i\in I} A_i \right) = \bigcap_{i\in i} (B \cup A_i)$

3) $\mathbf{C}\left(\bigcap_{i\in I} A_i \right) = \bigcup_{i\in I} \mathbf{C}A_i$; $\mathbf{C}\left(\bigcup_{i\in I} A_i \right) = \bigcap_{i\in I} \mathbf{C}A_i$

Dacă A și B sunt mulțimi și $a \in A$, $b \in B$, atunci putem forma (în mod intuitiv) **perechea ordonată** (a,b).

Avem $(a_1, b_1) = (a_2, b_2)$ dacă $a_1 = a_2$ și $b_1 = b_2$, de unde rezultă că $(a, b) \neq (b, a)$ pentru $a \neq b$. Noțiunea de pereche ordonată pentru două elemente oarecare a, b este dată (în mod riguros) de K. Kuratowski prin $\{\{a\}, \{a, b\}\}$ și notată (a, b).

Mulțimea $\{(a, b) \mid a \in A, b \in B\}$ este notată cu $A \times B$ și este numită **produsul cartezian** al mulțimilor A și B. Pentru A = B notăm $A \times A$ cu A^2.

Inductiv, definim pentru mulțimile A_1, A_2, ..., A_n produsul cartezian $A_1 \times A_2 \times ... \times A_n = \{(a_1 ,..., a_n) \mid \forall\ i = \overline{1, n}$, $a_i \in A_i$, $\}$ iar în cazul $A_1 = A_2 = ... = A_n = A$ notăm $\underbrace{A \times A \times ... \times A}_{n \quad ori}$ cu A^n. Observăm că dacă $A \neq B$ atunci $A \times B \neq B \times A$.

Avem : $A \times \varnothing = \varnothing \times B = \varnothing$ și $(A \times B) \times D \neq A \times (B \times D)$.

Mulțimea $(A - B) \cup (B - A)$ se numește **diferența simetrică** (sau **suma booleană**) a mulțimilor A și B și se notează cu $A \Delta B$.

Pentru orice mulțimi A, B, D au loc egalitățile:

1) $(A \Delta B) \Delta D = A \Delta (B \Delta D)$;
2) $A \Delta B = B \Delta A$;
3) $A \Delta \varnothing = A$; $A \Delta A = \varnothing$;
4) $A \cap (B \Delta D) = (A \cap B) \Delta (A \cap D)$.

Fie A, B două mulțimi.

De utilitate se va dovedi şi operația de **reuniune disjunctă** (notată $\cup$) dată de $A \cup B = (\{A\} \Delta A) \cup (\{B\} \Delta B)$. Remarcăm faptul că, în cazul în care $A \cap B = \varnothing$, se poate considera că $A \cup B = A \cup B$. Operația anterioară se extinde în mod natural pentru cazul unei familii de mulțimi.

2. Relații

Definiție: Fiind date mulțimile A şi B se numeşte **relație** între A şi B, orice submulțime (notată de obicei ρ) a produsului cartezian $A \times B$[1].

Dacă A = B, atunci o submulțime $\rho \subseteq A \times A$ este numită **relație** (sau **relație binară**) pe mulțimea A.

Deseori, vom scrie a ρ b în loc de $(a, b) \in \rho$.

Domeniul relației ρ este mulțimea $\{a \in A \mid$ există $b \in B$; aşa încât a ρ b$\}$.

Codomeniul relației ρ este mulțimea $\{ b \in B \mid$ există $a \in A$, aşa încât a ρ b$\}$.

Relația $\Delta_A = \{ (a, a) \mid a \in A\}$ se numeşte **relație diagonală** pe A.

Deoarece $\varnothing \subseteq A \times B$, rezultă că $\varnothing$ reprezintă o relație între A şi B numită **relație vidă**. În mod similar, $A \times B$ este numită **relația totală** între A şi B.

Dacă $\rho \subseteq A \times B$, atunci **inversa** relației ρ, notată cu ρ^{-1} este relația $\{(b, a) \mid (a, b) \in \rho\} \subseteq B \times A$.

Dacă $A_0 \subseteq A$, submulțimea $\rho (A_0) = \{ y \in B \mid$ există $x \in A_0$, aşa încât $(x, y) \in \rho\}$ a mulțimii B, este numită **imaginea directă** a submulțimii A_0 prin relația ρ.

[1] Pentru a simplifica formulările ulterioare se va presupune că A şi B sunt nevide.

Dacă $B_0 \subseteq B$, atunci $\rho^{-1}(B_0) = \{x \in A \mid$ există $y \in B_0$, aşa încât $(x, y) \in \rho\}$ este numită **imaginea inversă** a submulţimii B_0 prin relaţia ρ.

Dacă $\rho \subseteq A \times B$ şi $\tau \subseteq B \times C$, atunci relaţia $\{(a, c) \mid$ există $b \in B$, aşa încât $(a, b) \in \rho$ şi $(b, c) \in \tau\}$ este numită **compusa** relaţiilor ρ şi τ şi se notează $\tau \circ \rho$.

În cazul în care există compunerile ce urmează, avem:
$(\rho_3 \circ \rho_2) \circ \rho_1 = \rho_3 \circ (\rho_2 \circ \rho_1)$; $\rho_1 \circ \rho_2 \neq \rho_2 \circ \rho_1$;
dacă $\rho \subseteq A \times B$, atunci $\rho \circ \Delta_A = \rho = \Delta_B \circ \rho$ şi $\Delta_B \subseteq \rho \circ \rho^{-1}$, $\Delta_A \subseteq \rho^{-1} \circ \rho$;
$(\rho \circ \tau)^{-1} = \rho^{-1} \circ \tau^{-1}$;
$\rho_1 \subseteq \rho_2 \Rightarrow \tau \circ \rho_1 \subseteq \tau \circ \rho_2$ şi $\rho_1 \circ \gamma \subseteq \rho_2 \circ \gamma$.

Definiţie: Fie $\rho \subseteq A \times A$. ρ este numită:

- **relaţie reflexivă** dacă oricare ar fi $a \in A$, avem $a \rho a$ (altfel spus $\Delta_A \subseteq \rho$);
- **relaţie simetrică** dacă pentru orice $a_1, a_2 \in A$, avem $a_1 \rho a_2 \Rightarrow a_2 \rho a_1$ (altfel spus $\rho = \rho^{-1}$);
- **relaţie antisimetrică** dacă din $a_1 \rho a_2$ şi $a_2 \rho a_1$ rezultă $a_1 = a_2$ (altfel spus $\rho \cap \rho^{-1} = \Delta_A$);
- **relaţie tranzitivă** dacă din $a_1 \rho a_2$ şi $a_2 \rho a_3$ rezultă $a_1 \rho a_3$ (altfel spus $\rho \circ \rho \subseteq \rho$).

i) Relaţia $\rho \subseteq A \times A$ se numeşte **relaţie de echivalenţă** dacă este reflexivă, simetrică şi tranzitivă.

ii) Relaţia $\rho \subseteq A \times A$ se numeşte **relaţie de preordine** dacă este reflexivă şi tranzitivă.

iii) O relaţie de preordine, care este în plus şi antisimetrică se numeşte **relaţie de ordine**.

iv) O relaţie de ordine ρ pe A care satisface condiţia: oricare ar fi $a,b \in A$ avem $a \rho b$ sau $b \rho a$ se numeşte **relaţie de ordine totală** pe A.

Prin **mulţime ordonată** se înţelege o mulţime nevidă A, împreună cu o relaţie de ordine pe A.

Prin **mulţime total ordonată (lanţ)** se înţelege o mulţime nevidă A, împreună cu o relaţie de ordine totală pe A.

Fie $(A, \leq)$ o mulțime ordonată şi $A_0 \subseteq A$. Elementul $a \in A$ se numeşte **minorant (majorant)** pentru A_0 dacă pentru orice $x \in A_0$, avem $a \leq x$ ($x \leq a$).

Elementul $a \in A$ se numeşte **margine inferioară (superioară)** a lui A_0 şi este notat inf A_0 (sup A_0) dacă a este minorant (majorant) pentru A_0 şi pentru orice $a' \in A$ minorant (majorant) pentru A_0 avem $a' \leq a$ ($a \leq a'$). Dacă există, inf A_0 şi sup A_0, atunci aceste elemente sunt unic determinate de condițiile din definiție.

Un element $a_0 \in A_0$ se numeşte **element inițial (element final)** în A_0 dacă pentru orice $x \in A_0$, avem $a_0 \leq x$ ($x \leq a_0$).

Dacă a_0 este element inițial (final) atunci $a_0 = \inf A_0$ (sup A_0).

Un element $a_0 \in A_0$ se numeşte element minimal (element maximal) în A_0 dacă din $x \leq a_0$ ($a_0 \leq x$) şi $x \in A_0$ rezultă $x = a_0$.

Un element inițial (final) este şi element minimal (maximal), dar nu şi invers. În plus, nu este asigurată unicitatea elementului minimal (maximal).

Definiție: O mulțime ordonată este numită **mulțime inductiv ordonată** dacă orice lanț al ei admite majorant.

Lema lui Zorn: O mulțime inductiv ordonată are cel puțin un element maximal.

Definiție: O mulțime ordonată se numeşte **mulțime bine ordonată** dacă orice submulțime nevidă a sa, admite element inițial.

Mulțimea numerelor naturale **N** este bine ordonată, în schimb mulțimile **Z, Q, R,** împreună cu relația uzuală de ordine, nu sunt bine ordonate. Se acceptă că $\varnothing$ este bine ordonată.

Vom arăta în capitolul următor că principiul inducției matematice este echivalent cu faptul că **N** este bine ordonată.

Principiul inducției transfinite

Fie $(A, \leq)$ o mulțime bine ordonată şi $A_0 \subseteq A$.

Dacă:

i) A_0 conține elementul inițial al lui A;

ii) pentru orice $\{ x \in A \mid x < a \} \subseteq A_0$ avem $a \in A_0$,

atunci $A_0 = A$.

Menționăm faptul că dacă $(A, \leq)$ este total ordonată şi unica submulțime A_0 a lui A, care satisface i) şi ii) este A, atunci $(A, \leq)$ este bine ordonată.

Teorema Zermelo: Pe orice mulțime nevidă A se poate introduce o relație de ordine "≤" așa încât (A, ≤) să fie bine ordonată.

În continuare cnsiderăm ρ o relație de echivalență pe A şi a ∈ A.

Definiție: i) Se numeşte **clasă de echivalență** a elementului "a modulo ρ" mulțimea {x ∈ A | x ρ a} (notată $\hat{a}$ sau ρ_a).

ii) Mulțimea claselor de echivalență modulo ρ, notată cu A/ρ poartă numele de **mulțimea factor** a lui A relativ la ρ (reamintim că dacă a, b ∈ A, a ≠ b, dar $\hat{a} = \hat{b}$, atunci în A | ρ vom avea doar $\hat{a}$ (sau $\hat{b}$)).

Definiție: Familia de submulțimi $\{A_i\}_{i\in I}$ ale unei mulțimi nevide A se numeşte **partiție** a lui A dacă au loc următoarele proprietăți:

1) ∀ i ∈ I, $A_i \neq \varnothing$;
2) pentru orice i, j ∈ I cu i ≠ j, avem $A_i \cap A_j = \varnothing$;
3) $\bigcup_{i\in I} A_i = A$.

Remarcăm faptul că A/ρ conduce la o partiție a mulțimii A.

Reciproc, dată o partiție $\{A_i\}_{i\in I}$ a mulțimii A, relația definită astfel:

x ρ y dacă ∃ i ∈ I, aşa încât x, y ∈ A_i

este o relație de echivalență.

Observație: Dacă A este o mulțime înzestrată cu o relație de preordine "≤", atunci relația definită astfel: a ~ b dacă a ≤ b şi b ≤ a este o relație de echivalență pe A, iar pe mulțimea factor A/~ relația $\hat{x} \leq \hat{y} \Leftrightarrow x \leq y$ este o relație de ordine.

3. Funcții

Definiție: O relație ρ ∈ A × B este numită **funcție** dacă sunt îndeplinite următoarele două condiții:

1) ∀ a ∈ A, ∃ b ∈ B, aşa încât (a, b) ∈ ρ;
2) (a, b_1) ∈ ρ şi (a, b_2) ∈ ρ ⇒ $b_1 = b_2$.

A poartă numele de **domeniul** de definiție al funcției f, iar B poartă numele de **codomeniul** funcției f.

Vom spune că două funcţii f şi g **coincid** dacă au acelaşi domeniu de definiţie A, acelaşi codomeniu B şi $\forall$ x $\in$ A, avem f(x) = g(x).

Notaţia consacrată pentru o funcţie f cu domeniul de definiţie A şi codomeniul B este: f : A $\to$ B.

Mulţimea funcţiilor f : A $\to$ B va fi notată B^A.

Fie f : A $\to$ B, A' $\subseteq$ A şi B' $\subseteq$ B.

f(A') = {f(x) | x $\in$ A'} este numită **imaginea directă a submulţimii A'** prin funcţia f, iar $f^{-1}(B') = \{x \in A \mid f(x) \in B'\}$ este numită **imaginea inversă a submulţimii B'** prin funcţia f.

Se arată că $f(f^{-1}(B')) \subseteq B'$ şi $A' \subseteq f^{-1}(f(A'))$ de unde obţinem că $f(f^{-1}(f(A'))) = f(A')$ şi $f^{-1}(f(f^{-1}(B'))) = f^{-1}(B')$.

Au loc proprietăţile: pentru orice familie de submulţimi ale lui A, $\{A_i\}_{i\in I}$, şi pentru orice familie de submulţimi ale lui B, $\{B_i\}_{i\in I}$, avem:

i) $$f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i); \quad f^{-1}\left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I} f^{-1}(B_i);$$

ii) $$f\left(\bigcap_{i\in I} A_i\right) \subseteq \bigcap_{i\in I} f(A_i); \quad f^{-1}\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} f^{-1}(B_i).$$

Definiţie: Fie f : A $\to$ B, g : B $\to$ C. Funcţia g $\circ$ f : A $\to$ C, $\forall$ x $\in$ A, (g $\circ$ f) (x) = g (f (x)) este numită **compusa** funcţiilor g şi f.

Se remarcă faptul că, dacă f : A $\to$ B, g : B $\to$ C şi h : C $\to$ D atunci: h $\circ$ (g $\circ$ f) = (h $\circ$ g) $\circ$ f.

Definiţie: Fie f : A $\to$ B o funcţie.

i) f este numită funcţie **injectivă** dacă:

$\forall$ $x_1, x_2 \in A$, $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ (sau, echivalent $\forall$ $x_1, x_2 \in A$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$).

ii) f este numită funcţie **surjectivă** dacă $\forall$ b $\in$ B, $\forall$ a $\in$ A, aşa încât f (a) = b.

iii) f este numită funcţie **bijectivă** dacă este injectivă şi surjectivă.

Observaţie: Fie f : A $\to$ B, g : B $\to$ C

i) Dacă f şi g sunt injective (surjective), atunci g $\circ$ f este injectivă (surjectivă);

ii) Dacă g $\circ$ f este injectivă (surjectivă), atunci f este injectivă (g este surjectivă).

Definiție: Funcția $h : B \to A$ se numeşte **inversa** funcției $f : A \to B$ dacă $h \circ f = 1_A$ şi $f \circ h = 1_B$.

Inversa funcției f, dacă există, se notează cu f^{-1}. În acest caz, funcția f se numeşte funcție **inversabilă**. Reamintim faptul că o funcție este inversabilă dacă şi numai dacă este bijectivă.

Notăm cu $\mathcal{P}(A)$ mulțimea submulțimilor (părților) lui A. Fiind dată funcția $f : A \to B$, definim funcțiile:

$F^{\wedge} : \mathcal{P}(A) \to \mathcal{P}(B)$, $F^{\wedge}(A') = f(A')$ şi

$F^{-} : \mathcal{P}(B) \to \mathcal{P}(A)$, $F^{-}(B') = f^{-1}(B')$.

$F^{\wedge}$ este numită **funcție imagine directă,** iar F^{-} este numită **funcție imagine inversă**.

Propunem ca exercițiu demonstrarea următoarelor propoziții:

Propoziție: Fie $f : A \to B$ o funcție. Următoarele afirmații sunt echivalente:

i) f este injectivă;

ii) $\forall X_1, X_2 \in \mathcal{P}(A)$, $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$;

iii) $\forall X \in \mathcal{P}(A)$, $f^{-1}(f(X)) = X$;

iv) $\exists r : B \to A$, aşa încât $r \circ f = 1_A$ (r se numeşte **retractă** a lui f şi nu este, în general, unică);

v) $\forall A' \subseteq A$, $f(A - A') \subseteq B - f(A')$;

vi) $F^{\wedge}$ este injectivă;

vii) $F^{\vee}$ este surjectivă;

viii) $F^{\wedge} \circ F^{\vee} = 1_{\mathcal{P}(A)}$.

Propoziție: Fie $f : A \to B$ o funcție. Următoarele afirmații sunt echivalente:

i) f este surjectivă;

ii) $\forall Y \subseteq B$, $f(f^{-1}(Y)) = Y$

iii) $\exists s : B \to A$, aşa încât $f \circ s = 1_B$ (s se numeşte **secțiune** pentru f şi, nu este, în general, unică);

iv) $F^{\wedge}$ este surjectivă;

v) $F^{\vee}$ este injectivă;

vi) $\forall A' \subseteq A$, $B - f(A') \subseteq f(A - A')$;

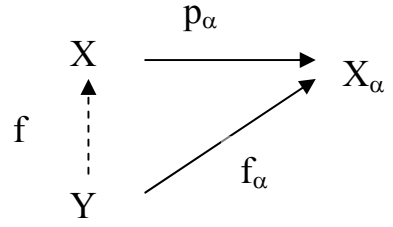
vii) $F^{\wedge} \circ F^{\vee} = 1_{\mathcal{P}(B)}$.

În final, ca exercițiu, se propune să se demonstreze că între mulțimile $(B\times C)^A$ şi $B^A \times C^A$ şi între mulțimile $A^{B\times C}$ şi $(A^B)^C$ există bijecții.

4. Produse directe. Sume directe.

Fie $(X_\alpha)_{\alpha\in I}$ o familie de mulțimi nevide, $I \neq \emptyset$.

Definiție: Perechea $(X, (p_\alpha)_{\alpha\in I})$, unde $X \neq \emptyset$ şi $p_\alpha : X \to X_\alpha$, $\alpha\in I$, se numeşte **produs direct** pentru familia $(X_\alpha)_{\alpha\in I}$ dacă pentru orice mulțime nevidă Y şi pentru orice familie de funcții $(f_\alpha)_{\alpha\in I}$, unde $\forall\ \alpha\in I$, $f_\alpha : Y \to X_\alpha$, există o funcție f, unică, $f : Y \to X$, aşa încât următoarea diagramă să fie comutativă:



adică $p_\alpha \circ f = f_\alpha$, $\forall\ \alpha \in I$

Teoremă: Oricare ar fi $(X_\alpha)_{\alpha\in I}$ unde $I \neq \emptyset$ şi $\forall\ \alpha \in I$, $X_\alpha \neq \emptyset$ există şi este unic, până la o bijecție, produsul direct al familiei date.

Demonstrație: Notăm cu $\prod_{\alpha\in I} X_\alpha$ mulțimea

$$\left\{\varphi \,\middle|\, \varphi : I \to \bigcup_{\alpha\in I} X_\alpha, \varphi(\beta) \in X_\beta, \forall \beta \in I\right\}$$

Pentru orice $\beta\in I$, definim aplicația $p_{X_\beta} : \prod_{\alpha\in I} X_\alpha \to X_\beta$ prin $p_{X_\beta}(\varphi) = \varphi(\beta)$. Este evident că aplicațiile p_{X_β} sunt surjective.

Perechea $\left(\prod_{\alpha\in I} X_\alpha, (p_{X_\alpha})_{\alpha\in I}\right)$ este produs direct pentru familia $(X_\alpha)_{\alpha\in I}$.

Într-adevăr, dacă $(f_\alpha)_{\alpha\in I}$ este o familie de funcții, cu $f_\alpha : Y \to X_\alpha$, atunci definim funcția $f : Y \to \prod_{\alpha\in I} X_\alpha$ astfel:

f (y) = φ, unde $p_{X_\alpha}(\varphi) = f_\alpha(y)$, pentru $\forall\ \alpha \in I$.

Un astfel de φ există, datorită surjectivității lui p_{X_α}. În plus, f este bine definită.

În adevăr, dacă ar exista φ' ∈ $\prod_{\alpha\in I} X_\alpha$, aşa încât $\forall\ \alpha \in I$, $p_{X_\alpha}(\varphi) = p_{X_\alpha}(\varphi') = f_\alpha(y)$ atunci $\forall\ \alpha \in I$, φ(α) = φ'(α), adică φ = φ'.

Mai mult, $(p_{X_\alpha} \circ f)(y) = p_{X_\alpha}(f(y)) = p_{X_\alpha}(\varphi) = f_\alpha(y)$, pentru $\forall$ y∈Y, adică $p_{X_\alpha} \circ f = f_\alpha$.

Să verificăm acum unicitatea produsului direct. Presupunem că perechea $(X', (p'_\alpha)_{\alpha\in I})$ satisface condițiile pentru a fi produs direct pentru familia $(X_\alpha)_{\alpha\in I}$.

Atunci, din faptul că $\left(\prod_{\alpha\in I} X_\alpha, (p_{X_\alpha})_{\alpha\in I}\right)$ este produs direct rezultă că există o unică funcție f : X' → $\prod_{\alpha\in I} X_\alpha$ astfel încât $p_{X_\alpha} \circ f = p'_\alpha$, pentru orice α∈I şi există o unică funcție h : $\prod_{\alpha\in I} X_\alpha \to \prod_{\alpha\in I} X_\alpha$, încât $p_{X_\alpha} \circ h = p_{X_\alpha}, \forall \alpha \in I$.

Pe de altă parte, folosind faptul că $(X', (p'_\alpha)_{\alpha\in I})$ este produs direct rezultă că există o unică funcție g : $\prod_{\alpha\in I} X_\alpha \to X'$, astfel încât $p'_\alpha \circ g = p_{X_\alpha}$, pentru $\forall\ \alpha \in I$ şi există o unică funcție k:X'→ $\prod_{\alpha\in I} X_\alpha$, încât $p'_\alpha \circ k = p'_\alpha, \forall \alpha \in I$.

Avem $p'_\alpha \circ (g \circ f) = p_{X_\alpha} \circ f = p'_\alpha$ şi $p'_\alpha \circ 1_{X'} = p'_\alpha$ şi din unicitatea lui k rezultă că $g \circ f = 1_{X'} = k$.

Pe de altă parte, $p_\alpha \circ (f \circ g) = p'_\alpha \circ g = p_{X_\alpha}$ şi $p_{X_\alpha} \circ 1_{\prod_{\alpha\in I} X_\alpha} = p_{X_\alpha}$ şi din unicitatea lui h rezultă că $f \circ g = 1_{\prod_{\alpha\in I} X_\alpha} = h$. Aşadar, f şi g sunt inverse una alteia, deci sunt bijecții.

Mulțimea $\prod_{\alpha\in I} X_\alpha$ este numită **produs cartezian generalizat**, iar aplicațiile p_{X_α} sunt numite proiecții canonice.

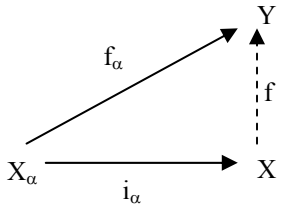
Observație: Dacă I = {1, 2, ..., n} atunci produsul direct se identifică cu produsul cartezian uzual, familia $\{p_{X_1}, p_{X_2}, ..., p_{X_n}\}$ fiind familia de **proiecții canonice**:

$$\forall j \in \{1,2,...,n\},\ p_{X_j} : \prod_{i=1}^{n} X_i \to X_j,\ p_{X_j}(x_1, x_2, ..., x_j, ..., x_n) = x_j$$

Definiție: Fie X o mulțime, $(X_\alpha)_{\alpha\in I}$ o familie nevidă de mulțimi nevide şi $(i_\alpha)_{\alpha\in I}$ o familie de funcții $i_\alpha : X_\alpha \to X$.

Perechea $(X, (i_\alpha)_{\alpha\in I})$ se numeşte **sumă directă** pentru familia $(X_\alpha)_{\alpha\in I}$ dacă pentru orice mulțime Y şi pentru orice familie de funcții $(f_\alpha)_{\alpha\in I}$, unde $f_\alpha : X_\alpha \to Y$, există şi este unică funcția $f : X \to Y$, astfel încât $f \circ i_\alpha = f_\alpha$, $\forall \alpha \in I$.

Altfel spus, diagrama



este comutativă, $\forall\ \alpha \in I$

Teoremă: Orice familie de mulțimi admite suma directă şi aceasta este unică până la o bijecție.

Demonstrație: Presupunem întâi că toate mulțimile din familia dată sunt disjuncte două câte două. Atunci suma directă este perechea $(X, (i_\alpha)_{\alpha\in I})$, unde $X = \bigcup_{\alpha\in I} X_\alpha$ şi pentru $\forall \alpha \in I$, $i_\alpha : X_\alpha \to \bigcup_{\alpha\in I} X_\alpha$ este incluziunea.

Într-adevăr, dacă Y este o mulțime oarecare şi $(f_\alpha)_{\alpha\in I}$ este o familie de funcții, astfel încât $\forall \alpha \in I$, $f_\alpha : X_\alpha \to Y$, atunci există $f : \bigcup_{\alpha\in I} X_\alpha \to Y$, unde $\forall \alpha \in I$, $\forall\ x \in X_\alpha$, $f(x) = f_\alpha(x)$. f este bine definită, pentru că $\forall \alpha, \beta \in I, \alpha \neq \beta \Rightarrow X_\alpha \cap X_\beta = \varnothing$. În plus, $f \circ i_\alpha = f_\alpha$.

Pentru demonstrarea unicității funcției f, considerăm o altă funcție g : X → Y, pentru care $g \circ i_\alpha = f_\alpha$, $\forall \alpha \in I$. Avem:

$\forall \alpha \in I$, $\forall\, x \in X_\alpha$, $g(x) = g(i_\alpha(x)) = f_\alpha = f(x)$, de unde f = g.

În cazul în care mulțimile din familia $(X_\alpha)_{\alpha \in I}$ nu sunt disjuncte, vom construi o altă familie de mulțimi disjuncte $\left(\overline{X_\alpha}\right)_{\alpha \in I}$, astfel: $\forall \alpha \in I$, $\overline{X_\alpha} = X_\alpha \times \{\alpha\}$.

Observăm că dacă $\alpha, \beta \in I$ și $\alpha \neq \beta$, atunci $\overline{X_\alpha} \cap \overline{X_\beta} = \varnothing$. Considerăm $\overline{X} = \bigcup_{\alpha \in I} \overline{X_\alpha}$ și notăm $\overline{X} = \coprod_{\alpha \in I} X_\alpha$; pentru orice $\alpha \in I$, considerăm $i_\alpha : X_\alpha \to \coprod_{\alpha \in I} X_\alpha$, $i_\alpha(x) = (x, \alpha)$, unde $x \in X_\alpha$. Rezultă că $(\coprod_{\alpha \in I} X_\alpha, (i_\alpha)_{\alpha \in I})$ este suma directă pentru familia $(X_\alpha)_{\alpha \in I}$.

Într-adevăr, dacă Y este o mulțime oarecare, $(f_\alpha)_{\alpha \in I}$ o familie de funcții astfel încât $\forall\ \alpha \in I$, $f_\alpha : X_\alpha \to Y$, atunci considerăm funcția $f : \coprod_{\alpha \in I} X_\alpha \to Y$, unde $\forall\ (x,\alpha) \in \overline{X_\alpha}$, $f((x,\alpha)) = f_\alpha(x)$.

Avem $(f \circ i_\alpha)(x) = f((x,\alpha)) = f_\alpha(x)$, pentru orice $x \in X_\alpha$, deci $f \circ i_\alpha = f_\alpha$, $\forall\ \alpha \in I$.

În plus, funcția f e unică, pentru că dacă g ar fi o altă funcție ce ar satisface condițiile $g : \coprod_{\alpha \in I} X_\alpha \to Y$, $g \circ i_\alpha = f_\alpha$, $\forall\ \alpha \in I$, atunci

$\forall \alpha \in I$, $\forall (x,\alpha) \in \overline{X_\alpha}$, $g((x,\alpha)) = (g \circ i_\alpha)(x) = f_\alpha(x) = f((x,\alpha))$, adică f = g.

Să arătăm acum unicitatea până la o bijecție a sumei directe. Presupunem că $(X, (i_\alpha)_{\alpha \in I})$ și $(X', (i'_\alpha)_{\alpha \in I})$ ar fi sume directe pentru familia $(X_\alpha)_{\alpha \in I}$.

Considerând în definiția sumei directe Y = X' și $\forall \alpha \in I$, $f_\alpha = i'_\alpha$ rezultă că există și este unică funcția $f : X \to X'$, astfel încât $\forall \alpha \in I$, $f \circ i_\alpha = i'_\alpha$.

Aplicăm acum definiția pentru suma directă $(X', (i'_\alpha)_{\alpha \in I})$, Y = X și $\forall \alpha \in I$, $f_\alpha = i_\alpha$. Rezultă că există și este unică funcția $g : X' \to X$, astfel încât $\forall \alpha \in I$, $g \circ i'_\alpha = i_\alpha$.

Vom arăta că $f \circ g = 1_{X'}$.

Într-adevăr, considerând suma directă $(X', (i'_\alpha)_{\alpha\in I})$ şi $Y = X'$, $\forall\alpha\in I$, $f_\alpha = i'_\alpha$ rezultă că există şi este unică funcţia $h : X' \to X'$ astfel încât $\forall\alpha\in I$, $h \circ i'_\alpha = i'_\alpha$.

Funcţiile $f \circ g$ şi $1_{X'}$ verifică condiţiile satisfăcute de h şi din unicitatea lui h rezultă că $f \circ g = 1_{X'}$.

Similar, considerând suma directă $(X, (i_\alpha)_{\alpha\in I})$ şi $Y = X$, $\forall\alpha\in I$, $f_\alpha = i_\alpha$ rezultă că $g \circ f = 1_{X'}$.

Prin urmare, f este bijectivă, de aceea vom spune că suma directă este unică până la o bijecţie.

5. Axioma alegerii

În cadrul teoriei mulţimilor un rol deosebit de important (şi în anumită măsură controversat) este avut de aşa numita axiomă a alegerii (a permite "abstragerea" elementelor din mulţimile ce le conţin).

Axioma alegerii: Pentru orice familie nevidă, F, de mulţimi nevide, disjuncte două câte două, există o mulţime A care are în comun cu fiecare mulţime din F un element şi numai unul.

O familie F de mulţimi este numită familie de **caracter (local) finit** dacă satisface condiţia: "$A \in F$ dacă şi numai dacă orice parte finită a lui A aparţine lui F ".

Se dovedeşte că axioma alegerii este echivalentă cu fiecare dintre următoarele propoziţii:

- **Lema lui Tukey:** Orice familie nevidă de mulţimi, de caracter finit (parţial ordonată relativ la incluziune), are cel puţin un element maximal.
- **Principiul de maximalitate al lui Hausdorff:** Orice lanţ al unei mulţimi parţial ordonate este inclus într-un lanţ maximal.
- **Teorema produsului cartezian:** Produsul cartezian al unei familii de mulţimi nevide este nevid.

precum şi cu Lema Zorn şi Teorema Zermelo prezentate anterior.

1.2. Numere cardinale. Numere ordinale.

1. Numere cardinale.

Definiție: Fie X, Y două mulțimi. Spunem că X, Y sunt **echipotente** (cardinal echivalente, au aceeaşi putere cardinală) dacă există o bijecție $f : X \to Y$.

Vom nota $X \sim Y$.

Observație: Echipotența este o relație de echivalența pe clasa tuturor mulțimilor.

Teorema lui Cantor: Dacă X este o mulțime, atunci $X \not\sim \mathsf{P}(X)$, unde $\mathsf{P}(X)$ este mulțimea părților lui X.

Demonstrație: Presupunem că $X \sim \mathsf{P}(X)$ şi atunci există o bijecție $\varphi : X \to \mathsf{P}(X)$.

Considerăm mulțimea: $A = \{x \mid x \in X \text{ şi } x \notin \varphi(x)\}$.

Evident $A \in \mathsf{P}(X)$ şi cum φ este surjecție, rezultă că $\exists\, a \in X$, aşa încât $\varphi(a) = A$.

Dacă $a \in A$, atunci $a \in \varphi(a)$; dar din definiția mulțimii A rezultă că $a \notin \varphi(a)$, contradicție.

Dacă $a \notin A$, adică $a \notin \varphi(a)$, atunci conform definiției mulțimii A ar rezulta că $a \in A$, contradicție.

Prin urmare, presupunerea făcută este falsă, deci $X \not\sim \mathsf{P}(X)$.

Teorema lui Cantor-Bernstein:

Fie X_0, X_1, X_2 trei mulțimi, astfel încât $X_0 \supseteq X_1 \supseteq X_2$.
Dacă $X_0 \sim X_2$, atunci $X_0 \sim X_1$.

Demonstrație:

Din $X_0 \sim X_2$ rezultă că există o bijecție $\varphi : X_0 \to X_2$.

Construim şirul de mulțimi:

$X_3 = \varphi(X_1), X_4 = \varphi(X_2), \ldots, X_{n+2} = \varphi(X_n)\ldots$

Avem $X_0 \supseteq X_1 \supseteq X_2 \supseteq X_3 \supseteq X_4 \supseteq \ldots \supseteq X_n \supseteq X_{n+1} \supseteq \ldots$

Notăm: $Y = \bigcap_{n \in \mathbf{N}^*} X_n = \bigcap_{n \in \mathbf{N}^*} X_n$

Să arătăm că:

(a) $X_0 = \bigcup_{i \in \mathbf{N}^*} (X_i - X_{i+1}) \cup Y$ şi că

(b) $X_1 = \bigcup_{i \in \mathbf{N}^*} (X_i - X_{i+1}) \cup Y$

Pentru egalitatea (a), considerăm $x \in X_0$: dacă $x \in Y$, atunci $x \in \bigcup_{i \in \mathbf{N}} (X_i - X_{i+1}) \cup Y$; dacă $x \notin Y$, atunci există $i \in \mathbf{N}$, aşa încât $x \notin X_i$.

Cum $x \in X_0$, rezultă că $i \geq 1$.

Fie n cel mai mic număr natural pentru care $x \notin X_n$. Din minimalitatea lui n rezultă că $x \in X_{n-1}$ şi deci $x \in X_{n-1} - X_n$, de unde $x \in \bigcup_{i \in \mathbf{N}} (X_i - X_{i+1}) \cup Y$.

În concluzie, $X_0 \subseteq \bigcup_{i \in \mathbf{N}} (X_i - X_{i+1}) \cup Y$.

Cum incluziunea inversă este evidentă, rezultă egalitatea (a).

Analog se arată şi egalitatea (b).

În continuare, considerăm familiile de mulțimi $(A_i)_{i \in \mathbf{N}}$ şi $(B_i)_{i \in \mathbf{N}}$, definite astfel:

$A_0 = Y$ şi $A_i = X_{i-1} - X_i$, pentru $i \geq 1$

$B_0 = Y$ şi $B_i = \begin{cases} X_{i+1} - X_{i+2} & pentru\ i\ impar \\ X_{i-1} - X_i, & pentru\ i\ par \end{cases}$

Să observăm că dacă $i \neq j$, atunci $A_i \cap A_j = \varnothing$ şi $B_i \cap B_j = \varnothing$.

Definim familia de aplicații $(f_i)_{i \in \mathbf{N}}$, $f_i : A_i \to B_i$ în felul următor:

$f_0 = 1_Y$;

$f_i = \begin{cases} 1_{X_{i-1} - X_i}, pentru\ \ i \quad par; \\ \varphi\big/_{X_{i-1} - X_i}, pentru\ \ i \quad impar. \end{cases}$

Aplicațiile f_i sunt bijective: pentru i par este evident, iar pentru i impar, avem: din φ injectivă rezultă că $f_i = \varphi\big/_{X_{i-1} - X_i}$ este injectivă.

Fie acum $y \in X_{i+1} - X_{i+2}$, adică $y \in X_{i+1}$ şi $y \notin X_{i+2}$ şi cum $X_{i+1} = \varphi(X_{i-1})$ rezultă că $\exists\, x \in X_{i-1}$ astfel încât $y = \varphi(x)$.

Deoarece $y \notin X_{i+2}$ rezultă că $x \notin X_i$ şi deci $x \in X_{i-1} - X_i$. Prin urmare, $y = f_i(x)$, adică f_i este şi surjectivă.

Aşadar funcțiile f_i sunt bijective, iar $X_0 = \coprod_{i \in \mathbf{N}} A_i$ şi $X_1 = \coprod_{i \in \mathbf{N}} B_i$, deci există o bijecție $f : X_0 \to X_1$, adică $X_0 \sim X_1$.

Consecință: Dacă X şi Y sunt două mulțimi aşa încât X ~ Y', unde Y'⊆Y şi Y ~ X', unde X' ⊆ X, atunci X ~ Y.

Demonstrație: În adevăr, din X ~ Y' rezultă că ∃ f : X → Y', f bijecție. Dacă Y" = f (X') atunci X' ~ Y" şi cum Y ~ X' rezultă Y"~Y. Se obține Y" ⊆ Y' ⊆ Y şi Y ~ Y".

Din teorema precedentă rezultă Y ~ Y' şi deci Y ~ X.

Definiție: Fie X o mulțime. Clasa $\overline{\overline{X}} = \{Y \mid Y \sim X\}$ este numită **numărul cardinal** al acestei mulțimi. Vom arăta ulterior că se obține clasa (nu mulțimea) numerelor cardinale.

Notăm

$\overline{\overline{\varnothing}} = 0, \overline{\overline{\{\varnothing\}}} = 1, \overline{\overline{\{\varnothing, \{\varnothing\}\}}} = 2, \ldots\ldots; \quad N = \{0,1,2,\ldots\ldots\}, \overline{\overline{N}} = \aleph_0$ (vom avea $N = \mathbf{N}$).

2. Operații cu numere cardinale

Fie $(m_\alpha)_{\alpha \in I}$ o familie (mulțime) de numere cardinale $m_\alpha = \overline{\overline{X_\alpha}}$, ($I \neq \varnothing$). Vom numi **suma** familiei $(m_\alpha)_{\alpha \in I}$ numărul $\overline{\overline{\coprod_{\alpha \in I} X_\alpha}}$ (notat cu $\sum_{\alpha \in I} m_\alpha$).

Dacă I= {1, 2, 3, ..., n} vom scrie $\sum_{\alpha=1}^{n} m_\alpha = m_1 + \ldots. + m_n$.

În cele ce urmează vom arăta că rezultatul nu depinde de reprezentanți. Pentru I = {1,2}, fie m_1, m_2 două numere cardinale şi A, $A_1 \in m_1$; B, $B_1 \in m_2$. Avem A ~ A_1 şi B ~ B_1. Putem presupune fără a restrânge generalitatea, că $A \cap B = \varnothing$ şi $A_1 \cap B_1 = \varnothing$.

Într-adevăr, dacă am avea $A \cap B \neq \varnothing$, atunci putem construi mulțimile A' = {(a, x) | a ∈ A}, B' = {(b, y) | b ∈ B}, unde x şi y sunt două elemente diferite. Avem A' ~ A, B'~ B şi, în plus, $A' \cap B' = \varnothing$.

Vom arăta că $A \cup B \sim A_1 \cup B_1$.

Considerăm bijecțiile $f_1 : A \to A_1$ şi $f_2 : B \to B_1$ şi definim funcția $f : A \cup B \to A_1 \cup B_1$ prin $f(x) = \begin{cases} f_1(x), & pentru \quad x \in A \\ f_2(x), & pentru \quad x \in B \end{cases}$

Funcția f astfel definită este o bijecție.

Folosind proprietățile sumei directe, se poate trece la cazul general.

Teoremă: Fie $(m_\alpha)_{\alpha \in I}$ şi $(n_\beta)_{\beta \in J,}$ ($I \neq \varnothing$, $J \neq \varnothing$) două familii de numere cardinale (indexate după I şi respectiv J). Dacă există o bijecție $\varphi : I \to J$, aşa încât $\forall\ \alpha \in I$, $m_\alpha = n_{\varphi(\alpha)}$, atunci $\sum_{\alpha \in I} m_\alpha = \sum_{\beta \in J} n_\beta$.

Demonstrație: Fie $A_\alpha \in m_\alpha$ şi $B_\beta \in n_\beta$, aşa încât familiile $(A_\alpha)_{\alpha \in I}$ şi $(B_\beta)_{\beta \in J}$ sunt formate din mulțimi disjuncte două câte două.

Avem $\sum_{\alpha \in I} m_\alpha = \overline{\overline{\coprod_{\alpha \in I} A_\alpha}}$ şi $\sum_{\beta \in J} n_\beta = \overline{\overline{\coprod_{\beta \in J} B_\beta}}$.

Din ipoteză rezultă că $\coprod_{\alpha \in I} A_\alpha$ şi $\coprod_{\beta \in J} B_\beta$ sunt echipotente ($\forall \alpha \in I$, există $\varphi_\alpha : A_\alpha \to B_{\varphi(\alpha)}$ bijecție, fapt ce conduce la o bijecție $\Psi : \coprod_{\alpha \in I} A_\alpha \to \coprod_{\beta \in J} B_\beta$, $\Psi(x) = \varphi_\alpha(x)$, dacă $x \in A_\alpha$) şi deci numerele cardinale corespunzătoare sunt egale.

Consecință: Dacă $(m_\alpha)_{\alpha \in I}$ este o familie de numere cardinale şi $\varphi : I \to I$ este o bijecție (permutare a mulțimii I), atunci: $\sum_{\alpha \in I} m_\alpha = \sum_{\alpha \in I} m_{\varphi(\alpha)}$. Altfel spus, adunarea numerelor cardinale este comutativă.

Teorema (de asociativitate): Fie $(m_\alpha)_{\alpha \in I}$ ($I \neq \varnothing$) o familie de numere cardinale şi presupunem că $I = \bigcup_{\lambda \in \Lambda} I_\lambda$ cu $I_\lambda \cap I_{\lambda'} = \varnothing$, pentru orice $\lambda \neq \lambda'$.

Atunci : $\sum_{\alpha \in I} m_\alpha = \sum_{\lambda \in \Lambda} \left(\sum_{\alpha \in I_\lambda} m_\alpha \right)$.

Demonstrație: Fie $(A_\alpha)_{\alpha \in I}$ o familie de reprezentanți disjuncți pentru $(m_\alpha)_{\alpha \in I}$.

Atunci avem: $\coprod_{\alpha\in I} A_\alpha = \coprod_{\lambda\in\Lambda}\left(\coprod_{\alpha\in I_\lambda} A_\alpha\right)$.

Prin urmare şi cardinalele lor sunt egale.

Dacă avem familia de numere cardinale $(m_\alpha)_{\alpha\in I}$, pentru care $\forall\ \alpha\in I$, $m_\alpha = m$, iar $I \sim \{1, 2, ..., n\}$, atunci $\sum_{\alpha\in I} m_\alpha$ nu depinde de alegerea mulțimii I şi, în plus, putem scrie: $\sum_{\alpha\in I} m_\alpha = \underbrace{m+m+.....+m}_{n\ ori}$

Definiție: Fie $(m_\alpha)_{\alpha\in I}$, $(I\neq\varnothing)$ o familie de numere cardinale şi $(X_\alpha)_{\alpha\in I}$ o familie de mulțimi aşa încât:

$$\forall \alpha \in I, m_\alpha = \overline{\overline{X_\alpha}}.$$

Vom numi **produsul** familiei $(m_\alpha)_{\alpha\in I}$ numărul cardinal $\overline{\overline{\prod_{\alpha\in I} X_\alpha}}$, notat $\prod_{\alpha\in I} m_\alpha$.

Dacă I = {1, 2, ..., n}, scriem $\prod_{\alpha\in I} m_\alpha = m_1 \cdot m_2 \cdot ... \cdot m_n$.

Teoremă: Dacă $\forall \alpha \in I, m_\alpha = \overline{\overline{X_\alpha}}$ şi $X_\alpha \sim X'_\alpha$, atunci $\overline{\overline{\prod_{\alpha\in I} X_\alpha}} = \overline{\overline{\prod_{\alpha\in I} X'_\alpha}}$ (adică $\prod_{\alpha\in I} m_\alpha$ nu depinde de alegerea reprezentanților).

Demonstrație: Raționamentul pentru cazul general urmează aceeaşi linie de demonstrație ca în cazul I = {1, 2}, de aceea vom considera doar această situație.

Fie $X_1, Y_1 \in m_1$ şi $X_2, Y_2 \in m_2$. Atunci $X_1 \times X_2 \sim Y_1 \times Y_2$.

Într-adevăr, din $X_1 \sim Y_1$ şi $X_2 \sim Y_2$ rezultă că există bijecțiile $\varphi_1: X_1 \to Y_1$ şi $\varphi_2 : X_2 \to Y_2$.

Definim $F : X_1 \times X_2 \to Y_1 \times Y_2$ prin $F(x_1,x_2) = (\varphi_1(x_1), \varphi_2(x_2))$.

F este bijectivă, deci $\overline{\overline{X_1 \times X_2}} = \overline{\overline{Y_1 \times Y_2}}$.

Demonstrațiile următoarelor teoreme sunt asemănătoare cu cele de la sumă.

Teoremă: Fie $(m_\alpha)_{\alpha\in I}$ şi $(n_\beta)_{\beta\in J}$, ($I \neq \varnothing$, $J \neq \varnothing$) două familii de numere cardinale. Presupunem că există bijecția $\varphi : I \to J$, aşa încât $m_\alpha = n_{\varphi(\alpha)}$, $\forall \alpha \in I$. Atunci

$$\prod_{\alpha\in I} m_\alpha = \prod_{\beta\in J} n_\beta .$$

Teoremă (de comutativitate): Dacă $(m_\alpha)_{\alpha\in I}$ este o familie de numere cardinale şi $\varphi: I \to I$ este o bijecție (permutare), atunci

$$\prod_{\alpha\in I} m_\alpha = \prod_{\alpha\in I} m_{\varphi(\alpha)} .$$

Teoremă (de asociativitate): Fie $(m_\alpha)_{\alpha\in I}$ o familie de numere cardinale, $I \neq \varnothing$ şi $I = \bigcup_{\lambda\in\Lambda} I_\lambda$ cu $I_\lambda \cap I_{\lambda'} = \varnothing$ pentru $\lambda \neq \lambda'$. Atunci

$$\prod_{\alpha\in I} m_\alpha = \prod_{\lambda\in\Lambda}\left(\prod_{\alpha\in I_\lambda} m_\alpha\right) .$$

În cazul în care $I \sim \{1, 2, ..., n\}$ şi $(m_\alpha)_{\alpha\in I}$ este aşa încât $m_\alpha = m$, pentru orice $\alpha \in I$, rezultă imediat că $\prod_{\alpha\in I} m_\alpha$ nu depinde de alegerea mulțimii I şi convenim să scriem:

$$\prod_{\alpha\in I} m_\alpha = \underbrace{m \cdot m \cdot \ldots \cdot m}_{n\ ori}$$

Propunem ca exercițiu demonstrația următoarei teoreme:

Teoremă (de distributivitate): Fie $(m_\alpha)_{\alpha\in I}$ şi $(n_\beta)_{\beta\in J}$ (I, J nevide) două familii de numere cardinale. Atunci

$$\left(\sum_{\alpha\in I} m_\alpha\right)\cdot\left(\sum_{\beta\in J} n_\beta\right) = \sum_{(\alpha,\beta)\in I\times J} m_\alpha \cdot n_\beta .$$

Are loc şi următoarea legătură între produs şi sumă.

Teoremă: Fie m şi n două numere cardinale.

$$m \cdot n = \underbrace{m + m + \ldots\ldots + m}_{n\ ori} = \underbrace{n + n + \ldots\ldots + n}_{m\ ori}$$

Atunci

Demonstrație: Fie $m = \overline{\overline{X}}$ şi $n = \overline{\overline{Y}}$. Atunci $m \cdot n = \overline{\overline{X \times Y}}$. Pe de altă parte,

$$X \times Y = \bigcup_{y\in Y} X \times \{y\} = \bigcup_{x\times X} \{x\} \times Y .$$

Familiile $\{X \times \{y\}\}_{y \in Y}$ şi $\{\{x\} \times Y\}_{x \in X}$ sunt formate din mulţimi disjuncte două câte două, deoarece avem: dacă y, y'∈Y şi y ≠ y', atunci (X × {y})∩(X × ×{y'}) = ∅ şi analog, dacă x, x'∈X şi x ≠ x', atunci ({x} × Y)∩({x'} × Y) = =∅.

Deci, $\overline{\overline{X \times Y}} = \sum_{y \in Y} \overline{\overline{X \times \{y\}}} = \sum_{x \in X} \overline{\overline{\{x\} \times Y}}$.

Dar, ∀y∈Y, avem X ~ X × {y} şi ∀x∈X, avem Y ~ {x} × Y, deoarece $\varphi_1: X \to X \times \{y\}$, $\varphi_1(x) = (x,y)$ şi $\varphi_2: Y \to \{x\} \times Y$, $\varphi_2(y) = (x, y)$ sunt bijecţii şi deci $\overline{\overline{X \times \{y\}}} = m$ şi $\overline{\overline{\{x\} \times Y}} = n$, de unde obţinem egalităţile dorite.

Dacă $m = \overline{\overline{X}}$ şi $n = \overline{\overline{Y}}$, atunci vom nota $n^m = \overline{\overline{Y^X}}$.

3. Relaţii de ordine pe mulţimea numerelor cardinale

Definiţie: Fie $m = \overline{\overline{X}}$ şi $n = \overline{\overline{Y}}$. Vom spune că m ≤ n dacă există o submulţime Y'⊆Y astfel încât X ~ Y'.

Dacă m ≤ n şi m ≠ n, atunci se notează m < n (în caz contrar m ɜ n).

Observaţie: Relaţia "≤" definită mai sus nu depinde de reprezentanţi.

Demonstraţie: Fie X ~ A şi Y ~ B şi X ~ Y', unde Y'⊆Y. Atunci există o bijecţie f:Y→B. Notăm B' = f(Y'). Deoarece f este injectivă rezultă că B' ~ Y'; dar Y' ~ X şi deci B' ~ X şi cum X ~ A, obţinem B' ~ A, ceea ce ne arată că relaţia "≤" definită anterior nu depinde de reprezentanţi.

Teoremă: Au loc următoarele proprietăţi:

a) pentru orice număr cardinal m, avem m ≤ m, dar m ɜ m;

b) dacă m şi n sunt numere cardinale, astfel încât m ≤ n şi n ≤ m, atunci n = m;

c) dacă m, n şi p sunt numere cardinale, astfel încât m ≤ n şi n ≤ p, atunci m ≤ p;

c') dacă m, n şi p sunt numere cardinale, astfel încât m < n şi n < p, atunci m < p.

Demonstrație: a) Fie $m = \overline{\overline{X}}$ şi atunci avem X $\subset$X şi X ~ X, deci m ≤ m. Dacă am avea m < m, atunci ar trebui ca m ≠ m, ceea ce este fals.

b) Fie m şi n numere cardinale, încât m ≤ n şi n ≤ m şi fie $m = \overline{\overline{X}}$ şi $n = \overline{\overline{Y}}$. Atunci există Y' $\subset$Y, încât X ~ Y' şi există X' $\subseteq$ X, încât Y ~ X', de unde rezultă că există funcția bijectivă f : X $\rightarrow$ Y'. Notăm Y" = f(X') şi cum f este bijectivă, rezultă Y" ~ X'. Dar X' ~ Y, deci Y" ~ Y.

Din Y" $\subseteq$Y' $\subseteq$Y şi Y" ~ Y rezultă, conform teoremei lui Cantor-Bernstein, că Y' ~ Y şi cum Y' ~ X, se obține X ~ Y, de unde $\overline{\overline{X}} = \overline{\overline{Y}}$, adică m = n.

c) Fie m, n, p numere cardinale, încât m ≤ n şi n ≤ p. Fie $m = \overline{\overline{X}}$, $n = \overline{\overline{Y}}$ şi $p = \overline{\overline{Z}}$. Există Y' $\subseteq$ Y şi Z' $\subseteq$ Z, aşa încât X ~ Y' şi Y ~ Z', deci există bijecția f : Y $\rightarrow$ Z'. Notăm Z" = f (Y').

Atunci Y' ~ Z" şi cum X ~ Y' rezultă X ~ Z", unde Z" $\subseteq$ Z' $\subseteq$ Z, deci $m = \overline{\overline{X}} \le p = \overline{\overline{Z}}$.

c') Conform cu c), avem m ≤ p. Să mai arătăm că m ≠ p, adică X ? Z, unde $m = \overline{\overline{X}}$ şi $p = \overline{\overline{Z}}$. Dacă am presupune X ~ Z, atunci am avea Y' ~ Z, unde Y' $\subseteq$ Y, aşa încât X~Y'. Aceasta ar însemna că $p = \overline{\overline{Z}} \le n = \overline{\overline{Y}}$; dar din ipoteză n ≤ p şi atunci conform cu b) avem n = p, ceea ce contrazice n < p. Aşadar, X ? Z, adică m ≠ p. Deci m < p.

Aşadar, pe mulțimea numerelor cardinale relația "≤" este o relație de ordine (parțială).

Teoremă: Fie familiile de numere cardinale $(m_\alpha)_{\alpha\in I}$; $(n_\alpha)_{\alpha\in I}$ şi $m_\alpha \le n_\alpha$, $\forall\alpha\in$I, (I≠∅). Atunci $\sum_{\alpha\in I} m_\alpha \le \sum_{\alpha\in I} n_\alpha$ şi $\prod_{\alpha\in I} m_\alpha \le \prod_{\alpha\in I} n_\alpha$.

Demonstrație: Fie $m_\alpha = \overline{\overline{X_\alpha}}$ şi $n_\alpha = \overline{\overline{Y_\alpha}}$, $\forall\alpha\in$I. Din ipoteză, există $Y'_\alpha \subseteq Y_\alpha$, astfel încât $X_\alpha \sim Y'_\alpha$.De aici rezultă că:

$$\coprod_{\alpha\in I} X_\alpha \sim \coprod_{\alpha\in I} Y'_\alpha \text{ şi } \prod_{\alpha\in I} X_\alpha \sim \prod_{\alpha\in I} Y'_\alpha$$

Cum $\coprod_{\alpha\in I} Y'_\alpha \subseteq \coprod_{\alpha\in I} Y_\alpha$ şi $\prod_{\alpha\in I} Y'_\alpha \subseteq \prod_{\alpha\in I} Y_\alpha$, rezultă inegalităţile din enunţ.

Teoremă: Dacă X este o mulţime, atunci $\mathsf{P}(X) \sim \{0,1\}^X$.

Demonstraţie: Definim $\varphi : \{0,1\}^X \to \mathsf{P}(X)$ prin $\varphi(f) = f^{-1}(\{1\})$, unde $f : X \to \{0,1\}$. Se verifică cu uşurinţă faptul că φ este o bijecţie.

Consecinţă: Pentru orice mulţime X, avem $\overline{\overline{X}} < 2^{\overline{\overline{X}}}$ (reamintim că 2 notează $\overline{\overline{\{\varnothing, \{\varnothing\}\}}}$ şi că $\{0,1\} \in 2$)

Demonstraţie: Notăm $X' = \{\{x\} \mid x \in X\}$. Avem $X' \subseteq \mathsf{P}(X)$ şi $X \sim X'$, de unde $\overline{\overline{X}} \le \overline{\overline{\mathsf{P}(X)}}$. Pe de altă parte, din teorema lui Cantor $X \not\sim \mathsf{P}(X)$, deci $\overline{\overline{X}} \ne \overline{\overline{\mathsf{P}(X)}}$. Aşadar, $\overline{\overline{X}} < \overline{\overline{\mathsf{P}(X)}} = \overline{\overline{\{0,1\}^X}} = 2^{\overline{\overline{X}}}$.

Pentru orice număr cardinal n, se obţine şirul $n < 2^n < 2^{2^n} < .....$

În particular, se obţine şirul $\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < .....$

Notăm $c = 2^{\aleph_0}$ şi vom numi c **puterea continuului.**

Teoremă: Dacă M este o mulţime de numere cardinale, atunci există un număr cardinal strict mai mare decât orice cardinal din M.

Demonstraţie: Fie $m_0 = \sum_{m\in M} m$. Evident că $\forall m \in M$, $m \le m_0$. Avem $m_0 < 2^{m_0}$ şi deci $m < 2^{m_0}, \forall m \in M$.

Observaţie: Presupunând că ar exista mulţimea K a tuturor numerelor cardinale, conform teoremei precedente ar exista un număr cardinal m, strict mai mare decât orice cardinal din K. Cum $m \in K$ rezultă că $m < m$, contradicţie. Aşadar, nu există mulţimea numerelor cardinale, ci **clasa numerelor cardinale**.

4. Mulţimi numărabile

Definiţie: Se spune că o mulţime X este **numărabilă,** dacă $X \sim \mathbf{N}$, adică $\overline{\overline{X}} = \aleph_0$.

Teoremă: Reuniunea a două mulţimi numărabile este o mulţime numărabilă.

Demonstrație: Fie X, Y două mulțimi numărabile şi presupunem, mai mult, că $X \cap Y = \varnothing$. Din ipoteză, $\exists\ \Psi : \mathbf{N} \to X$, $\exists\ \Psi : \mathbf{N} \to Y$ funcții bijective. Definim $\eta: \mathbf{N} \to X \cup Y$ prin

$$\eta(n) = \begin{cases} \varphi\left(\frac{n}{2}\right), & \text{dacă n par} \\ \Psi\left(\frac{n+1}{2}\right), & \text{dacă n impar} \end{cases}$$

η este injectivă. Într-adevăr, dacă $\eta(n) = \eta(n')$, atunci din $X \cap Y = \varnothing$ urmează că n şi n' au aceeaşi paritate, deci $\varphi\left(\frac{n}{2}\right) = \varphi\left(\frac{n'}{2}\right)$ sau $\Psi\left(\frac{n+1}{2}\right) = \Psi\left(\frac{n'+1}{2}\right)$, ceea ce conduce la n = n', în ambele cazuri.
Pe de altă parte, dacă $x \in X \cup Y$, adică $x \in X$ sau $x \in Y$, atunci avem:
dacă $x \in X$ rezultă că $\exists\ k \in \mathbf{N}$, aşa că $\varphi(k) = x$ şi deci $\eta(2k) = x$;
dacă $x \in Y$ rezultă că $\exists\ l \in \mathbf{N}$, aşa că $\varphi(l) = x$ şi deci $\eta(2l-1) = x$.
Prin urmare, η este şi surjectivă. Deci, η este bijecție, de unde $\overline{\overline{X \cup Y}} = \aleph_0$.

Teoremă: Fie $(X_i)_{i \in \mathbf{N}}$ o familie de mulțimi, aşa încât pentru $i, j \in \mathbf{N}$, $i \neq j$ să avem $X_i \cap X_j = \varnothing$. Dacă pentru orice $i \in \mathbf{N}$, X_i este numărabilă, atunci $\bigcup_{i \in \mathbf{N}} X_i$ este numărabilă.

Demonstrație: Folosind metoda inducției matematice se arată că pentru orice $n \in \mathbf{N}$, există numerele naturale k şi j unice, astfel încât

1) $k \geq 0, \quad 1 \leq j \leq k+1$ şi

2) $n = \frac{k(k+1)}{2} + j$.

Notăm $\alpha(n) = k$ şi $\beta(n) = j$.
Pe de altă parte, din faptul că $\forall i \in \mathbf{N}$, X_i este numărabilă rezultă că există bijecția $f_i : \mathbf{N} \to X_i$.
Definim aplicația $f : \mathbf{N} \to \bigcup_{i \in \mathbf{N}} X_i$ prin $f(n) = f_{\alpha(n)-\beta(n)+2}(\beta(n))$.

Să verificăm faptul că f este bijectivă. Pentru verificarea injectivității, vom considera n şi n' numere naturale, aşa încât f(n) = f(n'). Atunci $f_{\alpha(n)-\beta(n)+2}(\beta(n)) = f_{\alpha(n')-\beta(n')+2}(\beta(n'))$.
Deoarece familia $\{X_i\}_{i \in \mathbf{N}}$ conține mulțimi disjuncte două câte două, rezultă că $\alpha(n)-\beta(n)+2 = \alpha(n')-\beta(n')+2$. Pe de altă parte, $f_{\alpha(n)-\beta(n)+2}$ este bijecție, deci vom obține $\beta(n)=\beta(n')$ şi atunci folosind egalitatea anterioară rezultă $\alpha(n) = \alpha(n')$.
Din $\beta(n)=\beta(n')$ şi $\alpha(n) = \alpha(n')$ rezultă că n = n', adică f este injectivă.
Pentru a verifica surjectivitatea, vom considera x un element arbitrar din $\bigcup_{i\in\mathbf{N}} X_i$; deci există $i\in\mathbf{N}$, i unic (datorită faptului că $\{X_i\}_{i \in \mathbf{N}}$ conține mulțimi disjuncte), astfel ca $x\in X_i$.
Cum f_i este surjectivă, rezultă că există $m\in\mathbf{N}$, astfel încât $x = f_i(m)$.
Fie $\beta(n) = m$ şi $\alpha(n)-\beta(n)+2 = i$. Atunci $\alpha(n) = i + m - 2$ şi deci $n = \frac{(i+m-2)(i+m-1)}{2} + m$, de unde $f(n) = f_i(m) = x$, adică f este surjectivă. În concluzie, $\bigcup_{i\in\mathbf{N}} X_i \sim \mathbf{N}$, adică $\bigcup_{i\in\mathbf{N}} X_i$ este numărabilă.

Teoremă: Fie $(X_\alpha)_{\alpha\in I}$ o familie de mulțimi numărabile şi I o mulțime numărabilă. Atunci $\coprod_{\alpha\in I} X_\alpha$ este numărabilă.

Demonstrație: Dacă $(X_\alpha)_{\alpha\in I}$ conține numai mulțimi disjuncte două câte două, atunci rezultatul este imediat. În caz contrar putem construi familia de mulțimi disjuncte $\left(\overline{X_\alpha}\right)_{\alpha\in I}$, unde $\forall\alpha\in I$, $\overline{X_\alpha} = (X_\alpha, \alpha)$. Remarcăm că $\forall \alpha \in I, X_\alpha \sim \overline{X_\alpha}$, deci problema se reduce la familii numărabile de mulțimi numărabile şi disjuncte.

Consecință: Dacă X şi Y sunt mulțimi numărabile, atunci mulțimea $X\times Y$ este numărabilă.

Demonstrație: Aşa cum am văzut,
$X \times Y = \bigcup_{y\in Y} X \times \{y\} \sim \coprod_{y\in Y} X \times \{y\}$. Dar, $X\times\{y\}\sim X$, pentru orice $y\in Y$, deci $X\times Y$ este numărabilă, conform teoremei anterioare.
Din cele de mai sus rezultă:

Teoremă: 1) $\pm_0 + \pm_0 = \pm_0$;

2) $\underbrace{\aleph_0 + \aleph_0 + ... + \aleph_0}_{\aleph_0 ori} = \aleph_0^2 = \aleph_0$;

3) $c^2 = c$;

4) $c^{\aleph_0} = c$;

5) $c + c = c$;

6) $\aleph_0^{\aleph_0} = c$;

7) $\aleph_0 c = c$.

Demonstrație:

1) Evident;

2) Rezultă din teorema precedentă;

3) Avem $c^2 = c \cdot c = 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0} = c$;

4) Avem $c^{\aleph_0} = \left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = c$;

5) Arătăm, mai întâi că dacă $2 \le m$, atunci $m + m \le m \cdot m$.

Fie $m = \overline{\overline{X}}$. Din $2 \le m$ rezultă că $\exists\ x_0, y_0 \in X$, $x_0 \ne y_0$ şi $\varphi : X \times \{1\} \cup X \times \{2\} \to X \times X$, aşa încât $\varphi(x,1) = (x,y_0)$ şi $\varphi(x,2) = (x_0,x)$. Se verifică uşor că aplicația φ este injectivă, de unde rezultă că $m + m = \overline{\overline{X \times \{1\} \cup X \times \{2\}}} \le \overline{\overline{X \times X}} = m \cdot m$.

Din $2 < c$ şi din inegalitatea precedentă rezultă $c + c \le c^2$. Dar $c \le c + c$ şi din 3) rezultă că $c^2 = c$; se obține $c \le c + c \le c^2 = c$, deci $c+c=c$.

6) Din $2 < \aleph_0 < 2^{\aleph_0} = c$ obținem $2^{\aleph_0} \le \aleph_0^{\aleph_0} \le c^{\aleph_0}$ şi deci, conform cu 4), rezultă $c \le \aleph_0^{\aleph_0} \le c$, adică $\aleph_0^{\aleph_0} = c$.

7) Din $2 < \pm_0 < c$ deducem $c = 2 \cdot c \le \pm_0 c \le c^2 = c$ de unde $\pm_0 c = c$.

5. Mulțimi infinite. Mulțimi finite

Definiția 1 (Dedekind): O mulțime X este **infinită** dacă $\exists\ X' \subseteq X$, $X' \ne X$, astfel încât $X \sim X'$.

Definiția 2 (Cantor): O mulțime X este **infinită** dacă conține o submulțime numărabilă.

Observație: Condițiile din definițiile anterioare sunt echivalente.

Demonstrație: "$D_1 \Rightarrow D_2$"

Fie X o mulțime infinită conform definiției lui Dedekind. Atunci $\exists$ X' $\subseteq$ X, X' $\neq$ X, X'~ X. Notăm cu f : X $\rightarrow$ X' bijecția corespunzătoare. Cum X' $\neq$ X rezultă că există $x_1 \in X$ încât $x_1 \notin X'$.

Construim inductiv şirul de elemente:

$x_2 = f(x_1)$, $x_3 = f(x_2)$, ... , $x_{n+1} = f(x_n)$, ...

Funcția φ : **N** $\rightarrow$ X definită prin $\varphi(n) = x_n$ este injectivă. Vom verifica aceasta prin inducție după n.

Dacă n = 1, atunci pentru orice n' $\neq$ 1 avem $\varphi(1) = x_1$ şi $\varphi(n') = f(x_{n'-1}) \in X'$. Cum $x_1 \notin X'$ rezultă că $\varphi(1) \neq \varphi(n')$.

Presupunem acum că pentru orice n'$\neq$ n rezultă $\varphi(n') \neq \varphi(n)$ şi fie n', aşa încât n' $\neq$ n+1.

Dacă n' = 1, atunci $\varphi(n') = x_1 \notin X'$ şi $\varphi(n+1) = f(x_n) \in X'$, deci $\varphi(n') \neq \varphi(n+1)$.

Dacă n' $\neq$ 1, atunci $\varphi(n') = f(x_{n'-1})$, iar $\varphi(n+1) = f(x_n)$.

Din n'-1 $\neq$ n rezultă conform ipotezei inductive că $\varphi(n'-1) \neq \varphi(n)$ adică $x_{n'-1} \neq x_n$ şi cum f este injectivă, se obține $f(x_{n'-1}) \neq f(x_n)$, de unde $\varphi(n') \neq \varphi(n+1)$.

Deci φ este injectivă şi atunci $\varphi(\mathbf{N}) \sim \mathbf{N}$, adică X conține submulțimea numărabilă φ (**N**).

"$D_2 \Rightarrow D_1$"

Fie X o mulțime infinită, conform definiției lui Cantor. Rezultă că X conține o submulțime numărabilă A, deci există bijecția f : **N** $\rightarrow$ A.

Să considerăm aplicația:

φ : X $\rightarrow$ X – {f(1)} definită prin:

$$\varphi(x) = \begin{cases} x, & \text{dacă } x \notin A \\ f(n+1), & \text{dacă } x = f(n) \in A \end{cases}$$

Vom arăta că φ este bijectivă.

Pentru a verifica injectivitatea, considerăm x, x' $\in$ X aşa încât $\varphi(x) = \varphi(x')$. Din X = A $\cup$ (X - A) şi $\varphi(x) = \varphi(x')$ rezultă că x, x' $\in$ A sau x, x' $\notin$ A.

Dacă x, x' $\in$ A, atunci din $\varphi(x) = \varphi(x')$ rezultă $\varphi(x) = f(k+1)$, unde x = f(k) şi $\varphi(x') = f(l+1)$, unde x' = f(l). Din injectivitatea funcției f rezultă că avem k = l şi deci x = x'.

Aşadar aplicația φ este injectivă.

Să dovedim că φ este surjectivă.

Fie $y \in X - \{f(1)\}$. Dacă $y \in A$, atunci $\exists\, n \in \mathbf{N}$, încât $y = f(n)$. Cum $y \neq f(1)$, atunci $n \neq 1$ şi deci putem scrie $y = f(n-1+1) = \varphi(x)$, unde $x = f(n-1)$.

Dacă $y \notin A$, atunci $y = \varphi(y)$.

Deci, φ este şi surjectivă.

Prin urmare φ este bijectivă, deci $\exists\, X' = X - \{f(1)\} \subset X$, $X' \neq X$ şi $X \sim X'$, ceea ce înseamnă că X este infinită şi conform definiţiei lui Dedekind.

O mulţime ce nu este infinită, va fi numită **mulţime finită** .

Definiţie: Cardinalul unei mulţimi infinite se numeşte **cardinal transfinit,** iar cardinalul unei mulţimi finite se numeşte **cardinal finit.**

Numerele cardinale $\aleph_0$, c sunt transfinite.

Observaţie: Definiţia D_2 şi teorema de echivalenţă a celor două definiţii arată că $m \leq \aleph_0$, pentru orice cardinal finit m.

În contextul anterior apare următoarea problemă:

Există oare numere cardinale cuprinse între a şi 2^a ?

Ipoteza alefilor (a lui Cantor) afirmă că nu există astfel de numere.

În particular, pentru că $a = \aleph_0$ se obţine **ipoteza continuului:** între $\aleph_0$ şi $2^{\aleph_0} = c$ nu mai există alte numere cardinale.

6. Numere ordinale

Fie U_0 clasa ("universul") mulţimilor total ordonate.

Definiţie: Două mulţimi total ordonate $(A, \leq)$ şi $(B, \leq)$ se numesc **asemenea** şi scriem $A \approx B$ dacă există o bijecţie $f : A \to B$ (numită şi asemănare) cu proprietatea:

$\forall\, x, y \in A,\ x \leq y \Rightarrow f(x) \leq f(y)$.

După cum este uzual s-au notat cu acelaşi simbol "$\leq$" relaţiile de ordine date pe A şi pe B.

Observaţie: Relaţia "$\approx$" este o relaţie de echivalenţă pe U_0.

Clasa de echivalenţă, în raport cu relaţia "$\approx$", a unei mulţimi total ordonate $(A, \leq)$ se notează prin ord A şi se numeşte **tipul de ordine** al lui A.

Tipurile de ordine ale mulţimilor bine ordonate se numesc **numere ordinale.**

Dacă (A, ≤) este bine ordonată, atunci orice element (B, ≤) din ord A va fi o mulțime bine ordonată.

Vom nota 0 = ord ∅.

Dacă n este un număr natural, mulțimea $\{ x \in \mathbf{N} \mid x < n\}$, în raport cu ordinea uzuală, este bine ordonată şi vom nota tot cu n numărul său ordinal.

Pentru mulțimile **N, Q** şi **R** ordonate cu ordinea uzuală, notăm ord **N** = w, ord **Q** = η, ord **R** = λ.

w este număr ordinal, dar η şi λ sunt doar tipuri de ordine.

Aritmetica tipurilor de ordine este complicată, deoarece operațiile de adunare şi de înmulțire nu sunt comutative.

Vom defini însă o relație de ordine parțială notată "$\preccurlyeq$" astfel: dacă (A, ≤) şi (B, ≤) sunt două mulțimi bine ordonate şi α = ord A, β = ord B, vom pune $\alpha \prec \beta$ dacă $\exists$ B' $\subseteq$ B cu proprietatea A ≈ B'.

Notăm $\alpha \preccurlyeq \beta$ dacă $\alpha \prec \beta$ sau α = β.

Se verifică uşor că $\alpha \preccurlyeq \beta$ depinde doar de numerele ordinale α şi β şi nu depinde de reprezentanții (A, ≤) şi (B, ≤).

Următoarele teoreme sunt utile în aplicații:

Teoremă: Dacă (A, ≤) este o mulțime bine ordonată şi f:A→ A este o asemănare, atunci x ≤ f(x), ∀ x ∈ A.

Demonstrație: Presupunem prin reducere la absurd, că ar exista $x_0 \in A$, aşa încât $f(x_0) < x_0$. Fie a cel mai mic element x_0 cu această proprietate. Avem f(a) < a şi cum f este o asemănare, rezultă f(f(a)) < <f(a), adică f(a) = b este un element cu proprietatea f(b) < b.
Dar f(a) = b < a ceea ce contrazice minimalitatea elementului a. Aşadar, ∀ x ∈ A, x ≤ f(x).

Teoremă: Dacă (A, ≤) este mulțime bine ordonată, atunci A nu este asemenea cu nici o submulțime de forma $A_a = \{x \in A \mid x<a\}$ (A_a este numită **segment** al lui A).

Demonstrație: Presupunem că există o asemănare f : A → A_a, unde a ∈ A. Conform demonstrației teoremei anterioare, rezultă că a ≤ f(a).

Dar f(a) ∈ A_a şi atunci conform definiției lui A_a avem f(a) < a, contradicție.

În baza axiomei alegerii, putem demonstra că relația de ordine "$\preccurlyeq$" este o ordine totală, astfel:

Teoremă: Pentru orice două numere ordinale α şi β are loc una şi numai una dintre situațiile: $\alpha \prec \beta$, $\alpha = \beta$, $\beta \prec \alpha$.

Demonstrație: Conform teoremei precedente, rezultă că cel mult una dintre aceste situații are loc.

Fie ord A = α, ord B = β, unde (A, $\leq$) şi (B, $\leq$) sunt bine ordonate. Considerăm familia tuturor asemănărilor de la A sau de la segmentele lui A la B, respectiv, segmentele lui B.

Notăm cu F acestă familie. Dacă a este primul element al lui A şi b este primul element al lui B, atunci f : {a} $\rightarrow$ {b} pe care o notăm (a, b) este o asemănare, deci $\mathsf{F} \neq \varnothing$.

Conform principiului de maximalitate al lui Hausdorff (echivalent cu axioma alegerii), exisă un lanț maximal $\mathsf{L} \subset \mathsf{F}$.

Fie h = $\cup \mathsf{L}$. Se arată cu uşurința că h $\in \mathsf{F}$.

Dacă domeniul lui h, dom h, este segmentul A_x al lui A, iar codomeniul, codom h, este segmentul B_y al lui B atunci h $\cup$ {(x, y)} poate fi adăugată lui L, contrazicând astfel maximalitatea lui L.

Putem avea, atunci, situațiile:

1. dom h = A şi codom h = B, caz în care rezultă $\alpha = \beta$;
2. dom h = A şi codom h = B_y, unde y $\in$ B, caz în care rezultă $\alpha \prec \beta$;
3. dom h = A_x, unde x $\in$ A şi codom h = B, caz în care rezultă $\beta \prec \alpha$.

Observație: Dacă (A, $\leq$) este o mulțime bine ordonată, iar dacă x, y sunt două elemente arbitrare ale lui A, atunci are loc implicația:

$A_x \approx A_y \Rightarrow x = y$.

Într-adevăr, dacă am presupune că ar exista x, y $\in$ A, aşa încât $x \neq y$ şi $A_x \approx A_y$, atunci putem presupune, fără a restrânge generalitatea, că $x < y$ şi atunci A_y ar fi asemenea cu un segment al său A_x, ceea ce este exclus.

Deci, pentru $\forall$ x, y $\in$ A, aşa încât $A_x \approx A_y$, avem x = y.

Fie Z mulțimea numerelor ordinale.

Teoremă: Pentru orice număr ordinal a, avem ord Z_a = a.

Demonstrație: Fie A o mulțime bine ordonată cu ord A = a. Vom arăta că Z_a şi A sunt asemenea. Fie $x \in Z_a$, adică $x \prec a$. Conform definiției relației "$\prec$" rezultă că există $A' \subseteq A$, $A' \neq A$, aşa încât, dacă B este o mulțime bine ordonată, pentru care ord B = x, atunci $B \approx A'$. Mai mult din faptul că A este bine ordonată rezultă că există y în A, y fiind prim element al submulțimii A – A'. Rezultă de aici că A' coincide cu segmentul A_y a lui A, deci $B \approx A_y$.

Considerăm funcția f : $Z_a \to A$, f(x) = y.

f este bine definită, conform observației anterioare.

Se verifică uşor faptul că f este bijecție.

Mai mult, f păstrează ordinea. Într-adevăr, dacă x, x' $\in Z_a$, $x \prec x'$ şi dacă x = ord B, x' = ord B', atunci există segmentul B'_z al lui B', aşa încât $B \approx B'_z$.

Dar $B \approx A_y$ şi $B' \approx A_{y'}$, unde f(x) = y şi f(x') = y'.

Deci, $B'_z \approx A_y$, $B' \approx A_{y'}$ şi cum ord $B'_z \prec$ ord B', rezultă că $y \leq y'$ şi $y \neq y'$, unde am notat cu "$\leq$" ordinea pe A.

Aşadar, pentru orice x, x' $\in Z_a$, dacă x] x', atunci $f(x) \leq f(x')$.

Deci, ord Z_a = ord A = a.

Teoremă: Pentru orice număr cardinal a există un număr ordinal α, aşa încât $a = \overline{\overline{Z_\alpha}}$.

Demonstrație: Fie $\overline{\overline{A}} = a$. Conform teoremei lui Zermelo (echivalentă cu axioma alegerii) rezultă că există o bună ordonare $\leq$ pe A. Notăm α=ord A. Conform teoremei precedente, $(A, \leq)$ este asemenea cu $(Z_\alpha, \preccurlyeq)$, deci $\overline{\overline{A}} = \overline{\overline{Z_\alpha}} = a$.

Menționăm faptul că pe o mulțime se pot imagina bune ordonări diferite, care pot conduce la diverse numere ordinale, toate beneficiind de notația ord A. Această ambiguitate, care provine din faptul că nu se specifică o anume bună ordonare pe A, nu creează însă confuzii.

Teoremă: Relația de ordine "$\leq$" definită pentru numere cardinale este o ordine totală.

Demonstrație: Fie U clasa mulțimilor. Putem preciza pentru fiecare mulțime nevidă o relație de bună ordine, conform teoremei lui Zermelo.

Conform teoremei precedente oricărui număr cardinal a îi putem pune în corespondență un număr ordinal α, aşa încât a = $\overline{\overline{Z_\alpha}}$.

Dacă unui alt cardinal b îi punem în corespondență ordinalul β, aşa încât b = $\overline{\overline{Z_\beta}}$, atunci are loc echivalența $a \le b \Leftrightarrow \alpha \preccurlyeq \beta$.

Deoarece relația "$\preccurlyeq$" este de ordine totală rezultă că şi relația "$\le$" este de ordine totală.

Tipurile de ordine ale mulțimilor bine ordonate infinite se numesc **numere ordinale transfinite**.

Mulțimile finite pot fi şi ele bine ordonate şi mai mult, mulțimile cardinal echivalente, care sunt finite, au şi acelaşi tip de ordine, deci au acelaşi **cardinal** şi acelaşi **ordinal**.

Rezultă că, în cazul finit, o clasă cardinală de mulțimi finite este şi o clasă de echivalență ordinală.

CAPITOLUL II. MULȚIMI NUMERICE

2.1. Mulțimea numerelor naturale

Modul intuitiv de percepere a numerelor naturale a fost finalizat anterior prin intermediul numerelor cardinale.

În cele ce urmează va fi dată abordarea axiomatică a mulțimii numerelor naturale.

1. Axiomatica Peano

Definiție. Numim **sistem Peano** un triplet ($\mathbf{N}$, o, σ), unde:

a) $\mathbf{N}$ este o mulțime nevidă;
b) $o \in \mathbf{N}$;
c) $\sigma : \mathbf{N} \to \mathbf{N}$ este o aplicație numită **de succesiune,** care verifică următoarele condiții (axiome):

α) $o \notin Im\sigma$ (adică $\forall n \in \mathbf{N}$, $o \neq \sigma(n)$);

β) σ este o aplicație injectivă;

γ) **Axioma inducției:** Dacă $M \subseteq \mathbf{N}$ satisface proprietățile:

i) $o \in M$;
ii) $n \in M \Rightarrow \sigma(n) \in M$,

atunci $M = \mathbf{N}$.

Vom nota $\sigma(n) = n^*$ şi vom spune că n^* este **succesorul** lui n.

Dând statut de axiome proprietăţilor α), β), γ) matematicianul Giuseppe Peano (1858-1932), a reuşit să construiască cu ajutorul lor întreaga teorie a numerelor naturale. Teoria axiomatică a lui Peano foloseşte pentru numere modelul metodei logice, întrebuinţat cu succes de Euclid în geometrie, încă din antichitate.

Conform definiţiei axiomatice dată de Peano, numerele naturale sunt elementele unei mulţimi **N**, în care se fixează un element o, împreună cu funcţia de succesiune, astfel încât sunt satisfăcute axiomele α), β), γ).

Propoziţie: Pentru orice $n \in \mathbf{N}$, $n \neq o$, există $u \in \mathbf{N}$, astfel încât $n = u^*$.

Demonstraţie: Considerăm $M = \sigma(\mathbf{N}) \cup \{o\}$; atunci $M \subseteq \mathbf{N}$, $o \in M$ şi "$n \in M \Rightarrow \sigma(n) \in M$", pentru că $\sigma(\mathbf{N}) \subset M$. Din axioma inducţiei rezultă că $M = \mathbf{N}$ şi cum $o \notin \sigma(\mathbf{N})$ rezultă că orice element din **N**, diferit de o, este succesorul unui alt element din **N**.

Teorema recursiei. Dacă (**N**, o, σ) este un sistem Peano şi (S, a, φ) este un triplet, unde S este o mulţime nevidă, $a \in S$ şi $\varphi : S \to S$ o funcţie, atunci există o unică funcţie $f : \mathbf{N} \to S$ cu proprietăţile:

1) $f(o) = a$;
2) $f(\sigma(n)) = \varphi(f(n))$, $\forall\, n \in \mathbf{N}$.

Demonstraţie: Considerăm produsul cartezian $\mathbf{N} \times S$ şi fie $F^* = \{U \subseteq \mathbf{N} \times S \mid (o,a) \in U$ şi "$(n, b) \in U \Rightarrow (\sigma(n), \varphi(b)) \in U$"$\}$. Observăm că $F^* \neq \emptyset$, deoarece $\mathbf{N} \times S \in F^*$; în plus, pentru orice familie nevidă $(U_i)_{i \in I}$, unde $\forall i \in I$, $U_i \in F^*$, rezultă că $\bigcap_{i \in I} U_i \in \mathbf{F}^*$.

Fie $f = \bigcap_{U \in F^*} U$. Conform observaţiei anterioare, se obţine că $f \in F^*$. Arătăm că f reprezintă o funcţie, adică satisface următoarele două condiţii:

c1) $\forall n \in \mathbf{N}$, $\exists b \in S$, astfel încât $(n, b) \in f$;

c2) dacă $(n, b) \in f$ şi $(n, b') \in f$, atunci $b = b'$.

Pentru a verifica prima condiţie, vom considera mulţimea $M = \{n \in \mathbf{N} \mid \exists b \in S$, astfel încât $(n, b) \in f\}$ şi vom arăta că $M = \mathbf{N}$, folosind axioma inducţiei. $M \subseteq \mathbf{N}$ şi $o \in M$, pentru că $(o, a) \in f$.

Din $n \in M$ rezultă că $\exists b \in S$, astfel încât $(n, b) \in f$ şi cum $f \in F^*$, se obţine $(\sigma(n), \varphi(b)) \in f$, deci $\sigma(n) \in M$. Aşadar, $M = \mathbf{N}$.

Verificăm acum condiția c2).

Considerăm mulțimea $M'=\{n\in\mathbf{N} \mid$ "$(n, b)\in f$ şi $(n, b')\in f \Rightarrow b=b'$ "$\}$. Vom aplica şi pentru M' axioma inducției. $M'\subseteq\mathbf{N}$. Presupunem, prin reducere la absurd, că $o\notin M'$. Deoarece $(o, a)\in f$ rezultă că există $b\in S$, $b \neq a$, astfel încât $(o, b)\in f$.

Notăm cu $f_1 = f - \{(o, b)\}$; deci $f_1 \subset f$, $f_1 \neq f$. Arătăm că $f_1 \in F^*$. Mai întâi, $(o, a) \in f_1$ şi considerând $(n, b_1) \in f_1 \subset f$, obținem $(\sigma(n), \varphi(b_1))\in f$ şi deci $(\sigma(n), \varphi(b_1))\in f_1$, deoarece $\sigma(n) \neq o$, $\forall n\in\mathbf{N}$. Aşadar, $f_1 \in F^*$ şi din definiția lui f rezultă $f \subseteq f_1$, ceea ce este absurd. Prin urmare, $o\in M'$.

Conform cu c1), există $b\in S$, încât $(n, b)\in f$ şi cum $n\in M'$, rezultă că b este unic. Se obține de aici $(\sigma(n), \varphi(b))\in f$. Presupunând că $\sigma(n)\notin M'$, rezultă că există $c\in S$, $c \neq \varphi(b)$, astfel încât $(\sigma(n), c)\in f$.

Notăm cu $f_2 = f - \{(\sigma(n), c)\}$; deci $f_2 \subset f$, $f_2 \neq f$. Arătăm că $f_2\in F^*$. Avem $(o, a)\in f_2$ şi considerăm $(m, s)\in f_2 \subset f$.

Se obține $(m^*, \varphi(s))\in f$.

Apar două situații:

I) Dacă $m \neq n$, atunci în baza injectivității funcției σ, rezultă că $m^* \neq \sigma(n)$ şi deci $(m^*, \varphi(s)) \neq (\sigma(n), c)$, de unde $(m^*, \varphi(s))\in f_2$.

II) Dacă $n = m$, atunci $(m^*, \varphi(s)) = (\sigma(n), \varphi(s))$.

Din $(m, s) = (n, s)\in f$ şi din unicitatea lui b, rezultă că $s = b$, deci, $(m^*, \varphi(s)) = (\sigma(n), \varphi(b))$.

Deoarece $\varphi(b) \neq c$, se obține $(\sigma(n), \varphi(b)) \neq (\sigma(n), c)$, adică $(m^*, \varphi(s)) = (\sigma(n), \varphi(b))\in f_2$.

Aşadar $f_2\in F^*$, de unde $f \subseteq f_2$, ceea ce este absurd. Prin urmare, $\sigma(n)\in M'$ şi conform axiomei inducției, obținem $M' = \mathbf{N}$.

Folosind notațiile consacrate funcțiilor, condițiile $(o, a)\in f$, respectiv $(n, b)\in f \Rightarrow (\sigma(n), \varphi(b))\in f$ se scriu astfel: $f(o) = a$, respectiv $f(n) = b \Rightarrow f(\sigma(n)) = \varphi(b)$, adică tocmai condițiile ce trebuiau satisfăcute de funcția f.

Unicitatea funcției f se demonstrează prin "reducere la absurd". Considerăm o funcție g care satisface condițiile 1) şi 2).

Fie $M'' = \{n\in\mathbf{N} \mid f(n) = g(n)\}$. Avem $M'' \subset \mathbf{N}$ şi $o\in M''$, deoarece $f(o) = g(o) = a$. Dacă $n\in M''$, atunci $f(n) = g(n)$, deci $\varphi(f(n)) = \varphi(g(n))$, de unde $f(\sigma(n)) = g(\sigma(n))$, adică $\sigma(n)\in M''$.

Aplicând din nou axioma inducției, rezultă $M'' = \mathbf{N}$, adică $f = g$.

Teoremă. Dacă (**N**, o, σ) şi (S, a, φ) sunt sisteme Peano, atunci există o unică funcție f : **N**→S, astfel încât f(o) = a, f∘σ = φ∘f şi f este o bijecție.

Demonstrație: Mai rămâne de arătat că f este bijectivă. Aplicând teorema recursiei pentru sistemul Peano (S, a, φ) şi tripletul (**N**, o, σ), rezultă că există o unică funcție g : S→**N**, pentru care g(a) = o şi g∘φ = =σ∘g. Vom arăta că g este inversa lui f.

Pentru aceasta, vom aplica teorema recursiei pentru sistemul Peano (**N**, o, σ) şi tripletul (**N**, o, σ). Rezultă că există o unică funcție h : **N**→**N**, astfel încât h(o) = o şi h∘σ = σ∘h. Însă 1_N şi g∘f verifică condițiile satisfăcute de h, deoarece: (g∘f)(o) = g(a) = o = $1_{\mathbf{N}}$(o) şi (g∘f)∘σ = =g∘(f∘σ) = g∘(φ∘f) = (g∘φ)∘f = (σ∘g)∘f = σ∘(g∘f), iar 1_N∘σ = σ∘$1_{\mathbf{N}}$. Din unicitatea lui h rezultă că g∘f = $1_{\mathbf{N}}$.

Similar, aplicând de această dată teorema recursiei pentru sistemul Peano (S, a, φ) şi tripletul (S, a, φ) se obține că f∘g = 1_S.

Aşadar f este bijectivă.

În baza acestei teoreme, vom considera că există un unic sistem Peano (pentru că între oricare două sisteme Peano există o bijecție care satisface condițiile din teorema de mai sus).

N va fi numită mulțimea numerelor naturale şi vom nota o cu 0 (numărul natural zero), succesorul lui 0 cu 1, succesorul lui 1 cu 2, ş.a.m.d.

Propoziție. N este o mulțime infinită.

Demonstrație: Presupunem prin reducere la absurd că **N** este finită şi aplicăm următorul rezultat:

"Dacă A este o mulțime finită, iar f :A→A este o aplicație, atunci următoarele afirmații sunt echivalente:

i) f este injectivă;
ii) f este surjectivă;
iii) f este bijectivă."

Pentru A = **N** şi f = σ, observăm că σ este injectivă, dar nu este surjectivă (0∉Imσ), prin urmare presupunerea făcută este falsă, deci **N** este infinită.

2. Adunarea numerelor naturale

Fie m un element oarecare, dar fixat al lui **N**. Considerăm în teorema recursiei S = **N**, a = m şi φ = σ. Conform teoremei, rezultă că există o aplicație unică $f_m : \mathbf{N} \to \mathbf{N}$, astfel încât:

1. $f_m(0) = m$;
2. $f_m(\sigma(n)) = \sigma(f_m(n))$, $\forall\, n \in \mathbf{N}$.

Notăm $f_m(n) = n + m$.

Condițiile 1. şi 2. se vor scrie astfel:

1) $0 + m = m$;
2) $n^* + m = (n + m)^*$, $\forall\, n \in \mathbf{N}$

şi vor fi numite **condițiile de definiție ale adunării**.

Propoziție. Au loc următoarele afirmații:

1′. $n + 0 = n$, $\forall\, n \in \mathbf{N}$

2′. $n + m^* = (n + m)^*$, $\forall\, n \in \mathbf{N}$

Demonstrație: Se aplică, pentru demonstrarea ambelor afirmații, axioma inducției, considerând mulțimile:

1′ $M_1 = \{n \in \mathbf{N} \mid n + 0 = n\}$, respectiv

2′ $M_2 = \{n \in \mathbf{N} \mid n + m^* = (n + m)^*\}$

1′. Avem $M_1 \subseteq \mathbf{N}$, $0 \in M_1$ (rezultă din 1) pentru m = 0) şi dacă $n \in M_1$, adică n + 0 = n, atunci în baza condiției 2) $n^* + 0 = (n + 0)^* = n^*$, adică $n^* \in M_1$. Deci $M_1 = \mathbf{N}$.

2′. Avem $M_2 \subseteq \mathbf{N}$, $0 \in M_2$, deoarece în baza condiției 1) avem $0 + m^* = m^* = (0 + m)^*$. În plus, dacă $n \in M_2$, adică $n + m^* = (n + m)^*$, rezultă că $n^* + m^* = (n + m^*)^* = ((n + m)^*)^* = (n^* + m)^*$, utilizând condiția 2) pentru m^* şi apoi pentru m. Prin urmare $n^* \in M_2$ şi deci $M_2 = \mathbf{N}$.

Considerăm funcția "+" : $\mathbf{N} \times \mathbf{N} \to \mathbf{N}$, care asociază perechii $(n, m) \in \mathbf{N} \times \mathbf{N}$ elementul $n + m = f_m(n)$. Această funcție se numeşte **adunarea numerelor naturale.**

Propoziție: Au loc următoarele:

A1. Asociativitatea adunării

pentru orice $n, m, p \in \mathbf{N}$, $(n + m) + p = n + (m + p)$;

A2. Comutativitatea adunării

pentru orice $n, m \in \mathbf{N}$, $n + m = m + n$;

A3. 0 este elementul neutru la adunare

$\forall n \in \mathbf{N}$, $n + 0 = 0 + n$;

A4. Legea de simplificare la adunare (numită reducere)

$\forall p \in \mathbf{N}$, $n + p = m + p \Rightarrow n = m$;

Fie $n, m \in \mathbf{N}$. Au loc implicațiile:

A5. $n + m = 0 \Rightarrow n = 0$ şi $m = 0$;

A6. $m + n = 1 \Rightarrow (m = 1$ şi $n = 0)$ sau $(m = 0$ şi $n = 1)$.

Demonstrație:

A1. Considerăm, mai întâi m şi p fixate.

Fie $M_1 = \{n \in \mathbf{N} \mid (n + m) + p = n + (m + p)\}$. Aplicând axioma inducției pentru M_1 se obține $M_1 = \mathbf{N}$, folosind condițiile de definiție ale adunării, 1′ şi 2′.

Considerăm acum n şi p fixate şi mulțimea:

$M_2 = \{m \in \mathbf{N} \mid (n + m) + p = n + (m + p)\}$; aplicând din nou axioma inducției se obține $M_2 = \mathbf{N}$.

Cazul în care m şi n sunt fixate este similar primului caz. Prin urmare, pentru m, n, p oarecare în **N**, are loc proprietatea:

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

Demonstrațiile pentru A2 şi A3 sunt similare cu cele de mai sus.

Pentru A4, mulțimea căreia i se aplică axioma inducției este $M = \{p \in \mathbf{N} \mid n + p = m + p \Rightarrow n = m\}$.

A5. Presupunem $n \neq 0$. Atunci, conform unei propoziții anterioare (§ 2.1.; 1.), există $u \in \mathbf{N}$, astfel încât $n = u^*$.

Obținem $n + m = 0 \Leftrightarrow u^* + m = 0 \Leftrightarrow (u + m)^* = 0$, contradicție. Aşadar $n = 0$ şi deci $0 + m = 0$, adică $m = 0$.

A6. Presupunem, prin reducere la absurd, că ($m \neq 1$ sau $n \neq 0$) şi ($m \neq 0$ sau $n \neq 1$). Sunt posibile următoarele patru situații:

1°. $m \neq 1$ şi $m \neq 0$;

2°. $m \neq 0$ şi $n \neq 0$;

3°. $m \neq 1$ şi $n \neq 1$;

4°. $n \neq 0$ şi $n \neq 1$.

1°. Din $m \neq 0$ rezultă că există $u \in \mathbf{N}$ aşa încât $m = u^*$.

Se obține $m + n = 1 \Leftrightarrow (u + n)^* = 0^* \Leftrightarrow u + n = 0 \Leftrightarrow u = 0$ şi $n = 0$, în baza injectivității lui σ şi a proprietății A5 şi obținem $m = 1$, fals. Din contradicția obținută rezultă că această situație nu poate avea loc.

Similar se arată că situațiile 2° şi 4° nu pot avea loc.

3°. Avem $n \neq 0$, pentru că altfel din $m + n = 1$ ar rezulta că $m = 1$, fals. Putem acum repeta raționamentul de la 1° şi deducem că şi această situație este imposibilă.

Observație: Pentru orice $n \in \mathbf{N}$, avem $\sigma(n) = (n + 0)^* = n + 0^* = n + 1$.

3. Înmulțirea numerelor naturale

Fie m un element oarecare, dar fixat, al lui **N**. Aplicând teorema recursiei pentru $S = \mathbf{N}$, $a = 0$ şi $\varphi = f_m$, rezultă că există o aplicație unică $g_m : \mathbf{N} \to \mathbf{N}$, astfel încât:

1. $g_m(0) = 0$;
2. $g_m(\sigma(n)) = f_m(g_m(n))$, $\forall n \in \mathbf{N}$.

Notăm $g_m(n) = n \cdot m$.

Condițiile 1. şi 2. se vor scrie astfel:

1) $0 \cdot m = 0$;
2) $n^* \cdot m = n \cdot m + m$, $\forall n \in \mathbf{N}$.

şi vor fi numite **condițiile de definiție ale înmulțirii.**

Propoziție: Au loc următoarele afirmații:

$1'$ $n \cdot 0 = 0$, $\forall n \in \mathbf{N}$;

$2'$ $n \cdot m^* = n \cdot m + n$, $\forall n \in \mathbf{N}$.

Demonstrație: În demonstrație se aplică axioma inducției procedându-se în mod asemănător cazului operației de adunare.

Considerăm funcția "$\cdot$" : $\mathbf{N} \times \mathbf{N} \to \mathbf{N}$, care asociază perechii $(n, m) \in \mathbf{N} \times \mathbf{N}$ elementul $n \cdot m = g_m(n)$.

Propoziție: Au loc următoarele:

D. Distributivitatea înmulțirii față de adunare

pentru orice $m, n, p \in \mathbf{N}$, $n \cdot (m + p) = n \cdot m + n \cdot p$;

M_1. Asociativitatea înmulțirii

pentru orice $n, m, p \in \mathbf{N}$, $(n \cdot m) \cdot p = n \cdot (m \cdot p)$;

M_2. Comutativitatea înmulțirii

pentru orice $n, m \in \mathbf{N}$, $n \cdot m = m \cdot n$;

M_3. 1 este element neutru la înmulțire

$\forall n \in \mathbf{N}$, $n \cdot 1 = 1 \cdot n = n$;

M_4. Legea de simplificare la înmulțire

$\forall p \in \mathbf{N}$, $p \neq 0$, $n \cdot p = m \cdot p \Rightarrow n = m$.

Fie $n, m \in \mathbf{N}$. Au loc implicațiile:

M_5. $n \cdot m = 1 \Rightarrow n = 1$ şi $m = 1$;

M_6. $n \cdot m = 0 \Rightarrow n = 0$ sau $m = 0$.

Demonstrație: D, M_1, M_2, M_3 se demonstrează utilizând axioma inducției.

Demonstrarea proprietății M_4, va fi dată ulterior (după introducerea relației de ordine "$\leq$" pe **N)**.

M_5. Observăm că $n \neq 0 \neq m$, altfel $n \cdot m$ ar fi zero. Deci există $u, v \in \mathbf{N}$, astfel încât $n = u^*$ şi $m = v^*$. Avem $n \cdot m = u^* \cdot v^* = u \cdot v^* + v^* = =(u \cdot v^* + v)^*$,deci $(u \cdot v^* + v)^* = 1$, de unde $u \cdot v^* + v = 0$ şi conform cu A_5 se obține $u \cdot v^* = v = 0$. Rezultă că $m = 1$ şi utilizând M_3 rezultă că $n = 1$.

M_6. Presupunem, prin reducere la absurd, că $n \neq 0$ şi $m \neq 0$. Atunci există $u, v \in \mathbf{N}$, astfel încât $n = u^*$ şi $m = v^*$.
Avem $n \cdot m = u^* \cdot v^* = u^* \cdot v + u^*$ şi conform cu A_5 se obține $u^* \cdot v = u^* = 0$, contradicție. Deci $n = 0$ sau $m = 0$.

În vederea simplificării scrierii vom mai nota mn în loc de $m \cdot n$.

4. Relația de ordine "≤" pe mulțimea N

Definiție: Fie $m, n \in \mathbf{N}$. Spunem că $m \leq n$ dacă există $p \in \mathbf{N}$ astfel încât $n = m + p$. Spunem că $m < n$ dacă există $p \in \mathbf{N}$, $p \neq 0$, astfel încât $n = m + p$.

Propoziție: Relația "$\leq$" este o relație de ordine pe **N**.

Demonstrație: Se verifică, folosind definiția, următoarele proprietăți:

O1 : $n \leq n$, $\forall n \in \mathbf{N}$ (reflexivitatea);

O2 : $m \leq n$ şi $n \leq m \Rightarrow m = n$ (antisimetria);

O3 : $m \leq n$ şi $n \leq p \Rightarrow m \leq p$ (tranzitivitatea).

O1. Rezultă din faptul că $\exists 0 \in \mathbf{N} : n = n + 0$.

O2. Din $m \leq n$ rezultă că există $p_1 \in \mathbf{N}$ aşa încât $n = m + p_1$, iar din $n \leq m$ rezultă că există $p_2 \in \mathbf{N} : m = n + p_2$. Se obține $n = n + (p_2 + p_1)$, de unde, conform condiției A4, rezultă că $p_2 + p_1 = 0$ şi, aplicând A5, vom avea $p_1 = p_2 = 0$, deci $n = m$.

O3. Similar cu O2, $m \leq n \Rightarrow \exists\, t \in \mathbf{N}$ aşa încât $n = m + t$ şi $n \leq p \Rightarrow$ $\Rightarrow \exists s \in \mathbf{N}$, $p = n + s$, deci $\exists t + s \in \mathbf{N}$, astfel încât $p = m + (t + s)$, adică $m \leq p$.

Menționăm că, în cele ce urmează vom scrie uneori $m \geq n$ în loc de $n \leq m$, respectiv $m > n$ în loc de $n < m$.

Propoziție: Fie m, n ∈ **N**. Au loc următoarele afirmații:

OA1. $\forall p \in \mathbf{N}$, $[m \le n \Rightarrow m + p \le n + p]$;
OA2. $\forall p \in \mathbf{N}$, $[m + p \le n + p \Rightarrow m \le n]$;
OA3. $\forall p \in \mathbf{N}$, $[m < n \Rightarrow m + p < n + p]$;
OA4. $\forall p \in \mathbf{N}$, $[m + p < n + p \Rightarrow m < n]$;
OM1. $\forall p \in \mathbf{N}$, $[m \le n \Rightarrow mp \le np]$;
OM2. $\forall p \in \mathbf{N}$, $[m < n \Rightarrow mp \le np]$;
OM3. $\forall p \in \mathbf{N}$, $p \ne 0$, $[m < n \Rightarrow mp < np]$;
OM4. $\forall p \in \mathbf{N}$, $p \ne 0$, $[mp < np \Rightarrow m < n]$;
OM5. $\forall p \in \mathbf{N}$, $p \ne 0$, $[mp \le np \Rightarrow m \le n]$;

Demonstrație. OA1. Din $m \le n$ rezultă că există $q \in \mathbf{N}$, astfel încât $n = m + q$, deci $n + p = (m + p) + q$, pentru orice $p \in \mathbf{N}$, (datorită comutativității şi asociativității adunării). Rezultă că $m + p \le n + p$.

Analog se arată OA3 cu singura deosebire că elementul $q \in \mathbf{N}$ este şi nenul.

OA2. Din $m + p \le n + p$ rezultă că există $q \in \mathbf{N}$, astfel încât $n + p = m + p + q$ şi în baza comutativității şi a legii de simplificare pentru adunare, se obține $n = m + q$, de unde $m \le n$.

Analog se arată şi OA4 cu singura deosebire că elementul $q \in \mathbf{N}$ este şi nenul.

OM3. Fie $p \in \mathbf{N}$, $p \ne 0$ şi $m < n$. Rezultă că există $q \in \mathbf{N}$, $q \ne 0$ astfel încât $n = m + q$, de unde în baza distributivității înmulțirii față de adunare, se obține $n \cdot p = m \cdot p + q \cdot p$. Dacă am presupune că $q \cdot p = 0$, atunci ar rezulta că $p = 0$ sau $q = 0$, ceea ce este fals. Deci $q \cdot p \in \mathbf{N}$, $q \cdot p \ne 0$, de unde $m \cdot p < n \cdot p$.

Analog se arată OM1 şi OM2 cu singura deosebire că de această dată $q \cdot p$ poate fi şi zero şi deci se obține $m \cdot p \le n \cdot p$.

Vom reveni la demonstrarea proprietăților OM4 şi OM5 după prezentarea principiului trihotomiei.

5. Principiul trihotomiei

Orice două numere naturale m şi n se află în una şi numai una dintre situațiile:

$$m < n, \qquad m = n, \qquad n < m$$

Demonstrație. Fie n un număr natural, dar fixat. Considerăm mulțimea $M = \{m \in \mathbf{N} \mid m < n \text{ sau } m = n \text{ sau } n < m\}$. Vom arăta că $M = \mathbf{N}$, folosind axioma inducției.

i) Dacă $n = 0$, atunci $0 \in M$.

Dacă $n \neq 0$, atunci ținând cont de egalitatea $n = 0 + n$ rezultă că $0 < n$, de unde $0 \in M$.

ii) Fie $m \in M$. Vom arăta că $m^* \in M$. Putem avea următoarele situații:

I) $m < n$, de unde $\exists p \in \mathbf{N}$, $p \neq 0$ astfel încât $n = m + p$. Din $p \neq 0$ rezultă că $\exists u \in \mathbf{N}$, astfel încât $p = u^*$. Atunci vom obține $n = m + u^* = =(m + u)^* = m^* + u$. Pentru $u = 0$, avem $m^* = n$, iar pentru $u \neq 0$, avem $m^* < n$, deci în ambele cazuri rezultă că $m^* \in M$.

II) $m = n$, de unde $m^* = n^* = (n + 0)^* = n + 0^*$. Rezultă că $n < m^*$, prin urmare $m^* \in M$.

III) $n < m$, de unde $\exists p \in \mathbf{N}$, $p \neq 0$, astfel încât $m = n + p$. Rezultă că $m^* = (n + p)^* = n + p^*$ şi cum $p^* \neq 0$ se obține $n < m^*$.

Prin urmare $m^* \in M$.

Din i) şi ii) rezultă că $M = \mathbf{N}$.

Să arătăm acum că nu putem avea decât una din cele trei situații $m < n$, $m = n$, $n < m$.

Presupunem că ar fi posibile simultan situațiile $m < n$ şi $m = n$. Din $m < n$ rezultă că $\exists p \in \mathbf{N}$, $p \neq 0$, astfel încât $n = m + p$ şi cum $m = n$, obținem $n = n + p$, adică $n + 0 = n + p$ şi în baza legii de simplificare la adunare s-ar obține $0 = p$, ceea ce este fals!

Similar se arată că nu putem avea simultan situațiile $n < m$ şi $m = n$.

Presupunem acum că ar fi posibile simultan situațiile $m< n$ şi $n < m$. Ar rezulta că există $p, q \in \mathbf{N}$, $p \neq 0 \neq q$, astfel încât $n = m + p$ şi $m = n + q$, de unde s-ar obține $n = n + (q + p)$, deci $q + p = 0$. Deoarece p şi q sunt numere naturale, rezultă că $p = q = 0$, contradicție.

Prin urmare, putem concluziona că avem una şi numai una din cele trei situații.

Revenim acum la demonstrarea legii de simplificare la înmulțire M4: $\forall p \in \mathbf{N}$, $p \neq 0$, $n \cdot p = m \cdot p \Rightarrow n = m$.

Presupunem că $n \neq m$. Atunci în baza principiului trihotomiei avem $n < m$ sau $m < n$. Dacă $n < m$ atunci $n \cdot p < m \cdot p$, iar dacă $m < n$

atunci $m \cdot p < n \cdot p$ (conform proprietății OM3). Dar $n \cdot p = m \cdot p$, prin urmare $m = n$.

Să demonstrăm OM4: $\forall p \in \mathbf{N}$, $p \neq 0$, $m \cdot p < n \cdot p \Rightarrow m < n$.

Prin reducere la absurd, presupunem că nu ar avea loc inegalitatea $m < n$. În baza principiului trihotomiei am avea $m = n$, de unde $m \cdot p = n \cdot p$ sau $n < m$, de unde $n \cdot p < m \cdot p$ (din OM3). Se contrazice astfel ipoteza $m \cdot p < n \cdot p$, prin urmare $m < n$.

Similar se verifică proprietatea OM5: $\forall p \in \mathbf{N}$, $p \neq 0$, $m \cdot p \leq n \cdot p \Rightarrow$ $\Rightarrow m \leq n$.

6. Principiul bunei ordonări (P.B.O.)

Pentru orice $S \subset \mathbf{N}$, $S \neq \varnothing$, există $e \in S$ astfel încât $e \leq s$, $\forall s \in S$ (adică S are un **prim element e**).

Demonstrație:

Considerăm mulțimea $M = \{m \in \mathbf{N} \mid m \leq s, \forall s \in S\}$. Din faptul că $0 \in M$ rezultă că $M \neq \varnothing$. Din $S \neq \varnothing$ rezultă că $\exists s \in S$ şi din $s^* = s + 1$ obținem $s < s^*$. Deci, conform principiului trihotomiei nu putem avea $s^* \leq s$, adică $s^* \notin M$, de unde rezultă că $M \neq \mathbf{N}$.

Ținând cont de axioma inducției rezultă că $\exists e \in M$ şi $e^* \notin M$. Din $e \in M$ rezultă că $e \leq s$, $\forall s \in S$. Arătăm şi că $e \in S$. Presupunând că $e \notin S$ şi ținând cont că $e \leq s$, $\forall s \in S$, se obține $e < s$, $\forall s \in S$, deci pentru orice $s \in S$, există $p \in \mathbf{N}$, $p \neq 0$, astfel încât $s = e + p$. Din $p \neq 0$ rezultă că $\exists u \in \mathbf{N}$, astfel încât $p = u^*$, deci $s = e + u^* = (e + u)^* = e^* + u$, de unde $e^* \leq s$, $\forall s \in S$, adică $e^* \in M$, contradicție. Aşadar $e \in S$ şi demonstrația este încheiată.

7. Principiul I al inducției matematice

Dacă o propoziție P(n) (ce poate fi asociată cu orice $n \in \mathbf{N}$) satisface următoarele două condiții:

(a) P(0) este adevărată;

(b) $\forall m \in \mathbf{N}$, [P(m) adevărată $\Rightarrow$ P(m*) adevărată].

atunci, $\forall n \in \mathbf{N}$, P(n) este adevărată.

Demonstrație: Fie $M = \{n \in \mathbf{N} \mid$ P(n) este adevărată$\}$. Vom aplica pentru M axioma inducției şi vom obține $M = \mathbf{N}$, adică $\forall n \in \mathbf{N}$, P(n) este adevărată.

Precizăm că (a) poate fi înlocuită cu condiția "$P(k_0)$ adevărată", unde $k_0 \in \mathbf{N}$, caz în care concluzia are forma "$\forall\, n \in \mathbf{N}$, $n \geq k_0$, $P(n)$ este adevărată".

Înlocuind (a) în acestă ultimă formulă (de exemplu) prin

- $P(k_0)$, $P(k_0+1)$, ..., $P(k_0+ p-1)$ adevărate şi b) prin:
- $P(m)$ adevărată $\Rightarrow P(m+p)$ adevărată, concluzia se păstrează.

8. Principiul al II-lea al inducției matematice

Dacă o propoziție $P(n)$, (ce poate fi asociată cu orice $n \in \mathbf{N}$), satisface următoarele condiții:

(a) $P(0)$ este adevărată;

(b′) $\forall m \in \mathbf{N}$, [$P(r)$ adevărată pentru orice $r \in \mathbf{N}$, $r < m \Rightarrow P(m)$ adevărată].

atunci $\forall n \in \mathbf{N}$, $P(n)$ este adevărată.

Teoremă: Principiul bunei ordonări, principiul I al inducției matematice şi principiul al II-lea al inducției matematice sunt echivalente.

Demonstrație: Vom arăta că:

(1) Principiul I al inducției matematice implică principiul bunei ordonări;
(2) Principiul bunei ordonări implică principiul al II-lea al inducției matematice;
(3) Principiul al II-lea al inducției matematice implică principiul I al inducției matematice.

(1). Fie $P(m)$ propoziția "$m \leq s$, $\forall s \in S$". Observăm că $P(0)$ este adevărată, dar pentru $s \in S$, $P(s^*)$ este falsă. Conform principiului I al inducției matematice, $\exists e \in \mathbf{N}$, pentru care $P(e)$ este adevărată şi $P(e^*)$ este falsă. Din $P(e)$ adevărată rezultă că $e \leq s$, $\forall s \in S$. În plus, $e \in S$, pentru că altfel $e < s$, $\forall s \in S$ şi deci $e^* \leq s$, $\forall s \in S$, adică $P(e^*)$ adevărată, contradicție.

(2). Fie $P(n)$ o propoziție, astfel încât $P(0)$ este adevărată şi $\forall m \in \mathbf{N}$, [$P(r)$ adevărată, $\forall r < m \Rightarrow P(m)$ adevărată]. Vom arăta că $P(n)$ este adevărată, $\forall n \in \mathbf{N}$. Fie $S = \{s \in \mathbf{N} \mid P(s) \text{ falsă}\}$. Demonstrăm că $S = \emptyset$. Presupunem că $S \neq \emptyset$. Conform P.B.O. rezultă că $\exists l \in S$, $l \leq s$, $\forall s \in S$. Din $l \in S$ rezultă că $P(l)$ falsă. Pe de altă parte, să observăm că $\forall r \in \mathbf{N}$, $r < l$, $P(r)$ este adevărată, altfel, dacă $P(r)$ ar fi falsă ar rezulta $r \in S$ şi cum

$l \leq s$, $\forall s \in S$, s-ar obține $l \leq r$, contradicție. Deci, $\forall r \in \mathbf{N}$, $r < l$, P(r) este adevărată şi atunci, în baza lui (b′), ar rezulta că P(l) este adevărată, contradicție.
Aşadar, $S = \emptyset$.
(3). Sunt presupuse satisfăcute ipotezele principiului I al inducției matematice. Vom verifica faptul că au loc ipotezele celui de-al II-lea principiu.

Ipoteza (a) este comună celor două principii, deci P(0) este adevărată. Fie acum $m \in \mathbf{N}$, $m \neq 0$. Rezultă că $\exists u \in \mathbf{N}$, astfel încât $m = u^*$. Avem $u < m$. Pentru a demonstra (b′), presupunem că P(r) este adevărată, pentru orice $r < m$. Atunci P(u) este adevărată şi conform cu (b) rezultă că P(u*), adică P(m) este adevărată, prin urmare are loc (b′). Aplicând acum cel de-al II-lea principiu al inducției matematice, rezultă că $\forall n \in \mathbf{N}$, P(n) este adevărată.

Propoziție: Nu există nici un număr natural între 0 şi 1.

Demonstrație: Presupunem, prin reducere la absurd, că există un număr natural k, astfel încât $0 < k < 1$. Mulțimea $A=\{k \in \mathbf{N} \mid 0<k < 1\}$ este deci nevidă şi conform principiului bunei ordonări are un prim element a, astfel încât $0 < a < 1$. Multiplicând cu a, obținem $0 < a \cdot a < a$, ceea ce contrazice faptul că a este primul element al lui A. Această contradicție demonstrează propoziția.

9. Lema lui Arhimede

Fie $m \in \mathbf{N}$. Pentru orice $n \in \mathbf{N}$, $n \neq 0$, există $t \in \mathbf{N}$, astfel încât $m < t \cdot n$.

Demonstrație: Dacă $m < n$, considerăm $t = 1$.
Dacă $n = m$, considerăm $t = n + 1$ şi avem $n < n + n \cdot n = (n + 1) \cdot n = t \cdot n$, deoarece $n \neq 0$.

Dacă $n < m$, atunci există $u \in \mathbf{N}$, $u \neq 0$, astfel încât $m = n + u$. Apar două situații:

i) dacă $n = 1$, considerăm $t = m + 1$. Avem $m < m + 1 = t = t \cdot n$;

ii) dacă $n \neq 1$, considerăm $t = u + 1$. Avem $1 < n$, de unde $u < u \cdot n$, deci $m = n + u < n + u \cdot n = (u + 1) \cdot n = t \cdot n$.

10. Teorema împărțirii cu rest (Euclid)

Pentru orice a, b∈**N**, cu b ≠ 0, există q, r∈**N**, unic determinate, astfel încât a = b·q + r, 0 ≤ r < b.

Demonstrație: Fie a, b∈**N,** b fiind oarecare, nenul, dar fixat.

Fie A = {a∈**N** | ∃q, r∈**N**: a = b·q + r, 0 ≤ r <b}. Vom aplica axioma inducției.

0∈A, pentru că ∃q = 0 şi ∃r = 0, astfel încât 0 = b·0 + 0. Dacă a∈A, adică ∃q, r∈**N**: a = b·q + r, 0 ≤ r < b, atunci a* = (b·q +r)* = b·q + r*. Dacă r* = b, atunci considerăm $q_1 = q + 1 \in \mathbf{N}$ şi $r_1 = 0$ şi avem egalitatea a* = b·q_1 + r_1, deci a*∈A. Conform axiomei inducției A=**N**.

Să demonstrăm acum unicitatea lui q şi r. Presupunem că există q_1, r_1∈**N**, astfel încât a = b·q_1 + r_1, 0 ≤ r_1 < b.

Presupunem q ≠ q_1 . Putem avea situațiile: q < q_1 sau q_1 < q. Dacă q < q_1, atunci există p∈**N**, p ≠ 0: q_1 = q + p. Din b·q + r = b·q_1 + r_1 rezultă că b·q + r = b·q + b·p +r_1, de unde r = b·p + r_1. Din p∈**N**, p ≠ 0 rezultă că ∃u∈**N**: p = u*, deci b·p +r_1 = b·u* + r_1 = b·u + b + r_1. Obținem b ≤ b·u + b + r_1 = b·p + r_1 = r, contradicție.

Dacă q_1 < q, procedăm în mod analog obținem de asemenea, o contradicție.

Deci q_1 = q şi atunci r_1 = r.

Observație: Putem demonstra existența numerelor q şi r (astfel încât a = b·q + r, 0 ≤ r < b) şi în alt mod şi anume:

considerăm A = {b·k | k∈**N** şi a < b·k}. Conform lemei lui Arhimede rezultă că A ≠ ∅.

Aplicând P.B.O., ∃b·l∈A aşa încât b·l ≤ b·k, ∀ b · k ∈ A.

Observăm că l ≠ 0, altfel am avea a < 0 = b·l, ceea ce este absurd. Rezultă că ∃q∈**N**: l = q*. Avem b·q < b·l şi cum b·l este prim element al lui A rezultă că b·q∉A, adică b·q ≤ a, de unde rezultă că există r∈**N**, astfel încât a = b·q + r.

Dacă am presupune că b ≤ r, atunci ar exista u∈**N**: r = b + u, de unde a = b·q + r = b·q + b + u = b·(q + 1) + u = b·l + u, deci b·l ≤ a, ceea ce este absurd. Deci, r <b.

2.2. Mulțimea numerelor întregi Z

1. Construcția mulțimii Z

Considerăm pe mulțimea $\mathbf{N}\times\mathbf{N}$ următoarea relație:
$(m, n) \sim (p, q)$ dacă $m + q = n + p$, unde $(m, n), (p, q)\in\mathbf{N}\times\mathbf{N}$.
Aceasta este o relație de echivalență:

- este reflexivă, deoarece $m + n = n + m$ ceea ce implică $(m, n) \sim (m, n)$;
- este simetrică, deoarece presupunând $(m, n) \sim (p, q)$ rezultă că $m + q = n + p$, de unde deducem $p + n = q + m$, deci $(p,q) \sim (m,n)$;
- este tranzitivă, deoarece presupunând $(m, n) \sim (p, q)$ și $(p, q) \sim (r, s)$ rezultă că $m + q = n + p$ și $p + s = q + r$, de unde deducem $(m + s) + (p + q) = (m + q) + (p + s)=(n + p)+ + (q + r) = (n + r) + (p + q)$, deci $m + s = n + r$, adică $(m, n) \sim (r, s)$.

Clasa de echivalență a lui (m, n) o vom nota cu

$$\overline{(m,n)} =\{(p,q)\in\mathbf{N}\times\mathbf{N} / (m,n) \sim (p,q)\}.$$

Definiție. Mulțimea factor $\mathbf{N}\times\mathbf{N}/_{\sim} = \left\{\overline{(m,n)} / (m,n)\in\mathbf{N}\times\mathbf{N}\right\}$ se numeşte **mulțimea numerelor întregi** şi se notează cu **Z**.

Se numeşte **număr întreg** orice element $\overline{(m,n)}$ al lui **Z**.

2. Adunarea numerelor întregi

Definim pe **Z** următoarea lege de compoziție "+" : $\mathbf{Z}\times\mathbf{Z} \to \mathbf{Z}$,
$\overline{(m,n)} + \overline{(p,q)} = \overline{(m + p, n + q)}$
"+" este bine definită. Într-adevăr, dacă $(m, n) \sim (m', n')$ şi $(p,q) \sim (p', q')$, atunci $m + n' = n + m'$ şi $p + q' = q + p'$, de unde deducem că $(m + p) +(n' + q') =(m + n') + (p + q')= (n + m')+(q + p')= = (n + q) + (m' + p')$, adică $(m + p, n + q) \sim (m' + p', n' + q')$.

Legea de compoziție "+" pe **Z** se numeşte **adunarea numerelor întregi**, iar $\overline{(m + p, n + q)}$ se numeşte **suma** numerelor întregi $\overline{(m,n)}$ şi $\overline{(p,q)}$.

Au loc următoarele:

1) **Asociativitatea**. Date numerele întregi x = $\overline{(m,n)}$, y = $\overline{(p,q)}$, z = $\overline{(r,s)}$ rezultă că

(x + y) + z = $\overline{((m+p)+r,(n+q)+s)} = \overline{(m+(p+r),n+(q+s))}$ =
= x + (y + z), deoarece adunarea numerelor naturale este asociativă.

2) **Comutativitatea**. Date numerele întregi x = $\overline{(m,n)}$, y = $\overline{(p,q)}$ rezultă că y + x = $\overline{(p+m,q+n)}$ = $\overline{(m+p,n+q)}$ = x + y, deoarece adunarea numerelor naturale este comutativă.

3) Elementul neutru. Să observăm că pentru orice n∈**N**, avem (n, n) ~ (0, 0), deci $\overline{(n,n)}$ = $\overline{(0,0)}$. În plus, pentru orice y = $\overline{(p,q)}$ ∈**Z**, avem $\overline{(p,q)} + \overline{(0,0)} = \overline{(0,0)} + \overline{(p,q)} = \overline{(p,q)}$, adică $\overline{(0,0)}$ este element neutru la adunarea numerelor întregi.

4) Elemente simetrizabile. Pentru orice număr întreg x = $\overline{(m,n)}$, există x′ = $\overline{(n,m)}$ ∈**Z**, astfel încât x + x′ = x′ + x = $\overline{(0,0)}$. Astfel orice număr întreg x este simetrizabil în raport cu adunarea numerelor întregi.

3. Înmulțirea numerelor întregi

Definim pe **Z** următoarea lege de compoziție " · " : **Z**×**Z**→**Z**, $\overline{(m,n)} \cdot \overline{(p,q)} = \overline{(mp+nq,mq+np)}$.

"·" este bine definită. Într-adevăr, dacă (m, n) ~ (m′, n′) şi (p, q) ~ (p′, q′), atunci avem m + n′ = n + m′ şi p + q′ = p′ + q, de unde rezultă că (mp + nq) + (m′q′ + n′p′) + (n′p + m′q) = (m + n′)p + +(n + m′)q + (m′q′ + n′p′) = (n + m′)p + (m + n′)q + (m′q′ + n′p′) = =(mq + np)+ m′(p + q′) + n′(q+p′)=(mq + np) + m′(q + p') + n′(p + q')= =(mq + np)+ (m′p′ + n′q′) + (n′p + m′q), deci (mp + nq) + (m′q′ + n′p′)= = (mq + np) + (m′p′ + n′q′) adică

(mp + nq, mq + np) ~ (m′p′ + n′q′, m′q′ + n′p′).

Legea de compoziție "·" pe **Z** se numeşte **înmulțirea numerelor întregi**, iar $\overline{(mp+nq,mq+np)}$ se numeşte **produsul** numerelor întregi $\overline{(m,n)}$ şi $\overline{(p,q)}$.

Au loc următoarele:

1) **Asociativitatea.** Date numerele întregi x = $\overline{(m,n)}$, y = $\overline{(p,q)}$, z = $\overline{(r,s)}$, rezultă că

$$(xy)z = \overline{((mp+nq)r+(mq+np)s,(mp+nq)s+(mq+np)r)} =$$
$$= \overline{(mpr+nqr+mqs+nps,mps+nqs+mqr+npr)} =$$
$$= \overline{(m(pr+qs)+n(ps+qr),m(ps+qr)+n(pr+qs))} = x(yz).$$

2) **Comutativitatea.** Date numerele întregi x = $\overline{(m,n)}$, y = $\overline{(p,q)}$ rezultă că $xy = \overline{(mp+nq,mq+np)} = \overline{(pm+qn,pn+qm)} = yx$.
3) **Elementul neutru.** Să observăm că pentru orice n∈**N**, avem (n*,n) ~ (1, 0), adică $\overline{(n^*,n)} = \overline{(1,0)}$. Mai mult, pentru orice y = $\overline{(p,q)}$ ∈**Z** avem $\overline{(p,q)}\cdot\overline{(1,0)} = \overline{(1,0)}\cdot\overline{(p,q)} = \overline{(p,q)}$, adică $\overline{(1,0)}$ este elementul neutru la înmulțirea numerelor întregi.
4) **Distributivitatea înmulțirii față de adunare.** Pentru orice trei numere întregi x, y, z avem x·(y + z) = x·y + x·z.

Într-adevăr, dacă x = $\overline{(m,n)}$, y = $\overline{(p,q)}$, z = $\overline{(r,s)}$ atunci

$$x\cdot(y+z) = \overline{(m(p+r)+n(q+s),m(q+s)+n(p+r))} =$$
$$= \overline{((mp+nq)+(mr+ns),(mq+np)+(ms+nr))} = x\cdot y + x\cdot z,$$

deoarece înmulțirea numerelor naturale este distributivă față de adunarea numerelor naturale.

4. Relația de ordine pe Z

Fie $\overline{(m,n)}$, $\overline{(p,q)}$ două numere întregi.

Definiție: Spunem că $\overline{(m,n)}$ este **mai mic sau egal** față de $\overline{(p,q)}$, şi scriem $\overline{(m,n)} \le \overline{(p,q)}$, dacă m + q ≤ n+p.

Să observăm că relația binară astfel definită nu depinde de reprezentanți. Într-adevăr, dacă (m, n) ~ (m_1, n_1) şi (p, q) ~ (p_1, q_1), iar

$m + q \le n + p$, atunci $m_1 + q_1 \le n_1 + p_1$. Din $m + q \le n + p$ rezultă că $\exists u \in \mathbf{N}$: $n + p = m + q + u$, de unde $n_1 + p_1 + m + q = (m + n_1) + (q + p_1) = (n + m_1) + (p + q_1) = n + p + m_1 + q_1 = m + q + u + m_1 + q_1$, aşadar $n_1 + p_1 = m_1 + q_1 + u$, adică $m_1 + q_1 \le n_1 + p_1$.

Au loc următoarele:

1) "$\le$" este o relaţie de ordine totală pe $\mathbf{Z}$:
   - este reflexivă: $\forall \overline{(m,n)} \in \mathbf{Z}$, $\overline{(m,n)} \le \overline{(m,n)}$, deoarece $m + n \le n + m$;
   - este antisimetrică: dacă $\overline{(m,n)} \le \overline{(p,q)}$ şi $\overline{(p,q)} \le \overline{(m,n)}$, atunci $m + q \le n + p$ şi $p + n \le q + m$, de unde $m + q = n + p$, adică $(m, n) \sim (p, q)$ şi deci $\overline{(m,n)} = \overline{(p,q)}$;
   - este tranzitivă: dacă $\overline{(m,n)} \le \overline{(p,q)}$ şi $\overline{(p,q)} \le \overline{(r,s)}$, atunci $m + q \le n + p$ şi $p + s \le q + r$, de unde $m + q + p + s \le n + p + q + r$; urmează că $m + s \le n + r$, adică $\overline{(m,n)} \le \overline{(r,s)}$;
   - pentru orice $\overline{(m,n)}$ şi $\overline{(p,q)}$ numere întregi avem $\overline{(m,n)} \le \overline{(p,q)}$ sau $\overline{(p,q)} \le \overline{(m,n)}$; aceasta rezultă din faptul că pentru numerele naturale $m + q$ şi $n + p$ avem $m + q \le n + p$ sau $p + n = n + p \le m + q = q + m$.
2) OA : Pentru orice $x, y, z \in \mathbf{Z}$, avem $x \le y \Leftrightarrow x + z \le y + z$. Verificarea acestei afirmaţii este lăsată ca exerciţiu.
   OM : Dacă $x, y \in \mathbf{Z}$, $x \le y$, atunci pentru orice $z \in \mathbf{Z}$, avem $xz \le yz$ şi pentru orice $z \in \mathbf{Z}$, $z \le 0$, avem $yz \le xz$, unde cu 0 am notat numărul întreg $\overline{(0,0)}$.

Să arătăm că dacă $x \le y$ şi $z \le \overline{(0,0)}$, atunci $yz \le xz$. Fie $x = \overline{(m,n)}$, $y = \overline{(p,q)}$, $z = \overline{(r,s)}$. Din $x \le y$ rezultă că $m + q \le n + p$, iar din $z \le 0$ rezultă că $r \le s$, deci $\exists u \in \mathbf{N}$: $s = r + u$.

Avem $yz = \overline{(pr + qs, ps + qr)} = \overline{(pr + qr + qu, pr + pu + qr)}$, iar $xz = \overline{(mr + ns, ms + nr)} = \overline{(mr + nr + nu, mr + mu + nr)}$.

$yz \le xz \Leftrightarrow pr + qr + qu + mr + mu + nr \le pr + pu + qr + mr + nr + nu \Leftrightarrow$
$\Leftrightarrow qu + mu \le pu + nu \Leftrightarrow (m + q)u \le (n + p)u$, care este adevărată deoarece $m + q \le n + p$. Deci, $yz \le xz$.

Similar se arată că dacă $x \le y$ şi $z \in \mathbf{Z}$, $0 \le z$, atunci $xz \le yz$.

Definiție. Spunem că $\overline{(m,n)}$ este **mai mic** decât $\overline{(p,q)}$ şi scriem $\overline{(m,n)} < \overline{(p,q)}$ dacă $m + q < n + p$.

5. Principiul trihotomiei numerelor întregi

Oricare două numere întregi x, y se află în una şi numai una dintre situațiile: $x < y$, $x = y$, $y < x$.

Demonstrația are la bază faptul că principiul trihotomiei are loc pentru numere naturale.

Au loc şi:

- pentru orice x, y, $z \in \mathbf{Z}$, avem $x < y \Leftrightarrow x + z < y + z$;
- dacă x, y, $z \in \mathbf{Z}$, $0 < z$, atunci $x < y \Leftrightarrow xz < yz$;
- dacă x, y, $z \in \mathbf{Z}$, $z < 0$, atunci $x < y \Leftrightarrow yz < xz$.

Pentru a verifica implicația "$\Leftarrow$" din afirmațiile anterioare se foloseşte principiul trihotomiei numerelor întregi.

Observație: Fie $\overline{(m,n)} \in \mathbf{Z}$.

i) $\overline{(0,0)} < \overline{(m,n)} \Leftrightarrow n < m \Leftrightarrow \exists u \in \mathbf{N}$, $u \neq 0$, astfel încât $m = n + u$.

Avem $\overline{(m,n)} = \overline{(n+u,n)} = \overline{(u,0)}$, unde $u \in \mathbf{N}$, $u \neq 0$.

ii) $\overline{(m,n)} < \overline{(0,0)} \Leftrightarrow m < n \Leftrightarrow \exists v \in \mathbf{N}$, $v \neq 0$, astfel încât $n = m + v$.

Avem $\overline{(m,n)} = \overline{(m,m+v)} = \overline{(0,v)}$, unde $v \in \mathbf{N}$, $v \neq 0$.

În plus, simetricul la adunare al elementului $\overline{(u,0)}$ este $\overline{(0,u)}$.

Definim funcția $\varphi : \mathbf{N} \to \mathbf{Z}$, $\varphi(a) = \overline{(a,0)}$, pentru orice $a \in \mathbf{N}$.

Se verifică uşor următoarele proprietăți ale lui φ:

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\forall a, b \in \mathbf{N}$;
2. $\varphi(0) = \overline{(0,0)}$;
3. $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, $\forall a, b \in \mathbf{N}$;
4. $\varphi(1) = \overline{(1,0)}$;
5. este injectivă;

6. $\varphi(a) \le \varphi(b) \Leftrightarrow a \le b$, unde $a, b \in \mathbf{N}$ (se mai spune că φ păstrează ordinea).

Fie $N' = \{\overline{(a,0)} \in \mathbf{Z} \mid a \in \mathbf{N}\}$ mulțimea imaginilor lui φ. Obținem că $\psi : \mathbf{N} \to N'$, $\psi(a) = \varphi(a)$, pentru orice $a \in \mathbf{N}$, este o bijecție. În cele ce urmează vom identifica pe $\mathbf{N}$ cu N', adică pentru orice $u \in \mathbf{N}$, identificăm u cu $\overline{(u,0)}$. Putem atunci considera că avem $\mathbf{N} \subset \mathbf{Z}$.

Vom nota cu –u pe $\overline{(0,u)}$, unde $u \in \mathbf{N}$.

6. Scăderea numerelor întregi

Dacă x, y sunt două numere întregi, notăm cu x–y suma x + (–y).
Legea de compoziție $\varphi : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ definită prin $\varphi(x, y) = x–y$ se numeşte **scăderea** numerelor întregi.

Au loc următoarele:

- Pentru orice două numere întregi x şi y avem $x–y = 0 \Leftrightarrow x = y$.

Într-adevăr, dacă x =y avem x–y = x–x = x + (–x) = 0, deoarece - x este simetricul lui x. Reciproc, dacă x–y = 0, avem y = 0 + y = (x–y) + y = =[x + (–y)] + y = x + [(–y) + y] = x + 0 = x. Din x + y + (–x) + (–y) = 0 rezultă că - (x + y) = (–x) + (–y).
Egalitatea –(x–y) = (–x) + y rezultă astfel: –(x–y) = –[x + (–y)] = =(–x)–(–y) = (–x) + y.
Analog se demonstrează că –(–x + y) = x–y şi că –(–x–y) = x + y.

- Pentru oricare trei numere întregi x, y, z avem x(y–z) = xy–xz.

Într-adevăr, avem x(y–z) + xz = x[(y–z) + z] = xy, de unde rezultă că xy–xz =[x(y–z) + xz] + (–xz) = x(y–z).

Observație: Pentru $x, y \in \mathbf{Z}$, avem $xy = 0 \Leftrightarrow x = 0$ sau y = 0.

Demonstrație: "⇐": Considerăm $x = 0 = \overline{(0,0)}$, $y = \overline{(m,n)}$. Rezultă că $xy = \overline{(0,0)} \cdot \overline{(m,n)} = \overline{(0,0)}$.

"⇒": Dacă $0 \le x$ şi $0 \le y$, atunci $x = \overline{(u,0)}$, $y = \overline{(v,0)}$, unde $u, v \in \mathbf{N}$. Rezultă că $xy = \overline{(uv,0)}$ şi cum $xy = 0 = \overline{(0,0)}$ rezultă că uv = 0, de unde u = 0 sau v = 0, adică x = 0 sau y = 0.

Similar, dacă $x \le 0$ şi $y \le 0$, atunci $x = \overline{(0,u)}$, $y = \overline{(0,v)}$, unde $u, v \in \mathbf{N}$. $xy = \overline{(uv,0)} = \overline{(0,0)}$, deci $u = 0$ sau $v = 0$, adică $x = 0$ sau $y = 0$.

Pentru $0 \le x$ şi $y \le 0$, $x = \overline{(u,0)}$ şi $y = \overline{(0,v)}$ unde $u, v \in \mathbf{N}$. Atunci $xy = \overline{(0,uv)} = \overline{(0,0)}$, deci $u = 0$ sau $v = 0$, adică $x = 0$ sau $y = 0$.

Analog se tratează cazul $x \le 0$ şi $0 \le y$.

Să remarcăm faptul că demonstrația poate fi făcută şi folosind identificarea numerelor întregi pozitive cu numerele naturale.

Dacă x, y, z sunt numere întregi, avem $xy = xz$ şi $x \neq 0 \Rightarrow y = z$. Într-adevăr, din egalitatea $xy = xz$ rezultă că $x(y-z) = xy-xz = 0$. Deoarece $x \neq 0$ rezultă că $y-z = 0$, adică $y = z$.

Definiție: Se numeşte **modulul** unui număr întreg x, numărul natural notat cu |x|, definit astfel: $|x| = \begin{cases} x, \text{dacă } \mathbf{x > 0} \\ 0, \text{dacă } x = 0 \\ -x, \text{dacă } x < 0 \end{cases}$.

7. Teorema împărțirii cu rest pentru numere întregi

Pentru orice două numere întregi x şi y, $y \neq 0$, există şi sunt unice numerele întregi q şi r, astfel încât $x = yq + r$ şi $0 \le r < |y|$.

Demonstrație: Dacă $x, y \in \mathbf{N}$, $y \neq 0$, atunci aplicăm teorema cu rest pentru numere naturale şi obținem că există q, $r \in \mathbf{N}$, deci întregi, astfel încât $0 \le r < y = |y|$.

Dacă $x \le 0$, iar $y > 0$, atunci pentru |x| şi y există q_1, r_1 naturale, deci întregi, astfel încât $-x = |x| = yq_1 + r_1$ şi $0 \le r_1 < y = |y|$. Avem $x = y(-q_1)-r_1$. Dacă $r_1 = 0$, atunci $q = -q_1$ şi $r = 0$. Dacă $0 < r_1$, atunci $x = y(-q_1-1) + y-r_1$.

Considerăm $q = -q_1-1 \in \mathbf{Z}$ şi $r = y-r_1 > 0$ şi $r < y = |y|$.

Dacă $x \ge 0$ şi $y < 0$, atunci aplicăm teorema împărțirii cu rest pentru numerele naturale x şi |y|. Rezultă că $\exists q_2, r_2 \in \mathbf{N}$: $x = |y|q_2 + r_2$ şi $0 \le r_2 < |y|$, de unde $x = y(-q_2) + r_2$. Alegem $q = -q_2$ şi $r_2 = r$.

Dacă $x \le 0$ şi $y < 0$, atunci $\exists q_3, r_3 \in \mathbf{N}$: $|x| = |y|q_3 + r_3$ şi $0 \le r_3 < |y|$, adică $-x = (-y)q_3 + r_3$ şi $0 \le r_3 < |y|$.

Dacă $r_3 = 0$, atunci $x = yq_3$ şi alegem $q = q_3$ şi $r = 0$.

Dacă $r_3 > 0$, atunci $x = yq_3 - r_3 = y(q_3 + 1) + (-y - r_3)$. Alegem $q = q_3 + 1$ şi $r = -y - r_3 > 0$ şi $r < -y = |y|$.

Verificăm acum unicitatea numerelor q şi r. Presupunem că $yq + r = yq' + r'$, cu $0 \le r < |y|$ şi $0 \le r' < |y|$. Rezultă că $y(q-q') = r'-r$, deci $yu = r'-r$, unde $u = q-q'$. Deoarece $|ab| = |a|\cdot|b|$, pentru orice $a, b \in \mathbf{Z}$, obţinem că $|y|\cdot|u| = |r'-r|$.

Dacă $r' \le r$, atunci $0 \le r - r' \le r < |y|$, iar dacă $r \le r'$, atunci $0 \le r'-r \le r' < |y|$. În ambele cazuri, avem $|r - r'| < |y|$.

Pe de altă parte, presupunând că $u \ne 0$ rezultă că $|u| \ge 1$, deci $|y|\cdot|u| \ge |y|$, de unde $|r'-r| \ge |y|$, contradicţie. Aşadar, $u = 0$, deci $q = q'$ şi $r = r'$.

8. Semnul unui număr întreg. Regula semnelor

Definim funcţia **semn**, notată $\text{sgn} : \mathbf{Z} \to \mathbf{Z}$ prin

$$\text{sgn}(x) = \begin{cases} 1, \text{dacă } x \in Z, x > 0 \\ 0, \text{dacă } x = 0 \\ -1, \text{dacă } x \in Z, x < 0 \end{cases}$$

Egalitatea $\text{sgn}(xy) = \text{sgn}(x)\cdot\text{sgn}(y)$ este valabilă pentru orice numere întregi x şi y şi se numeşte **regula semnelor**.

Vom demonstra acum regula semnelor analizând toate situaţiile posibile.

Dacă x şi y sunt numere întregi pozitive $x = \overline{(m,0)}$, $y = \overline{(n,0)}$, avem $xy = \overline{(mn,0)}$, deci xy este un număr întreg pozitiv.
Avem $\text{sgn}(xy) = 1 = 1\cdot 1 = \text{sgn}(x)\cdot\text{sgn}(y)$.

Dacă x este întreg pozitiv $x = \overline{(m,0)}$ şi y este întreg negativ $y = \overline{(0,n)}$, avem $xy = \overline{(m0 + 0n, mn + 00)} = \overline{(0,mn)}$, deci xy este număr negativ. Avem $\text{sgn}(xy) = -1 = 1\cdot(-1) = \text{sgn}(x)\cdot\text{sgn}(y)$.

Analog se verifică egalitatea pentru x întreg negativ şi y întreg pozitiv.

Dacă x şi y sunt întregi negative $x = \overline{(0,m)}$ şi $y = \overline{(0,n)}$, avem $xy = \overline{(00 + mn, 0n + m0)} = \overline{(mn,0)}$, deci xy este un număr întreg pozitiv şi avem $\text{sgn}(xy) = 1 = (-1)\cdot(-1) = \text{sgn}(x)\cdot\text{sgn}(y)$.

2.3. Mulțimea numerelor raționale

1. Construcția lui Q

Notăm cu $\mathbf{Z}^*$ mulțimea numerelor întregi nenule şi definim pe $\mathbf{Z} \times \mathbf{Z}^*$ următoarea relație: dacă $(x, y), (z, t) \in \mathbf{Z} \times \mathbf{Z}^*$, $(x, y) \sim (z, t)$ dacă $xt = yz$.

Aceasta este o relație de echivalență:

- este reflexivă, deoarece $xy = yx$, deci $(x, y) \sim (y, x)$, pentru orice $(x, y) \in \mathbf{Z} \times \mathbf{Z}^*$;
- este simetrică, deoarece presupunând $(x, y) \sim (z, t)$ rezultă $xt = yz$, deci $zy = tx$, adică $(z, t) \sim (x, y)$;
- este tranzitivă, deoarece presupunând $(x, y) \sim (z, t)$ şi $(z, t) \sim (u, v)$ rezultă $xt = yz$, $zv = tu$ şi deci: $(xv)t = (xt)v = =(yz)v = y(zv) =y(tu) = (yu)t$ şi cum $t \neq 0$, obținem $xv=yu$, adică $(x, y) \sim (u, v)$.

Clasa de echivalență a lui (x, y) o vom nota cu:

$\overline{\frac{x}{y}} = \{(z, t) | (x, y) \sim (z, t)\}$.

Definiție: Mulțimea factor $(\mathbf{Z} \times \mathbf{Z}^*) / \sim = \{\overline{\frac{x}{y}} \mid (x, y) \in \mathbf{Z} \times \mathbf{Z}^*\}$ se numeşte **mulțimea numerelor raționale** şi se notează cu **Q.**

Se numeşte **număr rațional** orice element $\overline{\frac{x}{y}}$ al lui **Q** .

Observație: Pentru orice pereche $(x, y) \in \mathbf{Z} \times \mathbf{Z}^*$ şi pentru orice element $z \in \mathbf{Z}^*$, avem $yz \in \mathbf{Z}^*$, deci $(xz, yz) \in \mathbf{Z} \times \mathbf{Z}^*$.

Deoarece $x(yz) = y(xz)$, rezultă că $(x, y) \sim (xz, yz)$, adică $\frac{x}{y} = \frac{xz}{yz}$.

Considerăm aplicația $i : \mathbf{Z} \to \mathbf{Q}$, $i(x) = \overline{\frac{x}{1}}$, pentru orice $x \in \mathbf{Z}$.

Aplicația i este injectivă.

Într-adevăr, $i(x) = i(y) \Rightarrow \frac{x}{1} = \frac{y}{1} \Rightarrow (x, 1) \sim (y, 1) \Rightarrow x \cdot 1 = y \cdot 1 \Rightarrow x = y$.

Faptul că i este o aplicație injectivă ne permite să nu mai facem distincție între numărul întreg n şi numărul rațional $i(n) = \frac{n}{1}$ (vom abuza de acest fapt scriind $n = \frac{n}{1}$).

Prin urmare, vom considera $\mathbf{Z} \subseteq \mathbf{Q}$, iar i este **incluziunea canonică a lui Z în Q.**

2. Adunarea numerelor raționale

Definim "+" : $\mathbf{Q} \times \mathbf{Q} \to \mathbf{Q}$, $\frac{x}{y} + \frac{z}{t} = \frac{xt + yz}{yt}$. "+" este bine definită. Într-adevăr, dacă (x, y) ~ (x', y') şi (z, t) ~ (z', t') atunci xy' = yx' şi zt' = tz', de unde:
(xt + yz) y't' = (xy')(tt') + (zt')(yy') = (yx')(tt') + (tz') (yy') = =(x't' + y'z')yt ceea ce arată că (xt +yz, yt) ~ (x't' +y'z', y't').

Dacă $x = \frac{x}{1}$ şi $y = \frac{y}{1}$ sunt două numere întregi atunci $x + y = \frac{x+y}{1}$ este tot un număr întreg.

Prin urmare, mulțimea **Z** a numerelor întregi este parte stabilă a lui **Q** relativ la "+" şi legea de compoziție indusă de "+" pe **Z** este exact adunarea numerelor întregi.

Legea de compoziție "+" se numeşte **adunarea numerelor raționale**, iar $\frac{xt + yz}{yt}$ se numeşte **suma** numerelor raționale $\frac{x}{y}$ şi $\frac{z}{t}$.

Observație: **Adunarea numerelor raționale este asociativă, comutativă, are element neutru şi orice număr rațional este simetrizabil.**

Demonstrație:

i) **asociativitatea:**

Fie $\frac{x}{y}, \frac{z}{t}, \frac{u}{v} \in \mathbf{Q}$

$$\left(\frac{x}{y}+\frac{z}{t}\right)+\frac{u}{v}=\frac{xt+yz}{yt}+\frac{u}{v}=\frac{(xt+yz)v+(yt)u}{(yt)v}=$$

$$=\frac{x(tv)+y(zv+tu)}{y(tv)}=\frac{x}{y}+\frac{zv+tu}{tv}=\frac{x}{y}+\left(\frac{z}{t}+\frac{u}{v}\right)$$

ii) **comutativitatea**:

Fie $\frac{x}{y}, \frac{z}{t} \in \mathbf{Q}$. Avem $\frac{x}{y}+\frac{z}{t}=\frac{xt+yz}{yt}=\frac{zy+tx}{ty}=\frac{z}{t}+\frac{x}{y}$;

iii) **element neutru:** numărul raţional $0=\frac{0}{1}$ este element neutru faţă de adunarea numerelor raţionale. În adevăr, $\forall \frac{x}{y} \in \mathbf{Q}$, avem $\frac{x}{y}+0=\frac{x}{y}+\frac{0}{1}=\frac{x\cdot 1+y\cdot 0}{y\cdot 1}=\frac{x}{y}$.

iv) **elemente simetrizabile:** $\forall \frac{x}{y} \in \mathbf{Q}$, $\exists \frac{-x}{y} \in \mathbf{Q}$ încât $\frac{-x}{y}=-\frac{x}{y}$, adică $\frac{-x}{y}$ este simetricul lui $\frac{x}{y}$ în raport cu adunarea.

Într-adevăr $\frac{x}{y}+\frac{-x}{y}=\frac{x+(-x)}{y}=\frac{0}{y}=\frac{0\cdot y}{y}=\frac{0}{1}=0$, de unde $-\frac{x}{y}=\frac{-x}{y}$.

Legea de compoziţie $\varphi : \mathbf{Q}\times\mathbf{Q}\to\mathbf{Q}$, $\varphi(r, s)= r+(-s)$ se numeşte **scăderea numerelor raţionale**. Numărul $r - s = r + (-s)$ se numeşte diferenţa numerelor raţionale r şi s.

Proprietăţi ale scăderii numerelor raţionale:

$r - s = 0 \Leftrightarrow r = s$;

$-(-r) = r$;

$-(r + s) = (-r) + (-s)$; $-(r - s) = (-r) + s$;

$-(-r + s) = r - s$; $-(-r - s) = r + s$.

3. **Înmulțirea numerelor raționale**

Definim "$\cdot$" : $\mathbf{Q} \times \mathbf{Q} \to \mathbf{Q}$, $\frac{x}{y} \cdot \frac{z}{t} = \frac{xz}{yt}$. "$\cdot$" este bine definită. Într-adevăr, dacă (x, y) ~ (x', y') şi (z, t) ~ (z', t'), atunci avem xy' = yx' şi zt' = tz'. Atunci (xz) (y't') = (xy') (zt') = (yx') (tz') = (yt) (x'z'), ceea ce arată că (xz, yt) ~ (x'z', y't').

Dacă $x = \frac{x}{1}$ şi $y = \frac{y}{1}$ sunt două numere întregi atunci $x \cdot y = \frac{x \cdot y}{1}$ este tot un număr întreg.

Prin urmare, mulțimea $\mathbf{Z}$ a numerelor întregi este parte stabilă a lui $\mathbf{Q}$ relativ la "$\cdot$" şi legea de compoziție indusă de "$\cdot$" pe $\mathbf{Z}$ este exact înmulțirea numerelor întregi.

Legea de compoziție "$\cdot$" se numeşte **înmulțirea numerelor raționale**, iar $\frac{x \cdot z}{yt}$ se numeşte **produsul** numerelor raționale $\frac{x}{y}$ şi $\frac{z}{t}$.

Observație: **Înmulțirea numerelor raționale este asociativă, comutativă, are element neutru şi orice număr rațional nenul este simetrizabil.**

Demonstrație:

i) asociativitatea:

Fie $\frac{x}{y}, \frac{z}{t}, \frac{u}{v} \in \mathbf{Q}$.

$$\left(\frac{x}{y} \cdot \frac{z}{t}\right) \cdot \frac{u}{v} = \frac{x \cdot z}{yt} \cdot \frac{u}{v} = \frac{(x \cdot z) \cdot u}{(yt)v} = \frac{x(zu)}{y(tv)} = \frac{x}{y} \cdot \left(\frac{z}{t} \cdot \frac{u}{v}\right)$$

ii) comutativitatea:

Fie $\frac{x}{y}, \frac{z}{t} \in \mathbf{Q}$. $\frac{x}{y} \cdot \frac{z}{t} = \frac{x \cdot z}{yt} = \frac{z \cdot x}{ty} = \frac{z}{t} \cdot \frac{x}{y}$;

iii) element neutru: numărul rațional $1 = \frac{1}{1}$ este element neutru față de înmulțirea numerelor raționale, deoarece,

pentru orice număr rațional $\frac{x}{y}$, avem $\frac{x}{y} \cdot 1 = \frac{x}{y} \cdot \frac{1}{1} = \frac{x \cdot 1}{y \cdot 1} = \frac{x}{y}$;

iv) **elemente simetrizabile:** Numărul rațional $0 = \frac{0}{1}$ nu este simetrizabil în raport cu înmulțirea numerelor raționale deoarece pentru orice $\frac{x}{y} \in \mathbf{Q}$, avem:

$\frac{x}{y} \cdot \frac{0}{1} = \frac{x \cdot 0}{y \cdot 1} = \frac{0}{y} = \frac{0 \cdot y}{y} = \frac{0}{1} = 0.$

Deci nu există nici un număr rațional r, încât $r \cdot 0 = 1$.

Pe de altă parte, orice număr rațional $r \neq 0$ este simetrizabil în raport cu înmulțirea numerelor raționale. Observăm că pentru $r = \frac{x}{y}$ avem: $r = 0 \Leftrightarrow \frac{x}{y} = \frac{0}{1} \Leftrightarrow x \cdot 1 = y \cdot 0 \Leftrightarrow x = 0$, deci $r \neq 0 \Leftrightarrow x \neq 0$.

Astfel, pentru $r = \frac{x}{y} \neq 0$, putem considera numărul rațional $\frac{y}{x}$ şi vom avea: $\frac{x}{y} \cdot \frac{y}{x} = \frac{x \cdot y}{y \cdot x} = \frac{1 \cdot x \cdot y}{1 \cdot y \cdot x} = \frac{1}{1} = 1.$

Pentru un număr rațional nenul r, notăm cu r^{-1} simetricul lui r, în raport cu înmulțirea. Avem $\left(\frac{x}{y}\right)^{-1} = \frac{y}{x}$.

Dacă r şi s $\in \mathbf{Q}$, $s \neq 0$, atunci notăm $r : s = r \cdot s^{-1}$ şi spunem că r : s este rezultatul **împărțirii** lui r la s.

Deci, $\left(\frac{x}{y}\right) : \left(\frac{z}{t}\right) = \frac{x}{y} \cdot \frac{t}{z}$

Observație: Are loc şi **distributivitatea înmulțirii față de adunare**.

Pentru $\frac{x}{y}, \frac{z}{t}, \frac{u}{v} \in \mathbf{Q}$, avem $\frac{x}{y}\cdot\left(\frac{z}{t}+\frac{u}{v}\right)=\frac{x}{y}\cdot\frac{z}{t}+\frac{x}{y}\cdot\frac{u}{v}$.

Într-adevăr,

$$\frac{x}{y}\cdot\left(\frac{z}{t}+\frac{u}{v}\right)=\frac{x}{y}\cdot\frac{zv+tu}{tv}=\frac{x(zv+tu)}{y(tv)}=\frac{xzv+xtu}{ytv}=\frac{xzv}{ytv}+\frac{xtu}{ytv}=$$

$$=\frac{xz}{yt}+\frac{xu}{yv}=\frac{x}{y}\cdot\frac{z}{t}+\frac{x}{y}\cdot\frac{u}{v}$$

4. Semnul unui număr raţional

Fie r $\in$**Q** şi (x, y), (z, t) $\in$**Z**$\times$ **Z***, r = $\frac{x}{y}=\frac{z}{t}$. Rezultă xt = yz, de unde :

sgn(x)$\cdot$ sgn(t) = sgn(y) $\cdot$ sgn(z). Din y $\neq$ 0 $\neq$ t, rezultă sgn(y) $\neq$ 0 $\neq$ $\neq$sgn(t), de unde: $\frac{\operatorname{sgn}(x)}{\operatorname{sgn}(y)}=\frac{\operatorname{sgn}(z)}{\operatorname{sgn}(t)}$.

Aşadar, numărul $\frac{\operatorname{sgn}(x)}{\operatorname{sgn}(y)}$ nu depinde de reprezentantul (x, y) al lui r, ci doar de r şi-l vom nota cu sgn(r).

Anume, dacă r = $\frac{x}{y}$, sgn (r) = $\frac{\operatorname{sgn}(x)}{\operatorname{sgn}(y)}=\begin{cases}1, \textit{dacă } \operatorname{sgn}(x)=\operatorname{sgn}(y);\\ 0, \textit{dacă } x=0\\ -1, \textit{dacă } \operatorname{sgn}(x)\neq\operatorname{sgn}(y);\end{cases}$

sgn(r) se numeşte **semnul numărului raţional** r, iar funcţia sgn:**Q**$\rightarrow$**Z** se numeşte **funcţia semn**.

Spunem că numărul raţional r este **pozitiv** dacă sgn(r) = 1 şi **negativ** dacă sgn(r) = -1 şi avem sgn(r) = 0 $\Leftrightarrow$ r = 0.

Mai mult,oricare ar fi r şi s două numere raţionale r = $\frac{x}{y}$, s = $\frac{z}{t}$,

sgn(rs) = $\frac{\operatorname{sgn}(xz)}{\operatorname{sgn}(yt)}=\frac{\operatorname{sgn}(x)\cdot\operatorname{sgn}(z)}{\operatorname{sgn}(y)\cdot\operatorname{sgn}(t)}=\frac{\operatorname{sgn}(x)}{\operatorname{sgn}(y)}\cdot\frac{\operatorname{sgn}(z)}{\operatorname{sgn}(t)}=$ sgn(r) $\cdot$ sgn(s)

Remarcăm faptul că $\forall$ r = $\frac{x}{y} \in \mathbf{Q}$, avem r = $\frac{x}{y} = \frac{-x}{-y}$ de unde rezultă că orice număr raţional poate fi scris ca fracţie cu numitorul număr întreg pozitiv.

Dacă r = $\frac{x}{y}$ şi y $\in$ **N***, atunci avem sgn(r) = $\frac{\operatorname{sgn}(x)}{\operatorname{sgn}(y)} = \frac{\operatorname{sgn}(x)}{1} =$ =sgn(x), adică r are acelaşi semn cu numărătorul x.

5. Relaţia de ordine pe mulţimea numerelor raţionale

Definiţie: Dacă r şi s sunt numere raţionale, scriem r < s şi citim "r este mai mic decât s " dacă diferenţa s – r este un număr raţional pozitiv.

Scriem r ≤ s şi citim "r este mai mic sau egal cu s" dacă r < s sau r = s.

Consider r şi s două numere raţionale r = $\frac{x}{y}$, s = $\frac{z}{t}$ şi presupunem că numitorii y şi t sunt pozitivi. Putem scrie r = $\frac{x}{y} = \frac{xt}{yt}$, s = $\frac{z}{t} = \frac{yz}{yt}$.

Aşadar, orice două numere raţionale r şi s pot fi scrise ca fracţii cu acelaşi numitor care să fie pozitiv: r = $\frac{x}{u}$, s = $\frac{z}{u}$, unde u > 0.

Avem s – r = $\frac{z-x}{u}$ de unde sgn(s - r) = sgn(z - x) sau, altfel spus, r ≤ s ⇔ x ≤ z.

Propoziţie: Relaţia "≤" este o relaţie de ordine totală pe **Q**.

Demonstraţie: Se foloseşte faptul că oricare două numere raţionale pot fi scrise ca fracţii cu acelaşi numitor, care să fie întreg pozitiv şi apoi concluzia că "≤" este o relaţie de ordine totală pe **Q** rezultă din accea că "≤" este o relaţie de ordine totală pe **Z**.

Propoziţie: Pentru orice numere raţionale r, s, u au loc afirmaţiile:

a) r < s ⇒ r + u < s + u;

b) $r < s$ şi $u > 0 \Rightarrow ru < su$;

c) $r < s \Rightarrow -s < -r$;

d) $0 < r < s \Rightarrow r^2 < s^2$.

Demonstrație: Putem presupune că $r = \frac{x}{t}$, $s = \frac{y}{t}$, $u = \frac{z}{t}$, unde $t \in \mathbf{N^* = N} \setminus \{0\}$.

Folosind proprietățile analoage relației "<" definite pe **Z**, obținem:

a) $r < s \Rightarrow x < y \Rightarrow x + z < y + z \Rightarrow \frac{x+z}{t} < \frac{y+z}{t} \Rightarrow r + u < s + u$;

b) $r < s$ şi $u > 0 \Rightarrow x < y$ şi $z > 0 \Rightarrow xz < yz \Rightarrow \frac{xz}{t} < \frac{yz}{t} \Rightarrow ru < su$;

c) $r < s \Rightarrow x < y \Rightarrow -y < -x \Rightarrow -\frac{y}{t} < -\frac{x}{t} \Rightarrow -s < -r$;

d) $0 < r < s \Rightarrow 0 < x < y \Rightarrow 0 < x^2 < y^2 \Rightarrow \frac{0}{t^2} < \frac{x^2}{t^2} < \frac{y^2}{t^2} \Rightarrow 0 < r^2 < s^2$.

Menționăm şi că, spre deosebire de **N** şi **Z**, pentru **Q** are loc **proprietatea de densitate**, anume pentru orice $a, b \in \mathbf{Q}$, $a < b$, există $c \in \mathbf{Q}$, aşa încât $a < c < b$.

Într-adevăr $c = \frac{a+b}{2}$ satisface condiția anterioară.

6. Modulul unui număr rațional

Prin orice număr rațional r, definim $|r| = r \cdot \operatorname{sgn}(r)$. Numărul $|r|$ se numeşte **modulul lui r** sau **valoarea absolută a lui r.**

Utilizând definiția modulului unui număr întreg, obținem că pentru $r = \frac{x}{y}$, avem $|r| = r \cdot \operatorname{sgn}(r) = \frac{x}{y} \cdot \frac{\operatorname{sgn}(x)}{\operatorname{sgn}(y)} = \frac{x \cdot \operatorname{sgn}(x)}{y \cdot \operatorname{sgn}(y)} = \frac{|x|}{|y|}$.

Folosind procedeul reducerii la acelaşi numior, sau făcând raționamente absolut analoage cu cele din cazul numerelor întregi, se obține:

$$|r| = \begin{cases} r, \text{ dacă } r > 0; \\ 0, \text{ dacă } r = 0; \\ -r, \text{ dacă } r < 0. \end{cases}$$

$$|r| \geq 0;$$

$$|r| = 0 \Leftrightarrow r = 0;$$

$$|r \cdot s| = |r| \cdot |s|;$$

$$|r + s| \leq |r| + |s|.$$

2.4. Sisteme de numerație

1. Generalități

Găsirea unor procedee de scriere a numerelor, care să permită o rapidă estimare a ordinului lor de mărime, cât şi elaborarea de reguli simple pentru a efectua principalele operații cu acestea, s-a impus din cele mai vechi timpuri.

Adoptarea sistemului de numerație zecimal s-a încheiat abia în secolele XVI – XVII, când acesta a cunoscut o largă răspândire în Europa.

În cele ce urmează, vom reprezenta numerele naturale în baza u, unde u este un număr natural, u > 1.

Teoremă: Dacă $u \in \mathbf{N}$, $u > 1$, atunci, oricare ar fi numărul natural $x > 0$, există numerele naturale n, x_0, x_1, ..., x_n, astfel încât: $x = x_n \cdot u^n + ...+ x_1 \cdot u + x_0$, unde $\forall\, i \in \{0, 1, 2,.., n\}$, $0 \leq x_i < u_n$ şi $x_n \neq 0$.

Demonstrație:

Vom arăta că au loc egalitățile:

$x = u \cdot q_0 + x_0, \quad 0 \leq x_0 < u,$

$q_0 = u \cdot q_1 + x_1, \quad 0 \leq x_1 < u,$

.....

$q_{n-2} = u \cdot q_{n-1} + x_{n-1}, \quad 0 \leq x_{n-1} < u,$

$q_{n-1} = x_n, \quad 0 \leq x_n < u,$

Dacă $x < u$, atunci avem $x = u \cdot 0 + x$ şi $0 < x < u$, deci putem considera $n = 0$, $q_0 = 0$, $x_0 = x$.

Dacă $x \geq u$, atunci vom folosi sucesiv teorema împărțirii cu rest. Avem:

$\exists\, q_0, x_0 \in \mathbf{N}$, astfel încât $x = u \cdot q_0 + x_0$, $0 \leq x_0 < u$. Deoarece $x \geq u$, avem $q_0 > 0$. Fie $q_1, x_1 \in \mathbf{N}$, astfel încât $q_0 = u \cdot q_1 + x_1$, $0 \leq x_1 < u$.

Dacă $q_1 = 0$, atunci $q_0 = x_1$ şi deci n = 1.

Dacă $q_1 \neq 0$ atunci, există q_2, $x_2 \in \mathbf{N}$, aşa încât $q_1 = u \cdot q_2 + x_2$, $0 \leq x_2 < u$.

şi procedeul se continuă.

Dacă $q_i \neq 0$, avem:

$q_i < u \cdot q_i \leq u \cdot q_i + x_i = q_{i-1}$, aşadar $x > q_0 > q_1 > ... > q_{i-1} > q_i > ... \geq 0$.

Notăm $A = \{q_i \mid q_i \neq 0\}$; avem $A \subseteq \mathbf{N}$, $A \neq \varnothing$ şi atunci conform cu P.B.O. rezultă că A are un cel mai mic element, pe care-l vom nota cu q_{n-1}. Din $q_n < q_{n-1}$ rezultă $q_n = 0$. Deci, $0 < q_{n-1} = x_n < u$ şi procedeul se încheie la acest pas. Înmulțind acum egalitățile obținute respectiv cu 1, u, u^2, .., u^n şi adunându-le membru cu membru, rezultă egalitatea din enunț.

Lemă: Dacă u, x_0, x_1, ..., x_n sunt numere naturale astfel încât $u > 1$, $0 \leq x_i < u$ pentru $0 \leq i < n-1$ şi $0 < x_n < u$, atunci:

$$\sum_{i=0}^{n} x_i u^i < u^{n+1}$$

.

Demonstrație: Pentru orice $i \in \{0,1,...,n-1\}$ avem $x_i \leq u - 1$ şi deci:

$$\sum_{i=0}^{n} x_i u^i \leq \sum_{i=0}^{n} (u-1)u^i = u^{n+1} - 1 < u^{n+1}$$

.

Teoremă: Dacă $u > 1$ este un număr natural, atunci oricare ar fi numărul natural $x > 0$, acesta se scrie **în mod unic** sub forma:

$$x = x_n u^n + x_{n-1} u^{n-1} + ... + x_1 \cdot u + x_0,$$

unde $n \in \mathbf{N}$ şi $\forall\, i \in \{0, 1, ..., n\}$, avem $x_i \in \mathbf{N}$, $0 \leq x_i < u$ şi $0 < x_n < u$.

Demonstrație: Conform teoremei anterioare, rezultă că există numerele naturale n, x_0, x_1, ..., x_n, astfel încât:

$x = x_n u^n + x_{n-1} u^{n-1} + ... + x_1 \cdot u + x_0$, unde $\forall i \in \{0, 1, .., n\}$, $0 \leq x_i < u$ şi $x_n \neq 0$.

Verificăm acum unicitatea numerelor n, x_0, x_1, ..., x_n. Presupunem că există, de asemenea, numerele naturale m, y_0, y_1, ..., y_m, aşa încât $x = y_m u^m + y_{m-1} u^{m-1} + ... + y_1 \cdot u + y_0$, unde $\forall\, i \in \{0,1,...,m-1\}$, $0 \leq y_i < u$ şi $0 < y_m < u$.

Să arătăm că $m = n$.

Presupunem că $n < m$, adică $n + 1 \leq m$. Avem:

$$x = \sum_{i=0}^{n} x_i u^i < u^{n+1} \leq u^m \leq y_m u^m \leq \sum_{i=0}^{m} y_i u^i = x$$

,

contradicție.

În mod similar, presupunând m < n, obținem, de asemenea, o contradicție, de unde rezulă că m = n.

Prin inducție matematică, vom demonstra că $\forall\ i \in \{0,1,...,n\}$, avem $x_i = y_i$.

Pentru n = 0, avem $x_0 = x = y_0$.

Fie acum n > 0 şi presupunem afirmația adevărată pentru n - 1.

Avem: $x = \left(x_n u^{n-1} + x_{n-1}u^{n-2} + ... + x_1\right)u + x_0, \quad 0 \le x_0 < u$

şi: $x = \left(y_n u^{n-1} + y_{n-1}u^{n-2} + ... + y_1\right)u + y_0, \quad 0 \le y_0 < u$.

Din unicitatea câtului şi restului împărțirii lui x la u rezultă $x_0 = y_0$ şi

$x_n u^{n-1} + x_{n-1}u^{n-2} + ... + x_1 = y_n u^{n-1} + y_{n-1}u^{n-2} + ... + y_1$.

Folosind ipoteza inductivă pentru n – 1 rezultă că $\forall\ i \in \{1,...,n\}$, avem $x_i = y_i$, şi deci, $\forall\ i \in \{0,1,...,n\}$ avem $x_i = y_i$.

Observație: Teorema precedentă permite scrierea lui x sub forma $x = \overline{x_n x_{n-1} ... x_0}$ sau $x_n x_{n-1} ... x_{0(u)}$.

Remarcăm faptul că se stabileşte o corespondență bijectivă între numerele naturale nenule şi şirurile finite $x_n x_{n-1} ... x_1 x_0$ de numere naturale $x_i < u$, cu $x_n \neq 0$.

Algoritmul de reprezentare a numerelor naturale într-o bază u se numeşte **algoritmul sistemelor de numerație**.

u precizat în teoremă se numeşte **bază de numerație** sau **sistem de numerație**, iar simbolurile care desemnează numerele naturale mai mici decât u se numesc **cifrele sistemului de numerație**.

Cel mai răspândit sistem de numerație este cel în baza zece, numit **sistemul zecimal**, iar cifrele acestui sistem sunt 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

Pentru u = 2, avem **sistemul de numerație binar**, cifrele binare fiind 0 şi 1. Printre sistemele de numerație mai des folosite se numără şi cel de bază $u = 16_{(10)}$ numit **sistemul de numerație hexagesimal**, cifrele hexagesimale fiind 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F (A = 10, B = 11, ...).

Teorema ce urmează, prezintă un mod de comparare a două numere naturale, scrise în acelaşi sistem de numerație.

Teoremă: Dacă u $\in \mathbf{N}$, u > 1 şi x, y sunt două numere naturale scrise în baza u:

$$x = \overline{x_m x_{m-1} \ldots x_1 x_0}, \quad y = \overline{y_n y_{n-1} \ldots y_1 y_0}.$$

atunci x < y dacă şi numai dacă m < n sau (m = n şi $x_k < y_k$, unde $k = \max\{i \mid x_i \neq y_i\}$).

Demonstrație: Dacă m < n, atunci m + 1 ≤ n şi conform lemei de mai sus, rezultă

$$x = \sum_{i=0}^{m} x_i u^i < u^{m+1} \leq u^n \leq y_n u^n \leq \sum_{i=0}^{n} y_i u^i = y$$

Dacă m = n şi $x_k < y_k$, unde $k = \max\{i \mid x_i \neq y_i\}$, atunci

$$x = \sum_{i=0}^{m} x_i u^i = \sum_{i=0}^{k-1} x_i u^i + x_k u^k + \sum_{i=k+1}^{m} x_i u^i < u^k + x_k u^k + \sum_{i=k+1}^{m} x_i u^i =$$

$$= (1 + x_k) u^k + \sum_{i=k+1}^{m} x_i u^i \leq y_k u^k + \sum_{i=k+1}^{m} x_i u^i = y_k u^k + \sum_{i=k+1}^{m} y_i u^i \leq \sum_{i=0}^{m} y_i u^i = y$$

deci x < y.

Invers, dacă x < y, atunci m ≤ n.

Într-adevăr, dacă am avea m > n, respectând raționamentul din prima parte a demonstrației, am obține x > y, ceea ce este fals.

Dacă m = n, considerăm $k = \max\{i \mid x_i \neq y_i\}$. Să observăm că un astfel de k există, deoarece din x < y rezultă că există $i \in \{0,1,...,n\}$, încât $x_i \neq y_i$.

Avem $x_k < y_k$, deoarece în caz contrar conform cu prima parte a demonstrației, ar rezulta y < x, ceea ce este fals.

Deci, pentru m = n, avem $x_k < y_k$, unde $k = \max\{i \mid x_i \neq y_i\}$.

2. Adunarea numerelor naturale scrise în baza u

Fie x şi y două numere naturale scrise în baza u > 1.

$$x = \overline{x_m x_{m-1} \ldots x_1 x_0} \text{ şi } y = \overline{y_n y_{n-1} \ldots y_1 y_0}.$$

Vom determina scrierea lui x+ y în baza u.

1° Dacă m = n, atunci avem

$x = x_0 + x_1 u + ... + x_{m-1} u^{m-1} + x_m u^m$,

$y = y_0 + y_1 u + ... + y_{m-1} u^{m-1} + y_m u^m$.

Din $0 \le x_0 < u$ şi $0 \le y_0 < u$ rezultă $0 \le x_0 + y_0 < 2u$. Atunci $x_0+y_0= ue_1+ c_0$, unde $0 \le c_0 < u$, iar $e_1 \in \{0,1\}$, adică pentru $e_1 = 0$ avem $x_0 + y_0 = c_0 < u$, iar pentru $e_1 = 1$ avem $x_0 + y_0 = u + c_0$.

Rezultă $x + y = c_0 + (x_1 + y_1 + e_1)\, u + (x_2 + y_2)u^2 + ...$

Din $x_1 < u$ şi $y_1 + e_1 \le u$ rezultă $x_1 + y_1 + e_1 < 2u$, deci $x_1+y_1+e_1=ue_2+c_1$, cu $0 \le c_1 < u$, şi $e_2 \in \{0,1\}$.

Aşadar, $x + y = c_0 + c_1u + (x_2 + y_2 + e_2)\, u^2 + ...$ şi procedeul se continuă.

Din cele de mai sus, rezultă că pentru $i \in \{0,1,2,...\}$, c_i este restul împărţirii lui $x_i + y_i + e_i$ la u, unde $e_1 = 0$ dacă $x_0 + y_0 < u$ şi $e_1 = 1$ dacă $u \le x_0 + y_0$. Pentru $i \ge 1$, avem $e_i = 0$ dacă $x_i + y_i + e_i < u$ şi $e_i = 1$ dacă $u \le x_i + y_i + e_i$.

În plus, dacă $x_m + y_m + e_m < u$, atunci x + y are m cifre, iar dacă $u \le x_m + y_m + e_m$, atunci x + y are m + 1 cifre, iar $c_{m+1} = 1$.

2° Dacă $m \ne n$, de exemplu dacă $m > n$, vom putea aplica raţionamentul precedent, considerând $y_{n+1} = ... = y_m = 0$.

3. Înmulţirea numerelor naturale scrise în baza u

Fie x, y două numere naturale scrise în baza $u > 1$.

Din $x\,y = \underbrace{x + x + ... + x}_{y\ ori}$, rezultă că efectuarea produsului xy se reduce la o adunare repetată, procedeu care nu este eficient pentru numerele mari.

Fie $x = \sum_{i=0}^{m} x_i u^i$ şi $y = \sum_{j=0}^{n} y_j u^j$.

Avem $x\,y = x\left(\sum_{j=0}^{n} y_j u^j\right) = \sum_{j=0}^{n} (x\,y_j)u^j = x\,y_0 + (x\,y_1)u + ... + (x\,y_n)u^n$.

Problema se reduce la următoarele tipuri de înmulţiri:

1) înmulţirea dintre un număr natural şi un număr natural mai mic decât u;
2) înmulţirea dintre un număr natural şi o putere u^t a bazei de numeraţie u;

În mod concret:

1) Fie l şi k două numere naturale, astfel încât $0 \le l < u$ şi $0 \le k < u$. Rezultă $0 \le lk < u^2$. Aplicând teorema împărţirii cu rest pentru lk şi u rezultă că există numere naturale q(l,k) şi r(l,k) unic determinate, aşa încât:

$lk = uq(l,k) + r(l,k)$, unde $0 \le r(l,k) < u$.

Din $0 \le lk < u^2$ rezultă $0 \le q(l,k) < u$.

Avem:

$$x\,k = \left(\sum_{i=0}^{m} x_i u^i\right) k = \sum_{i=0}^{m} (x_i k) u^i = \sum_{i=0}^{m} (uq(x_i,k) + r(x_i,k)) u^i =$$

$$= \sum_{i=0}^{m} r(x_i,k) u^i + \sum_{i=0}^{m} q(x_i,k) u^{i+1}$$

2) Dacă $c = \sum_{i=0}^{p} c_i u^i$ este un număr natural, atunci $cu^t = c_p u^{p+t} + c_{p-1} u^{p-1+t} + \ldots + c_1 u^{1+t} + c_0 u^t$, care reprezintă scrierea în baza u a numărului natural cu^t.

4. Schimbarea bazei de numeraţie

Fie $x = x_n v^n + x_{n-1} v^{n-1} + \ldots + x_1 v + x_0$ un număr natural scris în baza $v > 1$.

În vederea trecerii la baza $u \in \mathbf{N}$, $u > 1$, distingem trei variante de lucru:

1. trecerea lui x din baza v în baza u, cu efectuarea calculelor în baza v;
2. trecerea lui x din baza v în baza u, cu efectuarea calculelor în baza u;
3. trecerea lui x din baza v în baza u, cu efectuarea calculelor într-o bază intermediară w.

Prezentăm, pe scurt, cele trei variante:

1. Se reprezintă mai întâi u în baza v şi apoi se aplică algoritmul sistemelor de numeraţie pentru x şi u, cu efectuarea calculelor în baza v.

2. Se reprezintă, mai întâi $x_0, x_1, \ldots, x_n$ şi v în baza u, cu ajutorul algoritmului sistemelor de numeraţie. Se introduc $x_0, x_1, \ldots, x_n$ şi v astfel reprezentaţi în expresia $x_n v^n + x_{n-1} v^{n-1} + \ldots + x_1 v + x_0$ şi se face calculul acesteia folosind algoritmul adunării şi cel al înmulţirii în baza u.

3. Se trece x în baza w cu metoda 2° şi apoi îl trecem în baza u folosind 1°.

Cazuri particulare

1. Să considerăm cazul $v = u^r$, unde $r \in \mathbf{N}$, $r > 1$.

În acest caz, trecerea de la baza v la baza u se simplifică considerabil, aplicând varianta a doua.

Remarcăm că $\forall\ y \in \mathbf{N}$, $y < u^r$, y se scrie, în mod unic sub forma:

(*) $y = c_{r-1}u^{r-1} + ...+ c_1u + c_0$, $0 \le c_i \le u$, $0 \le i < r$.

Pentru a reprezenta numărul $x = x_nv^n + x_{n-1}v^{n-1} + ...+ x_1 v + x_0$ în baza u, unde $v = u^r$, $r > 1$, vom scrie fiecare cifră x_i ca în (*), astfel:

$x_i = c_{ir-1}u^{r-1} + ...+ c_{i1}u + c_{i0}$

Înlocuim fiecare x_i cu secvența $c_{ir-1} ... c_{i1}c_{i0(u)}$ şi obținem secvența

(**) $c_{n\,r-1} ... c_{n1}c_{n0}c_{n-1\,r-1} ... c_{n-1\,1}c_{n-1\,0} ... c_{01}c_{00(u)}$.

Înlăturând cifrele egale cu 0 de la începutul secvenței, obținem reprezentarea lui x în baza u.

De exemplu, numărul $x = 375_{(8)}$ se trece în baza u = 2 astfel:

$x_0 = 5 = 1 \cdot 2^2 + 0 \cdot 2 + 1 \cdot 1 = c_{02} \cdot 2^2 + c_{00}$

$x_1 = 7 = 1 \cdot 2^2 + 1 \cdot 2 + 1 \cdot 1 = c_{12} \cdot 2^2 + c_{11} \cdot 2 + c_{10}$

$x_2 = 3 = 0 \cdot 2^2 + 1 \cdot 2 + 1 \cdot 1 = c_{22} \cdot 2^2 + c_{21} \cdot 2 + c_{20}$

aşadar (**) este în acest caz secvența:

$01\ 11\ 1\ 11\ 0\ 1_{(2)}$, deci $11111101_{(2)}$ reprezintă scrierea în bază 2 a numărului $x = 375_{(8)}$.

2. Când $v^r = u$, $r > 1$, trecerea unui număr din baza v în baza u se face printr-o metodă ce urmează calea inversă celei date la 1° şi anume: pentru a trece în baza u numărul $x = x_nx_{n-1} ... x_1x_{0(v)}$ se separă de la dreapta la stânga secvențe de câte r cifre (ultima grupă având cel mult r cifre) şi fiecare sevență va reprezenta o cifră în baza u, cu care vom înlocui secvența respectivă.

Astfel, dacă u = 8 şi v = 2, numărul $x = 1111101_{(2)}$ are în baza 8 reprezentarea $x = 375_{(8)}$.

5. Criterii de divizibilitate

În vederea stabilirii unui criteriu general de divizibilitate a numărului $x = \sum_{i=0}^{n} x_i u^i$, scris în baza u, prin $m \in \mathbf{N}$, $m > 1$, notăm r_k restul

împărțirii lui u^k la m. Apoi fie $\rho_n = \begin{cases} r_k, & r_k \le \frac{m}{2} \\ r_k - m, & r_k > \frac{m}{2} \end{cases}$ (se numesc coeficienții de divizibilitate ai lui m în baza u).

Este clar că m|x dacă şi numai dacă m| $\sum_{i=0}^{n} x_i \rho^i$.

CAPITOLUL III. DIVIZIBILITATEA ÎN N ŞI Z

3.1. Cel mai mare divizor comun. Cel mai mic multiplu comun.

1. Relația de divizibilitate pe N

Definiție: Fie a, b ∈ **N**. Spunem că **b divide a** sau că a este **multiplu** de b şi notăm b | a dacă ∃ c ∈ **N**, astfel încât a = bc.
Observăm că dacă b = 0, atunci a = 0, deci în cele ce urmează, vom considera deseori doar cazul b ≠ 0.

Proprietăți: 1. ∀ a ∈**N**, 1 | a;
2. ∀ b ∈**N**, b | 0;
3. reflexivitatea: ∀ a ∈**N**, a | a;
4. antisimetria: dacă a, b ∈ **N**, astfel încât a | b şi b | a, atunci a = b;
5. tranzitivitatea: dacă a, b, c ∈ **N**, astfel încât a | b şi b | c, atunci a | c;
6. dacă a, b, c ∈ **N**, astfel încât a | b şi a | c, atunci pentru orice x, y ∈ **N**, avem a|(xb+ yc).
7. pentru orice a, b ∈ **N**, a ≠ 0, din b | a, rezultă b ≤ a.

Demonstrație: 4. Din b | a rezultă că ∃ c∈**N**, astfel încât a = bc şi din a | b rezultă ∃ d∈**N**, astfel încât b = ad. Obținem a = a (dc).
Dacă a = 0, atunci din a | b rezultă b = 0, deci a = b.

Dacă a ≠ 0, atunci din a = a (dc) rezultă 1 = dc (conform M_4) şi deci d = c = 1 (conform M_5). Aşadar a = b.

8. Din b | a rezultă că există c∈**N**, astfel încât a = bc. Cum a ≠ 0 rezultă că c ≠ 0, deci există u∈**N** aşa încât c = u*.

Se obține a = bu* = b + bu, de unde rezultă b ≤ a.

Celelalte proprietăți rezultă, cu uşurință, din definiție.

Proprietățile 3, 4, 5 arată că "|" este o relație de ordine. Nu este însă o relație de ordine totală, pentru că nu oricare două numere naturale pot fi comparate (în sensul relației "|"), de exemplu, 3 ∤ 7 şi 7 ∤ 3.

2. Relația de divizibilitate pe Z

Definiție: Date două numere întregi x şi y, spunem că **x divide y** sau că y este **multiplu** al lui x, dacă există un număr întreg z, astfel încât y = xz.

Vom scrie x | y.

Ca şi relația de divizibilitate pe **N**, relația de divizibilitate pe **Z** se dovedeşte a fi reflexivă şi tranzitivă:

- ∀ x∈**Z**, avem x = x·1, de unde x | x;
- dacă x, y, z∈**Z**, aşa încât x | y şi y | z, atunci ∃ x', y'∈**Z** aşa încât y = xx', z = yy', deci, z = (xx')y' = x(x'y'), de unde x | z.

Relația de divizibilitate pe **Z** nu este însă antisimetrică. De exemplu, avem 2 | -2, -2 | 2, dar 2 ≠ -2.

Definiție: Două numere întregi x şi y se numesc **asociate în divizibilitate** şi scriem x ~ y, dacă x | y şi y | x.

Propoziție: Două numere întregi x şi y sunt asociate în divizibilitate dacă şi numai dacă x = y sau x = -y.

Demonstrație: Dacă x = y, avem x | y şi y | x prin reflexivitatea relației de divizibilitate. Dacă x = -y, avem x = y(-1), deci y | x şi y = - (-y) = -x = x· (-1), deci x|y.

Reciproc să presupunem că x | y şi y | x. Atunci există x', y' ∈ **Z**, astfel încât y = xx' şi x = yy'. Dacă x = 0, atunci y = 0·x' = 0 = x.

Dacă x ≠ 0, avem x = yy' = (xx')y' = x(x'y') de unde rezultă x'y' = 1, deci x' = y' = 1 sau x' = y' = -1, adică y = x sau y = -x.

Observăm că ∀x∈**Z**, avem x = 1·x, deci 1 | x. Numerele întregi pentru care avem x | 1 se numesc **unități**. Conform propoziției anterioare, rezultă că: x | 1⇔ x~1⇔ x= 1 sau x = -1.

Aşadar, singurele unități ale lui **Z** sunt 1 şi -1.

Propoziția anterioară poate fi enunțată şi astfel: "Două numere întregi x şi y sunt asociate în divizibilitate dacă şi numai dacă există o unitate u, astfel încât x = uy".

Rezultă că $x \sim y \Leftrightarrow |x| = |y|$, iar de aici se obține că relația de asociere în divizibilitate este o relație de echivalență, ale cărei clase de echivalență sunt de forma $\{n, -n\}$, pentru $n \neq 0$ şi $\{0\}$, pentru $n = 0$.

3. Cel mai mare divizor comun a două numere naturale

Definiție: Fie $a, b \in \mathbf{N}$. $d \in \mathbf{N}$ se numeşte **cel mai mare divizor comun** al numerelor a şi b (notăm $d = (a, b)$), dacă:

1. $d \mid a, d \mid b$;
2. $\forall\, d' \in \mathbf{N}: d' \mid a, d' \mid b \Rightarrow d' \mid d$.

Lemă: Fie m, n, p trei numere naturale astfel încât $m = n + p$. Dacă numărul natural nenul q divide oricare două dintre numerele m, n, p atunci q divide şi pe al treilea număr.

Demonstrație: Fie $q \mid n$ şi $q \mid p$. Atunci $\exists\, u, v \in \mathbf{N}: n = qu$ şi $p = qv$. Rezultă $m = q(u+v)$, deci $q \mid m$. Fie acum $q \mid m$ şi $q \mid n$. Atunci $\exists\, t, s \in \mathbf{N}$: $m = qt$ şi $n = qs$. Din $qt = qs + p$ rezultă $qs \leq qt$ şi cum $q > 0$ obținem $s \leq t$, de unde rezultă că $\exists\, w \in \mathbf{N}$ aşa încât $t = s + w$. Din $qt = qs + p$ rezultă $qs + qw = qs + p$, deci $qw = p$, de unde $q \mid p$.

Analog se arată că din $q \mid m$ şi $q \mid p$, rezultă $q \mid n$.

Lemă: Dacă $x, y, q, r \in \mathbf{N}$, satisfac egalitatea $x = yq + r$ atunci există cel mai mare divizor comun al lui x şi y dacă şi numai dacă există cel mai mare divizor comun al lui y şi r. În plus, avem $(x,y) = (y,r)$.

Demonstrație: Presupunem că există cel mai mare divizor comun al lui x şi y, pe care-l notăm cu d. Din $d \mid x$ şi $d \mid y$ rezultă, conform lemei anterioare, că $d \mid r$, deci avem $d \mid y$ şi $d \mid r$.

Fie acum $d' \in \mathbf{N}$, aşa încât $d' \mid y$ şi $d' \mid r$. Conform aceleiaşi leme, rezultă că $d' \mid x$ şi deci $d' \mid x$ şi $d' \mid y$, adică $d' \mid d$.

Aşadar, d este cel mai mare divizor comun al lui y şi r şi avem $(y,r) = d = (x,y)$.

Reciproc, presupunând că există cel mai mare divizor comun al numerelor y şi r, pe care-l notăm cu d, va rezulta $d \mid y$ şi $d \mid r$, de unde $d \mid qy + r = x$, deci avem $d \mid x$ şi $d \mid y$.

Fie acum d'∈**N**, aşa încât d' | x şi d' | y. Obţinem d' | r, deci d' | y şi d' | r, de unde d' | d. Astfel, d este cel mai mare divizor comun al lui x şi y şi avem (x,y) = d = (y, r).

Teoremă: Fie a, b∈**N**. Atunci există şi este unic cel mai mare divizor comun al numerelor a şi b.

Demonstraţie: Dacă a = b = 0, atunci cel mai mare divizor comun este 0.

Presupunem, în continuare, b ≠ 0. Procedeul de determinare pe care-l vom folosi poartă numele de:

4. Algoritmul lui Euclid

Aplicăm teorema împărţirii cu rest pentru a şi b. Rezultă că există q_0, r_0∈**N**, unic determinate astfel încât:

(0) $a = bq_0 + r_0$, unde $0 \le r_0 < b$.

Dacă $r_0 = 0$, atunci $a = bq_0$, de unde b | a, deci (a,b)=b.

Dacă $r_0 \neq 0$, vom aplica teorema împărţirii cu rest pentru b şi r_0, iar dacă şi noul rest r_1 va fi nenul, vom repeta procedeul, împărţind r_i la r_{i+1}(i∈**N**), până când vom obţine un rest nul, astfel:

(1) există q_1, r_1∈**N**: $b = r_0q_1 + r_1$, $0 < r_1 < r_0$

(2) există q_2, r_2∈**N**: $r_0 = r_1q_2 + r_2$, $0 < r_2 < r_1$

.....

(n) există q_n, r_n∈**N**: $r_{n-2} = r_{n-1}q_n + r_n$, $0 < r_n < r_{n-1}$

(n+1) există q_{n+1}, r_{n+1}∈**N**: $r_{n-1} = r_nq_{n+1} + r_{n+1}$, $r_{n+1} = 0$

Şirul $b > r_0 > r_1 > ... > r_{i-1} > r_1 > r_{i+1} >...$ este un şir strict descrescător de numere naturale, deci cu siguranţă vom ajunge la un rest egal cu 0.

Am considerat că acest rest este r_{n+1}. Conform lemei anterioare avem:

$(a, b) = (b, r_0) = (r_0, r_1) = ... = (r_i, r_{i+1}) = ...= (r_{n-1}, r_n) = r_n$ deoarece $r_n \mid r_{n-1}$. Deci $(a, b) = r_n$

Verificăm unicitatea lui d = (a, b).

Presupunem că $d_1 \in$ **N** satisface cele două condiţii din definiţia celui mai mare divizor comun pentru a şi b , adică:

i) $d_1|a$ şi $d_1|b$;

ii) $\forall\ d_2 \in$ **N:** $d_2|a$ şi $d_2|b \Rightarrow d_2|d_1$.

Rezultă atunci că d | d_1 (din aceea că d | a, d | b) şi, analog, d_1 | d adică $d_1 = d$.

5. Cel mai mare divizor comun a două numere întregi

Definiție: Fie x, y $\in$ **Z**. Un element d$\in$**Z** se numeşte un **cel mai mare divizor comun al numerelor x şi y** dacă:

1) d $\mid$ x şi d $\mid$ y;
2) $\forall$ d'$\in$**Z :** d'$\mid$x şi d' $\mid$ y $\Rightarrow$ d' $\mid$ d.

Să observăm că dacă d este un cel mai mare divizor comun al numerelor x şi y, atunci şi – d satisface condițiile de a fi un cel mai mare divizor comun al numerelor x şi y.

Reciproc, dacă d şi d' sunt fiecare un cel mai mare divizor comun pentru x şi y, avem d' $\mid$ d, folosind faptul că d este cel mai mare divizor comun al numerelor x şi y; apoi, folosind faptul că d' este cel mai mare divizor comun pentru x şi y, avem d $\mid$ d', adică d ~ d', de unde d = d' sau d = -d'.

Observație: Dacă a, b, x, y, d $\in$ **Z** şi dacă d $\mid$ x şi d $\mid$ y, atunci, în baza definiției divizibilității numerelor întregi, rezultă că d $\mid$ (ax + by).

Pentru demonstrarea existenței celui mai mare divizor comun a două numere întregi se procedează în mod analog cazului numerelor naturale.

Fie x, y $\in$ **Z**.

Dacă y = 0, atunci există cel mai mare divizor comun al lui x şi 0 şi este (x,0) = x.

Presupunem acum y $\neq$ 0. Dacă y $\mid$ x, atunci (x,y) = $\pm$ y. Dacă y $\nmid$ x, atunci există n$\in$**N** şi $\exists$ $q_0, q_1, ..., q_{n+1}, r_0, r_1, ..., r_n \in$ **Z**, aşa încât:

$x = yq_0 + r_0$, $0 < r_0 < |y|$,
$y = r_0q_1 + r_1$, $0 < r_1 < r_0$,
$r_0 = r_1q_2 + r_2$, $0 < r_2 < r_1$,
.....
$r_{n-2} = r_{n-1}q_n + r_n$, $0 < r_n < r_{n-1}$,
$r_{n-1} = r_nq_{n+1}$.

Există cel mai mare divizor comun al numerelor x şi y şi acesta este ultimul rest nenul din şirul de egalități de mai sus.

Mai mult, din acest şir de egalități rezultă că există u, v $\in$ **Z**, aşa încât (x,y) = $r_n = ux + vy$.

Acest x se obține prin eliminarea resturilor intermediare $r_{n-1}, r_{n-2}, ..., r_0$ şi anume: $r_n = r_{n-2} – r_{n-1}q_n = r_{n-2} – (r_{n-3} – r_{n-2}q_{n-1})q_n = -r_{n-3} + +(1 + q_{n-1}q_n)\, r_{n-2} = -r_{n-3} + (1 + q_{n-1}q_n)\cdot(r_{n-4} – r_{n-3}q_{n-2}) = ...$

Prescurtat, cel mai mare divizor comun al elementelor întregi x şi y se notează c.m.m.d.c. (x,y) sau cu (x,y) (contextul urmând a selecta semnificaţia corectă pentru notaţie). Pentru a avea unicitatea în acest caz, se acceptă condiţia de pozitivitate pentru (x, y).

6. Cel mai mic multiplu comun a două numere naturale

Definiţie: Fie $a,b \in \mathbf{N}$. Se numeşte **cel mai mic multiplu comun** al numerelor a şi b şi se notează cu m = [a,b], numărul natural $m \in \mathbf{N}$, care satisface condiţiile:

1. $a \mid m, b \mid m$;
2. $\forall m' \in \mathbf{N}: a \mid m', b \mid m' \Rightarrow m \mid m'$.

Teoremă: Pentru orice $a, b \in \mathbf{N}$ există şi este unic cel mai mic multiplu comun al lor.

Demonstraţie: Dacă a = 0 sau b = 0, atunci singurul multiplu al lui a şi b este 0.

Presupunem în continuare că $a \neq 0$ şi $b \neq 0$, deci $ab \neq 0$, prin urmare $0 \nmid ab$, deci 0 nu satisface condiţiile de a fi cel mai mic multiplu comun pentru a şi b.

Considerăm mulţimea:

$M_{a,b} = \{m' \in \mathbf{N}^* \mid a \mid m' \text{ şi } b \mid m'\}$.

Din faptul că $ab \in M_{a,b}$ rezultă că $M_{a,b} \neq \varnothing$ şi atunci, în conformitate cu P.B.O. rezultă că $\exists\, m \in M_{a,b}: m \leq m', \forall\, m' \in M_{a,b}$.

Vom arăta că m = [a,b].

Din $m \in M_{a,b}$ rezultă $a \mid m$ şi $b \mid m$.

Aplicăm teorema împărţirii cu rest pentru m' şi m. Rezultă că $\exists\, q,r \in \mathbf{N}$ aşa încât $m' = mq + r$, $0 \leq r < m$. Să presupunem acum că $r \neq 0$. Din $a \mid m$, $a \mid m'$ şi $m' = mq + r$ rezultă că $a \mid r$. Analog din $b \mid m$ şi $b \mid m'$ rezultă că $b \mid r$. Aşadar, $r \in M_{a,b}$ şi cum $m \leq m', \forall\, m' \in M_{a,b}$, obţinem că $m \leq r$, ceea ce este fals.

Prin urmare, r = 0, de unde $m \mid m'$ şi cu aceasta am verificat faptul că m=[a,b].

Mai rămâne de arătat unicitatea lui m.

Presupunem că există $m_1 \in \mathbf{N}$, astfel încât să fie satisfăcute condiţiile:

i) $a \mid m_1, b \mid m_1$

ii) $\forall\, m_2 \in \mathbf{N}$: $a \mid m_2$, $b \mid m_2 \Rightarrow m_1 \mid m_2$.

Rezultă atunci că $m_1 \mid m$ şi $m \mid m_1$, deci $m = m_1$.

7. Cel mai mic multiplu comun a două numere întregi

Definiție: Cel mai mic multiplu comun a două numere întregi x şi y este un număr întreg m, satisfăcând următoarele condiții:

1) $x \mid m$, $y \mid m$;
2) $\forall\, m' \in \mathbf{Z}$: $x \mid m'$ şi $y \mid m' \Rightarrow m \mid m'$.

Ca şi în cazul celui mai mare divizor comun a două numere întregi, cel mai mic multiplu comun, dacă există, este unic până la o asociere în divizibilitate, adică dacă m este cel mai mic multiplu comun al elementelor x şi y, atunci şi –m este cel mai mic multiplu comun al acestor două elemente.

Prescurtat, notăm cel mai mic multiplu comun al elementelor x şi y cu c.m.m.m.c. (x,y) sau cu [x,y].

În vederea unicității se poate impune condiția de pozitivitate pentru [x, y].

Din proprietățile divizibilității numerelor întregi, rezultă că c.m.m.m.c.(x,y)=c.m.m.m.c.(-x,y)=c.m.m.m.c.(x,-y)=c.m.m.m.c.(-x,-y), aşadar putem reduce problema celui mai mic multiplu comun a două numere întregi la cel mai mic multiplu comun a două numere naturale, despre care ştim că există mereu.

8. Generalizare

Definițiile date pentru c.m.m.d.c. şi c.m.m.m.c (atât în cazul **N**, cât şi în cazul **Z**) pot fi extinse uşor pentru cazul a n numere, anume condițiile 1 şi 2 capătă forma:

1. $d \mid x_1, .., d \mid x_n$ (respectiv $x_1 \mid m, ..., x_n \mid m$),

2. $d' \mid x_1, ..., d' \mid x_n \Rightarrow d' \mid d$ (respectiv $x_1 \mid m', ..., x_n \mid m' \Rightarrow m \mid m'$).

Notând corespunzător $(x_1, ..., x_n)$, respectiv $[x_1, ..., x_n]$, se obține că

$(x_1,..., x_n) = (...(x_1, x_2), x_3), \ldots, x_n)...)$ şi

$[x_1,..., x_n] = [...[x_1, x_2], x_3] \ldots, x_n]...]$.

Din acest egalități pot fi decelate noi definiții (echivalente cu cele anterioare) pentru $(x_1,..., x_n)$, respectiv $[x_1, ..., x_n]$.

3.2. Numere prime

1. Numere prime. Numere indecompozabile

Definiție: Un număr natural $p \neq 0$, $p \neq 1$ se numeşte **prim** dacă oricare ar fi m, n numere naturale, din $p \mid mn$ rezultă $p \mid m$ sau $p \mid n$.

Definiție: Un număr natural $b \neq 0$, $b \neq 1$ se numeşte **indecompozabil (ireductibil)** dacă din $u \mid b$ rezultă $u = 1$ sau $u = b$.

Un număr natural $m \neq 0$, $m \neq 1$, care nu este indecompozabil se numeşte **decompozabil**.

Lema: Fie m un număr natural, $m \neq 0$, $m \neq 1$. Următoarele afirmații sunt echivalente:

1) m este decompozabil;
2) există $n, p \in \mathbf{N}$, astfel încât $m = np$, cu $1 < n < m$ şi $1 < p < m$.

Demonstrație: 1) $\Rightarrow$ 2). Cum m este decompozabil, rezultă că admite un divizor n diferit de 1 şi de m. Fie p, astfel încât $m = np$. Cum $m \neq 0$ şi $n \mid m$ rezultă $n \leq m$. Cum n este diferit de 1 şi de m, se deduce $1 < n < m$. Similar, avem $1 \leq p \leq m$.

Dacă $p = 1$, atunci $m = n$, iar dacă $p = m$, atunci $n = 1$. În ambele cazuri, se obține o contradicție, deci $1 < p < m$.

2) $\Rightarrow$ 1). Rezultă din definiție.

Lemă: Orice număr natural $m > 1$ admite un divizor indecompozabil.

Demonstrație: Mulțimea $P = \{q \in \mathbf{N} \mid q > 1, q \mid m\}$ nu este vidă, deoarece conține pe m. În conformitate cu P.B.O. , $\exists\ b \in P$, $b \leq q$, $\forall\ q \in P$.

Vom arăta că b este indecompozabil.

Presupunem că b ar fi decompozabil; atunci conform lemei anterioare, există n, $p \in \mathbf{N}$, astfel încât $b = np$, $1 < n < b$ şi $1 < p < b$.

Din $n \mid b$ şi $b \mid m$ rezultă $n \mid m$ şi cum $1 < n$ rezultă că $n \in P$.

Dar $n < b$ şi $n \in P$ contrazice alegerea lui b.

Prin urmare, b este indecompozabil şi este divizor al lui m.

Teoremă: Fie p un număr natural, $p \neq 0$, $p \neq 1$. Următoarele afirmații sunt echivalente:

1) p este prim;
2) p este indecompozabil.

Demonstrație: 1) $\Rightarrow$ 2). Fie k un divizor al lui p.

Există $t \in \mathbf{N}$, astfel încât $kt = p$, deci $p \mid kt$.

Cum p este prim, rezultă $p \mid k$ sau $p \mid t$. Dacă $p \mid k$, atunci $\exists v \in \mathbf{N}$: $k = pv$.

Din p = kt rezultă p = pvt, deci 1 = vt, rezultă v = t = 1, deci k = p.

Analog, dacă p | t deducem k = 1.

Aşadar, p este indecompozabil.

2) $\Rightarrow$ 1) Presupunem că există elemente indecompozabile, care nu sunt prime. Fie p cel mai mic element indecompozabil, care nu este prim (**N** este bine ordonată). Cum p nu este prim, rezultă că există m, n $\in$ **N**, astfel încât p | mn şi pΠm şi pΠn. Dar m > 1, deoarece dacă am avea m = 0, atunci p | m, iar dacă am avea m = 1, din p | mn ar rezulta p | n.

Similar, rezultă n > 1.

Să arătăm acum că putem considera m < p şi n < p.

Dacă m > p, atunci conform teoremei împărțirii cu rest, rezultă că $\exists$ q, r $\in$ **N**, unic determinate, astfel încât m = pq + r, cu 0 < r < p, de unde rezultă mn = pqn + rn; din p | mn şi p | pqn rezultă că p | rn.

În plus, din 0 < r < p rezultă că p$\nmid$ r.

Deci, dacă m > p, atunci am putea înlocui m cu r şi vom avea p | rn, p$\nmid$r, p$\nmid$n şi 0 < r < p. La fel se procedează dacă p < n.

Mai mult, putem alege m şi n, astfel încât produsul mn să fie minim (deoarece **N** este bine ordonată).

Din p | mn rezultă că există q $\in$ **N**, astfel încât mn = pq.

Avem q > 1, deoarece q=1 implică m | p şi cum p este indecompozabil rezultă m = 1 sau m = p.

Dar m < p, deci singura posibilitate ar fi m = 1, de unde rezultă n = p, ceea ce este în contradicție cu alegerea lui n.

Prin urmare q > 1 şi vom considera b un divizor indecompozabil al lui q; rezultă b ≤ q.

Avem pq = mn < pn < pp. De aici rezultă q < p, deci b ≤ q < p. Din b | q şi q | mn rezultă b | mn.

Deoarece p este cel mai mic număr indecompozabil care nu este prim, rezultă că b este prim şi deci, din b | mn rezultă b | m sau b | n.

Presupunem că b | m. Fie m_1, q_1 $\in$ **N** astfel încât m = bm_1 şi q = bq_1.

Din mn = qp rezultă $bm_1n = bq_1p$, deci $m_1n = q_1p$. Aşadar p | m_1n şi p$\nmid$n şi p$\nmid m_1$, pentru că dacă p ar divide m_1, atunci din m = bm_1 ar rezulta că p divide m, ceea ce este fals.

Din b > 1 şi m = bm_1 rezultă m > m_1 şi deci mn > m_1n.

Aşadar, $p \mid m_1 n$, $p \nmid m_1$, $p \nmid n$ şi $m_1 n < mn$, ceea ce intră în contradicție cu alegerea lui mn, deci, presupunerea făcută este falsă şi teorema este demonstrată.

Teorema lui Euclid: Există o infinitate de numere prime.

Demonstrație: Presupunem că există un număr finit de numere prime şi anume $p_1, p_2, ..., p_n$.

Considerăm numărul $a = p_1 p_2 ... p_n + 1$. Deoarece orice număr prim este prin definiție nenul, rezultă că $a > 1$, prin urmare, a admite un divizor indecompozabil, deci prim, anume va fi unul dintre $p_1, p_2, ..., p_n$.

Fie p_i, cu $i \in \{1,2,...,n\}$ acest divizor. Avem $p_i \mid a$ şi $p_i \mid p_1 p_2 ... p_n$ şi atunci, rezultă că $p_i \mid 1$, de unde $p_i \leq 1$, ceea ce este fals.

Aşadar, presupunerea făcută este falsă, deci există o infinitate de numere prime.

Propoziție: Fie $p \in \mathbf{N}$, $p > 1$. Dacă p este prim şi $p \mid a_1 \cdot a_2 \cdot ... \cdot a_n$, unde $n \geq 2$ şi $\forall\, i \in \{1,2,...,n\}$, $a_i \in \mathbf{N}$, atunci $\exists\, i \in \{1,2,...,n\}$, astfel încât $p \mid a_i$.

Demonstrație: Se verifică uşor prin inducție după n.

2. Teorema de descompunere a numerelor naturale în factori primi

Teoremă: Orice număr natural $a > 1$ poate fi descompus în mod unic (abstracție făcând de ordinea factorilor) în produs finit de numere prime.

Demonstrație: Să arătăm mai întâi existența unei astfel de scrieri. Considerăm $A = \{a \in \mathbf{N} \mid a > 1$, a nu este prim şi nici nu este produs de numere prime$\}$.

Vom arăta că $A = \varnothing$.

Presupunem prin absurd că $A \neq \varnothing$ şi atunci în conformitate cu P.B.O., $\exists\, t \in A$ încât $t \leq a$, $\forall\, a \in A$. Din faptul că $t \in A$ rezultă că t nu este prim, deci t este decompozabil.

Fie $t_1, t_2 \in \mathbf{N}$ aşa încât $t = t_1 t_2$ cu $1 < t_1 < t$ şi $1 < t_2 < t$.

Din faptul că $t_1 < t$ şi $t_2 < t$ şi din alegerea lui t rezultă că $t_1 \notin A$ şi $t_2 \notin A$, deci t_1 şi t_2 sunt prime sau sunt produse de numere prime:

$t_1 = p_1 \cdot p_2 \cdot ... \cdot p_h$, $t_2 = p_1' \cdot p_2' \cdot ... \cdot p_k'$,

unde $h, k \in \mathbf{N}$, $h \geq 1$, $k \geq 1$, iar $p_1, p_2, ..., p_h, p_1', p_2', ..., p_k'$ sunt numere prime.

Rezultă că $t = t_1t_2 = p_1\ p_2\ ...\ p_h\ p_1'\ p_2'\ ...\ p_k'$, adică t este un produs de numere prime, contradicție cu $t \in A$. Prin urmare $A = \emptyset$, deci orice număr natural $a > 1$ poate fi descompus în produs finit de numere prime.

În vederea demonstrării unicității scrierii, fie $a = p_1\ p_2\ ...\ p_h = q_1q_2...q_k$, unde $h, k \in \mathbf{N}$, $h \geq 1$, $k \geq 1$ şi $p_1, p_2, ..., p_h, q_1, q_2, ..., q_k$ sunt numere prime. Arătăm că $h = k$ şi eventual după o renumerotare a factorilor, $p_i = q_i$, pentru orice $i \in \{1,2,...,k\}$.

Demonstrăm prin inducție după h.

Dacă $h = 1$, atunci $a = p_1 = q_1\ q_2\ ...\ q_k$ şi p_1 fiind număr prim rezultă că $\exists\ i \in \{1,2,...,k\}$, astfel încât $p_1 \mid q_i$. Dar q_i este prim, deci indecompozabil, prin urmare $p_1 = q_i$. Presupunem $k > 1$. Obținem de aici egalitatea

$$1 = \prod_{\substack{s=1 \\ s \neq i}}^{k} q_s$$

, de unde rezultă $q_s = 1$, pentru orice $s \in \{1,2,...,k\} - \{i\}$, ceea ce contrazice faptul că numărul q_s este prim, pentru orice $s \in \{1,2,...,k\} - \{i\}$.

Aşadar, $k = 1$ şi $p_1 = q_1$.

Presupunem că unicitatea are loc pentru orice $a \in \mathbf{N}$, $a > 1$, care se scrie ca un produs de factori primi, iar numărul acestor factori primi este mai mic decât h şi vom demonstra că are loc pentru orice număr care se scrie ca un produs de h factori primi.

Fie $p_1\ p_2\ ...\ p_h = q_1\ q_2\ ...\ q_k$, unde $\forall\ i \in \{1,2,...,h\}$, $\forall\ j \in \{1,2,...,k\}$, p_i şi q_j sunt prime.

Din faptul că p_h este prim şi $p_h \mid q_1q_2...\ q_k$ rezultă că $\exists\ j \in \{1,2,...,k\}$, astfel încât $p_h \mid q_j$ şi cum q_j este prim rezultă $p_h = q_j$. Fără a restrânge generalitatea, putem presupune că $j = k$.

Obținem $p_1 \cdot ... \cdot p_{h-1} = q_1 \cdot ... \cdot q_{k-1}$ şi conform ipotezei inductive rezultă că $h - 1 = k - 1$ şi $p_i = q_i$, $\forall\ i \in \{1,2,...,h-1\}$, până la o renumerotare (cu h-1, respectiv k-1, am notat numărul natural al cărui succesor este h, respectiv k).

Aşadar, $h = k$ şi $\forall\ i \in \{1,2,...,h\}$, $p_i = q_i$.

Observație: Factorii $p_1, p_2, ..., p_h$ din descompunerea de mai sus pot să şi coincidă; de aceea, putem scrie

$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, unde $\forall\ i \in \{1,2,...,k\}$, p_i este prim, $\alpha_i \in \mathbf{N}$, $\alpha_i \geq 1$ şi $\forall\ i \neq j$, $i,j \in \{1,2,...,k\}$, $p_i \neq p_j$.

Scrierea de mai sus poartă numele de **scrierea canonică** a lui a.

Utilizând această scriere, putem caracteriza divizorii lui a şi anume:

Propoziție: Fie a $\in$ **N**, a > 1, cu scrierea canonică $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, unde $\forall$ i$\in$ {1,2,...,k}, p_i este prim, $\alpha_i \in$**N**, $\alpha_i \geq 1$ şi $\forall$ i$\neq$j, i,j$\in$ {1,2,...,k}, $p_i \neq p_j$.

Atunci d $|$ a dacă şi numai dacă $d = p_1^{\delta_1} p_2^{\delta_2} \ldots p_k^{\delta_k}$, cu $0 \leq \delta_i \leq \alpha_i$, $\forall$ i$\in$ {1,2,...,k}.

Demonstrație: Dacă $d = p_1^{\delta_1} p_2^{\delta_2} \ldots p_k^{\delta_k}$, cu $0 \leq \delta_i \leq \alpha_i$, $\forall$ i$\in$ {1,2,...,k}, atunci a = d·c, unde $c = p_1^{\alpha_1 - \delta_1} p_2^{\alpha_2 - \delta_2} \ldots p_k^{\alpha_k - \delta_k}$, deci d $|$ a.

Dacă d $|$ a, atunci există c$\in$**N**, astfel încât a=d·c, deci $a = p_1^{\delta_1} p_2^{\delta_2} \ldots p_k^{\delta_k} \cdot c$ adică p_i intră în descompunerea lui d cu exponentul $\delta_i \leq \alpha_i$, pentru orice i$\in$ {1,2,...,k}.

Remarcăm şi că pentru două numere naturale a şi b putem pune în evidență două descompuneri, în care apar aceeaşi factori primi, cu mențiunea că exponenții acestora pot fi şi zero, astfel

a,b$\in$**N**, $a \geq 1$, b $\geq$ 1, $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_h^{\alpha_h}$ şi $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_h^{\beta_h}$, unde $\forall$ i$\in$ {1,2,...,h}, $\alpha_i \geq 0$ şi $\beta_i \geq 0$ şi p_i prim, iar $\forall$ i,j$\in$ {1,2,...,h}, i$\neq$j, $p_i \neq p_j$.

Atunci:

$d = (a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot \ldots \cdot p_h^{\min(\alpha_h,\beta_h)}$,

iar $m = [a,b] = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdot \ldots \cdot p_h^{\max(\alpha_h,\beta_h)}$.

Teoremă: Pentru orice a,b$\in$**N**, a $\geq$ 1, b $\geq$ 1 are loc egalitatea ab=(a,b)·[a,b].

Demonstrație: Rezultă din faptul că pentru orice i$\in$ {1,2,...,h}, avem $\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i$.

Pentru orice număr întreg x $\notin$ {0,1,-1} avem x = sgn(x)· $|$x$|$, iar $|$x$|$ este un număr natural diferit de 0 şi de 1. Pentru $|$x$|$ aplicăm teorema fundamentală a aritmeticii numerelor naturale. Rezultă că $|$x$|$ se scrie ca produs de numere prime şi deci

x = sgn (x) $p_1 \cdot p_2 \cdot \ldots \cdot p_m$, unde $\forall$ i$\in$ {1,2,...,m}, p_i este prim.

Din sgn(x) $\in$ {1,-1} şi din faptul că 1 şi –1 sunt unităţi, rezultă că $x = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_m$, unde u este o unitate, iar $p_1, p_2, \ldots, p_m$ sunt numere prime.

Numerele $p_1, p_2, \ldots, p_m$ nu sunt neapărat distincte, deci grupându-le pe toate cele egale între ele, obţinem:

$$x = u \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n},$$

unde u este o unitate, $p_1, p_2, \ldots, p_n$ sunt numere prime distincte şi $\alpha_1, \alpha_2, \ldots, \alpha_n$ sunt numere naturale. În egalitatea de mai sus putem face să apară orice număr prim $p \notin \{ p_1, p_2, \ldots, p_n\}$, astfel:

$$x = u \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} \cdot p^0.$$

Notând cu P mulţimea tuturor numerelor prime şi cu $\alpha(p_i)$ exponentul α_i al lui p_i, putem scrie $x = u\prod_{p \in P} p^{\alpha(p)}$ (precizăm că $\alpha(p) \neq 0$ doar pentru un număr finit de elemente din P, altfel spus avem un produs finit).

Propoziţie: Fie $x,y,z \in \mathbf{Z}$, aşa încât $x \mid yz$, iar x şi y sunt prime între ele (au cel mai mare divizor comun 1). Atunci $x \mid z$.

Demonstraţie: Din faptul că x şi y sunt prime între ele rezultă că $\exists\, u,v \in \mathbf{Z}$ aşa încât ux + vy = 1.

Avem $z = z \cdot 1 = z(ux + vy) = (zu)x + v(yz)$, deci $z = (zu)x + v(yz)$. Deoarece $x \mid yz$ rezultă în baza ultimei egalităţi că $x \mid z$.

Corolar: Pentru orice număr prim p şi orice numere întregi x şi y are loc implicaţia:

$$p \mid xy \Rightarrow p \mid x \text{ sau } p \mid y.$$

Demonstraţie: Din $(p,x) \mid p$ şi p număr prim rezultă că (p,x) = 1 sau (p,x) = p.

Dacă (p,x) = 1 atunci $p \mid y$, conform propoziţiei precedente, iar dacă (p,x) = p avem că $p \mid x$.

Definiţie: Se numeşte **ordinul** lui p în x şi se notează $n = ord_p(x)$ numărul natural n, care satisface condiţia: $p^n \mid x$ iar $p^{n+1} \nmid x$.

Avem $ord_p(x) = 0 \Leftrightarrow p \nmid x$ şi $ord_p(x) \leq n \Leftrightarrow p^n \mid x$.

Corolar: Pentru $\forall\, x,y \in \mathbf{Z}$ şi pentru orice număr prim p, avem $ord_p(xy) = ord_p(x) + ord_p(y)$.

Demonstrație: Notăm $ord_p(x) = m$ şi $ord_p(y) = n$. Atunci $x = p^m x'$ şi $p \nmid x'$ şi respectiv $y = p^n y'$ şi $p \nmid y'$.Rezultă $xy = p^{m+n} x'y'$, iar din corolarul anterior rezultă că $p \nmid x'y'$, deci:
$ord_p(xy) = m + n = ord_p(x) + ord_p(y)$.

Teorema fundamentală a aritmeticii

Orice $x \in \mathbf{Z} - \{-1, 0, 1\}$ admite o descompunere în factori primi $x = u\prod_{p\in P} p^{\alpha(p)}$, unică până la o ordine a factorilor. Anume: dacă $x = u\prod_{p\in P} p^{\alpha(p)}$, u este o unitate şi $\alpha(p) \in \mathbf{N}^*$ numai pentru un număr finit de elemente din P, atunci $u = sgn(x)$ şi $\alpha(p) = ord_p(x)$, pentru orice $p \in P$.

Demonstrație: Existența rezultă din considerațiile anterioare. Din $x = u\prod_{p\in P} p^{\alpha(p)} = up_1^{\alpha(p_1)} p_2^{\alpha(p_2)} \ldots \cdot p_m^{\alpha(p_m)}$ rezultă că $\forall q$ număr prim, avem: $ord_q(x) = ord_q(u) + \alpha(p_1)\, ord_q(p_1) + \alpha(p_2)\, ord_q(p_2) + \ldots + \alpha(p_m)\, ord_q(p_m) = ord_q(u) + \sum_{p\in P} \alpha(p) ord_q(p)$.

Din $ord_q(u) = 0$ (deoarece u este o unitate) şi $ord_q(p) = 1 \Leftrightarrow q = p$, iar pentru $q \neq p$, avem $ord_q(p) = 0$, rezultă că $ord_q(x) = \alpha(q)$, pentru orice $q \in P$. Pe de altă parte, este clar că $u = sgn(x)$.

Propoziție: Fie $x, y \in \mathbf{Z}^*$. Avem $y \mid x \Leftrightarrow \forall p \in P$, $ord_p(y) \leq ord_p(x)$.

Demonstrație: "$\Rightarrow$" Din $y \mid x$ rezultă că $\exists\, z \in \mathbf{Z}$, aşa încât $x = yz$, de unde $\forall\, p \in P$, avem $ord_p(x) = ord_p(y) + ord_p(z) \geq ord_p(y)$.

"$\Leftarrow$" Presupunem că $ord_p(y) \leq ord_p(x)$, $\forall\, p \in P$ şi fie $x = u\prod_{p\in P} p^{\alpha(p)}$, $y = v\prod_{p\in P} p^{\beta(p)}$, unde u şi v sunt unități, iar pentru $\forall\, p \in P$, $\beta(p) = ord_p(y) \leq ord_p(x) = \alpha(p)$.

Fie $z = uv\prod_{p\in P} p^{\alpha(p)-\beta(p)}$. Obținem

$yz = uv^2 \prod_{p\in P} p^{\alpha(p)-\beta(p)} \cdot p^{\beta(p)} = u\prod_{p\in P} p^{\alpha(p)}$, deci $y \mid x$.

Observație:

Dacă considerăm acum x, z ∈ **Z**, $x = u\prod_{p\in P} p^{\alpha(p)}$ şi $z = w\prod_{p\in P} p^{\gamma(p)}$, $(x,y) = \prod_{p\in P} p^{\min(\alpha(p),\gamma(p))}$ atunci , iar $[x,y] = \prod_{p\in P} p^{\max(\alpha(p),\gamma(p))}$ şi cum ∀ p∈P, min(α(p),γ(p)) + max(α(p),γ(p)) = α(p) + γ(p), obținem că x·y = (x,y)·[x,y].

3.3. Funcții numerice

Prin **funcție numerică** vom înțelege orice funcție definită pe **N** (sau **N***) cu valori numerice (în **N, Z, Q**).

O funcție numerică este numită **multiplicativă** dacă pentru orice m, n ∈**N**, aşa încât (m,n) = 1, avem f(m·n) = f(m) · f(n).

Dacă funcția multiplicativă f nu este identic nulă (∃n∈**N** aşa încât f(n)≠0), atunci f(1) = 1. Într-adevăr, avem f(n) = f(n ·1) = f(n) · f(1), de unde rezultă f(1) = 1 (din f(n) ≠ 0).

Dacă pentru orice m,n ∈**N**, avem f(m·n) = f(m) · f(n) atunci se spune că funcția f este **total multiplicativă**.

Teoremă: Dacă f_1 şi f_2 sunt funcții multiplicative, atunci şi $f = f_1 \cdot f_2$ este funcție multiplicativă.

Demonstrație: Într-adevăr, dacă m,n ∈ **N**, încât (m,n) = 1, atunci $f(mn) = f_1(mn)f_2(mn) = f_1(m)\, f_1(n)\, f_2(m)\, f_2(n) = f(m)f(n)$.

Funcția numerică F definită prin $F(n) = \sum_{d|n} f(d)$ se numeşte **funcția sumatorie** a lui f(n).

Teoremă: Dacă f este multiplicativă, atunci F este multiplicativă.

Demonstrație: Fie m,n ∈ **N**, aşa încât (m,n) = 1 şi fie $d \mid mn$. Avem $d = d_1d_2$, unde $d_1 \mid m$, $d_2 \mid n$ şi $(d_1,d_2) = 1$.

Atunci

$$F(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1d_2) = \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = F(m)F(n)$$

.

Teoremă: Dacă f este o funcție multiplicativă şi $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_h^{\alpha_h}$ este descompunerea canonică a numărului *a*, atunci:

$$\sum_{d|a} f(d) = \left(1 + f(p_1) + f(p_1^2) + \ldots + f(p_1^{\alpha_1})\right) \cdot \ldots \cdot$$
$$\cdot \left(1 + f(p_h) + f(p_h^2) + \ldots + f(p_h^{\alpha_h})\right)$$

(în cazul *a* = 1 membrul al doilea se consideră egal cu 1).

Demonstrație: În membrul al doilea, obținem o sumă de termeni de forma:

$f(p_1^{\beta_1}) f(p_2^{\beta_2}) \cdot \ldots \cdot f(p_k^{\beta_k}) = f(p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k})$, unde $\forall$ $i \in \{1,2,...,k\}$, $0 \le \beta_i \le \alpha_i$.

Observăm că astfel, nu se omit şi nici nu se repetă termenii din $\sum_{d|a} f(d)$, adică suma considerată este chiar $\sum_{d|a} f(d)$.

Fie $m \in \mathbf{N}$, $m>1$ cu descompunerea canonică $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$.
Divizorii lui m sunt numerele naturale d de forma: $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, $0 \le \beta_i \le \alpha_i$, $\forall$ $i \in \{1,2,...,k\}$. Rezultă că m are $(\alpha_1 + 1)(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1)$ divizori. Singurul divizor al lui 1 este 1. Dintre toți divizorii lui 0 îl considerăm numai pe 0 (care nu-l depăşeşte pe 0).

Putem defini o funcție astfel:

Definiție: Funcția $\tau : \mathbf{N} \to \mathbf{N}$, dată prin:

$$\tau(n) = \begin{cases} (\alpha_1 + 1)(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1), & dacă \quad n > 1, n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \\ 1 \quad , & dacă \quad n = 0 \quad sau \quad n = 1 \end{cases}$$

este numită funcția **numărul divizorilor**.

Teoremă: Funcția τ este funcție multiplicativă.

Demonstrație: Fie $m,n \in \mathbf{N}$, astfel încât (m,n) = 1.

Vom verifica egalitatea: $\tau(mn) = \tau(m)\,\tau(n)$.

Dacă m = 0, atunci din (m,n) = 1 rezultă n = 1 şi deci $\tau(0 \cdot 1) = \tau(0) \cdot \tau(1)$.

Dacă m = 1, atunci $\tau(1 \cdot n) = \tau(1) \cdot \tau(n)$.

Considerăm acum cazul m > 1, n > 1 având descompunerile canonice $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, $n = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_h^{\beta_h}$.

Din (m,n) = 1 rezultă că $\forall$ $i \in \{1,2,...,k\}$, $\forall$ $j \in \{1,2,...,h\}$ $p_i \ne q_j$.

Obținem:

$m \cdot n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_h^{\beta_h}$ de unde $\tau(m \cdot n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1)(\beta_1 + 1)(\beta_2 + 1) \cdot \ldots \cdot (\beta_h + 1) = \tau(m) \cdot \tau(n)$.

Fie numărul natural $m > 1$, care are descompunerea canonică:

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}.$$

Avem $\dfrac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \dfrac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \dfrac{p_k^{\alpha_k+1}-1}{p_k-1} =$

$$= \left(1 + p_1 + p_1^2 + \ldots \cdot p_1^{\alpha_1}\right)\left(1 + p_2 + p_2^2 + \ldots \cdot p_2^{\alpha_2}\right) \cdot \ldots \cdot$$
$$\cdot \left(1 + p_k + p_k^2 + \ldots \cdot p_k^{\alpha_k}\right) = \sum_{\substack{0 \le \beta_i \le \alpha_i \\ i \in \{1,2,\ldots,k\}}} p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} = \sum_{d \mid m} d$$

Definiție: Funcția $\sigma : \mathbf{N} \to \mathbf{N}$, dată prin:

$$\sigma(m) = \begin{cases} \dfrac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \dfrac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \dfrac{p_k^{\alpha_k+1}-1}{p_k-1}, \text{ dacă } m > 1, m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \\ 1, \text{ dacă } m = 1 \\ 0, \text{ dacă } m = 0 \end{cases}$$

se numeşte funcția **suma divizorilor**.

Similar cu teorema precedentă, se arată că are loc:

Teoremă: Funcția σ este funcție multiplicativă.

Definiție: Indicatoarea lui Euler, notată cu φ, este funcția numerică definită astfel: $\varphi : \mathbf{N}^* \to \mathbf{N}^*$ şi $\forall\, n \in \mathbf{N}^*$, $\varphi(n)$ este numărul de numere naturale mai mici sau egale cu n şi prime cu n.

Remarcăm că, dacă $n = p$, unde p este număr prim atunci $\varphi(p) = p - 1$.

Fie acum $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$.

Pentru a calcula $\varphi(n)$, formăm, mai întâi, şirul: (*) 1, 2, 3, ..., n.

Eliminăm din acest şir p_1 şi toți multiplii săi.

Aceştia sunt: $p_1, 2p_1, 3p_1, \ldots, \dfrac{n}{p_1} p_1$ şi numărul lor este $\dfrac{n}{p_1}$.

Din şirul (*) rămân: $n-\frac{n}{p_1}=n\left(1-\frac{1}{p_1}\right)$ elemente.

Multiplii lui p_2 din (*) sunt: p_2, $2p_2$, ..., $\frac{n}{p_2}p_2$ şi numărul lor este $\frac{n}{p_2}$.

Între acestea, unele sunt divizibile şi cu p_1 şi numărul acestora este $\frac{n}{p_1p_2}$. Eliminăm dintre multiplii lui p_2, pe numerele divizibile cu p_1. Rămân $\frac{n}{p_2}-\frac{n}{p_1p_2}=\frac{n}{p_2}\left(1-\frac{1}{p_1}\right)$. După eliminarea acestor elemente din şirul (*), mai rămân $n-\frac{n}{p_1}-\left(\frac{n}{p_2}-\frac{n}{p_1p_2}\right)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)$.

Continuând raționamentul în acest mod, se obține:

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)=$$

$$=p_1^{\alpha_1-1}\cdot p_2^{\alpha_2-1}\cdot\ldots\cdot p_k^{\alpha_k-1}\cdot(p_1-1)(p_2-1)\cdot\ldots\cdot(p_k-1).$$

Într-adevăr, presupunând că după eliminarea multiplilor lui p_1, p_2, ..., p_i obținem $n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_i}\right)$, atunci, la următorul pas vom elimina şi multiplii lui p_{i+1}, care sunt în număr de $\frac{n}{p_{i+1}}$.

Dintre aceştia $\frac{n}{p_1p_{i+1}}$ sunt şi multipli de p_1, $\frac{n}{p_2p_{i+1}}$ sunt şi multipli de p_2, ..., $\frac{n}{p_ip_{i+1}}$ sunt şi multipli de p_i, iar $\frac{n}{p_1p_2p_{i+1}}$ sunt şi multipli de p_1 şi p_2 etc.

Deci, ar trebui să mai eliminăm din (*)

$$\frac{n}{p_{i+1}}-\frac{n}{p_1p_{i+1}}-\frac{n}{p_2p_{i+1}}-\ldots-\frac{n}{p_ip_{i+1}}+\frac{n}{p_1p_2p_{i+1}}+\ldots$$

$$\ldots.+\frac{n}{p_1p_ip_{i+1}}\ldots+(-1)^i\frac{n}{p_1p_2\cdots p_{i+1}}$$

şi atunci rămân $n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_{i+1}}\right)$.

În acest mod se obţine că φ (n) = $n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)$.

Teoremă: Funcţia φ este multiplicativă.

Demonstraţie: Rezultă din faptul că pentru orice n ∈ **N***, avem

$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)$, unde $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$.

Definiţie: Funcţia μ : **N*** → **Z**

$$\mu(n)=\begin{cases}0, & \text{dacă n se divide printr – un păătratdiferit de unitate;}\\ (-1)^k, & \text{dacă n} = p_1p_2\ldots p_k \text{ cu } p_i \text{ prim, } \forall i\in\{1,2,\ldots,k\}\\ & \text{şi } i\neq j\Rightarrow p_i\neq p_j;\\ 1, & \text{dacă n} = 1\end{cases}$$

este numită **funcţia lui Moebius**.

Teoremă: Fie f o funcţie multiplicativă şi $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$ descompunerea canonică a numărului a. Atunci

$$\sum_{d|a}\mu(d)f(d)=(1-f(p_1))(1-f(p_2))\cdot\ldots\cdot(1-f(p_k))$$

(dacă a = 1, membrul al doilea se consideră egal cu 1)

Demonstraţie: Funcţia μ este evident multiplicativă, de aceea va fi multiplicativă şi funcţia μ · f, pe care o notăm cu g.

Conform unei teoreme anterioare, avem

$$\sum_{d|a}g(d)=(1+g(p_1)+g(p_1^2)+..+g(p_1^{\alpha_1}))\cdot\ldots\cdot(1+g(p_k)+g(p_k^2)+..+g(p_k^{\alpha_k})),$$

unde $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$.

Utilizând acum că g(p) = - f(p) şi $g(p^s) = 0$ pentru s > 1 şi p prim, obţinem egalitatea din enunţ.

Cazuri particulare:

1. Pentru f(a) = 1, ∀ a∈**N***, egalitatea din teorema anterioară devine:

$$\sum_{d|a}\mu(d)=\begin{cases}0, & \text{dacă} \quad a>1\\ 1, & \text{dacă} \quad a=1\end{cases}$$

2. Pentru f(a) = $\frac{1}{a}$, ∀ a∈**N***, egalitatea din teorema anterioară devine:

$$\sum_{d|a}\frac{\mu(d)}{d}=\begin{cases}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right), & \text{dacă} \quad a>1\\ 1, & \text{dacă} \quad a=1\end{cases}.$$

Are loc şi următoarea:

Propoziţie: (formula de inversiune a lui Moebius)

Fie (G, +) grup abelian şi f, g : **N*** → G.

Atunci $g(n)=\sum_{d|n}f(d)$, ∀ n∈**N***⇔ $f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)g(d)$, ∀ n∈**N***.

(În scriere multiplicativă, pentru (G, ·),

$$g(n)=\prod_{d|n}f(d),\forall n\in \mathrm{N}^* \Leftrightarrow f(n)=\prod_{d|n}g(d)^{\mu\left(\frac{n}{d}\right)},\forall n\in \mathrm{N}^*$$

)

Demonstraţie:

"⇒" $$\sum_{d|n}\mu\left(\frac{n}{d}\right)g(d)=\sum_{d|n}\mu\left(\frac{n}{d}\right)\left(\sum_{t|d}f(t)\right)=\sum_{\substack{t|d\\ d|n}}\mu\left(\frac{n}{d}\right)f(t)=$$

$$=\sum_{\substack{t|n\\ d'|\frac{n}{t}}}\mu(d')f(t)=\sum_{t|n}\left(\sum_{d'|\frac{n}{t}}\mu(d')\right)f(t)=f(n)$$

"⇐" se demonstrează în mod analog folosind faptul că t | d şi d | n ⇔ ⇔t | n şi t | d şi $\frac{d}{t}\left|\frac{n}{t}\right.$.

În ambele situații s-a ținut cont că $\sum_{d|n}\mu(d)=\begin{cases}1, & \text{dacă } n=1;\\ 0, & \text{dacă } n\geq 2.\end{cases}$

3.4. Clase de numere remarcabile

1. Numere amiabile. Numere perfecte

Definiție: Numerele naturale a şi b sunt numite numere **amiabile** dacă σ(a)=σ(b)= a + b.

Un exemplu de pereche de numere amiabile este: 220 şi 284, cunoscută încă din timpul şcolii lui Pitagora.

Într-adevăr, σ(220) = σ(284) = 504 = 220 + 284

($220 = 2^5 \cdot 5 \cdot 11$ şi $284 = 2^2 \cdot 71$)

Ulterior, Euler a găsit alte 65 de perechi de numere amiabile, dintre care menționăm:

$18416 = 2^4 \cdot 1151$ şi $17296 = 2^4 \cdot 23 \cdot 47$.

Definiție: Numărul natural a se numeşte **perfect** dacă σ(a) = 2a. În antichitate se cunoşteau patru numere perfecte: 6, 28, 496, 8126, apoi în secolul al XV-lea s-a găsit al 5-lea număr perfect, anume 33550336, iar în secolul al XVI-lea s-au descoperit încă trei numere perfecte:

8.589.869.056, 137.438.691.328, 2.305.843.008.139.952.128

La sfârşitul secolului al XIX-lea s-a găsit cel de-al 9-lea număr perfect:

2.658.455.991.569.831.744.654.692.615.953.842.176

Astăzi se pot găsi alte numere perfecte pare, foarte mari, cu ajutorul calculatoarelor moderne.

Primul rezultat privind numerele perfecte pare se găseşte în "Elementele" lui Euclid.

Teoremă (Euclid): Dacă $n = 2^v(2^{v+1}-1)$, unde $v\in\mathbf{N}$, iar $p=2^{v+1}-1$ este număr prim, atunci n este număr perfect.

Demonstrație: Ținând cont de faptul că p este impar, obținem

$\sigma(n) = \sigma(2^v)\,\sigma(p) = (1+2+...+2^v)\cdot(p+1)= (2^{v+1}-1)(p+1)=(2^{v+1}-1)\,2^{v+1} =2\cdot n$

Două mii de ani mai târziu, Euler demonstrează reciproca acestei teoreme:

Teoremă (Euler): Dacă numărul natural par n este perfect, atunci n este de forma $n = 2^v\,(2^{v+1}-1)$, unde $v\in\mathbf{N}$ şi $2^{v+1}-1$ este număr prim.

Demonstrație: Putem scrie $n = 2^v \cdot u$, unde $v \in \mathbf{N}-\{0\}$, u impar şi n este perfect, adică $\sigma(n) = 2n$.

Din $(2^v, u) = 1$, rezultă $\sigma(n) = \sigma(2^v) \cdot \sigma(u) = (2^{v+1}-1)\,\sigma(u)$; dar $\sigma(n) = 2n$, deci $2^{v+1} \cdot u = (2^{v+1}-1) \cdot \sigma(u)$. Rezultă că $(2^{v+1}-1) \mid 2^{v+1} \cdot u$ şi cum $(2^{v+1}-1, 2^{v+1}) = 1$, obținem că $(2^{v+1}-1) \mid u$. Atunci $\exists\ t \in \mathbf{N}$, astfel încât $u = (2^{v+1}-1)t$. Prin urmare, din $2^{v+1} \cdot u = (2^{v+1}-1)\,\sigma(u)$ va rezulta că $2^{v+1} \cdot t = \sigma(u)$.

Avem $t + (2^{v+1}-1)t = 2^{v+1} \cdot t = \sigma(u)$, deci singurii divizori ai lui u sunt t şi $(2^{v+1}-1)\,t$, prin urmare $t = 1$ şi $u = 2^{v+1}-1$ este prim.

2. Numere prime Mersenne

Definiție: Un număr prim de forma $p = 2^m-1$, cu $m \in \mathbf{N}$, $m > 1$, se numeşte **număr prim Mersenne**.

Teoremă: Dacă $a,m \in \mathbf{N}$, $m > 1$ şi $a^m - 1$ este prim, atunci $a = 2$ şi m este număr prim.

Demonstrație:

Din faptul că $a^m - 1$ este prim, $a^m - 1 = (a-1)(a^{m-1}+a^{m-2}+...+1)$ şi $m > 1$ rezultă că $a - 1 = 1$, adică $a = 2$.

Presupunem acum că m nu ar fi prim, adică $m = u \cdot v$, unde $1 < u < m$, $1 < v < m$. Obținem $2^m - 1 = (2^v)^u - 1 = (2^v - 1)(2^{v(u-1)} + 2^{v(u-2)} + ... + 1)$.

Din $2^v - 1 > 1$ şi $2^{v(u-1)} + ... + 1 > 1$, rezultă că $2^m - 1$ nu este prim, ceea ce este fals. Prin urmare, m este număr prim.

Definiție: Şirul $(\pi_n)_{n \in \mathbf{N}^*}$, unde $\pi_n = 2^{p_n - 1}$, iar p_n este cel de-al n-lea număr prim se numeşte **şirul lui Mersenne**.

S-a observat că următoarele numere prime ne furnizează numere prime Mersenne: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 858433.

Nu s-a demonstrat însă dacă există sau nu o infinitate de numere prime, în şirul lui Mersenne, aşadar nu ştim dacă există o infinitate de numere pare perfecte.

Pe de altă parte, nu s-a găsit nici un exemplu de număr impar perfect. Boethius (475-524) numea **saturate** numerele care satisfac proprietatea $\sigma(n) > 2n$ şi **deficitare** numerele care satisfac proprietatea $\sigma(n) < 2n$.

Teoremă: Dacă n este un număr natural impar cu doi divizori diferiți, atunci n este deficitar.

Demonstrație: Considerăm $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$, cu $p_1 \geq 3$ şi $p_2 \geq 5$ (deoarece n este impar).
Avem:

$$\frac{\sigma(n)}{n} = \frac{1}{p_1^{\alpha_1} \cdot p_2^{\alpha_2}} \cdot \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} < \frac{p_1}{p_1-1} \cdot \frac{p_2}{p_2-1} \leq \frac{3}{2} \cdot \frac{5}{4} < 2.$$

Teoremă: Pentru orice k∈**N**, există n∈**N**, aşa încât $\frac{\sigma(n)}{n} > k$.

Demonstrație: Deoarece

$$\left\{ d \in N \mid \quad d|n \right\} = \left\{ \frac{n}{d} \mid \quad d|n \right\}$$, rezultă că $\frac{\sigma(n)}{n} = \sum_{d|n} \frac{d}{n} = \sum_{d|n} \frac{1}{d}$.

Fie k∈N. Din faptul că seria $\sum_{n=1}^{\infty} \frac{1}{n}$ este divergentă, rezultă că există s ∈ **N**, aşa încât $1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{s} > k$
Considerând n = s! (= 1·2·....·s), avem:

$$\frac{\sigma(n)}{n} > 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{s} > k.$$

3. Numere prime Fermat

Teoremă: Dacă numărul $p = 2^k + 1$ este prim, unde k ∈ **N,** atunci există n ∈**N**, aşa încât $k = 2^n$, n ∈ **N**.

Demonstrație: Presupunem prin reducere la absurd că numărul k nu este o putere a lui 2, deci există n ∈ **N**, u este impar, u ≠1 încât $k=2^n \cdot u$. Obținem:

$$p = 2^{2^n u} + 1 = \left(2^{2^n} + 1\right)\left(2^{2^n(u-1)} - 2^{2^n(u-2)} + 2^{2^n(u-3)} - ... + 1\right).$$

Deoarece $1 < 2^{2^n} + 1 < 2^{2^n u} + 1$ rezultă că p nu este prim, ceea ce este fals.
Prin urmare k este de forma $k = 2^n$, unde n ∈ **N**.

Definiție: Şirul $(F_n)_{n\in\mathbf{N}^*}$, unde $F_n = 2^{2^n}+1$ se numeşte **şirul lui Fermat**.

Numerele prime din şirul $(F_n)_{n\in\mathbf{N}^*}$, se numesc **numere prime Fermat**.

Remercăm că pentru $m\in\{0,1,2,3,4\}$ se obțin, respectiv, numerele prime 3, 5, 17, 257, 65537, însă nu toate elementele şirului $(F_n)_{n\in\mathbf{N}^*}$ sunt prime, aşa cum presupunea Fermat. De exemplu, Euler a observat că $F_5 = 641 \cdot 6700417$, deci F_5 nu este prim.

Până în prezent, nu se ştie dacă există sau nu o infinitate de numere prime în şirul lui Fermat.

Numerele prime Fermat au căpătat importanță în matematică şi datorită faptului că, dat un număr prim p, poligonul regulat cu p laturi poate fi construit cu rigla şi compasul dacă şi numai dacă p este un număr prim Fermat.

Teoremă: Pentru orice două numere naturale distincte m şi n, numerele F_m şi F_n sunt prime între ele, adică $(F_m, F_n) = 1$.

Demonstrație: Presupunem că $m > n$, deci există $k\in\mathbf{N}$, $k > 0$, aşa încât $m = n + k$.

Considerăm $x = 2^{2^n}$ şi avem

$$F_m - 2 = 2^{2^m} - 1 = 2^{2^n\cdot 2^k} - 1 = x^{2^k} - 1 =$$
$$= (x+1)\cdot(x-1)\cdot(x^2+1)\cdot(x^4+1)\cdot\ldots\cdot\left(x^{2^{k-1}}+1\right)$$

de unde rezultă că $F_n = 2^{2^n}+1 = x+1 \mid F_m - 2$.

Dacă d este un divizor comun al lui F_m şi F_n, atunci din $F_n \mid F_m - 2$ rezultă $d \mid 2$, deci $d = 1$ sau $d = 2$. Dar, cum F_n este impar rezultă că $d \neq 2$.

Aşadar, $d = 1$, de unde rezultă $(F_m, F_n) = 1$.

Dintre numerele lui Fermat, astăzi se ştie, pe bază de demonstrație că F_5, F_7, F_8, F_{12}, F_{23}, F_{36}, F_{73} etc. nu sunt prime.

CAPITOLUL IV. CONGRUENȚE

4.1. Noțiuni şi rezultate introductive

1. Inelul claselor de resturi modulo n

Fie $n \in \mathbf{N}$, $n > 1$. Pe inelul $\mathbf{Z}$ al numerelor întregi definim următoarea relație binară, numită **congruența modulo n**:
dacă $a, b \in \mathbf{Z}$, spunem că a este congruent cu b modulo n şi scriem $a \equiv b \pmod n$ dacă $n \mid (a - b)$.

Vom mai nota relația de congruență modulo n prin $\equiv_n$ (atunci când n nu se deduce din context).

Această relație binară este o relație de echivalență, deoarece:

1°. $\forall a \in \mathbf{Z}$, avem $n \mid (a - a)$, deci $a \equiv a \pmod n$;

2°. dacă $a, b \in \mathbf{Z}$, aşa încât $a \equiv b \pmod n$, adică $n \mid (a - b)$, atunci $n \mid -(a - b)$ sau, altfel spus, $n \mid (b - a)$, adică $b \equiv a \pmod n$;

3°. dacă $a, b, c \in \mathbf{Z}$, aşa încât $a \equiv b \pmod n$ şi $b \equiv c \pmod n$, atunci $n \mid (a - b)$ şi $n \mid (b - c)$, de unde $n \mid (a - b) + (b - c)$, adică $n \mid (a - c)$, prin urmare $a \equiv c \pmod n$.

Pentru $a \in \mathbf{Z}$, vom nota cu $\hat{a} = \{b \in \mathbf{Z} \mid a \equiv b (\mathrm{mod}\, n)\}$ clasa de echivalență a lui a, (va fi numită **clasă de resturi modulo n**).

Mulțimea factor, $\mathbf{Z} / \equiv_n = \{\hat{a} \mid a \in \mathbf{Z}\}$, o vom nota cu $\mathbf{Z}_n$.

Dacă $a \not\equiv b \pmod n$ vom spune că a şi b sunt **distincte modulo n.**

Observație:

1°. Pentru $n = 0$, avem $a \equiv b \pmod 0 \Leftrightarrow 0 \mid (a - b) \Leftrightarrow a = b$ deci, $\forall a \in \mathbf{Z}$, avem $\hat{a} = \{a\}$ şi atunci mulțimea factor $\mathbf{Z} / \equiv_0$ este echipotentă (în bijecție) cu $\mathbf{Z}$.

2°. Pentru $n = 1$, avem $a \equiv b \pmod 1 \Leftrightarrow 1 \mid (a - b)$, ceea ce are loc pentru orice $a,b \in \mathbf{Z}$. Deci, $\forall a \in \mathbf{Z}$, $\hat{a} = \mathbf{Z}$, de unde rezultă că mulțimea factor $\mathbf{Z} / \equiv_1$ este echipotentă (în bijecție) cu orice mulțime formată dintr-un singur element.

Să considerăm, în cele ce urmează, $n \in \mathbf{N}$, $n > 1$. Dacă $a,b \in \mathbf{Z}$, din teorema împărțirii cu rest pentru numere întregi, avem:

$a = nq_1 + r_1$, unde $0 \le r_1 < n$

$b = nq_2 + r_2$, unde $0 \le r_2 < n$.

De aici, se obține a – b = n $(q_1 - q_2)$ + $(r_1 - r_2)$ şi, deci avem $n \mid (a - b) \Leftrightarrow n \mid (r_1 - r_2)$. Pe de altă parte, $0 \leq |r_1 - r_2| < n$, deci $n \mid (r_1 - r_2) \Leftrightarrow r_1 = r_2$.

Aşadar, dacă a,b $\in \mathbf{Z}$, atunci a ≡ b (mod n) dacă şi numai dacă a şi b dau acelaşi rest la împărțirea cu n.

Deci, dacă a $\in \mathbf{Z}$, atunci a = nq + r, unde $0 \leq r < n$ şi deci $n \mid (a - r)$, adică a ≡ r (mod n), de unde $\hat{a} = \hat{r}$. În plus, să remarcăm că dacă $0 \leq r_1 < n$ şi $0 \leq r_2 < n$ cu $r_1 \neq r_2$, atunci $r_1 \not\equiv r_2$ (mod n) şi deci $\hat{r_1} \neq \hat{r_2}$.

Prin urmare, mulțimea claselor de resturi modulo n este :

$$\mathbf{Z}_n = \left\{\hat{0}, \hat{1}, ..., \widehat{n-1}\right\}.$$

Pe această mulțime putem defini operațiile de adunare şi înmulțire astfel:

$\hat{a} + \hat{b} = \widehat{a+b}$ şi $\hat{a} \cdot \hat{b} = \widehat{a \cdot b}$ pentru orice $\hat{a}, \hat{b} \in \mathbf{Z}_n$.

Cele două operații nu depind de alegerea reprezentanților.

Într-adevăr, dacă $\hat{a} = \hat{a}'$ şi $\hat{a} = \hat{b}'$, adică $n \mid (a - a')$ şi $n \mid (b - b')$, atunci $n \mid (a + b) - (a' + b')$, deci $\widehat{a+b} = \widehat{a'+b'}$.

Rezultă că adunarea este bine definită.

Pentru verificarea faptului că înmulțirea este bine definită, considerăm $\hat{a} = \hat{a}'$, $\hat{b} = \hat{b}'$, de unde rezultă că ∃ k, l ∈ **Z**, aşa încât a = a' + kn şi b = b' + ln. Avem ab = a'b' + n (a'l + kb' + kln), de unde $n \mid (ab - a'b')$, deci $\hat{a} \cdot \hat{b} = \widehat{a \cdot b}$.

Pe baza proprietăților adunării şi înmulțirii numerelor întregi, rezultă că pentru orice $\hat{a}, \hat{b}, \hat{c} \in Z_n$, au loc egalitățile:

$$\left(\hat{a} + \hat{b}\right) + \hat{c} = \hat{a} + \left(\hat{b} + \hat{c}\right), \quad \hat{a} + \hat{b} = \hat{b} + \hat{a}, \quad \hat{a} + \hat{0} = \hat{0} + \hat{a} = \hat{a},$$

$$\hat{a} + \left(-\hat{a}\right) = \left(-\hat{a}\right) + \hat{a} = 0, \quad \left(\hat{a}\,\hat{b}\right)\hat{c} = \hat{a}\left(\hat{b}\,\hat{c}\right),$$

$\hat{a}\left(\hat{b}+\hat{c}\right)=\hat{a}\,\hat{b}+\hat{a}\,\hat{c}$ şi $\left(\hat{a}+\hat{b}\right)\hat{c}=\hat{a}\,\hat{c}+\hat{b}\,\hat{c}$, $\hat{a}\cdot\hat{1}=\hat{1}\cdot\hat{a}=\hat{a}$

De aici rezultă următoarea :

Teoremă: Mulţimea $\mathbf{Z}_n = \{\hat{0},\hat{1},.....,\hat{n-1}\}$ a claselor de resturi modulo n, înzestrată cu operaţiile de adunare şi înmulţire a claselor de resturi formează un inel unitar şi comutativ.

Propoziţie: O clasă de resturi $\hat{a} \in \mathbf{Z}_n$ este inversabilă în inelul $\mathbf{Z}_n$ dacă şi numai dacă (a, n)=1.

Demonstraţie: "$\Rightarrow$" Dacă $\hat{a}$ este inversabil în $\mathbf{Z}_n$, atunci există $\hat{b} \in \mathbf{Z}_n$, aşa încât $\hat{a}\,\hat{b}=\hat{1}$, adică n | (ab-1), de unde $\exists$ k $\in \mathbf{Z}$, încât ab – 1 = nk.

Deci ab + n ·(-k)=1, de unde rezultă, în baza proprietăţilor celui mai mare divizor comun a două numere întregi, că (a, n) = 1.

" $\Leftarrow$ " Dacă (a, n) = 1, atunci $\exists$ h, k$\in \mathbf{Z}$, aşa încât ah + nk = 1, de unde $\hat{1}=\hat{ah}+\hat{nk}=\hat{a}\,\hat{h}+\hat{n}\,\hat{k}=\hat{a}\,\hat{h}$ adică $\hat{a}$ este element inversabil al lui $\mathbf{Z}_n$.

Vom nota $U(\mathbf{Z}_n) = \{\hat{a} \in \mathbf{Z}_n | (a, n)=1\}$.

Corolar: Următoarele afirmaţii sunt echivalente:

1. $\mathbf{Z}_n$ este domeniu de integritate;
2. n este număr prim;
3. $\mathbf{Z}_n$ este corp comutativ.

Demonstraţie: 1 $\Rightarrow$ 2. Dacă n nu ar fi număr prim, atunci ar exista h, k $\in$ **N**, 1 < h < n, 1 < k < n, aşa încât n = hk, de unde $\hat{h} \neq \hat{0}$, $\hat{k} \neq \hat{0}$ şi $\hat{h}\,\hat{k}=\hat{hk}=\hat{n}=\hat{0}$, adică $\mathbf{Z}_n$ nu ar fi domeniu de integritate, ceea ce este fals. Deci n este număr prim.

2 $\Rightarrow$ 3. Fie $\hat{a} \in \mathbf{Z}_n$ $\hat{a} \neq \hat{0}$.Din faptul că n este prim rezultă (a, n) = 1 şi, de aici, conform propoziţiei anterioare, rezultă că $\hat{a} \in U(\mathbf{Z}_n)$.

Aşadar, orice element nenul al inelului unitar comutativ $\mathbf{Z}_n$ este inversabil, de unde rezultă că $\mathbf{Z}_n$ este corp.

$3 \Rightarrow 1$. Rezultă din faptul că orice corp comutativ nu are divizori ai lui zero, deci este domeniu de integritate.

2. Cazul polinoamelor cu coeficienți întregi

Fie $f \in \mathbf{Z}[X]$ următorul polinom cu coeficienți întregi:

$f(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X^1 + a_0$.

Vom nota tot cu f funcția polinomială asociată polinomului f. Remarcăm că pentru orice $x_0 \in \mathbf{Z}$, avem $f(x_0) \in \mathbf{Z}$.

Propoziție: Dacă $x \equiv y \pmod m$, atunci $f(x) \equiv f(y) \pmod m$.

Demonstrație: Într-adevăr, din $x \equiv y \pmod m$ rezultă că $\forall k \in \{0, 1, ..., n\}$ avem $x^k \equiv y^k \pmod m$ şi apoi $\forall k \in \{0, 1, ..., n\}$ avem $a_k x^k \equiv a_k y^k \pmod m$.

De aici rezultă că $f(x) \equiv f(y) \pmod m$.

Corolar: Dacă $f(x) \equiv 0 \pmod m$ şi $x \equiv y \pmod m$, atunci $f(y) \equiv 0 \pmod m$.

Considerații analoage se pot face şi pentru polinoame în mai multe nedeterminate, cu coeficienți întregi.

Dacă $f(X_1, X_2, ..., X_n) \in \mathbf{Z}[X_1, X_2, ..., X_n]$ şi n-uplele de numere întregi $(x_1, x_2, ..., x_n)$ şi $(y_1, y_2, ..., y_n)$ sunt astfel încât $\forall i \in \{1, 2, ..., n\}$, $x_i \equiv y_i \pmod m$, atunci, considerând din nou funcția polinomială asociată, vom avea $f(x_1, x_2, ..., x_n) \equiv f(y_1, y_2, ..., y_n) \pmod m$.

Mai mult putem asocia polinomului $f(X_1, X_2, ..., X_n)$ polinomul $\bar{f}(X_1, X_2, ..., X_n)$ cu coeficienți în $\mathbf{Z}_m$, care se obțin înlocuind fiecare din coeficienții lui f cu clasa sa de resturi modulo m.

Se spune că polinomul $\bar{f}$ se obține din polinomul f, prin **reducerea coeficienților modulo m**.

Pentru orice n-uplă de numere întregi $(x_1, x_2, ..., x_n)$ avem:

$\bar{f}(\bar{x}_1, \bar{x}_2, ..., \bar{x}_n) = \overline{f(x_1, x_2, ..., x_n)}$ şi în particular, avem:

$\bar{f}(\bar{x}_1, \bar{x}_2, ..., \bar{x}_n) = \bar{0} \Leftrightarrow f(x_1, x_2, ..., x_n) \equiv 0 \pmod m \Leftrightarrow$

$\Leftrightarrow m \mid f(x_1, x_2, .., x_n)$

Observații:

1. Congruența $f(x) \equiv 0 \pmod m$, unde $f \in \mathbf{Z}[X]$ devine o ecuație algebrică şi anume, $\bar{f}(\bar{x}) = \bar{0}$.
2. Congruența $f(x) \equiv 0 \pmod 1$ unde $f \in \mathbf{Z}[X]$ este verificată de toate numerele întregi.

Teoremă: Fie următorul sistem de congruențe:

$$\begin{cases} f_1(x) \equiv 0 (\mathrm{mod}\, m_1) \\ f_2(x) \equiv 0 (\mathrm{mod}\, m_2) \\ \ldots\ldots\ldots\ldots \\ f_s(x) \equiv 0 (\mathrm{mod}\, m_s) \end{cases} \qquad (*)$$

unde $m_1, m_2, .., m_s$ sunt numere naturale mai mari decât 1, iar $f_1(X)$, $f_2(X)$, ..., $f_s(X)$ sunt polinoame cu coeficienți întregi şi fie $m = [m_1, m_2, .., m_s]$ cel mai mic multiplu comun al numerelor $m_1, m_2, .., m_s$.

Dacă x_0 este un număr întreg care verifică sistemul de mai sus şi $x_1 \equiv x_0 \pmod m$, atunci x_1 verifică acelaşi sistem.

Demonstrație: Din $x_1 \equiv x_0 \pmod m$ rezultă $\forall\, k \in \{1, 2, ..., s\}$ avem $x_1 \equiv x_0 \pmod{m_k}$ şi conform unei propoziții anterioare, avem: $f_k(x_1) \equiv f_k(x_0) \pmod{m_k}$ pentru orice $k \in \{1, 2, ..., s\}$.

Cum $f_k(x_0) \equiv 0 \pmod{m_k}$, $\forall\, k \in \{1, 2, ..., s\}$ rezultă că: $f_k(x_1) \equiv 0 \pmod{m_k}, \forall\, k \in \{1, 2, ..., s\}$.

Definiție: Dacă $f(X), g(X) \in \mathbf{Z}[X]$, atunci vom spune că $g(X)$ **divide** $f(X)$ **modulo m** dacă există un polinom $h(X) \in \mathbf{Z}[X]$, aşa încât $f(X) \equiv g(X)\, h(X) \pmod m$.

Teoremă: Dacă x_0 este o soluție a congruenței $f(x) \equiv 0 \pmod m$, atunci $X - x_0$ divide modulo m pe $f(X)$ şi reciproc.

Demonstrație: Din faptul că are loc egalitatea:

$f(X) = (X - x_0) \cdot g(X) + f(x_0)$, obținută prin împărțirea polinomului $f(X)$ la polinomul $X - x_0$, rezultă echivalența:

$f(x_0) \equiv 0 \pmod m \Leftrightarrow f(X) \equiv (X - x_0)\, g(X) \pmod m$.

4.2. Congruențe de gradul întâi

Dacă $f(X) = a_1X + a_0 \in \mathbf{Z}[X]$ este un polinom de gradul întâi, atunci congruența $f(x) \equiv 0 \pmod m$ devine $a_1x + a_0 \equiv 0 \pmod m$, sau încă $a_1x \equiv a_0 \pmod m$.

Forma generală a unei congruențe de gradul întâi cu o necunoscută este: $ax \equiv c \pmod m$, unde $a, c \in \mathbf{Z}$, $m \in \mathbf{N}$, $a \not\equiv 0 \pmod m$.

Cazurile $m = 0$ şi $m = 1$ nu prezintă interes, deoarece $ax \equiv c \pmod 0$ devine $ax = c$ şi congruența este verificată numai de $\frac{c}{a}$, dacă $\frac{c}{a} \in \mathbf{Z}$, iar $ax \equiv c \pmod 1$ este verificată de orice număr întreg.

Propoziție: Congruența $ax \equiv c \pmod m$ are soluții dacă şi numai dacă cel mai mare divizor comun $d = (a, m)$ divide pe c.

Demonstrație: Fie $x_0 \in \mathbf{Z}$ o soluție a congruenței date. Atunci $ax_0 \equiv c \pmod m$, adică $m \mid (ax_0 - c)$, deci $\exists\, y_0 \in \mathbf{Z}$, aşa încât $ax_0 - c = my_0$. Din $d \mid a$ şi $d \mid m$ rezultă că $d \mid ax_0 - my_0 = c$.

Reciproc, dacă $d = (a, m) \mid c$, atunci există x_0', y_0' numere întregi, astfel încât $ax_0' + my_0' = d$. Notăm $c' = \frac{c}{d}$ şi avem:

$c = dc' = a(x_0'c') + m(y_0'c')$, de unde rezultă că $a(x_0'c') \equiv c \pmod m$, ceea ce arată că $x_0'c' \in \mathbf{Z}$ este o soluție a congruenței date.

Teoremă: Fie $d = (a, m)$. Presupunem că $d \mid c$. Fie x_0 o soluție a congruenței $ax \equiv c \pmod m$ şi fie $m' = \frac{m}{d} \in \mathbf{Z}$.

Atunci $x_0, x_0 + m', x_0 + 2m', \ldots, x_0 + (d - 1)m'$, sunt toate soluțiile, distincte modulo m, ale congruenței date (numărul acestora este d).

Demonstrație: Fie x_0, x_1 soluții oarecare ale congruenței date. Obținem că $ax_0 \equiv ax_1 \pmod m$ şi deci $\exists\, k \in \mathbf{Z}$ aşa încât $a(x_1 - x_0) = km$.

Fie $a' = \frac{a}{d} \in \mathbf{Z}$. Cum $m = dm'$, rezultă că $da'(x_1 - x_0) = kdm'$, de unde $a'(x_1 - x_0) = km'$, adică $m' \mid a'(x_1 - x_0)$.

Din $(a, m) = d$, $a = da'$ şi $m = dm'$ rezultă $(a', m') = 1$ şi atunci din $a'(x_1 - x_0) = km'$ se obține $m' \mid (x_1 - x_0)$, deci $\exists\, h \in \mathbf{Z}$, aşa încât $x_1 = x_0 + hm'$. Împărțind pe h la d avem: $h = dq + r$ cu $0 \le r < d$ şi deci $hm' = dm'q + rm'$, adică $x_1 - x_0 = mq + rm'$, de unde $\overline{x_1} = \overline{x_0 + rm'}$.

Prin urmare x_1 şi $x_0 + rm'$ coincid modulo m.

Aşadar, dacă x_0 este o soluție a congruenței $ax \equiv c \pmod m$, atunci orice altă soluție coincide modulo m cu $x_0 + rm'$, unde $r \in \{0,1, ...,d-1\}$.

Pe de altă parte, dacă $x_1 = x_0 + rm'$, atunci $ax_1 \equiv ax_0 + arm' \pmod m \equiv$ $\equiv ax_0 \pmod m + ra'dm' \pmod m \equiv ax_0 + ra'm \pmod m \equiv ax_0 \equiv c \pmod m$, adică $\overline{x_1}$ este, de asemenea, o soluție a congruenței $ax \equiv c \pmod m$. În plus, soluțiile $x_0 + rm'$, cu $r \in \{0,1,..., d-1\}$, sunt distincte două câte două modulo m, pentru că, altfel, dacă ar exista r şi s, aşa încât $0 \le r < s < d$ şi $\overline{x_0 + rm'} = \overline{x_0 + sm'}$, atunci $x_0 + rm' \equiv x_0 + sm' \pmod m$, adică $rm' \equiv sm' \pmod m$. Deci $m = dm' \mid m'(r - s)$, adică: $d \mid (r - s)$, de unde rezultă $d \le s - r \le s < d$, ceea ce este absurd.

4.3. Congruențe de grad superior

Fie m un număr natural, $m > 1$ şi $f = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X^1 + a_0$ un polinom cu coeficienți întregi.

Ne propunem să determinăm numerele întregi x, astfel încât $m \mid f(x)$, adică să rezolvăm congruența: $a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x^1 + a_0 \equiv 0 \pmod m$.

Dacă $m \nmid a_n$, spunem că avem **o congruență de grad n**.

Asociem polinomului $f = a_n X^n + ... + a_1 X^1 + a_0 \in \mathbf{Z}[X]$ următorul polinom în X, cu coeficienți în inelul de clase de resturi $\mathbf{Z}_m$:

$$\overline{f} = \overline{a_n} X^n + ... + \overline{a_1} X + \overline{a_0} \in \mathbf{Z}_m[X],$$

numit **redusul modulo m al lui f**.

Observăm că $grad\,\overline{f} = n \Leftrightarrow \overline{a_n} \neq \overline{0} \Leftrightarrow a_n \not\equiv 0 \pmod m$.

Propoziție: Un număr întreg x_0 este soluție a congruenței $a_n x^n + ... + a_1 x + a_0 \equiv 0 \pmod m$ dacă şi numai dacă $\overline{x_0} \in \mathbf{Z}_m$ este

rădăcină a ecuației $\overline{a_n}x^n + ... + \overline{a_1}x + \overline{a_0} = \overline{0}$. Altfel spus, $m \mid f(x_0)$ dacă şi numai dacă $\overline{f}\left(\overline{x_0}\right) = \overline{0}$, unde $f = a_n X^n + ... + a_1 X + a_0$.

Demonstrație:

Dacă $x_0 \in \mathbf{Z}$ este astfel încât $a_n x_0^n + ... + a_1 x_0 + a_0 \equiv 0 \pmod m$, atunci $\overline{0} = \overline{a_n x_0^n + ... + a_1 x_0 + a_0} = \overline{a_n x_0^n} + ... + \overline{a_1}\,\overline{x_0} + \overline{a_0} = \overline{f}\left(\overline{x_0}\right)$.

Reciproc, dacă $\overline{f}\left(\overline{x_0}\right) = \overline{0}$, atunci

$$\overline{a_n x_0^n + ... + a_1 x_0 + a_0} = \overline{a_n x_0^n} + ... + \overline{a_1}\,\overline{x_0} + \overline{a_0} = \overline{f}\left(\overline{x_0}\right) = \overline{0},$$

de unde $a_n x_0^n + ... + a_1 x_0 + a_0 \equiv 0 \pmod m$.

Corolar: Dacă $x_0 \in \mathbf{Z}$ este soluție a congruenței

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x^1 + a_0 \equiv 0 \pmod m \qquad (**)$$

şi dacă $y \in \mathbf{Z}$ este astfel încât $y \equiv x_0 \pmod m$, atunci y este soluție a congruenței (**).

Reamintim că soluțiile $x_1, x_2, ..., x_k$ ale congruenței

$$a_n x^n + ... + a_1 x^1 + a_0 \equiv 0 \pmod m$$

sunt numite soluții distincte modulo m dacă $x_i \not\equiv x_j \pmod m$ pentru $i \neq j$.

Numărul maxim de soluții distincte modulo m coincide cu numărul rădăcinilor distincte din $\mathbf{Z}_m$ al redusului modulo m al polinomului f (spunem şi că alcătuiesc un **sistem maximal** de soluții).

Pentru a cunoaşte toate soluțiile congruenței (**) este suficient să cunoaştem un sistem maximal $x_1, x_2, ..., x_r$ de soluții distincte modulo m şi atunci, în baza corolarului precedent, se obțin soluțiile congruenței date.

Pe de altă parte, numărul soluțiilor distincte modulo m este $\leq m$. Dacă numărul natural m este prim, atunci numărul soluțiilor

distincte modulo m depinde şi de gradul congruenței, aşa după cum rezultă din următoarea teoremă:

Teoremă (Lagrange): Fie p un număr prim şi

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x^1 + a_0 \equiv 0 \pmod p$$

o congruență de grad n, modulo p (deci $a_n \not\equiv 0 \pmod p$). Atunci numărul soluțiilor distincte modulo p ale acestei congruențe nu depăşeşte n.

Demonstrație: Procedăm prin inducție după n.

Pentru n = 1, considerăm x_1 şi $x_2 \in \mathbf{Z}$ soluții ale congruenței

$$a_1 x + a_0 \equiv 0 \pmod p \qquad (***)$$

Atunci $a_1x_1 + a_0 \equiv 0 \pmod p$ şi $a_1x_2 + a_0 \equiv 0 \pmod p$, de unde $a_1(x_1 - x_2) \equiv 0 \pmod p$, adică $p \mid a_1(x_1 - x_2)$ şi cum $p \nmid a_1$, deoarece $a_1 \not\equiv 0 \pmod p$ rezultă că $p \mid (x_1 - x_2)$, de unde $x_1 \equiv x_2 \pmod p$.

Aşadar, numărul soluțiilor distincte modulo p, ale congruenței (***) este cel mult 1.

Presupunem că n > 1 şi că afirmația dată în enunț este adevărată pentru congruențe de grad n-1.

Notăm cu f polinomul $a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X^1 + a_0$. Fie x_1, ..., x_q un sistem de soluții distincte modulo p ale congruenței $f(x) \equiv 0 \pmod p$. Să arătăm că $q \le n$. Împărțind pe f la $X - x_1$, obținem $f = (X - x_1)g + r$, cu $g \in \mathbf{Z}[X]$, grad g = n – 1 şi $r \in \mathbf{Z}$.

Avem $f(x_1) = r$ şi $f(x_1) \equiv 0 \pmod p$, deci $p \mid r$.

Pe de altă parte, $f(x_i) = (x_i - x_1)g(x_i) + r$ şi $f(x_i) \equiv 0 \pmod p$, pentru orice $i \in \{2,3,...,q\}$, deci $p \mid (x_i - x_1)g(x_i)$, deoarece $p \mid r$.

Dar p nu divide pe $x_i - x_1$, pentru $2 \le i \le q$, deoarece x_1, ..., x_q sunt soluții distincte modulo p. Aşadar, $p \mid g(x_i)$, pentru $2 \le i \le q$, adică:

pentru $\forall$ i $\in$ {2,...,q}, avem $g(x_i) \equiv 0 \pmod p$.

Dar grad g = n – 1, deci congruența $g(x) \equiv 0 \pmod p$ are gradul n –1 şi x_2, ..., x_q sunt soluții ale acesteia, distincte modulo p. Conform ipotezei inductive, rezultă $q - 1 \leq n - 1$, deci $q \leq n$.

Corolar: Dacă următoarele congruențe de grad n:

$$x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \equiv 0 \pmod p,$$

$$x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0 \equiv 0 \pmod p,$$

unde p este număr prim, admit în comun n rădăcini distincte modulo p, atunci $a_i \equiv b_i \pmod p$ pentru orice i $\in$ {0,1,...,n-1}.

Demonstrație: Presupunem că există k $\in$ **N**, $0 \leq k < n$, aşa încât $a_k \not\equiv b_k \pmod p$.

Fie $t = \max \{k \mid a_k \not\equiv b_k \pmod p\}$. Considerăm congruența $(a_t - b_t)x^t + ... + (a_1 - b_1)x + a_0 - b_0 \equiv 0 \pmod p$.

Această congruență are gradul $t < n$ şi admite n rădăcini distincte modulo p, contradicție cu teorema anterioară. Aşadar, pentru orice i $\in$ {0,1,...,n-1}, avem $a_i \equiv b_i \pmod p$.

4.4. Teoremele Euler, Fermat, Wilson. Lema chineză a resturilor

Propoziție: Congruența $ax \equiv c \pmod m$ are soluție unică modulo m dacă şi numai dacă (a, m) = 1.

Demonstrație: Fie d = (a, m). Am arătat în 4.2. că o congruență $ax \equiv c \pmod m$ are soluție dacă şi numai dacă $d \mid c$, iar în acest caz numărul soluțiilor distincte modulo m este egal cu d. Aşadar, congruența $ax \equiv c \pmod m$ are o unică soluție modulo m dacă şi numai dacă d = (a, m) = 1.

Reamintim că pentru $m \in \mathbf{N}$, $m > 1$, indicatorul lui Euler al lui m, $\varphi(m)$, este cardinalul mulțimii $\{n \mid n \in \mathbf{N}, 1 < n < m, (n, m) = 1\}$.

Fie inelul $\mathbf{Z}_m$ şi grupul unităților sale (adică grupul multiplicativ al elementelor sale inversabile), $U(\mathbf{Z}_m)$.

În paragraful 4.1. am arătat că $U(\mathbf{Z}_m) = \{\overline{a_1}, \overline{a_2}, ..., \overline{a_{\varphi(m)}}\}$ unde $\{a_1, a_2, ..., a_{\varphi(m)}\} = \{n \mid n \in \mathbf{N}, 1 < n < m, (n, m) = 1\}$.

Se spune, în acest caz, că numerele $a_1, a_2, ..., a_{\varphi(m)}$ formează un **sistem complet de resturi reduse modulo m.** De asemenea, formează un sistem complet de resturi reduse modulo m, orice mulțime de reprezentanți ai claselor $\overline{a_1}, \overline{a_2}, ..., \overline{a_{\varphi(m)}}$.

Teorema lui Euler: Dacă $a \in \mathbf{Z}$, $(a, m) = 1$, atunci $a^{\varphi(m)} \equiv 1 \pmod m$.

Demonstrație: Fie $a_1, a_2, ..., a_{\varphi(m)}$ un sistem complet de resturi reduse modulo m. Vom arăta că $aa_1, aa_2, ..., aa_{\varphi(m)}$ este de asemenea un sistem complet de resturi reduse modulo m. În adevăr, din (a,m)=1 rezultă că $\overline{a} \in U(\mathbf{Z}_m)$ şi funcția $f : U(\mathbf{Z}_m) \to U(\mathbf{Z}_m)$, definită prin $f(\overline{x}) = \overline{ax}$ este bijectivă. Aşadar, $U(\mathbf{Z}_m) = \{\overline{aa_1}, \overline{aa_2}, ..., \overline{aa_{\varphi(m)}}\}$.

Pe de altă parte, avem :

$$\overline{a_1}\,\overline{a_2} \cdot ... \cdot \overline{a_{\varphi(m)}} = \overline{aa_1}\,\overline{aa_2} \cdot ... \cdot \overline{aa_{\varphi(m)}} = \overline{a}^{\varphi(m)}\,\overline{a_1} \cdot \overline{a_2} \cdot ... \cdot \overline{a_{\varphi(m)}}$$ şi de aici rezultă că $\overline{a}^{\varphi(m)} = \overline{1}$, adică $a^{\varphi(m)} \equiv 1 \pmod m$.

Teorema anterioară admite şi **altă demonstrație**, anume:

Ordinul elementului $\overline{a} \in U(\mathbf{Z}_m)$ coincide cu ordinul grupului ciclic generat de $\overline{a}$ şi acest ordin este, conform teoremei lui Lagrange (relativ la indicele unui subgrup într-un grup), un divizor al

ordinului grupului $U(\mathbf{Z}_m)$, adică un divizor al lui $\varphi(m)$. Aşadar, $\bar{a}^{\varphi(m)} = \bar{1}$, adică $a^{\varphi(m)} \equiv 1 \pmod m$.

Teorema lui Fermat: Dacă $a \in \mathbf{Z}$ şi p este număr prim astfel încât $p \nmid a$, atunci $a^{p-1} \equiv 1 \pmod p$.

Demonstraţie: Din faptul că p este prim rezultă că $\varphi(p) = p - 1$ şi evident $(p, a) = 1$. Se aplică apoi teorema lui Euler pentru $m = p$.

Se deduce din cele anterioare că $a^x \equiv 1(m)$, unde $a, m \in \mathbf{N}^*$, $(a, m) = 1$ admite soluţii în $\mathbf{N}^*$.

Fie atunci $g(m,a) \min\{x \in \mathbf{N}^* | a^x \equiv 1(m)\}$, număr numit **gaussianul** lui m în baza a. Are loc:

Propoziţie: Fie $a, m \in \mathbf{N}$, $a, m > 1$, $(a, m) = 1$ şi $h, k \in \mathbf{Z}$, $h > k$. Următoarele condiţii sunt echivalente:

i) $a^h \equiv a^k \pmod m$;

ii) $a^{h-k} \equiv 1 \pmod m$;

iii) $h \equiv k \pmod g$, unde $g = g(m, a)$.

Demonstraţie:

i) $\Leftrightarrow$ ii) $a^h \equiv a^k \pmod m \Rightarrow a^h - a^k \equiv 0 \pmod m \Rightarrow a^k(a^{h-k} - 1) \equiv 0 \pmod m$. Dar $(a^k, m) = 1$, deci $a^{h-k} \equiv 1 \pmod m$.

Reciproc, dacă $a^{h-k} \equiv 1 \pmod m$, atunci prin multiplicare cu a^k se obţine $a^h \equiv a^k \pmod m$.

ii) $\Leftrightarrow$ iii) Conform teoremei împărţirii cu rest vom avea că există $h = q_1 g + r_1$, $k = q_2 g + r_2$. Din $a^h \equiv a^k \pmod m$ rezultă $a^{h-k} \equiv 1 \pmod m$ adică $a^{r_1 - r_2} \equiv 1 \pmod m$. Dar $r_1 - r_2 < g$. În consecinţă $r_1 = r_2$, deci $h - k = (q_1 - q_2)g$.

Reciproc, din $h \equiv k \pmod g$ rezultă $h - k = \rho g$, adică $\left(a^g\right)^\rho \equiv 1 \pmod m$, de unde $a^{h-k} \equiv 1 \pmod m$.

Drept consecință se deduce imediat că a^0, a^1, ..., a^{g-1} sunt distincte modulo m. Trecând la clase de congruență modulo m se obține că $\hat{a}^0,...,\hat{a}^{g-1}$ constituie un subgrup multiplicativ al lui $\mathbf{Z}_m$.

Propunem ca exercițiu detalierea cazului când (a,m) ≠ 1. Notând $g_0 = g\left(\frac{m}{(a,m)}, a\right)$ se va obține că şirul resturilor împărţirilor numerelor a^k ($k \in \mathbf{N}$) la m, după $\alpha = \min\{x \in \mathbf{N}, x > 1, a^x \equiv 0(\mathrm{mod}(a,m))\}$ resturi distincte vom avea $r_{\alpha+h} = r_{\alpha+k} \Leftrightarrow h \equiv k(\mathrm{mod}\ g_0)$ unde r_n este dat de $a^n = q_n m + r_n$, $n \in \mathbf{N}$.

Teorema lui Wilson: Dacă p este un număr prim, atunci $(p-1)! + 1 \equiv 0 \pmod p$.

Demonstrație: Pentru p = 2, afirmația din enunț se verifică direct. Dacă p ≠ 2, atunci p este impar.

Din teorema lui Fermat rezultă că $\forall\ a \in \{1,2,...,p-1\}$ avem $a^{p-1} \equiv 1 \pmod p$.

Pe de altă parte, $\forall\ a \in \{1,2,..., p-1\}$, a este soluție a congruenței de grad p – 1:

$$(x-1)(x-2)\cdot\ldots\cdot(x-(p-1)) \equiv 0 \pmod p.$$

Aşadar, congruența de mai sus şi congruența $x^{p-1} - 1 \equiv 0(\mathrm{mod}\ p)$ are aceleaşi (p-1) rădăcini distincte modulo p şi anume 1, 2, ..., p-1.

Cum p – 1 este par, termenul liber al polinomului

$(X-1)(X-2)\ldots(X-(p-1))$ este $(-1)(-2)\ldots(-(p-1)) = (-1)^{p-1}(p-1)! = = (p-1)!$

Aplicând corolarul teoremei lui Lagrange (vezi paragraful 4.3.) rezultă că $(p-1)! \equiv -1 \pmod p$.

Este adevărată şi reciproca acestei teoreme:

Teoremă: Dacă $p \in \mathbf{N}$, $p > 1$, astfel încât $(p-1)! + 1 \equiv 0 \pmod p$, atunci p este prim.

Demonstrație: Aplicăm metoda reducerii la absurd. Presupunând că p nu ar fi prim, am avea: $p = ab$, unde $1 < a < p$ şi $1 < b < p$.

Aşadar, a este unul dintre numerele 2, 3, ..., p – 1 şi deci $a \mid (p-1)!$. Pe de altă parte, $a \mid p$ şi cum $(p-1)! + 1 \equiv 0 \pmod p$, adică $p \mid (p-1)! + 1$, rezultă $a \mid 1$, ceea ce contrazice faptul că $a > 1$.

Lemă: Fie $m \in \mathbf{N}^*$ şi $a_1, a_2, ..., a_n \in \mathbf{Z}$, astfel încât $\forall i \in \{1,2,...,n\}$, $(a_i, m) = 1$. Atunci $(a, m) = 1$, unde $a = a_1 a_2 ... a_n$.

Demonstrație: Din faptul că $\forall i \in \{1,2,...,n\}$, $(a_i, m) = 1$, rezultă că $\overline{a_1}, \overline{a_2}, ..., \overline{a_n} \in U(\mathbf{Z}_m)$.

Deducem că $\overline{a} = \overline{a_1 a_2 ... a_n} = \overline{a_1}\,\overline{a_2} ... \overline{a_n} \in U(\mathbf{Z}_m)$, de unde obținem că $(a, m) = 1$.

Lemă: Fie $n \in \mathbf{N}^*$ şi $a_1, a_2, ..., a_s \in \mathbf{Z}$, aşa încât $\forall i \in \{1,2,...,s\}$, $a_i \mid n$. Dacă pentru orice $i, j \in \{1,2,...,s\}$ încât $i \neq j$, avem $(a_i, a_j) = 1$, atunci $a \mid n$, unde $a = a_1 a_2 ... a_s$.

Demonstrație: Afirmația este evidentă pentru $s = 1$. Dacă $s > 1$, avem, conform lemei anterioare, $(a_1, a_2 \cdot ... \cdot a_s) = 1$, ceea ce arată că este suficient să facem demonstrația în cazul $s = 2$.

În acest caz, din $(a_1, a_2) = 1$ rezultă că există $x_1, x_2 \in \mathbf{Z}$, astfel încât $a_1 x_1 + a_2 x_2 = 1$. Pe de altă parte, din $a_1 \mid n$ şi $a_2 \mid n$ rezultă că există $y_1, y_2 \in \mathbf{Z}$, aşa încât $n = a_1 y_1$ şi $n = a_2 y_2$.

Aşadar, $n = (a_1 x_1 + a_2 x_2)n = a_1 x_1 n + a_2 x_2 n = a_1 x_1 a_2 y_2 + a_2 x_2 a_1 y_1 = a_1 a_2 (x_1 y_2 + x_2 y_1)$, deci $a_1 a_2 \mid n$.

Lema chineză a resturilor: Dacă $m_1, m_2, ..., m_s \in \mathbf{Z}$, cu $(m_i, m_j) = 1$, pentru orice $i, j \in \{1,2,..,s\}$, $i \neq j$ şi dacă $b_1, b_2, ..., b_s \in \mathbf{Z}$, atunci există un număr întreg x, soluție a sistemului de congruențe:

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \ldots\ldots\ldots\ldots \\ x \equiv b_s \pmod{m_s}. \end{cases}$$

În plus pentru orice altă soluție y a sistemului, avem $x \equiv y \pmod m$, unde $m = m_1 \cdot m_2 \cdot \ldots \cdot m_s$.

Demonstrație: Pentru $\forall i \in \{1,2,..,s\}$, vom nota $n_i = \frac{m}{m_i} = \prod_{\substack{j=1 \\ j \neq i}}^{s} m_j$. Conform unei leme anterioare avem $(n_i, m_i) = 1$ şi există $u_i, v_i \in \mathbf{Z}$, aşa încât $u_i m_i + v_i n_i = 1$. Notăm $e_i = v_i n_i$; rezultă că $e_i \equiv 1 \pmod{m_i}$ şi $e_i \equiv 0 \pmod{m_j}$, pentru $j \neq i$.

Considerăm $x = \sum_{i=1}^{n} b_i e_i$. Atunci din $e_i \equiv 1 \pmod{m_i}$ şi $e_i \equiv 0 \pmod{m_j}$ cu $i \neq j$ se obține că $x \equiv b_j e_j \pmod{m_j} \equiv b_j \pmod{m_j}$.

Aşadar, $\forall j \in \{1,2,...,s\}$, avem $x \equiv b_j \pmod{m_j}$, adică x este soluție a sistemului de congruențe dat.

Fie acum y o altă soluție a acestui sistem de congruențe.

Pentru $\forall i \in \{1,2,...,s\}$ avem $x \equiv y \pmod{m_i}$, adică $m_i \mid (x - y)$ dar pentru orice $i, j \in \{1,2,...,s\}$ încât $i \neq j$, avem $(m_i, m_j) = 1$ şi atunci obținem, în baza lemei anterioare, $m \mid (x - y)$, unde $m = m_1 m_2 \ldots m_s$, deci $x \equiv y \pmod m$.

Caz particular: Fie $m_1, m_2 \in \mathbf{Z}$, $(m_1, m_2) = 1$. Conform lemei chineze a resturilor rezultă că pentru orice $b_1, b_2 \in \mathbf{Z}$, există un număr întreg x, aşa încât:

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2}. \end{cases}$$

În plus, dacă $y \in \mathbf{Z}$ este o altă soluție a acestui sistem, atunci $x \equiv y \pmod{m_1 m_2}$.

Considerăm $\varphi : \mathbf{Z}_{m_1 m_2} \to \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2}, \varphi(\bar{x}) = (\hat{x}, \overline{\overline{x}})$, unde cu $\bar{x}$ am notat clasa elementului x modulo m_1m_2, cu $\hat{x}$ am nota clasa lui x modulo m_1 şi cu $\overline{\overline{x}}$ am notat clasa lui x modulo m_2.

Conform lemei chineze a resturilor, obținem că aplicația φ este bijectivă.

CAPITOLUL V. ELEMENTE DE TEORIA NUMERELOR

5.1. Fracții continue

Prin fracție continuă se înțelege o expresie de forma $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}}$, unde, în contextul prezentului paragraf, $a_0 \in \mathbf{Z}$, $a_1, a_2, \dots \in \mathbf{N}^*$.

Dacă mulțimea $\{ a_1, a_2, \dots\}$ este finită spunem că avem o fracție continuă finită, iar în caz contrar (aici numărabil infinită) spunem că avem o fracție continuă infinită.

Din motive tehnice noi vom nota $[a_0, a_1, a_2, \dots a_n, \dots]$ fracțiile continue (în cazul finit, notăm $[a_0, a_1, a_2, \dots a_n]$, $n \in \mathbf{N}$).

În ambele cazuri fracția continuă $[a_0, a_1, a_2, \dots a_k]$ ($k \le n$ în cazul finit) este numită **redusa de ordin k** a fracției continue date.

Este clar că, în contextul prezentat, $[a_0, a_1, a_2, \dots a_k]$ poate fi reprezentat în urma calculelor, sub forma $\delta_k = \frac{p_k}{q_k} \in \mathbf{Q}$ (cu $\frac{p_k}{q_k}$ fracție ireductibilă). În cazul infinit vom avea un şir $(\delta_k)_{k \in \mathbf{N}}$.

Observație: Procedând inductiv, se deduc relațiile:

i) $p_k = a_k p_{k-1} + p_{k-2}$ $(k \geq 2)$;

ii) $q_k = a_k q_{k-1} + q_{k-2}$ $(k \geq 2)$;

iii) $\delta_k - \delta_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$.

Propoziție: $\forall \alpha \in \mathbf{R}$, există şi este unică o fracție continuă infinită dacă α este irațional, $[a_0, a_1, a_2, ...]$, şi finită dacă $\alpha \in \mathbf{Q}$, $[a_0, a_1, a_2, ...a_n]$, aşa încât $\alpha = \lim_{k\to\infty} \frac{p_k}{q_k}$ (în primul caz) şi respectiv $\alpha = \frac{p_n}{q_n}$.

Demonstrație: Fie $\alpha \in \mathbf{R}$. Notăm $a_0 = [\alpha]$ (partea întreagă a lui α). Presupunând că $\alpha \notin \mathbf{Z}$, se determină:

$$r_1 = \frac{1}{\alpha - a_0},\ a_1 = [r_1];$$

.....

$$r_{k+1} = \frac{1}{r_k - a_k},\ a_{k+1} = [r_{k+1}];$$

.....

Dacă α este rațional, atunci toți r_n sunt rționali şi în acest caz există $n \in \mathbf{N}$, aşa încât $r_n = a_n \in \mathbf{N}^*$.

Dacă α este irațional, atunci toți r_n sunt iraționali, altfel spus procedeul anterior este infinit.

În acest caz $\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^2}$, aşadar $\delta_k \xrightarrow[k\to\infty]{} \alpha$

Unicitatea se demonstrează uşor, procedând prin "reducere la absurd".

Observație:

i) Pentru cazul finit ($\alpha \in \mathbf{Q}$) se recunoaşte, în procedeul descris în demonstrație, algoritmul lui Euclid.

ii) Pentru numere irașionale se pot găsi metode specifice, de exemplu

$$\sqrt{2} = 1 + \sqrt{2} - 1 = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{1+1+\sqrt{2}-1} =$$

$$= 1 + \frac{1}{1+1+\frac{1}{\sqrt{2}+1}} = 1 + \frac{1}{2+\frac{1}{\sqrt{2}+1}} = \ldots.$$

5.2.Ecuații diofantice

Prin ecuație diofantică vom înțelege o ecuație de forma $F(x_1,...,x_n)=0$, unde F este un polinom în n nedeterminate cu coeficienți în **Z**, pentru care se cer soluțiile $(x_1^0,....x_n^0)$ cu $x_i^0 \in \mathbf{Z}$, $\forall$ i $\in \{1, 2,..., n\}$.

În cele ce urmează ne vom opri doar asupra a două tipuri de ecuații diofantice: ax + by +c = 0, a, b, c $\in$ **Z**, a, b $\neq$ 0 şi $x^2 + y^2 = z^2$.

Propoziție: Ecuația ax + by +c = 0, a, b, c $\in$ **Z**, a, b $\neq$ 0 admite soluții dacă şi numai dacă (a, b)ξc.

Demonstrație: Dacă (x_1, y_1) reprezintă o soluție a ecuației şi (a, b)=d ($a = a_1d$, $b = b_1d$), atunci $d(a_1x_1 + b_1y_1) +c =0$ adică dξc.

Reciproc, fie $c_1 = \frac{c}{d}$. Întrucât d= (a, b) rezultă că există u, v $\in$**Z** aşa încât au + bv = d.

De aici, se deduce că: $a(-c_1u) + b(-c_1v) + c = 0$, deci $(-c_1u, -c_1v)$ este soluție a ecuației date.

În cele ce urmează, va fi considerat doar cazul (a, b) = 1.

Propoziție: Dacă (x_0, y_0) reprezintă o soluție întreagă a ecuației ax + by +c = 0, a, b, c $\in$ **Z**, a, b $\neq$ 0, atunci formulele $x=x_0–bt$, $y= y_0+ at$, t $\in$ **Z** dau toate soluțiile ecuației considerate.

Demonstrație: Fie (x_0, y_0) soluție a ecuației date $ax_0+by_0 +c= 0$. Scăzând membru cu membru din ax + by + c = 0 se obține:

$a x - a x_0 + by - by_0 = 0$, adică, de exemplu $y – y_0 = \frac{a}{b}(x – x_0)$.

Deoarece $y – y_0$ este necesar să fie număr întreg, iar (a, b)= 1, rezultă că $x_0 – x$ trebuie să fie divizibil cu b, adică să fie de forma $x_0 – x = bt$, cu t $\in$**Z**.

Se deduce că $x = x_0 – bt$, $y = y_0 + at$.

Prin verificare directă se deduce că orice pereche de numere $x = x_0 - bt$, $y = y_0 + at$, $t \in \mathbf{Z}$, este soluție a ecuației date.

Rămâne deschisă atunci problema găsirii unei soluții.

Folosind scrierea lui $\frac{a}{b}$ ca fracție continuă (finită) se obține: $\frac{a}{b} - \delta_{n-1} = \frac{(-1)^n}{bq_{n-1}}$, ceea ce conduce la $aq_{n-1} - bp_{n-1} = (-1)^n$, adică:

$a((-1)^{n-1} c\, q_{n-1}) + b((-1)^n c\, p_{n-1}) + c = 0$, altfel spus la o soluție a ecuației date.

În ceea ce priveşte ecuația $x^2 + y^2 = z^2$ remarcăm întâi că, fără a restrânge generalitatea, ne putem limita la cazul $x, y, z \in \mathbf{N}$ şi se pot cere doar soluțiile (x_0, y_0, z_0), cu $(x_0, y_0) = 1$.

În caz contrar, fie $(x_0, y_0) = d$ şi $x_0 = dx_1$, $y_0 = dy_1$. Vom înlocui şi obținem: $x_1^2 d^2 + y_1^2 d^2 = z_0^2$ adică $d^2 \mid z_0^2$ şi, prin urmare $d \mid z_0$, altfel spus $z_0 = z_1 d$ (aceasta are loc pentru orice soluție (x_0, y_0, z_0) a ecuației inițiale).

Propoziție: Soluțiile ecuației $x^2 + y^2 = z^2$ ce satisfac pe $(x, y) = 1$, sunt date de formulele $x = uv$, $y = \frac{u^2 - v^2}{2}$, $z = \frac{u^2 + v^2}{2}$, unde $u > v$, u, v impare, $(u,v)=1$.

Demonstrație:

Ecuația poate fi scrisă sub forma $x^2 = (z + y)(z - y)$. Notăm $d_1 = (z + y, z - y)$. Putem scrie $z + y = ad_1$ şi $z - y = bd_1$ cu $(a,b)=1$. Atunci $x^2 = ab d_1^2$, de unde rezultă că a, b sunt pătrate perfecte, $a = u^2$, $b = v^2$.

Se deduce $x = uvd_1$, $y = \frac{u^2 - v^2}{2} d_1$, $z = \frac{u^2 + v^2}{2} d_1$

dar $d_1 = 1$ ($(x, y)=1$) şi în consecință $x = uv$, $y = \frac{u^2 - v^2}{2}$, $z = \frac{u^2 + v^2}{2}$.

5.3. Şirul lui Fibonacci

Şirul lui Fibonacci se definişte recurent astfel:

$F_0 = 0$; $F_1 = F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$, $\forall\, n \geq 2$.

Observaţie: În general, un şir $(f_n)_{n\in\mathbf{N}}$ ce satisface $f_n = f_{n-1} + f_{n-2}$, $\forall n\geq 2$, este numit şir Fibonacci (nu al lui Fibonacci).

Observaţie: Relaţia de recurenţă de tipul anterior se generalizează la: $x_n = ax_{n-1} + bx_{n-2}$, $a, b \in \mathbf{R}$, $n \geq 2$.

Se obţine:

Propoziţie: Dacă $(x_n)_{n\in\mathbf{N}}$ este un şir de numere reale pentru care există $a, b\in\mathbf{R}$ aşa încât $x_n = ax_{n-1} + bx_{n-2}$, $a, b \in\mathbf{R}$, $n \geq 2$, atunci: $x_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} x_1 - \alpha\beta \cdot \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} x_0, \forall n \geq 1$ unde α şi β sunt rădăcinile ecuaţiei $x^2 = ax + b$ (numită ecuaţia caracteristică ataşată şirului $\{x_n\}_{n\in\mathbf{N}}$) şi $\alpha \neq \beta$.

Demonstraţie: Scriem relaţia de recurenţă $x_n - ax_{n-1} - bx_{n-2} = 0$ şi înlocuind a prin $\alpha+\beta$ şi b prin $-\alpha\beta$, obţinem:

$x_n - \alpha x_{n-1} = \beta (x_{n-1} - \alpha x_{n-2})$, $\forall\ n \geq 2$.

Notăm $y_n = x_n - \alpha x_{n-1}$ şi obţinem $y_n = \beta y_{n-1}$, $\forall\ n \geq 2$.

Rezultă că: $y_n=\beta^{n-1}y_1$, adică $x_n - \alpha x_{n-1} = \beta^{n-1}y_1$.

Dacă pentru orice $n \in\mathbf{N}$ notăm $z_n = \frac{x_n}{\beta^n}$ găsim $\beta z_n - \alpha z_{n-1} = y_1$, adică $z_n = \frac{\alpha}{\beta} z_{n-1} + \frac{y_1}{\beta}$.

Deducem că:

$$z_n - z_{n-1} = \frac{\alpha}{\beta}(z_{n-1} - z_{n-2}) = \ldots = \left(\frac{\alpha}{\beta}\right)^{n-2}(z_2 - z_1)$$

Altfel spus:

$$z_2 - z_1 = z_2 - z_1$$

$$z_3 - z_2 = \frac{\alpha}{\beta}(z_2 - z_1)$$

.....

$$z_n - z_{n-1} = \left(\frac{\alpha}{\beta}\right)^{n-2}(z_2 - z_1)$$

$$z_n = \left(\frac{\alpha}{\beta}\right)^{n-1} z_1 + \frac{\left(\frac{\alpha}{\beta}\right)^{n-1} - 1}{\left(\frac{\alpha}{\beta}\right) - 1} \cdot \frac{y_1}{\beta}$$

adică:

Se deduce imediat că: $x_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} x_1 - \alpha\beta \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} x_0, \forall n \geq 2$.

Observație: Dacă $\alpha = \beta$, atunci în loc de $\frac{\alpha^n - \beta^n}{\alpha - \beta}$ se scrie: $\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} = \alpha^{n-2} + .. + \beta^{n-2}$ şi analog: $\alpha^{n-1} + \alpha^{n-2}\beta + .. + \beta^{n-1}$.

Consecință: $F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$, $\forall$ n ≥ 0.

Observație: Pentru şirul lui Fibonacci au loc:

i) $F_{n+m} = F_{n-1} F_m + F_n F_{m+1}$, $\forall$ n ≥ 2 şi $\forall$ m ≥ 1. (cazuri particulare: $m = n = p \Rightarrow F_{2p} = F_p(F_p + 2 F_{p-1})$

$m = p - 1, n = p \Rightarrow F_{2p-1} = F_p^2 + F_{p-1}^2$

$m = kn$, $(n \mid m) \Rightarrow F_n \mid F_m$)

ii) $(F_n, F_m) = F_{(n,m)}$ ((a, b) notează cel mai mare divizor comun al numerelor a, b).

Demonstrație: i) Se fixează n şi se face inducție după m. Pentru m = 1 este evident. În continuare avem:

$F_{n+k} = F_{n+k-2} + F_{n+k-1} = F_{n-1} F_{k-2} + F_n F_{k-1} + F_{n-1} F_{k-1} + F_n F_k =$
$= F_{n-1} (F_{k-2} + F_{k-1}) + F_n (F_{k-1} + F_k) = F_{n-1} F_k + F_n F_{k+1}$.

i) (n, m) se obține prin algoritmul lui Euclid anume:

$n = mq_1 + r_1, 0 \leq r_1 < m$

$m = r_1 q_2 + r_2, 0 \leq r_2 < r_1$

.....

$r_{k-3} = r_{k-2} q_{k-2} + r_{k-1}, 0 \leq r_{k-1} < r_{k-2}$

$r_{k-2} = r_{k-1} q_{k-1}$, anume $d(n, m) = r_{k-1}$.

Avem şi că, pentru cazul $n = mq + r, 0 \leq r < m$, $(F_n, F_m) = (F_m, F_r)$.

Într-adevăr: $(F_n, F_m) = (F_{mq+r}, F_m) = (F_{mq-1}F_r + F_{mq}F_{r+1}, F_m)$, dar $F_m \mid F_{mq}$ (deoarece $m \mid mq$) şi atunci$(F_n, F_m) = (F_{mq-1}F_r, F_m)$.
Dar $(F_{mq-1}, F_m) = 1$(altfel $d = (F_{mq-1}, F_m) \Rightarrow d \xi F_{mq}, d \xi F_{mq-1}, \ldots, d \xi 1$).

Rezultă că $(F_n, F_m) = (F_m, F_r)$.

Aplicând această egalitate pentru fiecare dintre egalităţile date în algoritmul lui Euclid, se obtine: $(F_n,F_m) = (F_m, F_{r_1}) = (F_{r_{k-1}},0) = F_{r_{k-1}} = F_d = F_{(n,m)}$

Observaţie: O altă demonstraţie se obţine utilizând proprietăţile calculului matriceal. În acest sens este convenabil să considerăm şirul lui Fibonacci definit pe **Z** adăugând $F_{-n} = (-1)^{n+1}F_n$ pentru $n \in \mathbf{N}^*$ (aceasta se deduce din relaţia de recurenţă, prin inducţie).

Considerând matricea $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ se obţine prin inducţie că $A^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}$.

De exemplu, egalitatea $A^{m+n} = A^m \cdot A^n$ conduce la i) din observaţia anterioară.

Observaţie: Pot reţine atenţia două aspecte (ce vor fi abordate în continuare) şi anume:

1°) proprietatea $(F_n, F_m) = F_{(n,m)}$ întâlnită şi în cazul şirurilor date de $a_n = 2^n - 1$ (anume $(2^n - 1, 2^m - 1) = 2^{(n,m)} - 1$) şi în cazul polinoamelor $(X^n - 1, X^m - 1) = X^{(m,n)} - 1$.

2°) prezenţa numărului $\frac{1+\sqrt{5}}{2}$ numit şi numărul (raportul) de aur foarte utilizat şi în artă şi arhitectură.

Vom analiza cele două aspecte în ordinea prezentată.

1°) **Definiţie:** Un şir numeric $(a_n)_{n \in \mathbf{N}}$ este numit d – şir dacă satisface condiţia $(a_n, a_m) = a_{(n,m)}$ $\forall$ $n,m \in \mathbf{N}^*$.

Definiţie: Un şir numeric $(b_n)_{n \in \mathbf{N}}$ este numit D-şir dacă din $n \nmid m$ şi $m \nmid n \Rightarrow (b_m, b_n) = 1$.

Observaţie: Pentru orice d-şir $(a_n)_{n \in \mathbf{N}}$, avem că $n \mid m \Rightarrow a_n \mid a_m$.
Într-adevăr, $n \mid m \Rightarrow (n,m) = n \Rightarrow a_{(n,m)} = a_n \Rightarrow (a_n, a_m) = a_n \Rightarrow a_n \mid a_m$.

Observație: În ipoteza $a_k \neq a_t \ \forall \ k \neq t$ (într-un d-şir) avem că $a_n | a_m \Rightarrow n|m$.

Propoziție: Un şir $(a_n)_{n\in\mathbf{N}}$ este d- şir $\Leftrightarrow \exists$ un unic D-şir $(b_n)_{n\in\mathbf{N}}$ aşa încât $a_n = \prod_{d|n} b_d$ (relația este numită relația lui Dedekind), produsul făcându-se după toți divizorii naturali ai lui n.

Demonstrație: $b_1 = a_1$, $b_2 = \frac{a_2}{a_1}$, $b_3 = \frac{a_3}{a_1}$. Presupunând că s-au construit $b_1,..., b_{n-1}$ aşa încât $a_k = \prod_{d|k} b_d$ pentru k = 1, ..., n-1, construim b_n.

Întâi arătăm că $\prod_{\substack{d|n \\ d<n}} b_d$ coincide cu cel mai mic multiplu comun al elementelor mulțimii $\{a_d \mid d|n, d < n\}$ pe care îl notăm cu M.

Deoarece $\prod_{d|d_0} b_d = a_{d_0}$, pentru orice $d_0 | n$, $d_0 < n$ rezultă că $M | \prod_{\substack{d|n \\ d<n}} b_d$.

Pentru a arăta că $\prod_{\substack{d|n \\ d<n}} b_d \mid M$, fie p un număr prim ce divide $\prod_{\substack{d|n \\ d<n}} b_d$ (presupunem că $p^\alpha \mid \prod_{\substack{d|n \\ d<n}} b_d$). Se arată că există a_d unde $d | n$, $d<n$, cu $p^\alpha \mid a_d$, ceea ce conduce la $\prod_{\substack{d|n \\ d<n}} b_d \mid M$.

Definim acum $b_n = \frac{a_n}{M}$.

Se verifică apoi că b_k divide $\frac{a_k}{(a_k, a_t)}$ (pentru $k < t$, $k \nmid t$, $1 \le k,t \le n-1$ şi b_t divide $\frac{a_t}{(a_k, a_t)}$, deci (b_k, b_t) divide $\left(\frac{a_k}{(a_k, a_t)}, \frac{a_t}{(a_k, a_t)}\right) = 1$, de unde rezultă că $(b_n)_{n\in\mathbf{N}}$ este D - şir.

Unicitatea lui $(b_n)_{n\in\mathbf{N}}$ se arată prin reducere la absurd: presupunând că există şi un D – şir $(c_n)_{n\in\mathbf{N}}$ satisfăcând relația din enunț se demonstrează prin inducție că $b_n = c_n$, $\forall$ n $\in\mathbf{N}$.

Reciproc: să arătăm că în ipoteza $(b_n)_{n\in\mathbf{N}}$ este D – şir, atunci $(a_n)_{n\in\mathbf{N}}$, unde $a_n = \prod_{d|n} b_n$, este d- şir.

Avem că :

$$(a_n, a_m) = \left(\prod_{d|n} b_d, \prod_{d|m} b_d\right) = \prod_{d|(n,m)} b_d \left(\prod_{\substack{d'|n \\ d' \nmid m}} b_{d'}, \prod_{\substack{d''|m \\ d'' \nmid n}} b_{d''}\right) = \prod_{d|(n,m)} b_d = a_{(n,m)}$$

Am folosit faptul că din d’ $|$ n, d’ $\nmid$ m şi d” $|$ m, d” $\nmid$ n rezultă că d’ $\nmid$ d” şi d” $\nmid$ d’, deci $(b_{d'}, b_{d''}) = 1$.

Observație: Dacă $(a_n)_{n\in\mathbf{N}}$ este d – şir, atunci şirul $(b_n)_{n\in\mathbf{N}}$ dat de $b_n = \prod_{d|n} a_d^{\mu\left(\frac{n}{d}\right)}$ este D – şir, anume unicul D-şir precizat în propoziția anterioară (aici μ notează funcția lui Möbus, $\mu : \mathbf{N}^* \to \{-1, 0, 1\}$).

Exemple: D - şirul asociat şirului lui Fibonacci este dat de $b_n = \prod_{d|n} F_d^{\mu\left(\frac{n}{d}\right)}$.

- D – şirul asociat şirului $a_n = 2^{n-1}$, n$\in\mathbf{N}^*$ este dat de $b_n = \Phi_n(2)$ unde Φ_n este cel de-al n-lea polinom ciclotomic, n$\in\mathbf{N}^*$.
- D – şirul asociat şirului de polinoame $f_n = X^n - 1$ n$\in\mathbf{N}^*$ este tocmai şirul polinoamelor ciclotomice.

2°) Referitor la cel de-al doilea aspect (numărul de aur):

Se ştie că $\frac{\sqrt{5}+1}{2}$ este soluție a ecuației $x^2 – x – 1 = 0$ obținută, de exemplu, în problema determinării unui punct al unui segment care să împartă segmentul respectiv în două segmente aşa încât segmentul cel mai mare să fie medie geometrică dintre segmentul întreg şi segmentul rămas.

Acest număr se cunoaşte încă din antichitate sub numele de "numărul de aur"; în cazul piramidei lui Keops raportul dintre apotema unei fețe laterale şi apotema bazei este $\frac{\sqrt{5}+1}{2}$.

Numărul de aur a fost studiat în şcoala lui Pitagora. Platon aminteşte în "Dialoguri" de acest număr.

Problema 11 din Cartea a II-[a] a Elementelor lui Euclid (reluată şi în Cartea a VI-[a]) conduce la numărul de aur. El apare în cadrul construcțiilor poligoanelor regulate cu 5^k laturi ($k \in \mathbf{N}^*$).

Leonardo da Vinci a redescoperit acest număr studiind proporțiile dintre diferitele părți ale corpului uman.

În legătură cu şirul lui Fibonacci obținem că $\lim \frac{F_n}{F_{n-1}} = \frac{\sqrt{5}+1}{2}$ (din $F_n = F_{n-2} + F_{n-1}$).

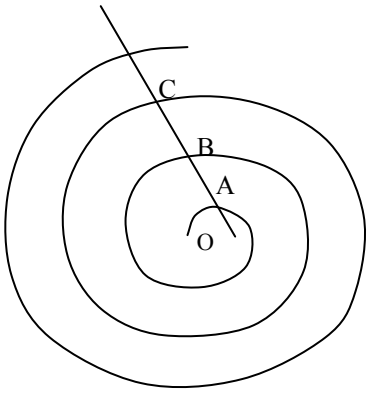
Notând $\frac{\sqrt{5}+1}{2} = \Phi$ se obține şirul 1, Φ, Φ^2, ... ce are şi proprietatea $\Phi^n = \Phi^{n-1} + \Phi^{n-2}$ (notând $u_n = \Phi^n$ obținem $u_n = u_{n-1} + u_{n-2}$). Reciproc orice şir $(u_n)_{n \in \mathbf{N}^*}$ cu proprietatea $u_n = q^n$ şi $q^n = q^{n-1} + q^{n-2}$ are forma generală (*) $u_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} + c_2\left(\frac{1-\sqrt{5}}{2}\right)^{n-1}$.

Condițiile $u_1 = u_2 = 1$ conduc la şirul lui Fibonacci.

De remarcat că toate şirurile obținute din (*) prin particularizarea constantelor c_1 şi c_2 au proprietatea că reflectă numeric însuşirile materiei vii de a se dezvolta.

Proprietatea a fost verificată de botanişti, atunci când au măsurat distanțele dintre nodurile de unde cresc frunzele, de zoologi prin observarea cochiliilor melcilor, a scoicilor etc.

Urmărind "spirala logaritmică" a cochiliei melcului (şi a cozii desfăcute a unui păun) se obține că:



$$\frac{OB}{OA} = \frac{OC}{OB} = \ldots = \frac{\sqrt{5}+1}{2}$$

Proprietatea acestei curbe de a rămâne egală cu ea însăşi când se transformă prin asemănare a fost remarcată de Iacob Bernoulli (a cerut ca această curbă să-i fie gravată pe mormânt cu inscripția "*Eadem mutato resugo*").

$$\Phi = 1 + \frac{1}{1 + \frac{1}{1 + ...}} = \sqrt{1 + \sqrt{1 + ...}}$$

Mai remarcăm şi că

$$\Phi = 1 + \frac{1}{1 \cdot 2} - \frac{1}{2 \cdot 3} + ... + \frac{(-1)^n}{F_n F_{n+1}} + ...$$

şi

$$\Phi = \left(1 + \frac{1}{1^2}\right)\left(1 - \frac{1}{2^2}\right)...\left(1 + \frac{(-1)^n}{F_n^2}\right)...$$

În arhitectură, încă Vitruviu (sec. I î.H) atrăgea atenția asupra acordului ce trebuie stabilit între diferitele părți ale unei clădiri şi clădirea întreagă şi ale întregii clădiri față de locul în care este situată.

Şi în acest context se ține seama de numărul Φ.

EXERCIȚII

1) Se consideră mulțimea X = {1, 2, 3, 4, 5, 6, 7, 8, 9}. Să se arate că pentru orice submulțime A a lui X, una din mulțimile A, X - A conține trei numere în progresie aritmetică.

Soluție:

Să presupunem că nu este posibil aşa ceva. Atunci numerele 4, 5, 6 nu pot aparține toate lui A şi nici lui X – A.

Dacă $4 \in A$ şi $6 \in A$, atunci $\{2, 5, 8\} \subset X - A$, ceea ce contrazice presupunerea.

Dacă $\{4, 5\} \subset A$, atunci $\{3, 6\} \subset X - A$ şi deci $\{4, 5, 9\}$_ A.

Pentru a fi satisfăcută presupunerea, va trebui ca $\{1, 7\} \subset X - A$ şi $8 \in A$. Cum 2 aparține lui A sau X – A, presupunerea făcută este falsă.

Analog rezolvăm cazul $\{5, 6\} \subset A$.

2) Fie $A, B \in \mathsf{P}(E)$. Se consideră aplicația

$$f : \mathsf{P}(E) \to \mathsf{P}(A) \times \mathsf{P}(B)$$

definită prin $f(X) = (X \cap A, X \cap B), \forall X \in \mathsf{P}(E)$.

1. Să se găsească o condiție necesară şi suficientă pentru ca f să fie injectivă;
2. Să se găsească o condiție necesară şi suficientă pentru ca f să fie surjectivă;
3. În cazul în care f este bijectivă, să se determine inversa sa.

Soluție:

1° f este injectivă dacă şi numai dacă $A \cup B = E$.

În adevăr, dacă $A \cup B \neq E$, atunci $\exists c \in E - (A \cup B)$. Fie $X \subset A \cup B$ şi $X' = X \cup \{c\}$. Evident $f(X) = f(X')$, adică f nu este injectivă.

Reciproc, dacă f nu este injectivă, atunci $\exists\ X, Y \in \mathsf{P}(E)$, $X \neq Y$, astfel încât $X \cap A = Y \cap A$ şi $X \cap B = Y \cap B$.

Deoarece $X \neq Y$, există $c \in X$ (sau în Y) care nu aparține lui Y (sau lui X); dar c nu poate aparține nici lui A, nici lui B, deci $c \in E - (A \cup B)$, adică $A \cup B \neq E$.

2° Printr-un raționament analog, se arată că f este surjectivă dacă şi numai dacă $A \cap B = \varnothing$.

3° Din 1° şi 2° rezultă că f este bijectivă dacă şi numai dacă $A = E - B$. Inversa funcției f este:

$f^{-1} : \mathsf{P}(A) \times \mathsf{P}(B) \to \mathsf{P}(E)$, $f^{-1}((P, Q)) = P \cup Q$

3) Fie $A \subseteq E$ şi f_A funcția caracteristică a submulțimii A:

$$f_A : E \to \{0, 1\}, \quad f_A(x) = \begin{cases} 1, & dacă \quad x \in A \\ 0, & dacă \quad x \notin A \end{cases}.$$

Să se arate că:

a) $A = B \Leftrightarrow f_A(x) = f_B(x), \forall x \in E$;

b) $f_{E-A}(x) = 1 - f_A(x), \forall x \in E$;

c) $f_{A \cap B}(x) = f_A(x) \cdot f_B(x), \forall x \in E$;

d) $f_{A \cup B}(x) = f_A(x) + f_B(x) - f_A(x) \cdot f_B(x), \forall x \in E$.

Soluție:

b) $\forall x \in E$, avem $f_A(x) + f_{E-A}(x) = 1$;

c) Fie $x \in A \cap B$, adică $x \in A$, $x \in B$. Avem $f_{A \cap B}(x) = 1$, $f_A(x) = 1$, $f_B(x) = 1$, deci egalitatea din enunț e satisfăcută;

Dacă $x \notin A \cap B$ rezultă că $x \notin A$ sau $x \notin B$ şi deci $f_{A \cap B}(x) = 0$ şi ($f_A(x) = 0$ sau $f_B(x) = 0$), de unde $f_A(x) \cdot f_B(x) = 0$, prin urmare are loc egalitatea din enunț.

d) Vom considera cazurile $x \in A \cup B$ şi $x \notin A \cup B$.

Avem $x \in A \cup B \Leftrightarrow x \in (A - B) \cup (A \cap B) \cup (B - A)$.

Se alcătuieşte tabelul:

	$f_A(x)$	$f_B(x)$	$f_{A \cap B}(x)$	$f_A(x) + f_B(x) - f_A(x) \cdot f_B(x)$
$x \in A - B$	1	0	1	1
$x \in A \cap B$	1	1	1	1
$x \in B - A$	0	1	1	1
$x \in E - (A \cup B)$	0	0	0	0

4) Fie A, B, C submulțimi ale lui E. Folosind proprietățile funcției caracteristice, să se arate:

1) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

2) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Soluție:

Determinăm funcțiile caracteristice ale mulțimilor din cei doi membri:

$\forall\ x \in E,\ f_{A\cup(B\cap C)}(x) = f_A(x) + f_{B\cap C}(x) - f_A(x) \cdot f_{B\cap C}(x) = f_A(x) + f_B(x)\cdot f_C(x) - f_A(x) \cdot f_B(x) \cdot f_C(x)$.

$f_{(A\cup B)\cap(A\cup C)}(x) = f_{A\cup B}(x) \cdot f_{A\cup C}(x) = [f_A(x) + f_B(x) - f_A(x) \cdot f_B(x)] \cdot [f_A(x) + f_C(x) - f_A(x) \cdot f_C(x)]$.

Folosim apoi că $f_A^2(x) = f_A(x)$ şi în urma calculelor obținem că $f_{A\cup(B\cap C)}(x) = f_{(A\cup B)\cap(A\cup C)}(x)$, $\forall\ x \in E$, adică $f_{A\cup(B\cap C)} = f_{(A\cup B)\cap(A\cup C)}$, deci $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Similar se arată şi cealaltă egalitate.

5) Cu ajutorul funcției caracteristice, să se arate că:

1) $A \cup B = A \cap B \Rightarrow A = B$;
2) $A \cup B = A \cup C$ şi $A \cap B = A \cap C \Rightarrow B = C$.

Soluție:

1) Avem $f_{A\cup B} = f_{A\cap B}$, adică $f_A + f_B - f_A\cdot f_B = f_A\cdot f_B$ deci $(f_A - f_B)^2 = 0$, de unde $f_A = f_B$, adică $A = B$;

2) Avem $f_{A\cap B} = f_{A\cap C}$ şi $f_{A\cup B} = f_{A\cup C}$, de unde $f_A\cdot f_B = f_A\cdot f_C$ şi $f_A + f_B - f_A\cdot f_B = f_A + f_C - f_A\cdot f_C$. Obținem că $f_B = f_C$, deci $B = C$.

6) Fie $A, B \in \mathsf{P}(E)$. Să se determine $f_{A\Delta B}$ şi să se arate că $A\Delta(B\Delta C) = (A\Delta B)\Delta C$.

Soluție:

Avem $A \Delta B = (A - B) \cup (B - A)$ şi $f_{A-B} = f_{A\cap(E - B)} = f_A \cdot f_{(E - B)} = f_A (1 - f_B) = f_A - f_A \cdot f_B$, deci $f_{A\Delta B} = f_{(A-B)\cup(B-A)} = f_{A-B} + f_{B-A} - f_{A-B}\cdot f_{B-A} = f_A (1 - f_B) + f_B (1 - f_A) - f_A (1 - f_B) \cdot f_B (1 - f_A) = f_A + f_B - 2 f_A \cdot f_B - (f_A - f_B^2)(f_B - f_B^2) = f_A + f_B - 2 f_A \cdot f_B = (f_A - f_B)^2$.

Aşadar, $f_{A\Delta B} = (f_A - f_B)^2$.

Avem: $f_{A\Delta(B\Delta C)} = (f_A - f_{B\Delta C})^2 = [f_A - (f_B - f_C)^2]^2$ şi $f_{(A\Delta B)\Delta C} = (f_{A\Delta B} - f_C)^2 = [(f_A - f_B)^2 - f_C)^2]^2$.

Alcătuim tabelul:

$f_A(x)$	$f_B(x)$	$f_C(x)$	$f_{A\Delta(B\Delta C)}(x)$	$f_{(A\Delta B)\Delta C}(x)$
1	0	0	1	1
0	1	0	1	1
0	0	1	1	1
1	1	0	0	0
1	0	1	0	0
0	1	1	0	0
0	1	1	0	0
1	1	1	1	1
0	0	0	0	0

7) Fie $\mathsf{P}(E)$ şi $F = \{0, 1\}^E$. Să se arate că aplicația $A \to f_A$ este o bijecție între $\mathsf{P}(E)$ şi F. Să se deducă numărul aplicațiilor lui E în $\{0, 1\}$.

Soluție:

Fie $\varphi : \mathsf{P}(E) \to F$, $\varphi(A) = f_A$. Dacă $A, B \in \mathsf{P}(E)$, $A \neq B$, atunci $\exists\, x_0 \in A$, $x_0 \notin B$. Avem $f_A(x_0) = 1$ şi $f_B(x_0) = 0$, deci $f_A \neq f_B$, adică $\varphi(A) \neq \varphi(B)$. Deducem de aici că φ este injectivă.

Fie f o funcție $f : E \to \{0, 1\}$ şi fie $A = \{x \in E \mid f(x) = 1\}$. Atunci f este funcția caracteristică mulțimii A, deci ecuația $\varphi(X) = f$ are soluția $X = A$. Aşadar, φ este şi surjectivă, deci este bijectivă. Dacă E are n elemente, atunci există 2^n aplicații de la E la $\{0, 1\}$.

8) Fie ρ_1 şi ρ_2 echivalențe pe X. Relația $\rho_1 \circ \rho_2$ este echivalență dacă şi numai dacă $\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$.

Soluție:

Dacă $\rho_1 \circ \rho_2$ este o echivalență, atunci $\rho_1 \circ \rho_2 = (\rho_1 \circ \rho_2)^{-1} = \rho_2^{-1} \circ \rho_1^{-1} = \rho_2 \circ \rho_1$.

Invers, fie $\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$.

Din ρ_1 şi ρ_2 rezultă că $\Delta_X \subseteq \rho_1 \cap \rho_2$, deci $\Delta_X \subseteq \rho_1 \circ \rho_2$, adică $\rho_1 \circ \rho_2$ este reflexivă.

Pe de altă parte, din $\rho_1 \circ \rho_2 = \rho_2 \circ \rho_1$, rezultă $(\rho_1 \circ \rho_2)^{-1} = \rho_2^{-1} \circ \rho_1^{-1} = \rho_2 \circ \rho_1 = \rho_1 \circ \rho_2$, deci $\rho_1 \circ \rho_2$ este simetrică.

În final, $(\rho_1 \circ \rho_2) \circ (\rho_1 \circ \rho_2) = \rho_1 \circ (\rho_2 \circ \rho_1) \circ \rho_2 = \rho_1 \circ (\rho_1 \circ \rho_2) \circ \rho_2 =$
$= \rho_1^2 \circ \rho_2^2 = \rho_1 \circ \rho_2$, adică $\rho_1 \circ \rho_2$ este şi tranzitivă.

Deci $\rho_1 \circ \rho_2$ este o relație de echivalență.

9) Fie E = {a, b, c, d} şi f : $\mathcal{P}(E) \to \mathcal{P}(E)$ definită astfel:

$$f(X) = X \cup \{a\}, \forall X \in \mathcal{P}(E).$$

1. Să se rezolve ecuația f(X) = E. Este f injectivă ?
2. Să se rezolve ecuația f(X) = ∅. Este f surjectivă ?
3. Fie P, Q ∈ $\mathcal{P}$ (E). Să se compare mulțimile: f(P∪Q) şi f(P) ∪ f(Q), apoi f(P∩Q) şi f(P) ∩ f(Q).

Soluție:

1. Se observă uşor că $X_1 = E$, $X_2 = \{b, c, d\}$ sunt soluțiile ecuației f(X) = E. Avem $X_1 \neq X_2$, şi $f(X_1) = f(X_2) = E$, deci f nu este injectivă.

2. Din $\{a\} \subseteq X \cup \{a\} = f(X) = \emptyset$ obținem o contradicție. Deci f nu este surjectivă, deoarece $\forall X \in \mathcal{P}(E)$, $f(X) \neq \emptyset \in \mathcal{P}(E)$.

3. Avem $f(P \cup Q) = P \cup Q \cup \{a\} = P \cup \{a\} \cup Q \cup \{a\} =$
$= f(P) \cup f(Q)$ şi $f(P \cap Q) = (P \cap Q) \cup \{a\} = (P \cup \{a\}) \cap (Q \cup \{a\}) =$
$f(P) \cap f(Q)$.

10) Fie E o mulțime şi A, B, C ∈ $\mathcal{P}$ (E). Să se arate că dacă $A \cup B \subseteq A \cup C$ şi $A \cap B \subseteq A \cap C$, atunci $B \subseteq C$.

Soluție:

Fie x ∈ B; atunci x ∈ A ∪ B, de unde x ∈ A ∪ C. Dacă x ∈ C, demonstrația este terminată.

Dacă x ∈ A, atunci x ∈ A ∩ B, deci x ∈ A ∩ C, de unde x ∈ C.

11) Fie A ≠ ∅ şi fie F : $\mathcal{P}(A) \to \mathcal{P}(A)$, aşa încât pentru orice X ⊂ A, Y ⊂ A, X ⊂ Y să rezulte F(X) ⊂ F(Y). Arătați că există T ∈ $\mathcal{P}$ (A), cu proprietatea F(T) = T.

Soluție:

Fie $\mathcal{H} = \{K \in \mathcal{P}(A) \mid F(K) \subseteq K\}$. Observăm că $\mathcal{H} \neq \emptyset$, deoarece $F(A) \in \mathcal{P}(A)$ şi deci $F(A) \subseteq A$, de unde rezultă $A \in \mathcal{H}$.

Considerăm $T = \bigcap_{K \in \mathcal{H}} K$. Pentru orice $K \in \mathcal{H}$, avem $T \subseteq K$, deci $F(T) \subseteq F(K) \subseteq K$, de unde rezultă că $F(T) \subseteq \bigcap_{K \in \mathcal{H}} K = T$. De aici, se obține că $F(F(T)) \subseteq F(T)$, deci $F(T) \in \mathcal{H}$, de unde $T \subset F(T)$. Aşadar, $F(T) = T$.

12) Determinați funcția $f : \mathbf{R} \to \mathbf{R}$, ştiind că
$xf(x) + yf(y) = (x + y) f(x) f(y), \ \forall x, y \in \mathbf{R}$.

Soluție:

Pentru $x = y$, obținem $2x f(x) = 2x[f(x)]^2$, de unde pentru $x \neq 0$ rezultă $f(x) = [f(x)]^2$ şi deci $f(x) \in \{0, 1\}$, pentru orice $x \neq 0$.

Considerăm acum $y = -x$ şi obținem $xf(x) = x f(-x)$, de unde pentru orice $x \neq 0$ rezultă $f(x) = f(-x)$.

1° Dacă $f(1) = 0$, atunci pentru orice $x \in \mathbf{R}$ avem:
$xf(x) = (x + 1)f(x)f(1) = 0$ şi alegând $x \neq 0$, obținem $f(x) = 0$.

Deci, se obține $f(x) = \begin{cases} 0, & x \neq 0 \\ a, & x = 0 \end{cases}$, unde $a \in \mathbf{R}$.

2° Dacă $f(1) = 1$ atunci pentru orice $x \in \mathbf{R}$, avem:
$1 + xf(x) = (x + 1) f(x)$, deci $f(x) = 1$, pentru orice $x \in \mathbf{R}$.
Aşadar, în acest caz $f(x) = 1, \forall x \in \mathbf{R}$.

13) Se consideră funcția $f : (0, \infty) \to \mathbf{R}$, $f(xy) = f(x) + f(y)$.

i) Să se determine $f(1)$.

ii) Presupunând că ecuația $f(x) = 0$ are soluție unică, arătați că $f(a) = f(b) \Rightarrow a = b$.

Soluție:

i) Pentru $x = y = 1$, avem $f(1) = f(1) + f(1)$, deci $f(1) = 0$.

ii) Fie $a, b \in (0, \infty)$, aşa încât $f(a) = f(b)$. Atunci $\exists k \in (0, \infty)$, astfel încât $ak = b$, deci $f(b) = f(ak) = f(a) + f(k)$ şi cum $f(a) = f(b)$ rezultă $f(k) = 0 = f(1)$. Ținem acum cont de faptul că ecuația $f(x) = 0$ are soluție unică şi obținem $k = 1$, deci $a = b$.

14) Arătați că dacă pentru $a \in \mathbf{R}-\{0\}$, avem $a + \frac{1}{a} \in \mathbf{Z}$, atunci $\forall n \in \mathbf{N}$, avem $a^n + \frac{1}{a^n} \in \mathbf{Z}$.

Soluție:

Se verifică prin inducție matematică după n şi se foloseşte faptul că:

$$\left(a+\frac{1}{a}\right)\left(a^n+\frac{1}{a^n}\right)=\left(a^{n+1}+\frac{1}{a^{n+1}}\right)+\left(a^{n-1}+\frac{1}{a^{n-1}}\right).$$

15) Să se afle cardinalele mulțimilor:

i) $A = \{x \in \mathbf{R} \mid x = \frac{n^2+1}{2n^2+n+1}, n \in \{1, 2, ..., 100\}\}$

ii) $B = \{x \in \mathbf{R} \mid x = \frac{an+b}{cn+d}, n \in \{1, 2, ..., p\}\}$,

unde $a, b, c, d \in \mathbf{R}$, $cd > 0$.

iii) $C = \{x \in \mathbf{N} \mid x = -n^2 + 6n - 7, n \in \mathbf{N}\}$

Soluție:

(i) A are cel mult 100 de elemente. Să studiem dacă aceste elemente pot fi şi egale.

Fie $p < q$, aşa încât $\frac{p^2+1}{2p^2+p+1} = \frac{q^2+1}{2q^2+q+1}$.

Rezultă că $(p - q)(p + q - pq + 1) = 0$ şi cum $p \neq q$, obținem

$p + q - pq + 1 = 0$ şi deci $p = 1 + \frac{2}{q-1}$, de unde $\frac{2}{q-1} \in \mathbf{N}$.

Deducem că $q = 2$ şi $p = 3$, sau $q = 3$ şi $p = 2$.

Dar $p < q$, deci $p = 2$ şi $q = 3$.

Aşadar, card A = 99.

(ii) Procedând similar ca la (i) se obține:

$$\text{card } B = \begin{cases} 1 & , \text{dacă } ad - bc = 0 \\ p & , \text{dacă } ad - bc \neq 0 \end{cases}$$

(iii) Impunem condiția $-n^2 + 6n - 7 \geq 0$, deci $3 - \sqrt{2} < n < 3 + \sqrt{2}$, de unde $n \in \{2, 3, 4\}$ şi de aici obținem card C = 2.

16) Să se arate că $\mathbf{N} \times \mathbf{N}$ este numărabilă.

Soluție:

a) Considerăm funcția f : $\mathbf{N} \to \mathbf{N}\times\mathbf{N}$, f(n) = (n, 0). Funcția f este injectivă, deci card $\mathbf{N} = \aleph_0 \leq$ card ($\mathbf{N}\times\mathbf{N}$).

b) Fie funcția g : $\mathbf{N}\times\mathbf{N} \to \mathbf{N}$, $g(m, n) = n + \frac{(m+n)(m+n+1)}{2}$.

Funcția g este surjectivă. Într-adevăr, dacă $(m , n) \in \mathbf{N}\times\mathbf{N} \ni (m', n')$ şi $(m, n) \neq (m' ,n')$, atunci avem următoarele posibilități:

1° . m+n = m' + n'. Presupunem g(m, n) = g(m', n'), atunci n = n' şi deci m = m', adică (m, n) = (m, n'), absurd.

Deci, în acest caz, $g(m, n) \neq g(m',n')$.

2°. $m + n \neq m' + n'$. Presupunem, fără a restrânge generalitatea, că $m' + n' \geq m + n + 1$. Atunci $g(m', n') = n' + \frac{(m'+n')(m'+n'+1)}{2} \geq$

$\geq n' + \frac{(m+n+1)(m+n+2)}{2} = n' + \frac{(m+n)(m+n+1)}{2} + m + n + 1 >$

$> n + \frac{(m+n)(m+n+1)}{2} = g(m, n)$.

Aşadar, şi în acest caz, $g(m, n) \neq g(m', n')$.

Deci, g este injectică, prin urmare card ($\mathbf{N}\times\mathbf{N}$) ≤ card $\mathbf{N} = \aleph_0$.

Din a) şi b) rezultă $\mathbf{N} \times \mathbf{N}$ că este numărabilă.

Funcția g se numeşte **numărare diagonală**.

17) Mulțimea **Z** a numerelor întregi este numărabilă.

Soluție:

Considerăm funcția f : $\mathbf{Z} \to \mathbf{N}$, $f(z) = \begin{cases} 2z , z \geq 0 \\ -1-2z , z < 0 \end{cases}$.

Se verifică uşor că f este bijectivă, deci **Z** este numărabilă.

18) Să se rezolve în **N** ecuația: $(n-3)! + n = n^3$.

Soluție:

Ecuația dată mai poate fi scrisă şi astfel:

$(n - 3)! = n(n - 1)(n +1)$. Pe de altă parte, avem $(n - 3)(n - 4)(n - 5) < (n - 1)n(n + 1)$, deci $(n - 3)!$ trebuie să mai aibă în dezvoltarea sa măcar încă un factor, adică $n – 6 > 1$, de unde obținem $n \geq 8$.

Însă, pentru $n \geq 10$, obținem:

(n- 3)! = (n - 3)(n - 4)(n - 5)(n - 6) · .....· 3·2 ·1 > $>6(n^2 - 9n + 18)(n^2 - 9n + 120) > 6(n^2 - 9n)(n^2 - 9n + 8) =$ $=6n(n - 9)(n - 1)(n - 8) > n(n - 1)(n + 1)$, deoarece pentru $n \geq 10$ avem $6(n - 9)(n - 8) > n + 1$.

Aşadar, pentru $n \geq 10$, avem $(n - 3)! > n(n - 1)(n + 1)$, adică ecuația dată nu are soluție pentru $n \geq 10$.

Mai observăm, în final, că $n = 8$ este soluție şi din analiza făcută, rezultă că este unica soluție a ecuației date.

19) Să se determine funcția $f : \mathbf{N} \to \mathbf{N}$, care satisface condițiile $f(1)= 1$ şi $f(n+1) = f(n) + a^n$, unde $a \in \mathbf{N}$.

Soluție:

Avem:

$f(1) = 1$

$f(2) = f(1) + a$

$f(3) = f(2) + a^2$

.....

$f(n) = f(n - 1) + a^{n-1}$

şi adunând aceste egalități obținem:

$f(n) = 1 + a + a^2 + ... + a^{n-1}$, deci $f(n) = \begin{cases} \dfrac{a^n - 1}{a - 1}, \ pentru \ a \neq 1 \\ n, \ \ pentru \ a = 1 \end{cases}$

20) Să se afle numărul de patru cifre care este pătrat perfect şi care are cifra miilor şi cifra zecilor egale, iar cifra sutelor este cu 1 mai mare decât cifra unităților.

Soluție:

Avem $N^2 = 1000 x + 100(y + 1) + 10x + y = 101(10x + y) + 100$, de unde $10x + y = \dfrac{(N+10)(N-10)}{101}$.

Ținând cont de faptul că $x, y \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ şi $x \neq 0$, se obține $N = 91$ şi $N^2 = 8281$.

21) Să se arate că pentru orice număr natural $n > 1$, numărul de forma $2^{2^n} + 1$ se termină cu cifra 7.

Soluție:

Considerăm numărul:

$\left(2^{2^n}+1\right)+3=2^2\left(2^{2^n-2}+1\right)=2^2\left(4^{2^{n-1}-1}+1\right)$.

Exponentul $2^{n-1}-1$ este număr impar, deci $4^{2^{n-1}-1}+1$ se divide cu 4 + 1 şi deci există m ∈ **N**, aşa încât $\left(2^{2^n}+1\right)+3 = 2^2(4 + 1)m = 20m$, de unde $2^{2^n}+1 = 20m - 3$ şi deci numărul $2^{2^n}+1$ are ultima cifră 7.

22) Să se găsească un număr de trei cifre exprimat în baza 7, care în baza 9 foloseşte aceleaşi cifre, în ordine inversă.

Soluție:

Avem $7^2x + 7y + z = 9^2z + 9y + x$, de unde x, y, z∈{0, 1, 2, 3, 4, 5, 6}, x ≠0. Din această egalitate obținem y = 8(3x – 5z). Pe de altă parte, y < 7 şi deci 3x – 5z = 0.

Folosind acum faptul că x, z ∈ {0, 1, 2, 3, 4, 5, 6} şi x ≠0 obținem x = 5, y = 0 şi z = 3 şi deci numărul căutat este 503_7.

23) Determinați n ∈**N***, astfel încât 1! + 2! + ...+ n! să fie pătrat perfect.

Soluție:

Observăm că pentru n ∈{1, 3} obținem pătratele perfecte 1! şi 1! + 2! +3! = 9, iar pentru n ∈ {2, 4, 5} sumele 1! + 2! = 3, 1! + 2! +3! +4! =33 şi 1! + 2! + 3! + 4! + 5! = 153 nu sunt pătrate perfecte. Mai mult, pentru n ≥ 5, toate sumele S_n = 1! + 2! +..... +n! vor avea utima cifră 3 + 0 = 3, deoarece pentru n ≥ 5, n! este multiplu de 10. Cum ultima cifră a unui număr părtrat perfect poate fi 1, 4, 9, 5, 6, 0 rezultă că n ∈{1, 3} sunt singurele valori ale lui n care satisfac condiția cerută.

24) Fie $x_1, x_2, ..., x_n$ ∈**N**, aşa încât $x_1 + x_2 + ... + x_n = k$ (constantă). Determinați max $(x_1 \cdot x_2 \cdot ...\cdot x_n)$.

Soluție:

Folosim inegalitatea mediilor

$\sqrt[n]{x_1x_2.....x_n} \le \frac{x_1+x_2+....+x_n}{n} = \frac{k}{n}$, cu egalitate pentru $x_1 = x_2 = .. = x_n$.

25) Fie $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n$ numere naturale. Să se arate că:

$$\sum_{i=1}^{n} a_i^2 \sum_{i=1}^{n} b_i^2 = \left(\sum_{i=1}^{n} a_i b_i\right)^2 + \sum_{1 \le i < k \le n} (a_i b_k - a_k b_i)^2$$

(Identitatea lui Lagrange)

Soluție:

Pentru n = 2 se face o verificare directă. Identitatea se demonstrează prin inducție matematică.

26) Fie a_1, a_2, ..., a_n numere naturale nenule. Să se arate că $\frac{a_1}{a_2} + \frac{a_2}{a_3} + ... + \frac{a_n}{a_1} \ge n$ şi $a_1 + ... + a_n + \frac{1}{a_1 \cdot a_2 \cdot ... \cdot a_n} \ge n + 1$.

Soluție:

Avem $\frac{a_1}{a_2} \cdot \frac{a_2}{a_3} \cdot ... \cdot \frac{a_n}{a_1} = 1$, de unde, din egalitatea mediilor, rezultă că $\frac{1}{n}\left(\frac{a_1}{a_2} + \frac{a_2}{a_3} + ... + \frac{a_n}{a_1}\right) \ge \sqrt[n]{1} = 1$, adică $\frac{a_1}{a_2} + \frac{a_2}{a_3} + ... + \frac{a_n}{a_1} \ge n$. Pe de altă parte, din $a_1 \cdot ... \cdot a_n \cdot \frac{1}{a_1 \cdot a_2 \cdot ... \cdot a_n} = 1$ şi din inegalitatea mediilor rezultă că: $a_1 + ... + a_n + \frac{1}{a_1 \cdot a_2 \cdot ... \cdot a_n} \ge n + 1$.

27) Să se arate că $n(n+1)a + 2n \ge 4\sqrt{a}\left(\sqrt{1} + \sqrt{2} + ... + \sqrt{n}\right)$, unde a, n$\in$**N**.

Soluție:

Folosind inegalitatea mediilor, obținem că

$$4\left(\sqrt{1 \cdot a} + \sqrt{1 \cdot 2a} + ... + \sqrt{1 \cdot na}\right) \le 4\left(\frac{1+a}{2} + \frac{1+2a}{2} + ... + \frac{1+na}{2}\right) =$$

=2n + n(n + 1)a.

28) Fie a, b $\in$**N***. Să se arate că $\forall$ k$\in$**Z**, avem $\left(1 + \frac{a}{b}\right)^k + \left(1 + \frac{b}{a}\right)^k \ge 2^{k+1}$.

Soluție:

Folosim inegalitatea lui Jensen: $\frac{x^n+y^n}{2} \geq \left(\frac{x+y}{2}\right)^n$, $\forall n \in \mathbf{N}^*$, $\forall$ x, y $\in \mathbf{Q}$, x>0, y>0.

Pentru k >0, avem

$$\left(1+\frac{a}{b}\right)^k + \left(1+\frac{b}{a}\right)^k \geq 2 \cdot \frac{1}{2^k}\left(1+1+\frac{a}{b}+\frac{b}{a}\right)^k;$$

dar $\frac{a}{b}+\frac{b}{a} \geq 2$, deci $\left(1+1+\frac{a}{b}+\frac{b}{a}\right)^k \geq 2^{2k}$, de unde

$$\left(1+\frac{a}{b}\right)^k + \left(1+\frac{b}{a}\right)^k \geq 2^{k+1}$$

Pentru k = 0, se verifică imediat inegalitatea.

Pentru k < 0, considerăm n = -k $\in \mathbf{N}^*$ şi avem:

$$\left(1+\frac{a}{b}\right)^k + \left(1+\frac{b}{a}\right)^k = \left(\frac{b}{a+b}\right)^n + \left(\frac{a}{a+b}\right)^n \geq 2 \cdot \frac{\left(\frac{b}{a+b}+\frac{a}{a+b}\right)^n}{2^n} =$$

$=2^{k+1}$.

29) Arătați că $n^n > 1 \cdot 3 \cdot 5 \cdot \ldots (2n-1)$, $\forall n \in \mathbf{N}^*$.

Soluție:

Din inegalitatea mediilor rezultă:

$$\sqrt[n]{1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1)} < \frac{1+3+5+\ldots+(2n-1)}{n} = \frac{n^2}{n} = n,$$

deci $n^n > 1 \cdot 3 \cdot 5 \cdot \ldots \cdot 2n-1$.

30) Arătați că ecuația $x^2 + y^2 - 8z = 6$ nu are soluții în **Z**.

Soluție:

Demonstrăm prin reducere la absurd.

Presupunem că $\exists$ x, y, z $\in \mathbf{Z}$, aşa încât $x^2 + y^2 - 8z = 6$. De aici rezultă că $2 \mid (x^2 + y^2)$. Dacă $2 \mid x$, atunci $\exists\, x_1 \in \mathbf{Z}$: $x = 2\, x_1$ şi obținem $2 \mid y$, deci $\exists\, y_1 \in \mathbf{Z}$: $y = 2\, y_1$. Ecuația devine: $4x_1^2 + 4y_1^2 - 8z = 6$, de

unde $2x_1^2 + 2y_1^2 - 4z = 3$, adică un număr par coincide cu un număr impar, ceea ce este fals.

Dacă $2 \nmid x$, adică $\exists\ x_1 \in \mathbf{Z}$: $x = 2x_1 + 1$, atunci $2 \nmid y$, deci $\exists\ y_1 \in \mathbf{Z}$: $y = 2y_1 + 1$. Obținem $4x_1^2 + 4y_1^2 + 4x_1 + 4y_1 + 2 - 8z = 6$, adică $x_1(x_1 + 1) + +y_1(y_1 + 1) - 2z = 1$ şi ajungem din nou la contradicția că un număr par coincide cu un număr impar.

Deci presupunerea făcută este falsă şi, prin urmare, ecuația dată nu are soluții în **Z**.

31) Arătați că ecuația $x^n + y^n = z^n$ nu are soluție în **N***, pentru $n \geq z > x$.

Soluție:

Presupunem prin reducere la absurd, că ecuația dată ar avea soluțiile naturale nenule x, y, z, cu $n \geq z > x$.

Avem $x < z$ şi $y < z$. Să presupunem, fără a restrânge generalitatea, că $x \leq y$.

Atunci $x^n = z^n - y^n = (z - y)(z^{n-1} + z^{n-2}y + ...+ y^{n-1}) \geq 1 \cdot n \cdot y^{n-1} \geq n \cdot x^{n-1}$, de unde obținem $x \geq n$, ceea ce contrazice faptul că $x < z \leq n$ şi deci ecuația dată nu are soluții în **N***, pentru $n \geq z > x$.

32) Să se arate că nu există ecuații de grad par cu coeficienți impari, care admit rădăcini raționale .

Soluție:

Să presupunem că ar exista o astfel de ecuație. Atunci avem:

$a_{2n}\left(\frac{p}{q}\right)^{2n} + ... + a_1 \cdot \frac{p}{q} + a_0 = 0$, unde $p \in \mathbf{Z}$, $q \in \mathbf{N}^*$ şi $\frac{p}{q}$ este ireductibilă.

Avem următoarele posibilități:

1°. Dacă p este par şi q impar, atunci obținem

$(a_{2n}p^{2n} + ...+ a_1pq^{2n-1}) = - a_0q^{2n}$,

adică un număr par ar fi egal cu unul impar, ceea ce este fals.

2°. Dacă p şi q sunt impare, atunci obținem că o sumă de $(2n + 1)$ numere impare coincide cu un număr par, ceea ce este fals.

3°. Dacă p este impar şi q este par, atunci $a_{2n}p^{2n} = - a_{2n-1}p^{2n-1} -....- a_0q^{2n}$, adică un număr impar coincide cu un număr par, ceea ce este fals.

Deci nu există ecuații de grad par cu coeficienți impari, care să aibă rădăcini raționale.

33) Fie $f(X) = a_0X^3 + a_1X^2 + a_2X + a_3$, unde $\forall\ i \in \{0, 1, 2, 3\}$, $a_i \in \mathbf{Z}$ şi $p > 3$, p prim.

a) Dacă $p \nmid a_0$, atunci rezultă că printre numerele $\frac{f(0)}{p}$, $\frac{f(1)}{p}$, ..., $\frac{f(p-1)}{p}$ există cel mult trei numere întregi;

b) Dacă printre numerele $\frac{f(0)}{p}$, ..., $\frac{f(p-1)}{p}$ există mai mult de trei numere întregi, atunci rezultă că $p \mid a_0$.

Soluție:

a) Presupunem că printre numerele date există patru numere întregi, deci $\exists\ x_1, x_2, x_3, x_4$ numere naturale cuprinse între 0 şi p-1, aşa încât $p \mid f(x_i)$, $\forall\ i \in \{1, 2, 3, 4\}$. Deci $p \mid (f(x_1) - f(x_2))$. Avem:

$f(x_1) - f(x_2) = a_0(x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2) + a(x_1 - x_2)(x_1 + x_2) + a_2(x_1 - x_2) = (x_1 - x_2)[a_0(x_1^2 + x_1x_2 + x_2^2) + a_1(x_1 + x_2) + a_2]$.

Putem presupune $x_1 > x_2$ şi avem $x_1 - x_2 \in \{1,.., p-1\}$, deci $p \nmid (x_1 - x_2)$ şi din $p \mid (f(x_1) - f(x_2))$ rezultă că $p \mid [a_0(x_1^2 + x_1x_2 + x_2^2) + a_1(x_1 + x_2) + a_2]$.

Similar, se arată că $p \mid [a_0(x_1^2 + x_1x_3 + x_3^2) + a_1(x_1 + x_3) + a_2]$, deci $p \mid [a_0(x_1 + x_2 + x_3) + a_1]$.

Similar, se arată că $p \mid [a_0(x_1 + x_2 + x_4) + a_1]$, deci $p \mid a_0(x_3 - x_4)$ şi cum $p \nmid (x_3 - x_4)$ rezultă că $p \mid a_0$, contradicție.

Aşadar există cel mult trei numere întregi între $\frac{f(0)}{p}$, $\frac{f(1)}{p}$, ..., $\frac{f(p-1)}{p}$.

b) Rezultă din a).

34) Suma cifrelor unui număr natural este 2000. Poate fi acest număr un pătrat perfect ?

Soluție:

Avem 2000 este de forma 3k+2, dar pătratele perfecte nu pot fi decât de forma 3p sau 3p+1, deci numărul considerat nu poate fi pătrat perfect.

35) Se consideră numerele naturale care se termină în 5. Dacă n este un asemenea număr, atunci penultima cifră a lui n^2 este pară sau impară ?

Soluție:

Avem n = 10p + 5, deci $n^2 = 100p^2 + 100p + 25 = 100p(p + 1) + 25$, deci penultima cifră este 2.

36) Fie $c \in \mathbf{N}$, c > 1. Să se studieze dacă există x, astfel încât numărul $m = \underbrace{11...1}_{n}\underbrace{xx...x}_{n}$ scris în baza $q = c^2 + 1$ să fie produs de două numere consecutive.

Soluție:

$m = \underbrace{11...1}_{n}\underbrace{00...0}_{n} + \underbrace{xx...x}_{n} = q^n\underbrace{11...1}_{n} + \underbrace{xx...x}_{n} = q^n(q^{n-1}+q^{n-2} + ...+1) + x(q^{n-1} +q^{n-2} +...+1) = (q^n + x)\frac{q^n-1}{q-1} = (q^n + x)\frac{q^n-1}{c^2} = \frac{q^n-1}{c}\left(\frac{q^n-1}{c}+\frac{x+1}{c}\right)$.

Luăm x = c – 1 şi obținem $m = \frac{q^n-1}{c}\left(\frac{q^n-1}{c}+1\right)$ care satisface cerința problemei.

37) Fie N un număr natural de n cifre, astfel încât N^2 are ultimele n cifre exact cifrele lui N, în aceeaşi ordine.

Să se arate că numărul natural N', pentru care $N + N' = 10^n + 1$ are aceeaşi proprietate ca şi N.

Soluție:

Avem $N' = 10^n + 1 – N$, de unde $(N')^2 = (10^n + 1)^2 – 2(10^n + 1)N + N^2 = 10^{2n} + 2\cdot10^n + 1 - 2\cdot10^n N – 2N + N^2 = 10^n (10^n + 1- N) + N^2 + 1 + 10^n - 10^n N – 2N = 10^n N' + N' + N^2 –N - 10^n N$.

Întrucât N satisface proprietatea din enunț, avem că ultimele n cifre ale lui $N^2 – N$ vor fi 0, deci, ultimele n cifre ale lui $(N')^2$ vor fi cifrele lui N', în aceeaşi ordine.

38) Să se arate că pentru orice număr întreg k, fracția $\frac{15k^2+8k+6}{30k^2+21k+13}$ este ireductibilă.

Soluție:

Numărătorul se scrie: $m = 15k^2 + 8k + 6 = (5k + 1)(3k + 1) + 5$, iar numitorul $n=30k^2 + 21k + 13=2 (15k^2 + 8k + 6)+5k +1=2m + (5k+ 1)$.
Din egalitatea $n = 2m + (5k + 1)$ rezultă că un divizor comun pentru n şi m trebuie să fie şi divizor al lui 5k+1 şi, pe de altă parte, din egalitatea $m = (5k + 1)(3k + 1) + 5$ rezultă că acel divizor comun pentru m şi n este şi divizor al lui 5. Dar cel mai mare divizor comun al lui 5k+1 şi 5 este 1, deci fracția dată este ireductibilă.

39) Cubul oricărui număr întreg este diferența a două pătrate, dintre care unul este multiplu de 9.

Soluție:

Observăm că $\forall$ a $\in$ **Z**, $a^3 = \left[\frac{a(a+1)}{2}\right]^2 - \left[\frac{a(a-1)}{2}\right]^2$ iar dintre numerele a – 1, a, a+1, unul este multiplu de trei.

40) Fie $E(n) = am^{\alpha n} + bn + c$, unde m, n $\in$**N**, m $\neq$ 0, a, b, c$\in$**Z** şi $\alpha\in$**N**. Dacă există un număr întreg d, astfel ca d | E(0), d | E(1) şi d | E(2), atunci d | E(n), pentru orice n$\in$**N**.

Soluție:

Vom arăta prin inducție matematică după n.
Conform ipotezei, avem că d | E(0), d | E(1).
Presupunem că d | E(n) şi vom demonstra că d | E(n+1).

Avem $E(n+1) - E(n) = a(m^{\alpha n+\alpha} - m^{\alpha n})+b$ şi deci $E(n+1) - E(n) - [E(1)-E(0)] = a(m^{\alpha} - 1)(m^{\alpha n} - 1)$.

Pe de altă parte, d | E(2) + E(0) – 2E(1), unde
$E(2)+E(0) – 2E(1)= a(m^{\alpha} - 1)^2$ şi cum $(m^{\alpha} - 1) | (m^{\alpha n} - 1)$ rezultă că d | E(n+1)-E(n) – [E(1)-E(0)].
Avem d | E(1) - E(0), unde $E(1) - E(0) = a (m^{\alpha} - 1) + b$.
Prin urmare, d | E(n+1) - E(n); dar din ipoteza inducției d | E(n). Aşadar d | E(n +1).
Deci, $\exists$ n $\in$ **N**, d | E(n).

41) Fie f∈**Z**[X], aşa încât f(k), f(k+1), f(k+2) sunt multipli de 3. Atunci f(m) este multiplu de 3 pentru orice m ∈**Z**.

Soluție:

Să observăm că dacă m, n ∈ **Z**, m ≠n, atunci (m - n) | [f(m) – f(n)]. Fie m ∈ **Z** oarecare. Avem că f(m) – f(k), f(m) – f(k + 1), f(m) – f(k+2) sunt divizibile prin m – k, m – (k + 1), m – (k + 2), respectiv, care sunt numere consecutive, deci unul dintre ele este multiplu de trei. Ținând cont acum de faptul că f(k), f(k + 1), f(k+2) sunt multipli de 3, obținem că f(m) este multiplu de trei.

42) Pentru orice n ∈ **N**, n ≥ 3, n impar, numărul întreg $\left(1+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{n-1}\right)(n-1)!$ se divide cu n.

Soluție:

Să observăm mai întâi că în suma $1+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{n-1}$ **apare un număr par de termeni.**

Avem $\mathbf{N}=\left(1+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{n-3}+\frac{1}{n-2}+\frac{1}{n-1}\right)(n-1)!=$

$=\left[\left(1+\frac{1}{n-1}\right)+\left(\frac{1}{2}+\frac{1}{n-2}\right)+\left(\frac{1}{3}+\frac{1}{n-3}\right)+....\right](n-1)!=$

$=\left[\frac{n}{1\cdot(n-1)}+\frac{n}{2\cdot(n-2)}+\frac{n}{3\cdot(n-3)}+....\right](n-1)!=$

$=n\left[\frac{(n-1)!}{1\cdot(n-1)}+\frac{(n-1)!}{2\cdot(n-2)}+\frac{(n-1)!}{3\cdot(n-3)}+....\right]$, de unde rezultă că n | N.

43) Să se arate că dacă mn + pq se divide cu m - p atunci mq + np se divide cu m - p, unde m, n, p, q ∈**Z**.

Soluție:

Fie $\frac{mn+pq}{m-p}=t\in\mathbf{Z}$.

Avem: $\frac{mn+pq}{m-p} - t = \frac{mq+pn}{m-p} - \frac{mn+pq}{m-p} = \frac{q(m-p)-n(m-p)}{m-p} =$
$=q - n.$

Deci $\frac{mq+pn}{m-p} = q - n + t \in \mathbf{Z}$, adică mq + np se divide cu m – p.

44) Să se arate că dacă un număr din cinci cifre se divide cu 41, atunci şi toate celelalte numere, obținute prin permutări circulare ale cifrelor, se divid cu 41.

Soluție:

Fie $N = 10^4a + 10^3b + 10^2c + 10d + e$ divizibil cu 41 unde a, b, c, d, e $\in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ şi $a \neq 0$.
Considerăm următorul număr obținut prin permutare cu o cifră:
$N_1 = 10^4b + 10^3c + 10^2d + 10e + a = 10 (10^4a + 10^3b + 10^2c + 10d + e) - -10^5a + a = 10N - 99999a$. Deoarece $41 \mid 99.999$ şi $41 \mid N$, obținem că $41 \mid N_1$.

Similar se procedează şi pentru toate celelalte numere obținute prin permutări circulare ale cifrelor lui N.

45) Să se arate că $\forall\, n \in \mathbf{N}$, produsul $(n+1)(n+2) \cdot ... \cdot (n+n)$ se divide cu 2^n.

Soluție:

Amplificând cu n! obținem $\frac{(2n)!}{n!}$. În (2n)! există n factori pari şi n fatori impari.

Deci, $\frac{(2n)!}{n!} = \frac{(1\cdot 3\cdot 5\cdot ...\cdot (2n-1))(1\cdot 2\cdot 3.....\cdot n)2^n}{n!} = 1\cdot 3\cdot 5 \cdot ..\cdot (2n-1)\cdot 2^n$, adică $(n + 1)(n + 2) .....(n + n)$ se divide cu 2^n.

46) Să se afle numărul natural prim p dacă se ştie că $4p^2 + 1$ şi $6p^2 + 1$ sunt numere prime.

Soluție:

Orice număr natural n se poate reprezenta sub forma 5m sau 5m ±1 sau 5m ± 2, unde m ∈ **N**. Un număr de forma 5m este prim numai dacă m = 1, adică p = 5. Obținem $4p^2 + 1 = 101$ şi $6p^2 + 1 = 151$, care sunt numere prime. Să arătăm acum că p = 5 este singurul număr prim cu proprietățile date.

Într-adevăr, dacă p = 5m ± 1, atunci $4p^2 + 1 = 5(20m^2 \pm 8m + 1)$, care nu este prim, iar dacă p = 5m ± 2, atunci $6p^2 + 1 = 5(30m^2 \pm 24m + 1)$, care nu este prim.

47) Dacă n numere prime formează o progresie aritmetică, atunci rația progresiei se divide cu fiecare număr prim p < n.

Soluție:

Fie a, a + d, a + 2d, ..., a + (n-1)d cele n numere prime în progresie aritmetică şi p un număr prim, p < n.

Împărțind la p cele n numere, resturile obținute vor fi elemente ale mulțimii {0, 1, 2, .., p-1}.

Numărul acestor resturi este mai mic decât n, deci vor exista măcar două numere care vor da acelaşi rest la împărțirea cu p.

Fie aceste numere: a + ip = q_1p + r şi a+ jp = q_2p + r, unde 0≤i<j≤ p-1. Rezultă (j- i)d = (q_2 – q_1)p, deci p | (j-i)d. Ținând cont de faptul că 0 ≤ j – i ≤ p - 1 rezultă că p | d, deoarece p este prim.

48) Dacă p este un număr prim de forma 12k + 5, atunci p | 3^{6k+2} + 1.

Soluție:

Să notăm cu $S = \prod_{j=1}^{6k+2} 3j = \prod_{j=1}^{2k} 3j \prod_{j=2k+1}^{4k+1} 3j \prod_{j=4k+2}^{6k+2} 3j$.

$S_2 = \prod_{j=2k+1}^{4k+1} 3j$ =(6k+3)(6k+6)..(12k+3) =(p – (6k+2))· (p – (6k-1))..·(p-2)=

=m_2p + $(-1)^{2k}$· 2· 5 · ...·(6k + 2) = m_2p - 2· 5 · ...·(6k + 2), cu m_2 ∈ **N**.

$S_3 = \prod_{j=4k+2}^{6k+2} 3j$ =(12k+6)(12k+9)...(18k+6) = (p +1)(p + 4)·.. (p +(6k +1)) =

=m_3p + 1· 4· ...·(6k + 1), cu m_3 ∈ **N**.

Deci, $S=\prod_{j=1}^{2k} 3j \cdot S_2 \cdot S_3 = (3 \cdot 6 \cdot \ldots \cdot 6k)(m_2p - 2 \cdot 5 \cdot \ldots \cdot (6k + 2)) \cdot (m_3p + +1 \cdot 4 \cdot \ldots \cdot (6k + 1)) = mp - 1 \cdot 4 \cdot \ldots \cdot (6k + 1) \cdot 2 \cdot 5 \cdot \ldots \cdot (6k + 2) \cdot 3 \cdot 6 \cdot \ldots \cdot 6k = = mp - (6k + 2)!$ (1)

Pe de altă parte, $S = \prod_{j=1}^{6k+2} 3j = 3^{6k+2} \prod_{j=1}^{6k+2} j = 3^{6k+2} (6k + 2)!$ (2)

Din (1) şi (2) rezultă că $mp = (6k + 2)! (3^{6k+2} + 1)$, deci $p \mid (6k + 2)! (3^{6k+2} + 1)$. Dar $p = 12k + 5$ şi p este prim, deci $p \Pi (6k+2)!$. Aşadar $p \mid 3^{6k+2} + 1$.

49) Dacă $(a + b) \mid (ma + nb)$, atunci $(a + b) \mid (mb + na)$ şi reciproc.
Soluție:

Vom face demonstrația numai într-un singur sens, în celălalt rezolvându-se analog. Avem $(a+b) \mid (m+n)(a+b) = (m+n)a + (m+n)b$ şi $(a+b) \mid (ma + nb)$, deci $(a + b) \mid (m+n)a + (m+n)b - ma - nb = mb + na$.

50) Determinați valorile lui $a \in \mathbf{Z}$ astfel încât $a \cdot 5^{6m - 1}$ să fie divizibil cu 21, pentru orice $m \in \mathbf{N}^*$.
Soluție:

Avem $21 \mid (a \cdot 5^{6m - 1} - 1) \Leftrightarrow 21 \mid (a \cdot 5^{6m} - 5) \Leftrightarrow 3 \mid (a \cdot 5^{6m} - 5)$ şi $7 \mid (a \cdot 5^{6m} - 5)$.

Dar $5^{6m} = (6 - 1)^{6m} = M_3 + (-1)^{6m} = M_3 + 1$ şi $5^{6m} = (5^3)^{2m} = (126 - 1)^{2m} = = (7 \cdot 18 - 1)^{2m} = M_7 + (-1)^{2m} = M_7 + 1$.

Deci $3 \mid (a \cdot 5^{6m} - 5)$ şi $7 \mid (a \cdot 5^{6m} - 5) \Leftrightarrow 3 \mid (a - 5)$ şi $7 \mid (a - 5) \Leftrightarrow \Leftrightarrow 3 \mid (a - 2)$ şi $7 \mid (a - 5) \Leftrightarrow 21 \mid 7(a - 2)$ şi $21 \mid 3(a - 5) \Leftrightarrow 21 \mid (7a - 14)$ şi $21 \mid (6a - 30) \Leftrightarrow 21 \mid (a + 16) \Leftrightarrow 21 \mid (a - 5) \Leftrightarrow a = M_{21} + 5$.

51) Expresia $u^{2222} - u^{1111} + 1$ se divide prin $u^2 - u + 1$.
Soluție:

Avem $u^{2222} - u^{1111} + 1 = u^2 \cdot (u^3)^{740} - u(u^3)^{370} + 1 = u^2 \cdot [(u^3)^{740} - 1] - -u[(u^3)^{370} - 1] + u^2 - u + 1$.

Pentru k par, $(u^3)^k - 1$ se divide prin $u^3 + 1 = (u + 1)(u^2 - u + 1)$, deci parantezele drepte se divid prin $u^2 - u + 1$, deci numărul dat se divide prin $u^2 - u + 1$.

52) Arătați că pentru n, nedivizibil cu 3, avem: $19 \mid 7^{2n} + 7^n + 1$.
Soluție:

Din teorema împărțirii cu rest rezultă că u = 3k + r, unde r ∈ {1, 2}. Rezultă $7^{2n} + 7^n + 1 = 7^{6k+2r} + 7^{3k+r} + 1 = (7^3)^{2k} \cdot 7^{2r} + (7^3)^k \cdot 7^r + 1 =$
$=343^{2k} \cdot 7^{2r} + 343^k \cdot 7^r + 1 = (19 \cdot 18 + 1)^{2k} \cdot 49^r + (19 \cdot 18 + 1)^k \cdot 7^r + 1 =$
$=(19m_1 + 1)\, 49^r + (19m_2 + 1)\, 7^r + 1 = 19m + 49^r + 7^r + 1.$

Pentru r = 1, avem $49^r + 7^r + 1 = 57 = 3 \cdot 19$, iar

pentru r = 2, avem $49^r + 7^r + 1 = 2451 = 129 \cdot 19$.

Deci $19 \mid (7^{2n} + 7^n + 1)$, pentru orice n, nedivizibil cu 3.

53) Să se arate că $11 \mid (3^{5k+1} + 4^{5m+1} + 5^{5n+1} - 1)$, pentru orice numere naturale k, m, n.

Soluție:

Avem $3^5 = 9\,(22 + 5) = 11m_0 + 45 = 11(m_0 + 4) + 1,$
$4^5 = 16 \cdot 64 = (11 + 5)(11 \cdot 6 - 2) = 11m_1 - 10 = 11(m_1 - 1) + 1,$
$5^5 = 25 \cdot 125 = (2 \cdot 11 + 3)(11 \cdot 11 + 4) = 11m_2 + 12 = 11(m_2 + 1) + 1.$
Astfel, $3^{5k+1} + 4^{5m+1} + 5^{5n+1} - 1 = (3^5)^k \cdot 3 + (4^5)^m \cdot 4 + (5^5)^n \cdot 5 - 1 =$
$=(11n_0 + 1)^k \cdot 3 + (11n_1 + 1)^m \cdot 4 + (11n_2 + 1)^n \cdot 5 - 1 = (11p_0 + 1) \cdot 3 +$
$+(11p_1 + 1) \cdot 4 + (11p_2 + 1) \cdot 5 - 1 = 11(3p_0 + 4p_1 + 5p_2 + 1)$, pentru orice k, m, n∈**N**.

54) Pentru orice număr impar pozitiv m şi orice număr întreg pozitiv k, avem $2^{k+2} \mid (m^{2^k} - 1)$.

Soluție:

Demonstrăm prin inducție după k.

Pentru k = 1, avem $m^2 - 1 = (2m' + 1)^2 - 1 = 4m'(m' + 1)$, deci $2^3 \mid m^2 - 1$, deoarece $2 \mid m'(m' + 1)$.

Presupunem afirmația adevărată pentru k = n şi o demonstrăm pentru k = n +1.

Avem $m^{2^{n+1}} - 1 = m^{2^n \cdot 2} - 1 = (m^{2^n} - 1)(m^{2^n} + 1)$.

Din ipoteza inductivă avem $2^{n+2} \mid (m^{2^n} - 1)$ şi cum m este impar rezultă $2 \mid (m^{2^n} + 1)$.

Aşadar, $2^{n+3} \mid (m^{2^{n+1}} - 1)$, adică afirmația este adevărată şi pentru k = n+ 1.

Deci, afirmația este adevărată pentru orice k întreg pozitiv.

55) Să se arate că dacă b | a(a-1), unde a şi b sunt întregi, atunci rezultă că (2a - 1, b) = 1.

Soluție:

Fie d un divizor comun pentru b şi 2a – 1. Din d | b şi b | a(a – 1) rezultă că d | a(a – 1) şi cum d | 2a –1 rezultă că d | [2 a^2 –a–(a^2- a)]=a^2, de unde d | [a^2- (a^2- a)] = a şi cu d | (2a - 1) rezultă că d | 1, deci (2a – 1, b)= 1.

56) Dacă un număr prim este de forma $2^n + 1$, atunci n = 0 sau n = 2^k cu k = 0, 1, 2, ...

Soluție:

Fie $n \neq 0$ cu proprietatea că $2^n + 1$ este prim şi presupunem prin absurd că n admite un divizor impar diferit de 1. Fie acesta $2n_0 + 1$.

Atunci $n = (2n_0 + 1)\cdot n_1$, cu $n_1 \in \mathbf{N}^*$.

Rezultă că $2^n + 1 = \left(2^{n_1}\right)^{2n_0+1} + 1 = (2^{n_1} + 1)(\left(2^{n_1}\right)^{2n_0} - \left(2^{n_1}\right)^{2n_0-1} + \ldots$ ... - $2^{n_1} + 1$), contradicție cu faptul că $2^n + 1$ este prim.

Deci n, cu proprietatea de mai sus, are ca divizori numai pe 2 sau puteri ale lui 2, deci este e forma 2^k.

57) Dacă 2^n - 1 este prim, atunci n este prim.

Soluție:

Presupunem prin reducere la absurd că n nu este prim, adică n = pq cu p, q ≥ 2, p, q ∈ **N**.

Rezultă că $2^n - 1 = (2^p)^q - 1 = (2^p - 1)((2^p)^{q-1} + (2^p)^{q-2} + \ldots + 1)$ contradicție cu faptul că $2^n - 1$ este prim. Deci n este prim.

58) Pentru orice număr întreg n > 1, numerele $\frac{1}{5}\left(2^{4n+2}+1\right)$ nu sunt prime.

Soluție:

Avem $2^{4n+2} + 1 = 2^{4n+2} + 2^{2n+2} + 1 - 2^{2n+2} = (2^{2n+1})^2 + 2 \cdot 2^{2n+1} + 1 - (2^{n+1})^2 = (2^{2n+1} - 2^{n+1} + 1) \cdot (2^{2n+1} + 2^{n+1} + 1)$.

Cum $5 = 2^2 + 1 \mid (2^2)^{2n+1} + 1 = 2^{4n+2} + 1$ şi pentru n >1 avem

$2^{2n+1} - 2^{n+1} + 1 = 2^{n+1}(2^n - 1) + 1 \geq 2^3 \cdot 3 + 1 = 25$, rezultă că numărul $\frac{1}{5}\left(2^{4n+2}+1\right)$ este produsul a doi factori mai mari decât 1, deci este prim.

59) Numerele $2^{2^{4n+1}} + 27$, cu n natural arbitrar, nu sunt prime.
Soluție:
$2^{4n} = 16^n = (15 + 1)^n = M_5 + 1$, de unde $2^{4n+1} = M_{10} + 2 = 10k + 2$.

Astfel, $2^{2^{4n+1}} + 27 = 2^{10k+2} + 27 = 4 \cdot 32^k \cdot 32^k + 27 =$
$= 4 \cdot (31+1)^k \cdot (31+1)^k + 27 = 4(M_{31} + 1) + 27 = M_{31} + 31 = M_{31}$.

60) Să se demonstreze că orice număr prim p, ce divide pe $a^3 + 1$, fără a divide pe a+1, divide pe $(a-1)^{6k} - 1$, pentru orice k natural.
Soluție:
Din $p \mid [a^3 + 1] = (a + 1)(a^2 - a + 1)$ şi din $p \nmid (a + 1)$ rezultă că:
$p \mid (a^2 - a + 1) = (a - 1)^2 + a$. Deci $(a - 1)^2 = M_p - a$, de unde $(a - 1)^6 - 1 = M_p - (a^3 + 1) = M_p$ şi cum $[(a - 1)^6 - 1] \mid [(a - 1)^{6k} - 1]$, $\forall k \in \mathbf{N}$, rezultă că $p \mid [(a - 1)^{6k} - 1]$, $\forall k \in \mathbf{N}$.

61) Să se arate că pentru orice n impar, avem $5^{2n} + 7^{2n} \equiv 0 \pmod{37}$.
Soluție:
$5^{2n} + 7^{2n} = 25^n + 49^n = (25 + 49)(25^{n-1} - 25^{n-2} \cdot 49 + \ldots + 49^{n-1}) = 2 \cdot 37 \cdot M$, unde $M = 25^{n-1} - 25^{n-2} \cdot 49 + \ldots + 49^{n-1}$, de unde rezultă că $5^{2n} + 7^{2n} \equiv 0 \pmod{37}$.

62) Dacă $(u, 10) = 1$, atunci $u^4 \equiv 1 \pmod{80}$.
Soluție:
Din $(u, 10) = 1$ rezultă că $(u, 2) = 1$, adică u este impar: $u = 2k+1$, unde $k \in \mathbf{Z}$. De aici rezultă că $u^2 = 4k(k+1) + 1 = 8l + 1$, unde $2t = k(k+1)$. Obținem $u^4 = 64t^2 + 16t + 1 = 16s + 1$, unde $s = 4t^2 + t$. De aici, $u^4 - 1 = 16s \equiv 0 \pmod{16}$. Pe de altă parte, din $(u, 10) = 1$ rezultă $(u, 5) = 1$ şi conform teoremei lui Euler avem $u^{\varphi(5)} \equiv 1 \pmod 5$, adică $u^4 \equiv 1 \pmod 5$, deci $u^4 - 1 \equiv 0 \pmod 5$.
Din $(5, 16) = 1$ rezultă $u^4 - 1 \equiv 0 \pmod{5 \cdot 16}$, de unde $u^4 \equiv 1 \pmod{80}$.

63) Arătați că $2^{32} + 1 \equiv 0 \pmod{641}$.

Soluție:
Avem $641 = 5 \cdot 128 + 1 = 5 \cdot 2^7 + 1$ şi $641 = 625 + 16 = 5^4 + 2^4$. De aici rezultă că $5 \cdot 2^7 \equiv (-1)^4 (\text{mod } 641)$ şi $5^4 \equiv -2^4 (\text{mod } 641)$.
Obținem: $(5 \cdot 2^7)^4 \equiv (-1)^4 (\text{mod } 641)$, adică $5^4 \cdot 2^{28} \equiv 1 (\text{mod } 641)$ şi cum şi $5^4 \equiv -2^4 (\text{mod } 641)$ rezultă $2^4 \cdot 2^{28} \equiv 1 (\text{mod } 641)$, adică:
$2^{32} + 1 \equiv 0 (\text{mod } 641)$.

64) Să se calculeze restul împărțirii numărului $67^{68} \cdot 68^{67}$ la 21.
Soluție:
Avem $67 \equiv 4 (\text{mod } 21)$ şi $68 \equiv 5 (\text{mod } 21)$, de unde $67^{68} \equiv 4^{68} \equiv \equiv 4 \cdot 4^{67} (\text{mod } 21)$ şi $68^{67} \equiv 5^{67} (\text{mod } 21)$.
Atunci $N = 67^{68} \cdot 68^{67} \equiv 4 \cdot 20^{67} (\text{mod } 21)$, deci $N \equiv 4 \cdot (21 - 1)^{67} (\text{mod } 21)$ şi cum $4 \cdot (21 - 1)^{67} \equiv 4 \cdot (-1)^{67} (\text{mod } 21)$ rezultă $N \equiv -4 (\text{mod } 21)$, adică $N \equiv 17 (\text{mod } 21)$.

65) Aflați restul împărțirii lui a la 13, ştiind că $3a^8 \equiv 9 (\text{mod } 13)$ şi $7a^5 \equiv 1 (\text{mod } 13)$.

Soluție:
Din $3a^8 \equiv 9 (\text{mod } 13)$ rezultă $a^8 \equiv 3 (\text{mod } 13)$, de unde $a^{24} \equiv 27 (\text{mod } 13)$, adică $a^{24} \equiv 1 (\text{mod } 13)$ şi de aici $a^{25} \equiv a (\text{mod } 13)$.
Pe de altă parte, din $7a^5 \equiv 1 (\text{mod } 13)$ rezultă $7a^5 \equiv 14 (\text{mod } 13)$ şi deci $a^5 \equiv 2 (\text{mod } 13)$.
Obținem $a^{25} \equiv 2^5 (\text{mod } 13)$, adică $a^{25} \equiv 6 (\text{mod } 13)$.
Folosind acum faptul că $a^{25} \equiv a (\text{mod } 13)$, rezultă $a \equiv 6 (\text{mod } 13)$.

66) Dacă p este prim şi a, b, c $\in \mathbf{Z}$, aşa încât $ab \equiv bc \equiv ca (\text{mod } p)$, atunci $a \equiv b \equiv c (\text{mod } p)$ sau $abc \equiv 0 (\text{mod } p^2)$.
Soluție:
Din $ab \equiv bc (\text{mod } p)$ rezultă $(a - c)b \equiv 0 (\text{mod } p)$.
Cazul 1. Dacă $b \equiv 0 (\text{mod } p)$, obținem că $ca \equiv 0 (\text{mod } p)$, deci $c \equiv 0 (\text{mod } p)$ sau $a \equiv 0 (\text{mod } p)$, aşadar $abc \equiv 0 (\text{mod } p^2)$.
Cazul 2. Dacă $a \equiv c (\text{mod } p)$ atunci putem presupune $a \equiv c \not\equiv 0 (\text{mod } p)$, deoarece altfel obținem ca şi la cazul 1, $abc \equiv 0 (\text{mod } p^2)$.

Aşadar, din c(a - b) ≡ 0 (mod p) şi c≢0(mod p) rezultă a ≡ b ≡ ≡ c (mod p).

67) Dacă p este prim şi 1 ≤ k ≤ p - 1, atunci avem $C_{p+k}^{p} \equiv 1 \pmod p$ şi $C_{p-1}^{k} \equiv (-1)^k \pmod p$.

Soluție:

Vom demonstra numai prima dintre congruențe, cea de–a doua arătându-se asemănător.

Astfel, $C_{p+k}^{p} \equiv 1 \pmod p \Leftrightarrow \dfrac{(p+k)\cdot....\cdot(p+1)}{k\cdot...\cdot 1} \equiv 1 \pmod p$.

Din 1 ≤ k ≤ p – 1 rzultă k! ≢ 0 (mod p).

Aşadar, $C_{p+k}^{p} \equiv 1 \pmod p \Leftrightarrow (p + k)\cdot \ldots\cdot(p + 1) \equiv k\cdot \ldots\cdot 1 \pmod p$ congruență adevărată, care se obține din înmulțirea congruențelor $p + i \equiv i \pmod p$, pentru $\forall\, i \in \{1, 2, .., k\}$.

68) Dacă p este prim şi $a^p \equiv b^p \pmod p$, atunci $a^p \equiv b^p \pmod{p^2}$.

Soluție:

Notăm c = a – b şi obținem $c^p = a^p - b^p + \sum_{k=1}^{p-1}(-1)^k C_p^k a^{p-k} b^k$ şi cum $p \mid (a^p - b^p)$ şi pentru $\forall\, k \in \{1, 2, .., p-1\}$ avem $p \mid C_p^k$, rezultă că $p \mid c^p$, deci $p \mid c$, adică $\exists q \in \mathbf{Z}$: c = pq. Deci a = b + pq, de unde $a^p = (b + pq)^p = b^p + \sum_{k=1}^{p} C_p^k b^{p-k} p^k$. Avem $p^2 \mid p^p$ şi $\forall\, k \in \{1, 2, ..., p-1\}$, $p \mid C_p^k$ şi $p \mid p^k$. De aici rezultă că $p^2 \mid a^p - b^p$, adică $a^p \equiv b^p \pmod{p^2}$.

69) Dacă p este prim şi p > 3, atunci $a^p - a \equiv 0 \pmod{6p}$.

Soluție:

Din teorema lui Fermat rezultă că $a^p - a \equiv 0 \pmod p$.

Pe de altă parte, din p > 3 şi p prim rezultă că p ≡ 1(mod 2). Aşadar, $a^p - a = (a - 1)a(a + 1)(a^{2\left(\frac{p-1}{2}-1\right)} + \ldots + 1) \equiv 0 \pmod 6$, deoarece orice produs de trei numere întregi consecutive este divizibil cu 6.

Din (p, 6) = 1 rezultă că $a^p - a \equiv 0 \pmod{6p}$.

70) Să se găsească restul împărţirii numărului a la 17, ştiind că $a^{27} \equiv 4 \pmod{17}$ şi $a^{37} \equiv 11 \pmod{17}$.

Soluție:

Din ipoteză rezultă că $a \not\equiv 0 \pmod{17}$ şi cum 17 este prim rezultă că (a, 17) = 1, iar în baza teoremei lui Fermat obţinem $a^{16} \equiv 1 \pmod{17}$, de unde $a^{27} \equiv a^{11} \pmod{17}$ şi $a^{32} \equiv 1 \pmod{17}$.

Folosind acum faptul că $a^{27} \equiv 4 \pmod{17}$, $a^{37} \equiv 11 \pmod{17}$, rezultă că $a^{11} \equiv 4 \pmod{17}$ şi $a^5 \equiv 11 \pmod{17}$, deci $a^{10} = 121 \equiv 2 \pmod{17}$, de unde $a^{11} \equiv 2a \pmod{17}$. Deci $2a \equiv 4 \pmod{17}$ şi cum (2, 17) = 1, rezultă $a \equiv 2 \pmod{17}$.

71) Dacă p şi q sunt două numere prime distincte şi $a^p \equiv b^p \pmod p$ şi $a^q \equiv b^q \pmod q$, atunci $a \equiv b \pmod{pq}$.

Soluție:

Din teorema lui Fermat rezultă $a^p \equiv a \pmod p$ şi $b^p \equiv b \pmod p$, respectiv $a^q \equiv a \pmod q$ şi $b^q \equiv b \pmod q$.

Rezultă că $a - b \equiv 0 \pmod p$ şi $a - b \equiv 0 \pmod q$ şi cum $p \neq q$, p, q prime, rezultă că $a \equiv b \pmod{pq}$.

72) Determinaţi numărul prim p, astfel încât să aibă loc congruenţa: $3^{p^2} + 11^{p^2} \equiv 0 \left(\mathrm{mod}\, p^2\right)$.

Soluție:

Din teorema lui Fermat rezultă $3^p \equiv 3(\text{mod } p)$ şi $11^p \equiv 11(\text{mod } p)$, deci $3^{p^2} \equiv 3^p \equiv 3(\text{mod } p)$ şi $11^{p^2} \equiv 11^p \equiv 11(\text{mod } p)$.

Obţinem $3^{p^2} + 11^{p^2} \equiv 14 \text{ (mod p)}$. Pe de altă parte, din $3^{p^2} + 11^{p^2} \equiv 0(\text{mod } p^2)$ rezultă $3^{p^2} + 11^{p^2} \equiv 0 \text{ (mod p)}$, deci $14 \equiv 0(\text{mod p})$, de unde p =2 sau p= 7.

Dar, pentru p = 2, obţinem $3^{p^2} + 11^{p^2} = 4k + 2$ şi 4Π4k+2.

Pentru p=7, avem $3^{7^2} + 11^{7^2} = (3^7 + 11^7)((3^7)^6 - (3^7)^5 \cdot 11^7 + ..+ (11^7)^6) =$

$= (3^7 + (14 - 3)^7) M = (14^7 + \sum_{k=1}^{6} (-1)^k C_7^k \cdot 14^k \cdot 3^{7-k}) \cdot M = 7^2 \cdot k \cdot M \equiv$

$\equiv 0(\text{mod } 7^2)$.

Aşadar, p = 7.

73) Să se deducă teorema lui Euler din teorema lui Fermat.

Soluţie:

Fie (a, p) = 1. Din $a^{p-1} \equiv 1(\text{mod p})$ rezultă $a^{p-1} = mp + 1$, din care prin ridicare la puterea p şi folosind binomul lui Newton, obţinem:

$a^{p(p-1)} = M p^2 + 1$, deoarece $\forall\ k \in \{1, 2, ..., k-1\}$, $C_p^k \equiv 0 \text{ (mod p)}$ şi $p^2 \mid p^k$ pentru $k \geq 2$.

Prin inducţie matematică, se demonstrează uşor că $a^{p^{\alpha-1}(p-1)} = M p^\alpha + 1$, de unde $a^{\varphi(p^\alpha)} \equiv 1(\text{mod } p^\alpha)$. Fie $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ descompunerea canonică a numărului n. Avem $a^{\varphi(p_i^{\alpha_i})} \equiv 1(\text{mod } p_i^{\alpha_i})$ pentru orice $i \in \{1, 2, ...,k\}$ şi cum $\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i})$ rezultă că $a^{\varphi(n)} \equiv 1(\text{mod } p_i^{\alpha_i})$, pentru orice $i \in \{1, 2, .., k\}$, de unde obţinem $a^{\varphi(n)} \equiv 1(\text{mod n})$.

74) Ţinând seama că dacă (a, m) = 1, atunci soluţia congruenţei $ax \equiv b \text{ (mod m)}$ este $x \equiv ba^{\varphi(m)-1} \text{ (mod m)}$, unde φ este funcţia lui Euler, să se rezolve congruenţele:

a) $5x \equiv 7 \text{ (mod 12)}$

b) $3x \equiv 7 \text{ (mod 8)}$

c) $4x \equiv 9 \pmod 5$
d) $129x \equiv 3 \pmod{14}$
e) $23x \equiv 149 \pmod{10}$
f) $25x \equiv 4 \pmod 6$

Soluție:

a) $5x \equiv 7 \pmod{12} \Rightarrow x \equiv 7 \cdot 5^{\varphi(12)-1} \pmod{12} \Rightarrow x \equiv 7 \cdot 5^3 \pmod{12}$, deci $x \equiv 7 \cdot 25 \cdot 5 = 7(2 \cdot 12 + 1) \cdot 5 \equiv 11 \pmod{12}$;

b) $3x \equiv 7 \pmod 8 \Rightarrow x \equiv 7 \cdot 3^{\varphi(8)-1} \pmod 8$, deci $x \equiv 7 \cdot 3^3 = 7 \cdot 9 \cdot 3 \equiv$ $\equiv 7 \cdot 3 \equiv 5 \pmod 8$;

c) $4x \equiv 9 \pmod 5 \Rightarrow x \equiv 9 \cdot 4^{\varphi(5)-1} \equiv 9 \cdot 4^3 = (10 - 1)(5 - 1)^3 \equiv 1 \pmod 5$;

d) $129x \equiv 3 \pmod{14} \Rightarrow x \equiv 3 \cdot 129^{\varphi(14)-1} = 3 \quad (9 \cdot 14 + 3)^5 \equiv 3^6 = 27^2 =$ $= (2 \cdot 14 - 1)^2 \equiv 1 \pmod{14}$;

e) $23x \equiv 149 \pmod{10} \Rightarrow x \equiv 149 \cdot 23^{\varphi(10)-1} = (15 \cdot 10 - 1)(2 \cdot 10 + 3)^3 \equiv$ $\equiv -27 \equiv 3 \pmod{10}$;

f) $25x \equiv 4 \pmod 6 \Rightarrow x \equiv 4 \cdot 25^{\varphi(6)-1} = 4 \cdot (4 \cdot 6 + 1) \equiv 4 \pmod 6$.

75) Dacă a şi b sunt prime între ele, atunci $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$.

Soluție:

Din (a, b) = 1 rezultă, în baza teoremei lui Euler, că $a^{\varphi(b)} \equiv 1 \pmod b$ şi $b^{\varphi(a)} \equiv 1 \pmod b$. Deci $a^{\varphi(b)} - 1 + b^{\varphi(a)} \equiv 0 \pmod b$ şi $b^{\varphi(a)} - 1 + a^{\varphi(b)} \equiv 0 \pmod a$. Ţinând acum cont de faptul că (a, b) = 1, obţinem $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$.

76) Să se arate că dacă (a, n) = 1, atunci $n \mid a^{(n-1)!} - 1$.

Soluție:

Din (a, n)=1 rezultă, în baza teoremei lui Euler, că $a^{\varphi(n)} \equiv 1 \pmod n$. Pe de altă parte, din $\varphi(n) \le n-1$ rezultă că $\varphi(n) \mid (n - 1)!$.

Aşadar, $a^{(n-1)!} \equiv 1 \pmod n$.

77) Dacă n este un întreg pozitiv par, atunci $(n^2 - 1) \mid (2^{n!} - 1)$.

Soluție:

Din faptul că n este par, rezultă că (2, n + 1) = 1 = (2, n - 1) şi atunci, conform exerciţiului anterior, obţinem că: $(n + 1) \mid (2^{n!} - 1)$ şi

$(n - 1) \mid 2^{(n-2)!} - 1$. Dar $(n - 2)! \mid n!$, deci $(n - 1) \mid (2^{n!} - 1)$. Pe de altă parte, $n + 1$ şi $n - 1$ sunt două numere impare consecutive, deci $(n - 1, n + 1) = 1$ şi, prin urmare, $(n^2 - 1) \mid (2^{n!} - 1)$.

78) Numerele p şi p + 2 sunt simultan prime dacă şi numai dacă are loc congruența:

$$4[(p - 1)! + 1] + p \equiv 0 \pmod{p(p+2)}$$

(Teorema lui Clement).

Soluție:

Considerăm p şi p + 2 prime. Conform teoremei lui Wilson, avem $(p - 1)! + 1 \equiv 0 \pmod{p}$ şi $(p + 1)! + 1 \equiv 0 \pmod{p+2}$. Înmulțind prima congruență cu 4 şi adunând-o cu congruența $p \equiv 0 \pmod{p}$, obținem:

$$4[(p - 1)! + 1] + p \equiv 0 \pmod{p}. \qquad (1)$$

Adunând a doua congruență cu congruența $p(p + 1) \equiv -p \pmod{p + 2}$ şi simplificând cu p + 1 obținem:

$$p[(p - 1)! + 1] \equiv -1 \pmod{p+2}.$$

Înmulțind-o pe aceasta cu 4 şi adunând-o cu $p^2 \equiv p^2 \pmod{p + 2}$, obținem:

$p\{4[(p - 1)! + 1] + p\} \equiv p^2 - 4 \equiv 0 \pmod{p + 2}$, de unde rezultă:

$$4[(p - 1)! + 1] + p \equiv 0 \pmod{p + 2} \qquad (2)$$

Din (1) şi (2) rezultă congruența cerută.

Reciproc, dacă are loc congruența din enunț (care nu este verificată pentru p = 2 sau p = 4), atunci din ea rezultă (1), iar din aceasta rezultă $(p - 1)! + 1 \equiv 0 \pmod{p}$ şi din reciproca teoremei lui Wilson rezultă că p este prim.

Tot din congruența din enunț rezultă (2), iar din aceasta obținem $(p + 1)! + 1 \equiv 0 \pmod{p + 2}$ şi din reciproca teoremei lui Wilson deducem că (p + 2) este prim.

BIBLIOGRAFIE

1. Becker O. - *Fundamentele matematicii*, Ed.Şt. Bucureşti, 1968
2. Borel E., Drach J. - *Théorie des nombres et algèbre supérieure,* Paris, 1895
3. Cohen I.P. – *The Independence of the Continuum Hypothesis*, Proc. of the Nat. Acad. of Sci., 50(1963) 1143-1148 şi 51 (1964), 105 – 110
4. Dorie H. - *100 Great Problems of Elementary Mathematics,* Dover Publ., N.York, 1965
5. Ion D. Ion, Năstăsescu C., Niţă C. – *Complemente de algenră,* Ed. Ştiinţifică şi Enciclopedică, Bucureşti,1984
6. Ion D. Ion, Niţă C. – *Elemente de aritmetică cu aplicaţii în tehnici de calcul,* Ed. Tehnică, Bucureşti,1978
7. Minuţ P. – *Teoria numerelor*, Vol.I, Ed. Crenguţa Gâldău, Iaşi, 1997.
8. Miron R., Brânzei D. – *Fundamentele aritmeticii şi geometriei*, Ed. Acad., Bucureşti, 1983
9. Năstăsescu C., Niţă C., Vraciu C. – *Aritmetică şi algebră*, Ed. Did. şi Ped., Bucureşti, 1993
10. Purdea I., Pic Ghe. – *Tratat de algebră modernă*, vol.I, Ed. Acad., 1977
11. Năstăsescu C. - *Introducere în teoria mulţimilor,* Ed.Did. şi Ped., Bucureşti, 1970
12. Radu N., Becheanu M., Dincă A., Ion D.I., Niţă C., Purdea I., Ştefănescu M., Vraciu C. – *Algebră pentru perfecţionarea profesorilor*, Ed. Did. şi Ped., Bucureşti, 1983
13. Radu Gh. – *Introducere în teoria categoriilor şi functorilor*, Partea a II-a, Ed. Universităţii "Al. I.Cuza", Iaşi, 1981
14. Radu Gh., Tamaş V. – *Elemente de algebră*, Ed. Universităţii "Al. I.Cuza", Iaşi, 1985
15. Sierpinski W. – *Ce ştim şi ce nu ştim despre numerele prime*, Ed. Şt., Bucureşti, 1966
16. Tofan I. – *Elemente de algebră*, Ed. Universităţii "Al.I.Cuza", Iaşi, 1998
17. Tamaş V., Tofan I., LeoreanuV. – *Curs de aritmetică*, Ed. Universităţii "Al. I.Cuza", Iaşi, 2001

18. Triandaf A. ş.a. – *Curs de aritmetică*, Lit. învăţământului, Iaşi, 1957
19. Ţena M. – *Cinci teme de aritmetică superioară*, Bibl. S.S.M.R.,Bucureşti, 1991
20. Vinogradov I.M. – *Bazele teoriei numerelor*, Ed. Acad., Bucureşti, 1954
21. Wieleitner H. - *Istoria matematicii de la Descartes până la mijlocul secolului al XIX-lea,* Ed. Şt., Bucureşti, 1964